Knowledge Base

Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available

PSS ID Number: 303215
Article Last Modified on 3/2/2004

The information in this article applies to:

- Microsoft Data Engine (MSDE)
- Microsoft Data Engine (MSDE) 1.0
- Microsoft Exchange 2000 Server
- Microsoft Exchange 2000 Server SP1
- Microsoft Exchange Server 5.5
- Microsoft Exchange Server 5.5 SP1
- Microsoft Exchange Server 5.5 SP2
- Microsoft Exchange Server 5.5 SP3
- Microsoft Exchange Server 5.5 SP4
- Microsoft Internet Explorer version 6 for Windows XP
- Microsoft Internet Explorer version 6 for Windows 2000
- Microsoft Internet Explorer 5.5 for Windows 2000
- Microsoft Internet Explorer 5.5 for Windows 2000 SP 1
- Microsoft Internet Explorer 5.5 for Windows 2000 SP 2
- Microsoft Internet Explorer 5.01 for Windows 2000
- Microsoft Internet Explorer 5.01 for Windows 2000 SP 1
- Microsoft Internet Explorer 5.01 for Windows 2000 SP 2
- Microsoft Internet Explorer version 6 for Windows NT 4.0
- Microsoft Internet Explorer 5.5 for Windows NT 4.0
- Microsoft Internet Explorer 5.5 for Windows NT 4.0 SP 1
- Microsoft Internet Explorer 5.5 for Windows NT 4.0 SP 2
- Microsoft Internet Explorer 5.01 for Windows NT 4.0
- Microsoft Internet Explorer 5.01 for Windows NT 4.0 SP 1
- Microsoft Internet Explorer 5.01 for Windows NT 4.0 SP 2
- Microsoft Internet Information Server 4.0
- Microsoft Internet Information Services 5.0
- Microsoft SQL Server 2000 (all editions) SP1
- Microsoft SQL Server 2000 (all editions) SP2
- Microsoft SQL Server 7.0
- Microsoft SQL Server 7.0 Service Pack 1
- Microsoft SQL Server 7.0 Service Pack 2
- Microsoft SQL Server 7.0 Service Pack 3
- Microsoft SQL Server 7.0 Service Pack 4
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, Standard Edition
- Microsoft Windows Server 2003, Web Edition
- Microsoft Windows XP Home Edition
- Microsoft Windows XP Professional
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server, Enterprise Edition 4.0
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows Small Business Server 2003, Premium Edition
- Microsoft Windows Small Business Server 2003, Standard Edition
- Microsoft Data Access Components 2.5
- Microsoft Data Access Components 2.6
- Microsoft Data Access Components 2.7
- Microsoft Data Access Components 2.8
- Microsoft Exchange Server 2003 Enterprise Edition
- Microsoft Exchange Server 2003 Standard Edition
- Microsoft Internet Information Services version 6.0
- Microsoft Windows Media Player 6.4
- Microsoft Windows Media Player 7

- Microsoft Windows Media Player 7.1
- Microsoft Windows Media Player 9 Series for Windows XP
- Microsoft Windows Media Player 9 Series for Windows 2000
- Microsoft XML 2.5
- Microsoft XML 2.6
- Microsoft XML 3.0
- Microsoft XML 4.0
- Microsoft Content Management Server 2001
- Microsoft Content Management Server 2002
- Microsoft Commerce Server 2000
- Microsoft Commerce Server 2002
- Microsoft BizTalk Server 2000
- Microsoft BizTalk Server 2002
- Microsoft SNA Server 4.0
- Microsoft Host Integration Server 2000
- Microsoft virtual machine

This article was previously published under Q303215

SUMMARY

The Hfnetchk tool is a command-line tool that administrators can use to centrally assess a computer or group of computers for the absence of security updates. As of the version 1.1 release of the Microsoft Baseline Security Analyzer (MBSA), Hfnetchk is exposed through the MBSA command-line interface, **mbsacli.exe /hf**. The latest version of the Hfnetchk engine is available in MBSA version 1.2. For additional information about how to obtain MBSA, click the following article number to view the article in the Microsoft Knowledge Base:

320454 Microsoft Baseline Security Analyzer (MBSA) version 1.2 is available

You can use the Hfnetchk tool to assess the security update status of computers that are running Windows Server 2003, Windows XP, Windows 2000, and Windows NT 4.0. You can also use the tool to assess security updates for Internet Information Services (IIS), SQL Server (including Microsoft Data Engine [MSDE]), Exchange Server, Windows Media Player, Internet Explorer 5.01, Microsoft Data Access Components (MDAC), Microsoft virtual machine (VM), Microsoft XML (MSXML), Content Management Server, Commerce Server, BizTalk, and Host Integration Server.

CONTENTS

For additional information about Hfnetchk, click the following article number to view the article in the Microsoft Knowledge Base:

305385 Frequently Asked Questions about the Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool

Shavlik Technologies developed Hfnetchk for Microsoft. For additional information about Shavlik, visit the following Shavlik Web site:

http://www.shavlik.com

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

MORE INFORMATION

Download

The following files are available for download from the Microsoft Download Center:

English

Download the MBSASetup-en.msi package now.

French

Download the MBSASetup-fr.msi package now.

German

Download the MBSASetup-de.msi package now.

Japanese

Download the MBSASetup-ja.msi package now.

Note Hfnetchk is available through the MBSA version 1.2 command-line interface, **mbsacli.exe /hf**.

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 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.

System Requirements

For information about the system requirements for Hfnetchk, view the Readme.html file that is included with MBSA 1.2.

Quick Start Guide

If you want to use the Hfnetchk tool now and read the rest of this document later, follow these steps:

1. Download MBSA version 1.2 from the link in the "Download" section of this article.
2. Double-click the MBSA file that you downloaded, and then follow the installation instructions.
3. Read the End-User License Agreement (EULA).
4. At a command prompt, locate the folder that the installation created.
5. Type `mbsacli.exe /hf -v -z -s 1`, and then press ENTER.

Description

The Hfnetchk engine is a command-line tool that you can use to assess a computer or group of computers for the absence of security updates. You use the **mbsacli /hf** command to run Hfnetchk. You can use Hfnetchk to assess the security update status for the Windows Server 2003, Windows XP, Windows 2000, and Windows NT 4.0 operating systems. You can also use it to assess security update status for IIS, SQL Server (including MSDE), Exchange Server, Windows Media Player, Internet Explorer, MDAC, Microsoft VM, MSXML, Content Management Server, Commerce Server, BizTalk, and Host Integration Server.

The Hfnetchk tool uses an XML file that indicates which hotfixes are available for each product. The XML file contains the security bulletin name and title, and it also contains detailed data about product-specific security hotfixes, including the following items (and much more):

- Files in each hotfix package and their file versions and checksums.
- Registry keys that the hotfix installation package applies.
- Information about which patches replace other patches.
- Related Microsoft Knowledge Base article numbers.

When you run the Hfnetchk tool for the first time from a command line (without any switches), the tool must obtain a copy of this XML file so that the tool can find the hotfixes that are available for each product. The XML file is available from the Microsoft Download Center Web site in compressed form. The file is a digitally signed .cab file. Hfnetchk downloads the .cab file, verifies the signature, and then decompresses the .cab file to your local computer. (A .cab file is a compressed file that is similar to a .zip file.)

After the .cab file is decompressed, Hfnetchk scans your computer (or the selected computers) to determine the operating system, service packs, and programs that are running. Hfnetchk then parses the XML file and identifies security patches that are available for your combination of installed software. Patches that are available for your computer but are not currently installed on your computer appear as "patch not found" in the resulting output. In the default configuration, the Hfnetchk output displays only those security patches that you must install to bring your computer up to date. Hfnetchk recognizes rollup packages and does not display those patches that are superseded by later patches.

How the Tool Works

For Hfnetchk to determine if a specific patch is installed on a certain computer, it evaluates the registry key that is installed by the patch, the file version, and the checksum for each file that is installed by the patch.

In the default configuration, Hfnetchk compares both file details and registry keys from the resulting XML subset to the files and registry details on the computer that is being scanned. If the file or registry key details on the computer do not match the information that is stored in the XML file, the associated security patch is identified as not installed ("patch not found"), and the results of the scan do not appear on the screen. However, the specific Microsoft Knowledge Base article number that relates to the patch appears on the screen. For additional information about the tool and frequently asked questions about the tool, click the following article number to view the article in the Microsoft Knowledge Base:

305385 Frequently Asked Questions about the Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool

Hfnetchk first examines the computer to determine if the registry key that is associated with the patch exists. If the registry key does not exist, the patch is considered not installed (see the "Usage Syntax" section in this article for information about the **-z** switch that disables checking for registry keys). If the registry key does exist, Hfnetchk searches for the related files on the computer and compares the file version and checksum from the XML file to the file version and checksum of the files on the computer. If any one of the file tests are not successful, the hotfix is listed as "patch not found."

Specific details about why a patch is considered not installed is available if you run the tool with the **-v** switch. To bypass the registry keys and look only for file details, use the **-z** switch and the **-v** switch:

```
mbsacli /hf -v -z
```

Additional command-line switches specify groups of computers to scan, output format, engine speed, types of checks, location of the XML file, and other functions. For detailed descriptions of the command-line switches, see the "Usage Syntax" section of this article.

Scanning Prerequisites

Make sure that you meet the following requirements so that Hfnetchk will scan successfully.

When you scan your local computer:

- You have administrative credentials on your local computer.
- The computer can download the patch database XML file from the Internet or obtain the file from another specified location (either on the local computer or from a specified network location).
- The local computer is running the Workstation service.

  Note You do not have to use the Server service on the local computer.

When you scan a remote computer:

- You meet all the requirements for a local scan.

- You have administrative credentials on the remote computer and can log on to the remote computer from the workstation from where you perform the scan.
- You can access the NetBIOS (tcp139) or Direct Host (tcp445) ports on the remote computer.
- The remote computer is running the Server service.

  Note You do not have to use the Workstation service on the remote computer.
- The remote computer is running the Remote Registry service.
- You can access the *%systemroot%* share on the remote computer.

Usage Syntax

To view the syntax for Hfnetchk, type the following command at a command prompt:

```
mbsacli /hf /?
```

Descriptions for each of the switches are listed in this section: **mbsacli /hf [-h *hostmane*] [-fh *filename*] [-i *ipaddress*] [-fip *filename*] [-r *ipaddressrange*] [-d *domainname*] [-n] [-sus *SUS server*|*SUS filename*] [-b] [-fq *filename*] [-s 1] [-s 2] [-nosum] [-sum] [-z] [-v] [-history *level*] [-nvc] [-o *option*] [-f *filename*] [-unicode] [-t] [-u *username*] [-p *password*] [-x] [-about] [-?]**

- **-h *hostname*** - This switch specifies the NetBIOS computer name to scan. The default location is the local host. You can scan multiple host names if you separate each host name entry with a comma. For example:

  ```
  mbsacli /hf -h hostname1,hostname2,hostname3
  ```
- **-fh *filename*** - This switch specifies the name of a file that contains NetBIOS computer names to scan. There is one computer name on every line, and a maximum of 256 computers in every file. For example:

  ```
  mbsacli /hf -fh hosts.txt
  ```
- **-i *xxx.xxx.xxx.xxx*** - This switch specifies the Internet Protocol (IP) address of the computer to scan. You can scan multiple IP addresses if you separate each IP address entry with a comma. For example:

  ```
  mbsacli /hf -i xxx.xxx.xxx.xxx, xxx.xxx.xxx.xxx
  ```
- **-fip *filename*** - This switch specifies the name of a file that contains addresses to scan. There is one IP address for every line, and a maximum of 256 lines for each file. For example:

  ```
  mbsacli /hf -fip IP_addresses_to_scan.txt
  ```
- **-r *xxx.xxx.xxx.xxx – yyy.yyy.yyy.yyy*** - This switch specifies the IP address range to be scanned, staring with xxx.xxx.xxx.xxx and ending with yyy.yyy.yyy.yyy. For example: *mbsacli /hf –r xxx.xxx.xxx.xxx - yyy.yyy.yyy.yyy*

  Note You can use the -h, -fh, -i, -fip, and -r switches in combination. For example: `mbsacli /hf –h hostname1,hostname2 -i xxx.xxx.xxx.xxx -fip ipaddresses.txt -r yyy.yyy.yyy.yyy-zzz.zzz.zzz.zzz`
- **-d *domainname*** - This switch specifies the domain name to scan. All computers in the domain are scanned. For example:
  ```
  mbsacli /hf –d domainname
  ```

  Note For TCP/IP networks, the local network must support User Datagram Protocol (UDP).
- **-n** - This switch scans all computers on the local network. For example: `mbsacli /hf -n`

  Note The -n switch is similar to the -d switch. However, all computers from all domains on the network are scanned when you use the -n switch.
- **-sus *SUS server* | *SUS filename*** – This switch specifies to scan only for security updates that are marked as approved. You can specify the URL of a Software Update Services (SUS) server, or the URL or UNC path for an Approveditems.txt file. For example: `mbsacli /hf -sus http://SUSserver` or `mbsacli /hf -sus \\server\share\approveditems.txt` If a URL or UNC path is not specified, the value stored in the registry on the client computer will be used.
- **-b** - This switch specifies to scan your computer only for those updates that are marked as baseline critical by the Microsoft Security Response Center. To perform a baseline scan, your computer must be running the latest service pack that is available for your operating system.
- **-fq *filename*** - This switch specifies the name of a file that contains "Qnumbers" for updates that you want to suppress on the output. Specify one "Qnumber" per line. You can use this switch to suppress the output of known note messages (such as MS01-022 on Windows 2000-based computers) or the Qnumbers of patches that you have not approved and whose status you do not assess. For example:

  ```
  hfnetchk –fq ignore.txt
  ```

  Note "Qnumbers" are numbers of Microsoft Knowledge Base articles that provide information about an update. Article numbers used to start with the letter "Q".
- **-s 1** - This switch suppresses security update check note messages.

  Note By default, security update check note message are not suppressed.
- **-s 2** - This switch suppresses security update check warning messages.

  Note By default, security update check warning message are not suppressed.
- **-nosum** - This switch specifies that you do not want the tool to perform checksum validation for the update files.
- **-sum** – This switch forces a checksum scan when you scan non-English-language computers. Use this switch only if you have a custom XML file with language-specific checksums.
- **-z** - This switch specifies that you do not want the tool to perform registry checks. For example: `mbsacli /hf -z`

  The -z switch disables the registry checking function of mbsacli /hf. By default, the registry key that is specific to each update is examined to determine if the patch is installed. If the registry key does not exist, mbsacli /hf displays the "Patch Not Found" message. If the registry key does exist, the file versions and file checksums are examined. To disable the registry check and perform only file checks, use the -z switch.

  The -z switch is an important switch to use when you troubleshoot output, particularly when you use the -v switch. Updates are typically identified as missing if one of the three update related tests fails: registry key, file version, and file checksum. Under some circumstances, a registry key may not exist even if the update is installed. Under these circumstances, you can instruct mbsacli /hf

to bypass the registry checks and perform only the file checks. If you use the -z switch with the -v switch, you can find the files that are missing instead of the registry keys.

- **-v** - This switch displays the reason why a test did not work in wrap mode. For example: `mbsacli /hf -v`

  You can use the -v switch to display the reason why an update is considered "not found," or the reason why you receive a warning or note message. If you use the -v switch without the -z switch, the -v switch either displays the registry key that must be present for the hotfix to be considered installed, or it displays the details of the warning message. When you use the -z switch, mbsacli /hf displays information about the files that are necessary for the patch to be considered as installed but are not found on the computer.

  You can use the -v and -z switches until you have installed all the required patches onto your computer, and then use the default syntax (no switches) to monitor changes on a daily basis.

-

- **-history *n*** - This switch displays updates that have been explicitly installed, explicitly not installed, or both. You do not require this switch for ordinary operation. However, you may require it under very specific circumstances. You can use any one of three values for n with this switch:
  - 1 - Displays those updates that have been explicitly installed.
  - 2 - Displays those updates that have been explicitly not installed.
  - 3 - Displays those updates that have explicitly been installed and not installed.

  Note An update that has been individually installed (not installed by means of a rollup package) is an *explicitly installed update*. For example, assume that a system administrator has a Windows NT 4.0-based computer that is running Service Pack 6a (SP6a) and no updates. The administrator installs the Windows NT 4.0 post-SP6a Security Rollup Package (MS01-041) on this computer. The MS01-041 update is explicitly installed. The MS01-041 update is an update rollup that replaces more than 20 earlier security updates, including MS01-033. In this example, MS01-033 has not been explicitly (individually) installed although it is included in the MS01-041 patch.

  If the administrator runs **mbsacli /hf** with the **-history 3** switch to view both the explicitly installed and the explicitly not installed updates, the output shows MS01-041 as "found" and MS01-033 and the more than 20 other replaced updates as "not found." If the administrator installed MS01-033 before MS01-041, Hfnetchk shows both of these updates as "found" and the other replaced updates as "patch not found." Although Hfnetchk lists the more than 20 updates as "not found" (explicitly not installed), the administrator does not have to install these updates because MS10-041 replaces them.

  By default, the output for **mbsacli /hf** (without the **-history** switch) works for replacements and update rollups and displays only those updates that are you need to bring your computer up to date.

  Use the **-history** switch only when you want to view a history of updates that were explicitly or individually installed. Remember that you cannot use the **-history** switch with update rollups or replacements. Use this switch only to determine if a specific update was individually installed on a specific computer.
- **-nvc** - This switch disables the check for a new version of MBSA.
- **-o [tab | wrap]** - This switch specifies the output format. You can use either of two values for the -o switch:
  - **tab** - Generates output in tab-delimited format.
  - **wrap** - Generates output in a word-wrapped format.

  For example: `mbsacli /hf -o tab -f scan.txt`

  The default value is wrap. You must use tab-delimited output when you scan more than 255 hosts. You can also use tab-delimited output when you want to redirect the screen output to a text file. Then, you can import the text file into a spreadsheet or database.

  Note Tab-delimited output may appear to be incorrectly formatted on the screen.
- **-f** - This switch specifies the name of a file to store the results of a scan. You can use this switch with both word- wrap and tab-delimited outputs. For example, to store the results of a tab-delimited output to a Scanresults.txt file on drive C, use the following command: `mbsacli /hf -o tab -f c:\scanresults.txt`
- **-unicode** – This switch specifies to generate unicode output. If you use a Japanese localized version of MBSA or scan computers that are running Japanese localized versions of Windows, it is a good idea to specify this switch.
- **-t** - This switch displays the number of threads that are used to run the scan. Possible values are from 1 to 128. The default value is 64. You can use this switch to increase or decrease the speed of the scanner.

  The **mbsacli /hf** switch uses standard Windows networking functions to identify computers that are running Windows. However, this can lead to longer wait times when no hosts are present in specified address spaces. Therefore, after a maximum number of threads are open and working, the scanner appears to slow down. You do not experience delays when you use the default number of threads on a populated network. For example:

  ```
  mbsacli /hf -t 128
  ```
- **-u *username*** - This switch specifies the user name to use when you scan a local or a remote computer or group of computers. You must use this switch with the -p (password) switch.

  By default, mbsacli /hf scans computers by using the credentials of the user who is currently logged on to the computer that is used to perform the scan. You can use the -u and -p switches to scan the specified computers with a user name and password that you specify on the command-line. For example: `mbsacli /hf -i 172.16.1.10 -u administrator -p password`. To use credentials from a specific domain, use domain_name\username format for username. For example: `mbsacli /hf -i ipaddress -u corpdomain\administrator -p password`
- **-p *password*** - This switch specifies the password to use when you scan a local or remote computer or group of computers. You must use it with the -u (username) switch.

  For security purposes, the password is not sent over the network in clear text. Instead, mbsacli /hf uses the Windows NT challenge-response mechanism that is built into Windows NT 4.0 and later to secure the authentication process.

  Important It is a good idea not to store the user name and password combination in a batch file. If you do this, any user with read access to the batch file could obtain the password in clear text by reading the batch file.
- **-x** - This switch specifies the XML data source that contains the hotfix information. The location may be an XML file name, a compressed XML .cab file, or a URL. The default file is the Mssecure.cab file from the Microsoft Web site.

When you run **mbsacli /hf** without the **-x** switch, the XML file is downloaded from the Microsoft Web site. The XML file is named Mssecure.xml and is typically located in the same folder as the Mbsacli_/hf.exe file. After you download the file, you can run future scans with the **-x** switch, for example:

```
mbsacli /hf -x mssecure.xml
```

This sample command assumes that you ran the command from a command prompt that is in the same folder as both the Mbsacli_/hf.exe file and the Mssecure.xml file.

You can also host the XML file on a Hypertext Transfer Protocol (HTTP) server (also known as a *Web server*) or on a network file share. For example:

```
mbsacli /hf -v -z -x http://webservername/hotfixfile.xml
```

```
mbsacli /hf -v -z -x s:\security\hotfixfile.xml
```

where *webservername* is the name of the Web server that contains the file and *Hotfixfile.xml* is the name of the Mssecure.xml file that is extracted from the .cab file.

- **-x [*URL* | *path*]** - This switch specifies the XML data source that contains the update information. The XML data source may be an XML file or a compressed .cab file. Specify with the URL or path of the XML data source. The default XML data source is the Mssecure.cab file from the Microsoft Web site.

  When you run mbsacli /hf without the -x switch, the XML file is downloaded from the Microsoft Web site. The XML file is named Mssecure.xml and is typically located in the same folder as the Mbsacli.exe file. After you download the file, you can run future scans with the -x switch. For example: `mbsacli /hf -x mssecure.xml`

  This sample command assumes that both the Mbsacli.exe and Mssecure.xml files are in the same folder. You can also host the XML file on a HTTP server or on a network file share. For example, use `mbsacli /hf -v -z -x http://webservername/XMLSourceFile.xml` to specify http://webservername/XMLSourceFile.xml as the XML source file, or use `mbsacli /hf -v -z -x s:\security\hotfixfile.xml` to specify s:\security\xmlsourcefile.xml as the XML source file.

- **-?** - This switch displays a menu. For example:

  ```
  mbsacli /hf -?
  ```

  You can also activate the **-?** switch by using the **/?** syntax.

Examples of Switches That You Can Use in Combination

- Mbsacli skips registry checks, provides the reasons why each hotfix is considered not installed, and uses the Mssecure.xml file in the local folder:

  ```
  mbsacli /hf -v -z -x mssecure.xml
  ```

- Mbsacli scans a computer that is named *labpc* and a different computer by using its IP address and suppresses note messages. The default wrap output displays only the hotfixes that you must install:

  ```
  mbsacli /hf -h labpc -i xxx.xxx.xxx.xxx -s 1
  ```

- Mbsacli scans computers that are named *labpc* and *testpc*, scans two computers by using their *ipaddresses*, skips registry keys, provides the reasons why the hotfix is not installed, and writes the output to the Scan.txt file:

  ```
  mbsacli /hf -h labpc,testpc -i xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx -v -z -f scan.txt
  ```

- Mbsacli scans a computer by using its IP address, identifies both the explicitly installed patches and the explicitly not-installed patches, provides the reasons why a hotfix is not found, suppresses both warning and note messages, and writes the output in tab-delimited format to a file that has as its name the IP address of the scanned computer:

  ```
  mbsacli /hf -i xxx.xxx.xxx.xxx -history 3 -v -o tab -s 2 -f xxx.xxx.xxx.xxx.txt
  ```

- Mbsacli scans two computers by using their IP addresses, scans one computer by using its name, scans computers that have the IP addresses that are specified in the Ipfile.txt file, and uses a local copy of the Mssecure.xml XML file:

  ```
  mbsacli /hf -i xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx -h hostname –fip Ipfile.txt -x mssecure.xml
  ```

- Mbsacli scans all the computers that are in a specific domain for explicitly installed hotfixes, writes the output in tab-delimited format, and uses the Hotfixes.xml XML file in the C:\Temp folder. In this case, the administrator uses the administrator account from the corporate domain with a password:

  ```
  mbsacli /hf -d -history 1 -u \ -p -o tab -x c:\temp\hotfixes.xml
  ```

- Mbsacli scans all the computers that are in a range of IP addresses and displays both explicitly installed and explicitly not-installed hotfixes. The scanning engine has been increased to 100 threads:

  ```
  mbsacli /hf -r xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx -history 3 -t 100
  ```

- Mbsacli scans the local computer by using the Mssecure.xml file from the Web server and ignores checksums:

  ```
  mbsacli /hf -x http://mssecure.xml -nosum
  ```

- Mbsacli scans the local computer by using the Mssecure.xml file from the specified folder.

  Note You must use quotation marks around the fully-qualified file name (path name and file name) if there is a space in the path name:

  ```
  mbsacli /hf -x c:\programfiles\mssecure.xml
  ```

Error Messages

When you use the **Mbsacli /hf** tool, you may receive any one of the following error messages. The following list describes the error messages and how to resolve them.

- Error: 200 - System not found. Scan not performed.
  This error message indicates that **mbsacli /hf** did not locate the specified computer and did not scan it. To resolve this error, verify that this computer is on the network and that the host name and IP address are correct.
- Error: 201 - System not found. *computer error message*
  You may receive this error message if a network problem prevents Mbsacli from scanning the specified computer. To resolve this error, verify that your computer (the computer that performs the scan) is correctly connected to the network and that you can remotely log on to the specified computer you want to scan.
- Error: 202 - System not found. Scan not performed.

You receive this error message because a network or computer error occurred during the scan. To resolve this error, verify that your scanning computer is correctly connected to the network and that the computer you are scanning is still connected to the network. Additionally, make sure that the remote computer is running the Server service.

- Error: 230 - Scan not performed. *computer error message*
  You receive this error message because a general network error occurred. See your computer documentation for more information.
- Error: 235 - System not found, or NetBIOS ports may be firewalled. Scan not performed.
  You may receive this error message if no computer has the specified IP address. If there is a computer at this address, a personal firewall or port filtering device may be dropping packets that are going to TCP ports 139 and 445.
- Error: 261 - System found but it is not listening on NetBIOS ports. Scan not performed.
  You receive this error message because there is a computer at this IP address, but it is either not listening or is blocking access to TCP ports 139 and 445.
- Error: 301 - SystemRoot share access required to scan. Unable to connect to the remote machine's system share.
  You may receive this error message if the administrator has unshared the systemroot (typically C$ or similar) or has disabled the AutoShareServer(Wks) by using the registry.
- Error: 451 - Admin rights are required to scan. Scan not performed.
  You receive this error message because the current or specified user account that performs the scan does not have administrative credentials for the computer that the user is scanning. To resolve this error, verify that the specified account is a member of the local administrators group on the computer you want to scan (or a member of a group that has local administrative credentials).
- Error: 452 - HFNetChk is unable to scan this computer. Please check to see that you have administrative rights to this machine and are able to login to this machine from your workstation. Scan not performed.
  To resolve this error, verify that the Server service is enabled on the remote computer and that you can remotely log on to that computer. Additionally, make sure that the Workstation service is running on the computer that performs the scan.
- Error: 501 - Remote registry access denied. Scan not performed.
  To resolve this error, verify that the Remote Registry service is enabled on the computer you want to scan.
- Error: 502 - Scan not performed. Error reading Registry. *Computer error message*
  You receive this error message because a general registry error occurred. See your computer documentation for more information.
- Error: 503 - Scan not performed. Error reading Registry.
  You receive this error message because a general registry error has occurred. There is no additional information that is available about this error message.
- Error: 553 - Unable to read registry. Please ensure that the remote registry service is running. Scan not performed.
  To resolve this error message, verify that the Remote Registry service is enabled on the computer that you want to scan.
- Error: 621 - Machine is not one of Windows (NT 4, 2000, XP or .NET). Scan not performed.
  The computer that you want to scan runs an operating system that the tool does not support. The computer that you want to scan may run a non-Microsoft operating system that is running SMB services, or it may emulate a Microsoft product in some other way.
- Error: 622 - Machine OS is not Recognized. Please run with tracing on and send to technical support. Scan not performed. Unable to determine the Operating System of the specified machine.
  You may receive this error message when you scan beta or unreleased versions of Microsoft operating systems.
- Error: 623 - Machine Service pack is not Recognized. Please run with tracing on and send to technical support. Scan not performed. Unable to determine the Service Pack of the specified machine.
  You may receive this error message if you scan beta or unreleased versions of Microsoft service packs.
- Error: 701 - File http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab was NOT downloaded. The signed, compressed .cab file containing the security patch information could not be obtained from the specified location.
  You may receive this error message if the computer that is performing the scan is not connected to a network or cannot access the specified file or location.

Support

Microsoft has created a public newsgroup to support MBSA. For support, visit microsoft.public.security.baseline_analyzer on the news.microsoft.com news server. When you ask for help, include the following details:

- Operating system and service pack.
- Version of Internet Explorer and Internet Explorer service pack.
- Version of the MBSA tool.
- Specific details about the problem, including the syntax that you used to run **mbsacli /hf** and the output you received.

For additional information and support, click the following article numbers to view the articles in the Microsoft Knowledge Base:

305385

For additional information and support, click the following article numbers to view the articles in the Microsoft Knowledge Base:

305385 Frequently Asked Questions about the Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool

306460 Hfnetchk.exe Returns Note Messages for Installed Patches

Keywords: kbenv kbinfo kbnetwork KB303215
Technology: kbAudDeveloper kbBizTalkSearch kbBizTalkServ2000 kbBizTalkServ2002 kbBiztalkServSearch kbCommServ2000 kbCommServ2002 kbCommServSearch kbContentMgtServ2001 kbContentMgtServ2002 kbContentMgtServ2002Search kbContentMgtServSearch kbExchange2000Search kbExchange2000Serv kbExchange2000ServSearch kbExchange2000ServSP1 kbExchange550 kbExchange550SP1 kbExchange550SP2 kbExchange550SP3 kbExchange550SP4 kbExchangeSearch kbExchangeServ2003Ent kbExchangeServ2003Search kbExchangeServ2003St kbHostIntegServ2000 kbIE2000Search kbIE500Search kbIE501Win2000 kbIE501Win2000SP1 kbIE501Win2000SP2 kbIE501WinNT400 kbIE501WinNT400SP1 kbIE501WinNT400SP2 kbIE550Search kbIE550Win2000 kbIE550Win2000SP1 kbIE550Win2000SP2 kbIE550WinNT400 kbIE550WinNT400SP1 kbIE550WinNT400SP2 kbIE600Search kbIE600Win2000 kbIE600WinNT400 kbIE600WinXPBeta kbIENT400Search kbIEsearch kbIEWinXPSearch kbiis400 kbiis500 kbiis600 kbiisSearch kbMDAC250 kbMDAC260 kbMDAC270 kbMDAC280 kbMDACSearch kbMSDE kbMSDESearch kbMSXML250 kbMSXML260 kbMSXML300 kbMSXML300Search kbMSXML400 kbMSXML400Search kbMSXMLSearch kbOSWin2000 kbOSWinSearch kbSBServ2003Pre kbSBServ2003Search kbSBServ2003St kbSBServSearch kbSNAServ400 kbSNAServSearch kbSQLServ2000 kbSQLServ2000Search kbSQLServ2000SP1 kbSQLServ2000SP2 kbSQLServ700 kbSQLServ700SP1 kbSQLServ700SP2 kbSQLServ700SP3 kbSQLServ700SP4 kbSQLServSearch kbVMSearch kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Pro kbwin2000ProSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinMediaPlayer640 kbWinMediaPlayer700 kbWinMediaPlayer710 kbWinMediaPlayer900Series kbWinMediaPlayer900Win2000 kbWinMediaPlayer900WinXP kbWinMediaPlayerSearch kbWinMediaPlayerXPSearch kbWinNT400search kbWinNTS400 kbWinNTS400search kbWinNTsearch kbWinNTSEnt400 kbWinNTSEntSearch kbWinNTSsearch kbWinNTW400 kbWinNTW400search kbWinNTWsearch kbWinServ2003Ent kbWinServ2003EntSearch kbWinServ2003Search kbWinServ2003St kbWinServ2003Web kbWinXPHome kbWinXPHomeSearch kbWinXPPro kbWinXPProSearch kbWinXPSearch kbZNotKeyword2
