



MD5 File Validation

Feature History

Release	Modification
12.2(4)T	This feature was introduced on the 12.2 T release train.
12.0(22)S	This feature was introduced on the 12.0 S release train.

This document describes the MD5 File Validation feature in Cisco IOS Releases 12.2(4)T and 12.0(22)S. It includes the following sections:

- [Feature Overview](#)
- [Supported Platforms](#)
- [Supported Standards, MIBs, and RFCs](#)
- [File Verification Tasks](#)
- [File Verification Examples](#)
- [Command Reference](#)

Feature Overview

The MD5 File Validation feature provides a Cisco IOS software command you can use to ensure file validation using the Message Digest 5 (MD5) algorithm in the Cisco IOS File System (IFS).

The MD5 File Validation feature allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

Benefits

- Provides a mechanism for users to verify that system image files are not corrupted or incomplete.
- Uses the industry-standard MD5 algorithm for improved reliability and security.
- Computes and displays the MD5 values from the Cisco IOS command-line interface (CLI); files do not have to be checked on another device.

Related Features and Technologies

- Cisco IOS File System (IFS)

Related Documents

- *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*

Supported Platforms

For a complete list of platforms, images, and software releases that support this feature, use Cisco Feature Navigator, available through Cisco.com at:

<http://www.cisco.com/go/fn>

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common. The list of supported platforms is regularly updated in Cisco Feature Navigator as new platform support is added for the feature.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Supported Standards, MIBs, and RFCs

MD5 if defined in RFC 1321.

File Verification Tasks

The MD5 File Validation feature allows you to generate the MD5 checksum for the Cisco IOS image stored on your router and compare it to the posted value posted on Cisco.com to verify that the image on your router is not corrupted.

You can obtain the MD5 value for your system image from the Software Center at Cisco.com. The most convenient way to get this value is to click on the name of the file prior to download. For example, if you select the 12.2.2T4 Release for the 3640 Platform with the Enterprise Plus Feature Set, before clicking the Download button, you can click on the file name for the image (c3640-js-mz.122-2.T4.bin) and the image information will be displayed.

Image information typically includes the Release, Description, File Size, BSD Checksum, Router Checksum, Date Published, and MD5 value for the image. You should record the MD5 value for the image prior to download. However, if you do not have the MD5 value for a previously downloaded image, you can select the same image on Cisco.com (using the same process you would use to download the image) to get the MD5 value.

To perform the MD5 integrity check after transferring an image file, use the following command:

Command	Purpose
Router# verify /md5 <i>filesystem:filename</i>	Calculates and displays the MD5 value for the software image.

Alternatively, you can specify the MD5 value in the command syntax, and the system will display a message indicating whether the values match. To specify a known MD5 value, use the following syntax:

Command	Purpose
Router# verify /md5 <i>filesystem:filename MD5-value</i>	Checks for a match with a specified MD5 value.

A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

File Verification Examples

In the following example, the **/md5** keyword is used to display the MD5 value for the image stored in disk1 of the device. The MD5 value shown in the last line can be compared to value provided on Cisco.com.

```
Router# verify /md5 disk1:
Verify filename []? c7200-js-mz
.....
.....
.....
.....
.....
.....Done!
verify /md5 (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

In the following example, the known MD5 value for the image is specified in the **verify** command, and the system checks the value against the stored value:

```
Router# verify /md5 disk1:c7200-js-mz ?
WORD Expected md5 signature
<cr>
router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3
.....
.....
.....
.....
.....Done!
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

Command Reference

This section documents the modified **verify** command. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

verify

To verify the checksum of a file on a memory file system, use the **verify** command in EXEC mode.

```
verify [/md5] filesystem:[file-url][filename] [md5-value]
```

Syntax Description	
/md5	(Optional) Calculates and displays the Message Digest 5 (MD5) value for the specified software image. Compare this value with the value available on Cisco.com for this image.
<i>md5-value</i>	(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system will calculate the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.
<i>filesystem:</i>	Filesystem prefix for the location of the file to be verified, followed by a colon. Standard Flash memory filesystem prefixes include: <ul style="list-style-type: none"> • bootflash: • flash: • slot0: • slot1: • disk0: • disk1: Protocol prefixes, such as tftp: can also be used. The available filesystem prefixes will depend on your hardware.
<i>file-url/</i>	(Optional) The URL (file path) for the file to be verified. Use a forward slash (/) between each directory.
<i>filename</i>	Name of the file to be verified. The file can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Defaults The current working device (filesystem) is the default device.

Command Modes EXEC

Command History	Release	Modification
	11.0	The verify command was introduced.
	12.2(4)T	The /md5 option was added.

Usage Guidelines Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory; it is not displayed when the image file is copied from one disk to another.

The **verify** command (when used without the MD5 option) will recompute and verify the image checksum after the image has been copied into Flash memory. Note, however, that the **verify** command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the router and saved in the file system without detection. If a corrupt image is transferred successfully to the router, the software will be unable to tell that the image is corrupted and the file will verify successfully. For this reason, use of the MD5 option is highly recommended.

To use the MD5 hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **verify /md5** command allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into Flash memory or onto a server. A variety of image information is available on Cisco.com. For example, you can get the Release, Feature Set, Size, BSD Checksum, Router Checksum, MD5, and Publication Date information by clicking on the image file name prior to downloading it from the Software Center on Cisco.com.

To perform the MD5 integrity check, use the **verify** command with the **/md5** keyword. For example, entering the **verify /md5 flash:c7200-is-mz.122-2.T.bin** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, executing the **verify /md5 flash:c7200-is-mz.122-2.T.bin 8b5f3062c4caeccae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch.

A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

The **verify** command replaces the **copy verify** and **copy verify flash** commands.

Examples

In the following example, the **verify** command is used to check the integrity of the file `c7200-js-mz` on the Flash memory card inserted in slot 0:

```
Router# dir slot0:
Directory of slot0:/
 1 -rw-      4720148   Aug 29 1997 17:49:36 hampton/nitro/c7200-j-mz
 2 -rw-      4767328   Oct 01 1997 18:42:53 c7200-js-mz
 5 -rw-         639   Oct 02 1997 12:09:32 rally
 7 -rw-         639   Oct 02 1997 12:37:13 the_time

20578304 bytes total (3104544 bytes free)
Router# verify slot0:c7200-js-mz
Verified slot0:c7200-js-mz
```

In the following example, the **/md5** keyword is used to display the MD5 value for the image:

```
Router# verify /md5 disk1:
Verify filename []? c7200-js-mz
.....
.....
.....
.....
.....
```

```

.....Done!
verify /md5 (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3

```

In the following example, the known MD5 value for the image (obtained from Cisco.com) is specified in the **verify** command, and the system checks the value against the stored value:

```

Router# verify /md5 disk1:c7200-js-mz ?
WORD Expected md5 signature
<cr>
Router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3
.....
.....
.....
.....
.....
.....
.....Done!
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3

```

Use of the MD5 option also allows access to more file systems, as shown in the following example:

```

Router#verify ?
/md5 Compute an md5 signature for a file
bootflash: File to be verified
flash: File to be verified
slot0: File to be verified
slot1: File to be verified

Router#verify /md5 ?
bootflash: File to be verified
disk0: File to be verified
disk1: File to be verified
flash: File to be verified
slot0: File to be verified
slot1: File to be verified

```

Note the addition of disk0: and disk1:.

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the cd command.
show file systems	Lists available file systems.
show flash	Displays the contents of Flash memory.