Availability and description of the File Checksum Integrity Verifier utility

Article ID: 841290 - View products that this article applies to.

Summary

The File Checksum Integrity Verifier (FCIV) is a command-prompt utility that computes and verifies cryptographic hash values of files. FCIV can compute MD5 or SHA-1 cryptographic hash values. These values can be displayed on the screen or saved in an XML file database for later use and verification.

INTRODUCTION

This article discusses the File Checksum Integrity Verifier (FCIV) utility.

Warning The Microsoft File Checksum Integrity Verifier (FCIV) utility is an unsupported command-line utility that computes MD5 or SHA1 cryptographic hashes for files. Microsoft does not provide support for this utility. Use this utility at your own risk. Microsoft Product Support Services (PSS) cannot answer questions about the File Checksum Integrity Verifier utility.

The File Checksum Integrity Verifier (FCIV) utility can generate MD5 or SHA-1 hash values for files to compare the values against a known good value. FCIV can compare hash values to make sure that the files have not been changed.

With the FCIV utility, you can also compute hashes of all your critical files and save the values in an XML file database. If you suspect that your computer may have been compromised, and important files have been changed, you can run a verification of the file system files against the XML database to determine which files have been modified.

The FCIV utility runs on Microsoft Windows 2000, Windows XP, and Windows Server 2003.

Features

The FCIV utility has the following features:

- Supports MD5 or SHA1 hash algorithms (The default is MD5.)
- Can output hash values to the console or store the hash value and file name in an XML file
- Can recursively generate hash values for all files in a directory and in all subdirectories (for example, **fciv.exe c:\ -r**)
- Supplies an exception list to specify files or directories to hash
- Can store hash values for a file with or without the full path of the file

Installation

To obtain the FCIV utility, follow these steps:

1. In Windows Explorer, create a new folder that is named FCIV.
2. The following file is available for download from the Microsoft Download Center:

   Download the File Checksum Integrity Verifier utility package now. (http://download.microsoft.com/download/c/f/4/cf454ae0-a4bb-4123-8333-a1b6737712f7/Windows-KB841290-x86-ENU.exe)
   Release Date: May 17, 2004

   For additional information about how to download Microsoft Support files, click the following article number to view the article in the Microsoft Knowledge Base:

   119591 (http://support.microsoft.com/kb/119591/) How to Obtain Microsoft Support Files from Online Services

   Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted. The file is stored on security-enhanced servers that help to prevent any unauthorized changes to the file.
3. In the **File Download** dialog box, click **Save**, and then save the file to the FCIV folder that you created in step 1.
4. When the download is completed, click **Close**.
5. In the FCIV folder, double-click **Windows-KB841290-x86-ENU.exe**.
6. Click **Yes** to accept the license agreement.
7. Click **Browse**, click the **FCIV** folder, and then click **OK**.
8. Click **OK** to extract the files.
9. When the file extraction is completed, click **OK**.
10. Add the FCIV folder to the system path.
11. To start a command prompt, click **Start**, click **Run**, type **cmd** in the **Open** box, and then click **OK**.
12. Type **fciv.exe /?**, and then press ENTER.

Note If FCIV was installed to the C:\FCIV directory, type **set path=%path%;c:\fciv** to add it to the system path in a command shell.

Usage

Syntax

```
fciv.exe [Commands] <Options>
```

Commands

- **-add** *file | dir*: Compute the hash and send it to an output device (default screen). The *dir* parameter has the following options:

    - **-r**: Recursive.
    - **-type**: Specify file type. For example, **-type *.exe**.
    - **-exc file**: Do not compute these directories.
    - **-wp**: Do not store the full path name. (By default, FCIV stores the full path name.)
    - **-bp**: Remove the base path from the path name of each entry.

- **-list**: List entries in the database.
- **-v**: Verify hashes. The **-v** option has the following option:

    - **-bp**: Remove the base path from the path name of each entry.

- **-?**, **-h**, or **-help**: Open extended help.

Options

- **-md5**, **-sha1**, or **-both**: Specify hash type. (By default, MCIV uses -md5.)
- **-xml db**: Specify database format and name.

    Note When you use the **-v** option to verify a hash, FCIV also sends a return error code to indicate whether a hash is verified. A zero (0) indicates success, and a 1 indicates failure. With the return error code, you can use FCIV in automated scripts to verify hashes.

Example usage

- To display the MD5 hash of a file, type the following command at a command prompt:
    fciv.exe *filename*

    Note *filename* is the name of the file.
- To compute a hash of a file, type a command line that is similar to any one of the following command lines:
    fciv.exe c:\mydir*myfile.dll*

    fciv.exe c:\ -r -exc exceptions.txt -sha1 -xml dbsha.xml

    fciv.exe c:*mydir* **-type *.exe**

    fciv.exe c:*mydir* **-wp -both -xml db.xml**

- To list the hashes that are stored in a database, type a command line that is similar to the following command line:
    fciv.exe -list -sha1 -xml db.xml

- To verify a hash in a file, type a command line that is similar to any one of the following command lines:
    fciv.exe -v -sha1 -xml db.xml

    fciv.exe -v -bp c:*mydir* **-sha1 -xml db.xml**

Database storage format

The File Checksum Integrity Verifier (FCIV) utility can store entries in an XML database file. When FCIV is configured to store hash values in an XML database file, the hexadecimal hash values are stored in base64 encoded format. When you view the XML database directly, the base64 encoded representation of the hash value does not visually match the hexadecimal value that the console displays. FCIV decodes the base64 encoded hashes when it displays the contents of the database to the screen. Therefore, it displays the correct hexadecimal value.

The following example shows how FCIV computes the MD5 hash value for Ntdll.dll and displays it at the command prompt:

```
C:\WINDOWS\system32>fciv -add ntdll.dll // // File Checksum Integrity Verifier version 2.05. //
6cbfd919baa7c9e03c8471ae4d8f8bb0 ntdll.dll
```

Here is the hash value for the same file that is base64 encoded and stored in an XML file by using the following command:

   C:\WINDOWS\system32>fciv -add ntdll.dll -xml c:\temp\ntdll.xml

```
<?XML version="1.0" encoding="utf-8"?> <FCIV> <FILE_ENTRY><name>ntdll.dll</name><MD5>bL/ZGbqnyeA8hHGuTY+LsA==</MD5>
</FILE_ENTRY></FCIV>
```

Here is the value that appears in the XML file that uses FCIV to list the contents.

Note It matches the value that was computed in the first example.

```
C:\WINDOWS\system32>fciv -list -XML c:\temp\ntdll.XML // // File Checksum Integrity Verifier version 2.05. // Listing entries
in database: ---------------------------- MD5 Filename ------------------------------------------------------------------------------
-- 6cbfd919baa7c9e03c8471ae4d8f8bb0 ntdll.dll Number of entries found: 1
```

Verification

How to generate and verify hash values for a Microsoft Download

- Download the file to a temporary directory (such as C:\Temp).
- To extract the contents of the file, use the **/x** switch. Specify an output directory for the extracted files when you are prompted (such as C:\Temp\Files).

  You can also use the **/extract** switch to extract the files without starting Setup.

  For additional information about the /extract switch, click the following article number to view the article in the Microsoft Knowledge Base:
  262841 (http://support.microsoft.com/kb/262841/) Command-Line switches for Windows software update packages

  The security update may be an IExpress package. If it is, see the following article in the Microsoft Knowledge Base about how to extract an IExpress package:

  197147 (http://support.microsoft.com/kb/197147/) Command-line switches for IExpress software update packages

- To create a database for a single file and to save it to the C:\Temp directory, type the following command:
  fciv.exe -add c:\temp\files*filename*.dll -wp c:\temp\files -XML c:\temp*filename*.XML

- To verify the contents of the XML database against an installed file, type the following command:
  fciv.exe -v -bp c:\installeddirectory -XML c:\temp\filename.XML

  Note *installeddirectory* is the location of the installed file.

  Note When you use the **-v** option to verify a hash, FCIV also provides a return error code to indicate success (0) or failure (1) to verify a hash. Because of the return error code, you can use FCIV in automated scripts to verify hashes.
- FCIV will confirm at the console if the hash values for the file matches the values that are stored in the XML database.

How to verify the hash values for the files in the Windows directory and in all sub-directories

You can also build a hash database of your sensitive files and verify them regularly.

- To create the database and to save it to the C:\Temp directory, type the following command:
  fciv.exe -add %systemroot% -r -XML c:\temp\windows-hashes.XML

- To list the contents of the database to the console, type the following command:
  fciv.exe -list -XML c:\temp\windows-hashes.XML

- To verify the contents of the XML database against the current file system files, type the following command:
  fciv -v -XML c:\temp\windows-hashes.XML

Note This is a "FAST PUBLISH" article created directly from within the Microsoft support organization. The information contained herein is provided as-is in response to emerging issues. As a result of the speed in making it available, the materials may include typographical errors and may be revised at any time without notice. See Terms of Use (http://go.microsoft.com/fwlink/?LinkId=151500) for other considerations.

Properties

Article ID: 841290 - Last Review: June 17, 2013 - Revision: 5.0

Applies to
- Customer Service and Support Information

Keywords: kmcustomerservice kbhowtomaster KB841290