Loading and Managing System Images Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **Digitally Signed Cisco Software** 3

- Finding Feature Information 3
- Restrictions for Digitally Signed Cisco Software 3
- Information About Digitally Signed Cisco Software 4
  - Features and Benefits of Digitally Signed Cisco Software 4
  - Digitally Signed Cisco Software Identification 4
    - Digitally Signed Cisco Software Key Types and Versions 4
  - Digitally Signed Cisco Software Key Revocation and Replacement 5
    - Key Revocation 5
    - Key Replacement 5
    - Key Revocation Image 5
    - Production Key Revocation 6
    - Special Key Revocation 7
- How to Work with Digitally Signed Cisco Software Images 7
  - Identifying Digitally Signed Cisco Software 7
  - Displaying Digitally Signed Cisco Software Signature Information 8
  - Displaying Digital Signature Information for a Specific Image File 8
  - Displaying Digitally Signed Cisco Software Key Information 9
  - Troubleshooting Digitally Signed Cisco Software Images 9
- Configuration Examples for Digitally Signed Cisco Software 10
  - Identifying Digitally Signed Cisco Software Example 10
  - Displaying Digitally Signed Cisco Software Signature Information Example 11
  - Displaying the Digital Signature Information for a Specific Image File Example 12
  - Displaying Digitally Signed Cisco Software Key Information Example 13

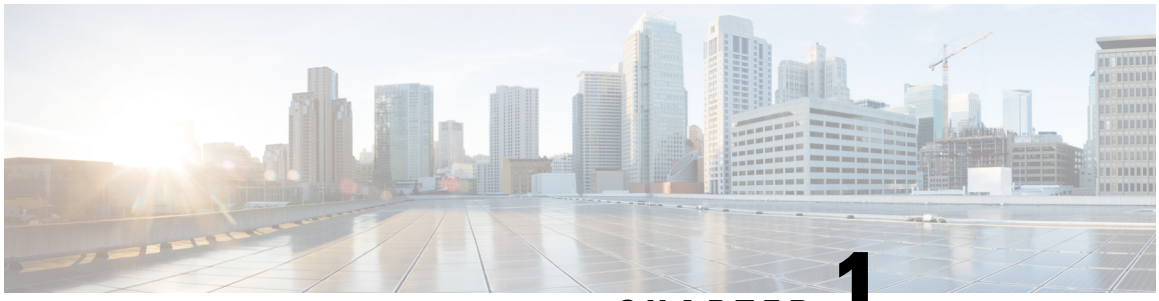
Enabling Debugging of Digitally Signed Cisco Software Image Key Information Example 14
Additional References 14
Feature Information for Digitally Signed Cisco Software 15

CHAPTER 3 **Using FTP to Manage System Images** 17
Finding Feature Information 17
Image Copying from Flash Memory to an FTP Server 17
Image Copy from an FTP Server to a Flash Memory File System 18
FTP Username and Password 18
Copying an Image from Flash Memory to an FTP Server 19
Examples 20
Copying from an FTP Server to Flash Memory 20
Examples 22

CHAPTER 4 **Configuring the Cisco IOS Auto-Upgrade Manager** 23
Finding Feature Information 23
Prerequisites for Cisco IOS Auto-Upgrade Manager 23
Restrictions for Cisco IOS Auto-Upgrade Manager 24
Information About Cisco IOS Auto-Upgrade Manager 24
Cisco IOS Auto-Upgrade Manager Overview 24
Specific Cisco IOS Software Image Download from the Cisco Website 26
Specific Cisco IOS Software Image Download from a Non-Cisco Server 26
Interactive and Single Command Line Mode 26
Interactive Mode 27
Single Command Line Mode 27
How to Upgrade a Cisco IOS Software Image Using the Cisco IOS Auto-Upgrade Manager 27
Configuring the SSL Certificate for a Cisco Download 27
Configuring the Cisco IOS Auto-Upgrade Manager 29
Downloading the Cisco IOS Software Image 30
Reloading the Router with the New Cisco IOS software Image 30
Canceling the Cisco IOS Software Image Reload 31
Configuration Examples for Cisco IOS Auto-Upgrade Manager 31
Configuring the DNS Server IP Address Example 31
Configuring the SSL Certificate for a Cisco Download Example 32

Configuring the Cisco IOS Auto-Upgrade Manager Example 32
Additional References 33
Feature Information for Cisco IOS Auto-Upgrade Manager 34
Glossary 34

CHAPTER 5 **Information About Boot Integrity Visibility 37**
Verifying the Software Image and Hardware 37
Verifying Platform Identity and Software Integrity 38
Verifying Platform Identity 38
Verifying Software Integrity 39



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

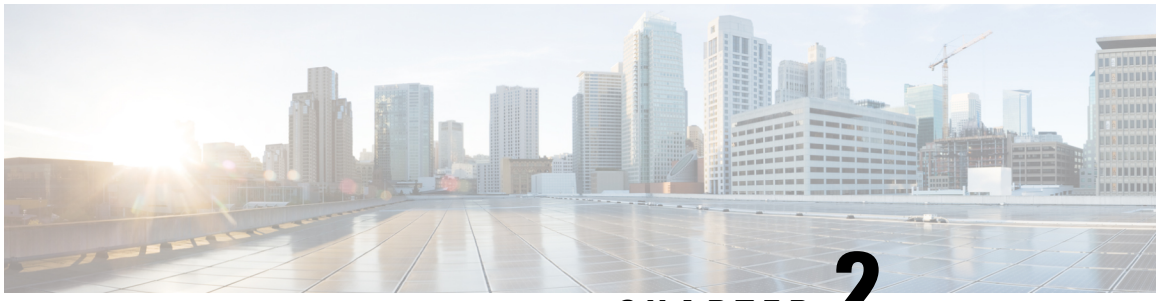
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.



CHAPTER 2

Digitally Signed Cisco Software

The Digitally Signed Cisco Software feature describes how to identify digitally signed Cisco software, gather software authentication information related to digitally signed images, and perform key revocation. Digitally Signed Cisco software is software that is digitally signed using secure asymmetrical (public-key) cryptography.

The purpose of digitally signed Cisco software is to ensure that customers are confident that the software running within their systems is secure and has not been tampered with, and that the software running in those systems originated from the trusted source as claimed.

For customers concerned about software updates involving digitally signed Cisco software--no action is necessary for customers to take advantage of the increased protection. The system operation is largely transparent to existing practices. Some minor changes in system displays reflect the use of digitally signed Cisco software.

- Finding Feature Information, on page 3
- Restrictions for Digitally Signed Cisco Software, on page 3
- Information About Digitally Signed Cisco Software, on page 4
- How to Work with Digitally Signed Cisco Software Images, on page 7
- Configuration Examples for Digitally Signed Cisco Software, on page 10
- Additional References, on page 14
- Feature Information for Digitally Signed Cisco Software, on page 15

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.

Restrictions for Digitally Signed Cisco Software

The Cisco Catalyst 4500 E+Series switches running Cisco IOS XE software include the functionality described in this document, except for Digitally Signed Software Key Revocation and Replacement.

Information About Digitally Signed Cisco Software

Features and Benefits of Digitally Signed Cisco Software

Three main factors drive digitally signed Cisco software and software integrity verification:

- The U.S. government is introducing a new version of the Federal Information Processing Standard (FIPS) 140. FIPS-140-3 is the latest draft and is scheduled for ratification in 2010 and to be effective in 2011. This standard requires software to be digitally signed and to be verified for authenticity and integrity prior to load and execution.
- The focus on product security provides increased protection from attacks and threats to Cisco products. Digitally signed Cisco software offers increased protection from the installation and loading of software that has been corrupted or modified.
- Digitally signed Cisco software provides counterfeit protection, which provides further assurance for customers that the equipment they purchase is as claimed.

Digitally Signed Cisco Software Identification

Digitally signed Cisco IOS software is identified by a three-character extension in the image name. The Cisco software build process creates a Cisco IOS image file that contains a file extension based on the signing key that was used to sign images. These file extensions are:

- .SPA
- .SSA

The significance of each character in the file extension is explained in the table below.

Table 1: Digitally Signed Cisco Software Images File Extension Character Meanings

File Extension Character	Character Meaning
S (first character)	Stands for digitally signed software.
P or S (second character)	P and S stand for a production and special (development) image, respectively. A production image is Cisco software approved for general release; a special image is development software provided under special conditions for limited use.
A (third character)	Indicates the key version used to digitally sign the image. A key version is identified by an alphabetical character - for example, A,B,C...

Digitally Signed Cisco Software Key Types and Versions

Digitally signed Cisco software keys are identified by the type and version of the key. A key can be a special, production, or rollover key type. Special and production keys can be revoked. A rollover key is used to revoke a production or special key. The second character in the file extension indicates whether the key type is a special or production key. The key type can be “P” for a production key or an “S” for a special key.

Production and special key types have an associated key version. The key version is defined by the third character in the file extension, in the form of an alphabetical character; for example A, B or C. When a key is replaced, the key version is incremented alphabetically. For example, after a key revocation of a key type "P" (production key) with a key version of "A", the new image will be signed with key version "B". Key type and key version are stored as part of the key record in the key storage of the device.

Digitally Signed Cisco Software Key Revocation and Replacement

Note Key revocation and replacement is not supported on Catalyst 4500 E+Series switches running IOS XE software.

Key Revocation

Key revocation is the process of removing a key from operational use in digitally signed Cisco software.

Key revocation takes place when a key becomes compromised or is no longer used. Key revocation and replacement is only necessary in the event of a certain type of vulnerability or catastrophic loss to Cisco's secure key infrastructure. Operational steps to remedy the situation would only be necessary if notified and directed by Cisco. Notification and direction would occur through posting of advisories or field notices on www.cisco.com.

There are two different key revocation processes depending on the type of key to be revoked:

- Production key replacement uses a revocation image and a production image
- Special key replacement uses a production image

Key Replacement

Key replacement is the process of providing a new key to replace a compromised key. The new key is added before the compromised key is revoked. Key replacement is a two-step process:

1. A new key is added to the key storage to replace the revoked key.
2. After the image is verified as operating correctly with the new key, the compromised key is revoked from the key storage.

Key Revocation Image

A revocation image is a basic version of the normal image whose function is to add a new production key to the key storage area. A revocation image has no other capabilities. When a key is to be revoked and replaced, one revocation image per key is provided.

A revocation image contains a new production key bundled within it.

A rollover key stored on the platform is used to verify the signature of the revocation image--a valid revocation image is signed using the same rollover key.

Note A revocation image can be used only in production key revocation.

Important Tasks Concerning the Revocation Image

There are two important tasks concerning the revocation image:

- Adding the new production key to the key storage area.
- Performing a production key upgrade check. For more information, see Step 2 in the "Production Key Revocation".

Adding the New Production Key to the Key Storage Area:

The revocation image adds the bundled production key to the key storage. The key is written to the primary and backup key storage areas after the revocation image checks that the key is already not part of the existing set of keys in the key storage.

Performing a Key Upgrade Check:

After the new key is added and the customer has upgraded the software (Cisco IOS and ROMmon), the show software authenticity upgrade-status command should be run. The user can review the command output to determine if the production key is successfully upgraded, and can be selected for the next boot.

Production Key Revocation

A production key (also called the release key) is revoked and replaced using a revocation image signed with a rollover key, because the images signed using the compromised production key cannot be trusted. The ROMmon can boot any image signed using a rollover key. The production key revocation and replacement process involves four steps:

1. Add the new production key to the key storage. The new production key is bundled within the revocation image.
2. Perform a software upgrade check using the show software authenticity upgrade-status command to verify the following:
   - The new production key version is installed.
   - The new production key is added to the primary key storage (if not, issue the software authenticity key add production command again with the existing revocation image).
   - The new production key is added to the backup key storage (if not, issue the software authenticity key add production command again with the existing revocation image).
   - The image is configured for autoboot (with the boot system command) signed with the new production key (if not, make sure the new production image is copied into the box and modify the boot system command to point to the new image).
   - The upgradable ROMmon is signed with the new production key (if not, upgrade the ROMmon to the one signed with the new production key).
3. Once everything is verified, the user may load the production image signed with the new production key by using the reload command.
4. Once the new production image is loaded, the user may revoke the compromised key using the software authenticity key revoke production command.

Steps 1 and 2 are done using the special revocation image. It is important for the user to do verifications in Step 2 because after a reboot (in Step 3), an old key will not be revoked if any of the software is still using the old key. The verifications help to ensure that the new key is fully installed and the next reboot (in Step 3)

will use the new release software and new ROMmon. Revoking the old production key (Step 4) can be done only after the new key and the new software are installed to the system.

Special Key Revocation

A special key is revoked using a production image signed with a production key. Each production image used for special key revocation has a bundled special key that is the latest at the time of building the production image. The special key revocation and replacement process involves three steps:

1. Add the bundled new special key to the key storage area.
2. Upgrade the ROMmon that is signed using the compromise special key, to the new ROMmon signed with the new special key.
3. Revoke the compromised key from the key storage.

Note that Step 3 does not require any reboot and will be done using the production image itself. This is because the customer is already running a production image and invalidation itself happens from the running production image. Special images do not have the capability to add or invalidate any key.

How to Work with Digitally Signed Cisco Software Images

Identifying Digitally Signed Cisco Software

Perform this task to identify digitally signed Cisco software by examining the image filename in the command output from the show version command, and judging it on the criteria described in the "Digitally Signed Cisco Software Identification" section.

Note If the image file has been renamed by the user, it may not be possible to identify the image because the user may have overwritten the criteria used to indicate that the image is digitally signed.

SUMMARY STEPS

1. **enable**
2. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show version** **Example:**	Displays information about the Cisco IOS software version running on a routing device, the ROM Monitor and

	Command or Action	Purpose
	`Device# show version`	Bootflash software versions, and the hardware configuration, including the amount of system memory.

Displaying Digitally Signed Cisco Software Signature Information

Perform this task to display information related to software authentication for the current ROMmon and the Cisco IOS image file used for booting. The display includes image credential information, the key type used for verification, signature information, and other attributes in the signature envelope.

SUMMARY STEPS

1. **enable**
2. **show software authenticity running**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show software authenticity running** **Example:** `Device# show software authenticity running`	Displays software authenticity-related information for the current ROMmon and the Cisco IOS image file used for booting.

Displaying Digital Signature Information for a Specific Image File

Perform this task to display the digital signature information related to software authentication for a specific image file.

SUMMARY STEPS

1. **enable**
2. **show software authenticity file {flash0:filename | flash1:filename | flash:filename | nvram:filename | flash0:filename | flash1:filename}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show software authenticity file {flash0:filename | flash1:filename | flash:filename | nvram:filename | flash0:filename | flash1:filename}** **Example:** `Device# show software authenticity file flash0:c3900-universalk9-mz.SPA`	Displays digital signature and software authenticity-related information for a specific image file.

Displaying Digitally Signed Cisco Software Key Information

Perform this task to display digitally signed Cisco software key information. The information details the software public keys that are in storage with the key types.

SUMMARY STEPS

1. **enable**
2. **show software authenticity keys**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show software authenticity keys** **Example:** `Device# show software authenticity keys`	Displays the software public keys that are in storage with the key types for digitally signed Cisco software.

Troubleshooting Digitally Signed Cisco Software Images

Perform this task to troubleshoot digitally signed Cisco software images.

SUMMARY STEPS

1. **enable**
2. **debug software- authenticity errors {envelope | errors | key | revocation | show | verbose}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**debug software- authenticity errors {envelope | errors | key | revocation | show | verbose}** **Example:** `Device# debug software-authenticity errors`	Enables the display of debug messages for digitally signed Cisco software.

Configuration Examples for Digitally Signed Cisco Software

Identifying Digitally Signed Cisco Software Example

The following example displays the digitally signed Cisco software image filename and allows a user to identify it based on the digitally signed Cisco software identification criteria:

```
Device# show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M),
12.4(20090904:044027) [i12 577]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Fri 04-Sep-09 09:22 by xxx
ROM: System Bootstrap, Version 12.4(20090303:092436)
C3900-2 uptime is 8 hours, 41 minutes
System returned to ROM by reload at 08:40:40 UTC Tue May 21 1901!
System image file is "xxx.SPA"
Last reload reason: Reload Command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco xxx (revision 1.0) with CISCxxx with 987136K/61440K bytes of memory.
Processor board ID xxx
3 Gigabit Ethernet interfaces
1 terminal line
1 Virtual Private Network (VPN) Module
1 cisco Integrated Service Engine(s)
DRAM configuration is 72 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
1020584K bytes of USB Flash usbflash0 (Read/Write)
1020584K bytes of USB Flash usbflash1 (Read/Write)
500472K bytes of ATA System CompactFlash 0 (Read/Write)
License Info:
License UDI:
------------------------------------------------
Device#   PID                   SN
```

```
-----------------------------------------------
xx        xxx                   xxxx
Technology Package License Information for Module:'xxx'
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
Configuration register is 0x2102
```

Note the digitally signed image file is identified in the following line:

```
System image file is "xxx.SPA"
```

The image has a three-character extension in the filename (.SPA) characteristic of digitally signed Cisco software. Based on the guidelines in the “Digitally Signed Cisco Software Identification” section the first character in the file extension “S” indicates that the image is a digitally signed software image, the second character “P” indicates that the image is digitally signed using a production key, and the third character “A” indicates that the key version is version A.

Displaying Digitally Signed Cisco Software Signature Information Example

The following example shows how to display information related to software authentication for the current ROMmon and Cisco IOS image file used for booting:

```
Device# show software authenticity running
SYSTEM IMAGE
-------------------
Image type                    : Development
    Signer Information
        Common Name           : xxx
        Organization Unit     : xxx
        Organization Name     : xxx
    Certificate Serial Number : xxx
    Hash Algorithm            : xxx
    Signature Algorithm       : 2048-bit RSA
    Key Version               : xxx

    Verifier Information
        Verifier Name         : ROMMON 2
        Verifier Version      :  System Bootstrap, Version 12.4(20090409:084310)
ROMMON 2
---------------
Image type                    : xxx
    Signer Information
        Common Name           : xxx
        Organization Unit     : xxx
        Organization Name     : xxx
    Certificate Serial Number : xxx
    Hash Algorithm            : xxx
    Signature Algorithm       : 2048-bit RSA
    Key Version               : xx

    Verifier Information
        Verifier Name         : ROMMON 2
        Verifier Version      :  System Bootstrap, Version 12.4(20090409:084310) [
```

The table below describes the significant fields shown in the display.

Table 2: show software authenticity running Field Descriptions

Field	Description
SYSTEM IMAGE	Section of the output displaying the system image information.
Image type	Displays the type of image.
Common Name	Displays the name of the software manufacturer.
Organization Unit	Displays the hardware the software image is deployed on.
Organization Name	Displays the owner of the software image.
Certificate Serial Number	Displays the certificate serial number for the digital signature.
Hash Algorithm	Displays the type of hash algorithm used in digital signature verification.
Signature Algorithm	Displays the type of signature algorithm used in digital signature verification.
Key Version	Displays the key version used for verification.
Verifier Name	Name of the program responsible for performing the digital signature verification.
Verifier Version	Version of the program responsible for performing the digital signature verification.
ROMMON 2	Section of the output displaying the current ROMmon information.

Displaying the Digital Signature Information for a Specific Image File Example

The following example shows how to display the digital signature information related to software authentication for a specific image file:

Device# **show software authenticity file flash0:**c3900-universalk9-mz.SSA

```
File Name                     : flash0:c3900-universalk9-mz.SSA
Image type                    : Development
    Signer Information
        Common Name           : xxx
        Organization Unit     : xxx
        Organization Name     : xxx
    Certificate Serial Number : xxx
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

The table below describes the significant fields shown in the display.
```

Table 3: show software authenticity file Field Descriptions

Field	Description
File Name	Name of the filename in the memory. For example, flash0:c3900-universalk9-mz.SSA refers to filename c3900-universalk9-mz.SSA in flash memory (flash0:).
Image type	Displays the type of image.
Signer Information	Signature information.
Common Name	Displays the name of the software manufacturer.
Organization Unit	Displays the hardware the software image is deployed on.
Organization Name	Displays the owner of the software image.
Certificate Serial Number	Displays the certificate serial number for the digital signature.
Hash Algorithm	Displays the type of hash algorithm used in digital signature verification.
Signature Algorithm	Displays the type of signature algorithm used in digital signature verification.
Key Version	Displays the key version used for verification.

Displaying Digitally Signed Cisco Software Key Information Example

The following example displays digitally signed Cisco software key information. The information details the software public keys that are in storage, including their key types.

```
Device# show software authenticity keys
Public Key #1 Information
-------------------------
Key Type             : Release  (Primary)
Public Key Algorithm : RSA
Modulus :
        CC:CA:40:55:8C:71:E2:4A:3A:B6:9D:5C:94:1D:02:BA:
       ...
        26:04:6B:33:EB:70:2B:18:24:C7:D9:31:3E:77:24:85
Exponent : xxx
Key Version          : A
Public Key #2 Information
-------------------------
Key Type             : Development  (Primary)
Public Key Algorithm : RSA
Modulus :
        CC:CA:40:55:8C:71:E2:4A:3A:B6:9D:5C:94:1D:02:BA:
       ....
        26:04:6B:33:EB:70:2B:18:24:C7:D9:31:3E:77:24:85
Exponent : xxx
Key Version          : A

The table below describes the significant fields shown in the display.
```

Table 4: show software authenticity keys Field Descriptions

Field	Description
Public Key #	Public key number.
Key Type	Displays the key type used for image verification.
Public Key Algorithm	Displays the name of the algorithm used for public key cryptography.
Modulus	Modulus of the public key algorithm.
Exponent	Exponent of the public key algorithm
Key Version	Displays the key version used for verification.

Enabling Debugging of Digitally Signed Cisco Software Image Key Information Example

The following example shows how to enable debugging of software authentication events relating to key information for digitally signed Cisco software:

```
Device# debug software authenticity key
```

Additional References

The following sections provide references related to the Digitally Signed Cisco Software feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
System Management Command Reference	http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/system_management/c

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	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

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 Digitally Signed Cisco Software

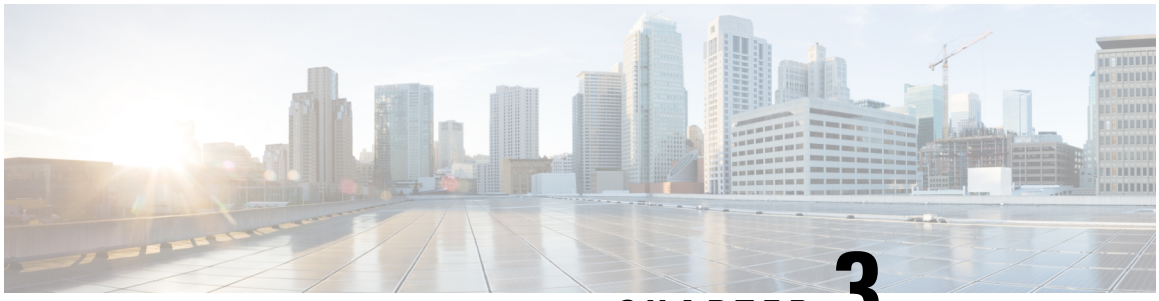
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 5: Feature Information for Digitally Signed Cisco Software

Feature Name	Releases	Feature Information
Digitally Signed Cisco Software		The Digitally Signed Cisco Software feature describes how to identify digitally signed Cisco software, gather software authentication information related to digitally signed images, and perform key revocation. Digitally Signed Cisco software is software that is digitally signed using secure asymmetrical (public-key) cryptography. The following commands were introduced or modified: **debug software authenticity, show software authenticity file, show software authenticity keys, show software authenticity running.**

Feature Name	Releases	Feature Information
Key Revocation Feature Support		Key revocation feature support was added. Key revocation removes a key from a platform's key storage. A platform can host a production or special image, and a production key (from a production image) or special key (from a special image) may be revoked during key revocation. The following section provides information about this feature: • Digitally Signed Cisco Software Key Revocation and Replacement The following commands were introduced or modified: **debug software authenticity, show software authenticity upgrade-status, software authenticity key add, software authenticity key revoke, upgrade rom-monitor file.**



CHAPTER 3

Using FTP to Manage System Images

This module contains information about using FTP to manage Cisco system images.

- Finding Feature Information, on page 17
- Image Copying from Flash Memory to an FTP Server, on page 17
- Image Copy from an FTP Server to a Flash Memory File System, on page 18
- Copying an Image from Flash Memory to an FTP Server, on page 19
- Copying from an FTP Server to Flash Memory, on page 20

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.

Image Copying from Flash Memory to an FTP Server

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the router to a server using FTP, the Cisco IOS software sends the first valid username it encounters in the following list:

1. The username specified in the **copy** privileged EXEC command, if a username is specified.
2. The username set by the **ipftpusername** global configuration command, if the command is configured.
3. Anonymous.

The router sends the first valid password it encounters in the following list:

1. The password specified in the **copy** privileged EXEC command, if a password is specified.
2. The password set by the **ipftppassword** global configuration command, if the command is configured.

The router forms a password *username @routername .domain* . The variable *username* is the username associated with the current session, *routername* is the configured hostname, and *domain* is the domain of the router.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the router.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user's name as the remote username.

Refer to the documentation for your FTP server for more information.

Use the **ipftpusername** and **ipftppassword** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify a username for that copy operation only.

Image Copy from an FTP Server to a Flash Memory File System

You can copy a system image from an FTP server to a flash memory file system.

FTP Username and Password

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the router to a server using FTP, the Cisco IOS software sends the first valid username it encounters in the following list:

1. The username specified in the **copy** privileged EXEC command, if a username is specified.
2. The username set by the **ipftpusername** global configuration command, if the command is configured.
3. Anonymous.

The router sends the first valid password it encounters in the following list:

1. The password specified in the **copy** privileged EXEC command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.

The router forms a password *username @routername .domain* . The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the router.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user's name as the remote username.

Refer to the documentation for your FTP server for more information.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify a username for that copy operation only.

Copying an Image from Flash Memory to an FTP Server

To copy a system image to an FTP network server, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ftp username** *username*
4. **ip ftp password** *password*
5. **end**
6. **show** *flash-filesystem* **:**
7. **copy** *flash-filesystem* **:** *filename* **ftp:** [[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*]

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:** `Router# configure terminal`	(Optional) Enters global configuration mode. This step is required only if you override the default remote username or password (see Steps 2 and 3).
Step 3	**ip ftp username** *username* **Example:** `Router(config)# ip ftp username user1`	(Optional) Changes the default remote username.
Step 4	**ip ftp password** *password* **Example:** `Router(config)# ip ftp password guessme`	(Optional) Changes the default password.
Step 5	**end** **Example:** `Router(config)# end`	(Optional) Exits global configuration mode. This step is required only if you override the default remote username or password (see Steps 2 and 3).
Step 6	**show** *flash-filesystem* **:** **Example:** `Router# show flash:`	(Optional) Displays the system image file in the specified flash directory. If you do not already know it, note the exact spelling of the system image filename in flash memory.

	Command or Action	Purpose
Step 7	**copy** *flash-filesystem* **:** *filename* **ftp:** [[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] **Example:** `Router# copy slot0:1:your-ios ftp://myuser:mypass@172.23.1.129/dirt/sysadmin/your-ios`	Copies the image to the FTP server. **Note** After you have issued the **copy** privileged EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **fileprompt** global configuration command.

Examples

The following example uses the **showslot1:privileged**EXEC command to display the name of the system image file in the second PCMCIA slot, and copies the file (test) to an FTP server:

```
Router# show slot1:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. 1        46A11866 2036C   4    746      May 16 1995 16:24:37 test
Router# copy slot1:test ftp://thisuser:thatpass@172.16.13.110/test
writing test!!!!...
successful ftp write.
```

In this example, the file named your-ios is copied from partition 1 of the flash memory PC card in slot 0 to the TFTP server at 172.23.1.129. The file will be saved with the name your-ios in the dirt/sysadmin directory relative to the directory of the remote username.

```
Router# show slot0: partition 1
PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   1711088 your-ios
[1711152 bytes used, 2483152 available, 4194304 total]
Router# copy slot0:1:your-ios ftp://myuser:mypass@172.23.1.129/dirt/sysadmin/your-ios
Verifying checksum for 'your-ios' (file # 1)...  OK
Copy 'your-ios' from Flash to server
  as 'dirt/sysadmin/ios-2'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

Copying from an FTP Server to Flash Memory

To copy a system image from an FTP server to a flash memory file system, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show** *flash-filesystem* **:**
3. **copy** *flash-url* **tftp** :[[[//*location*]/*directory*]/*filename*]
4. **configure terminal**
5. **ip ftp username** *username*

6. **ip ftp password** *password*
7. **end**
8. **copy ftp:** [[[//[*username* [**:***password*]**@**]*location*] */directory*]*/filename*]*flash-filesystem***:**[*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show** *flash-filesystem* **:** **Example:** `Router# show flash:`	(Optional) Displays the system image filename in Flash memory. Use this command to verify the url-path of the file and the exact spelling of the system image filename for use in the next command.
Step 3	**copy** *flash-url* **tftp** :[[[*//location*]*/directory*]*/filename*] **Example:** `Router# copy slot0:1:your-ios tftp://172.23.1.129/dirt/sysadmin/your-ios`	Copies the system image from Flash memory to a TFTP server. Specify the file location and filename as the *flash-url* argument. **Note** After you have issued the **copy** privileged EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **fileprompt** global configuration command.
Step 4	**configure terminal** **Example:** `Router# configure terminal`	(Optional) Enters global configuration mode from the terminal. This step is required only if you want to override the default remote username or password (see Steps 3 and 4).
Step 5	**ip ftp username** *username* **Example:** `Router(config)# ip ftp username netuser1`	(Optional) Changes the default remote username.
Step 6	**ip ftp password** *password* **Example:** `Router(config)# ip ftp password guessme`	(Optional) Changes the default password.
Step 7	**end** **Example:** `Router(config)# end`	(Optional) Exits global configuration mode. This step is required only if you override the default remote username or password (see Steps 3 and 4).

	Command or Action	Purpose
Step 8	**copy ftp:** [[[//[*username* [**:***password*]**@**]*location*] */directory*]*/filename*]*flash-filesystem***:**[*filename*] **Example:** `Router# copy ftp://myuser:mypass@theserver/tftpboot/sub3/c7200-js-mz slot1:c7200-js-mz`	Copies the configuration file from a network server to running memory or the startup configuration using rcp. **Note** After you have issued the **copy** privileged EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **fileprompt** global configuration command.

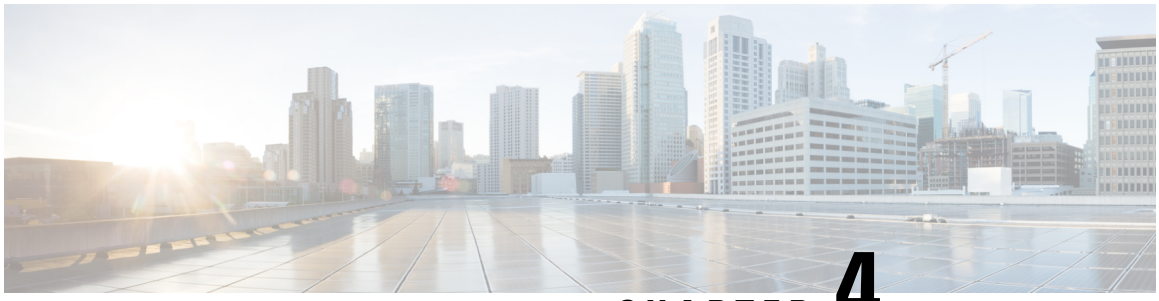
Examples

The following example illustrates how to use the **reload** command to reload the software on the router on the current day at 7:30 p.m.:

```
Router# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 1996 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

The following example illustrates how to use the **reload** command to reload the software on the router at a future time:

```
Router# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 1996 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```



CHAPTER 4

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 23
- Prerequisites for Cisco IOS Auto-Upgrade Manager, on page 23
- Restrictions for Cisco IOS Auto-Upgrade Manager, on page 24
- Information About Cisco IOS Auto-Upgrade Manager, on page 24
- How to Upgrade a Cisco IOS Software Image Using the Cisco IOS Auto-Upgrade Manager, on page 27
- Configuration Examples for Cisco IOS Auto-Upgrade Manager, on page 31
- Additional References, on page 33
- Feature Information for Cisco IOS Auto-Upgrade Manager, on page 34
- Glossary, on page 34

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

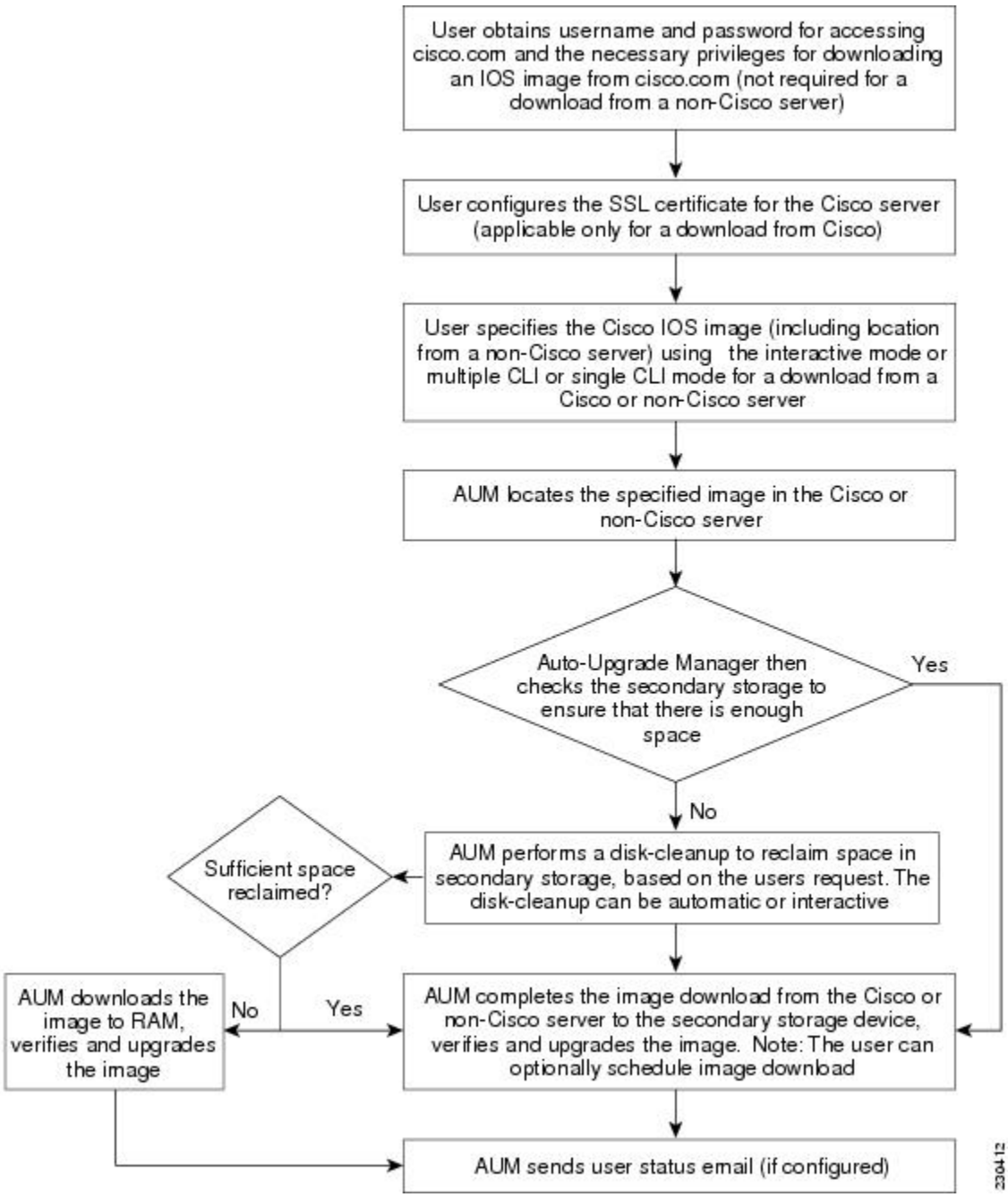
The Cisco IOS Auto-Upgrade Manager streamlines the process of upgrading to a new Cisco IOS software image. You can run the Cisco IOS Auto-Upgrade Manager through the command-line interface (CLI). AUM enables the router to connect to the Cisco website (www.cisco.com) and send the cisco.com username and 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 6: Feature Information for Cisco IOS Auto-Upgrade Manager

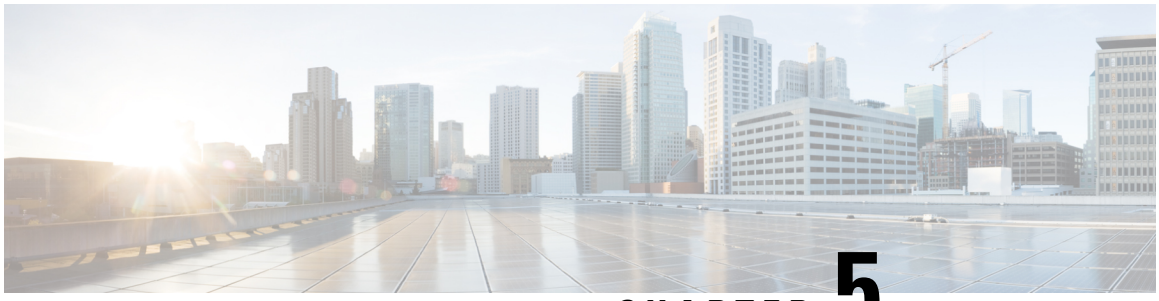
Feature Name	Releases	Feature Information
Cisco IOS Auto-Upgrade Manager	12.4(15)T Cisco IOS XE Release 3.9S	The Cisco IOS Auto-Upgrade Manager simplifies the software image upgrade process by providing a simple interface to specify, download, and upgrade a new Cisco IOS image. In 12.4(15)T, this feature 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



CHAPTER 5

Information About Boot Integrity Visibility

Boot Iintegrity Visibility allows Cisco's platform identity and software integrity information to be visible and actionable. Platform identity provides the platform's manufacturing installed identity. Software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted trusted code.

During the boot process, the software creates a checksum record of each stage of the bootloader activities.

You can retrieve this record and compare it with a Cisco-certified record to verify if your software image is genuine. If the checksum values do not match, you may be running a software image that is either not certified by Cisco or has been altered by an unauthorized party.

Note Boot Integrity Visibility is supported only on the active supervisor. It does not support high availability scenarios.

- Verifying the Software Image and Hardware, on page 37
- Verifying Platform Identity and Software Integrity, on page 38

Verifying the Software Image and Hardware

This task describes how to retrieve the checksum record that was created during a router bootup. Enter the following commands in privileged EXEC mode.

Note On executing the following commands, you might see the message % Please Try After Few Seconds displayed on the CLI. This does not indicate a CLI failure, but indicates setting up of underlying infrastructure required to get the required output. We recommend waiting for a few minutes and then try the command again.

The messages % Error retrieving SUDI certificate and % Error retrieving integrity data signify a real CLI failure.

1. show platform sudi certificate [sign [nonce nonce]]
2. show platform integrity [sign [nonce nonce]]

Verifying Platform Identity and Software Integrity

Verifying Platform Identity

The following example displays the Secure Unique Device Identity (SUDI) chain in PEM format. The first certificate is the Cisco Root CA 2048 and the second is the Cisco subordinate CA (ACT2 SUDI CA). Both certificates can be verified to match those published on https://www.cisco.com/security/pki/. The third is the SUDI certificate.

```
Device# show platform  sudi  certificate sign  nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQmqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgIEAYF/rTANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE3MDQyODEwNTU1NVoXDTI3
MDQyODEwNTU1NVowZTElMCMGA1UEBRMcUElEOkM5NTAwLTE2WCBTTjpGQ1cyMTE3
```

```
QTU2TTEOMAwGA1UEChMFQ2lzY28xGDAWBgNVBAsTD0FDVC0yIExpdGUgU1VESTES
MBAGA1UEAxMJQzk1MDAtMTZYMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAsenmrNybW0gLru4Y3UakblbFjmHvIwIdEro2HZPewrv/S014tPOAuXSfFdJh
SRAGwhB4ji71P4R9AqoQfrpybq3fJEaJCmakkdP5VBmPLm+QdJwGc7GGiUuXr6/R
PTjzdfVTJ0uvEi/holnTrYuHiu0JT3vsXi1bKkl1HJFeGspMCSZRRcoAxIZ8GRFt
+Y5f3QgV7b1Ce4zLSxJqTqiEDUNRuoeGwb+YtQOtep53hnwVoU6bjNaQXjq9pgcJ
dMyhh+zRtaRREpes4B7IZaFSMGeUbGvfVE6R+40mIM+T26fnZa2k4bQvrcm/1Vbe
/6Fy4rniHAXwzGCCgIHfIJMrSwIDAQABo28wbTAOBgNVHQ8BAf8EBAMCBeAwDAYD
VR0TAQH/BAIwADBNBgNVHREERjBEoEIGCSsGAQQBCRUCA6A1EzNDaGlwSUQ9VVlK
T1NqSk1Cd2dhVFc5dUlFOWpkQ0F4TUNBeE1qbzFORG96T0NENE9hQT0wDQYJKoZI
hvcNAQELBQADggEBADxO7Ks4AlSb8WnEq0OMoq+3tiXHLDYVdJUgH0w5FsUoE13f
yxn867saiJVMYrT7+/wTsexxdDJySGAJH5mPdwPPmEfLHw9/D6/l/d6Fsc1M/LeB
q+Q2a6L6oZd1rJJheNQyCN/jOCYuM0dK9JyDjLda9jSa3AL7UsOcr9aciBQ/CjZ6
8bV3x8LzAyPDs++qy6fHgB4OpP8vOJtQdnYGDZAtOun4Jlz3PyXjSJy9XWoWflG+
2nGXg9PCig8l1ppPjDg1prZ60lt+scEEJzqZmoHGn/lelOH4s+mJTVAxbgBudcA3
0XpdeHqOD0OdkG8JkXPYcUQ5in4R6zgwXEnqMzY=
-----END CERTIFICATE-----

Signature version: 1
Signature:
```

Verifying Software Integrity

The following example displays the checksum record for the boot stages. The hash measurements are displayed for each of the three stages of software successively booted. These hashes can be compared against Cisco-provided reference values. An option to sign the output gives a verifier the ability to ensure the output is genuine and is not altered. A nonce can be provided to protect against replay attacks.

```
Device# show platform integrity sign nonce 123
Platform: C9500-16X
Boot 0 Version: MA0081R06.1307262016
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
Boot Loader Version: System Bootstrap, Version 16.8.0.3, RELEASE SOFTWARE (P)
Boot Loader Hash:
F82826514658055C3993AB95F53512341BF20F3CC7D4083C980450FA6CD84608EE636B5B15D13414203CED35603F01974B8676C6AC6F9DC45B25CD1039E686C40A
OS Version: BLD_POLARIS_DEV_LATEST_20171213_030750
OS Hash:
E7336A416FB232CA87C73C5C6387EB7244560FBF9F977207D8783C113217DE3DD4CA16C40B16A8CC9841100264D04CAFE3AF863EB94EE561F9851AB167E913830A
PCR0: 9745B571B66D79F0936F4D292B5672B50F50FD1E56E74248D48A33582E992574
PCR8: 1CC295C233DA41BD3530A6F09C21991E8406BFFC88249D7778CA4BB0B9E71EB7
Signature version: 1
Signature:
```