

Using Microsoft Baseline Security Analyzer (MBSA)



Microsoft Baseline Security Analyzer Tutorial

This information was adapted from the following website:

<http://www.malwarehelp.org/using-microsoft-baseline-security.html>

MBSA is a free security scanner for Microsoft products which analyzes a computer or a group of computers for missing patches/updates and common security mis-configurations. When run MBSA provides a checklist of configuration problems and missing updates/patches. The most important part of the security report provided by the Microsoft Baseline Security Analyzer (MBSA) is the way information given on the lines of "**What was scanned**", "**Result details**" and "**How to correct this**".

Some of the checks that MBSA performs:

- Check for missing Windows security updates
- Check for missing IE security updates
- Check for missing Windows Media Player security updates
- Check for missing Office security updates
- Check for file system type on hard drives
- Check if Auto Logon feature is enabled
- Check if Guest account is enabled
- Check the number of local Administrator accounts
- Check for blank or simple local user account passwords
- Check if unnecessary services are running
- Check if Internet Connection Firewall is enabled
- Check if Automatic Updates is enabled

- List the Internet Explorer security zone settings for each local user
- Check if Internet Explorer Enhanced Security Configuration is enabled for Administrators
- Check if Internet Explorer Enhanced Security Configuration is enabled for non-Administrators
- List the Office products security zone settings for each local user

Note:

1. The computer must be running Microsoft Windows Server 2003, Windows 2000 Service Pack 3 or later, or Windows XP. Running MBSA on Windows NT, 95, 98 or Me systems is not supported.
2. The "**Workstation**" and "**Server**" services must be enabled when scanning a local computer.
3. The initial scan requires internet connection as MBSA downloads the security update catalog from the Microsoft Web site in the form of a cabinet file called **wsusscan.cab**.
4. You must have local administrative privileges on the computer being scanned.

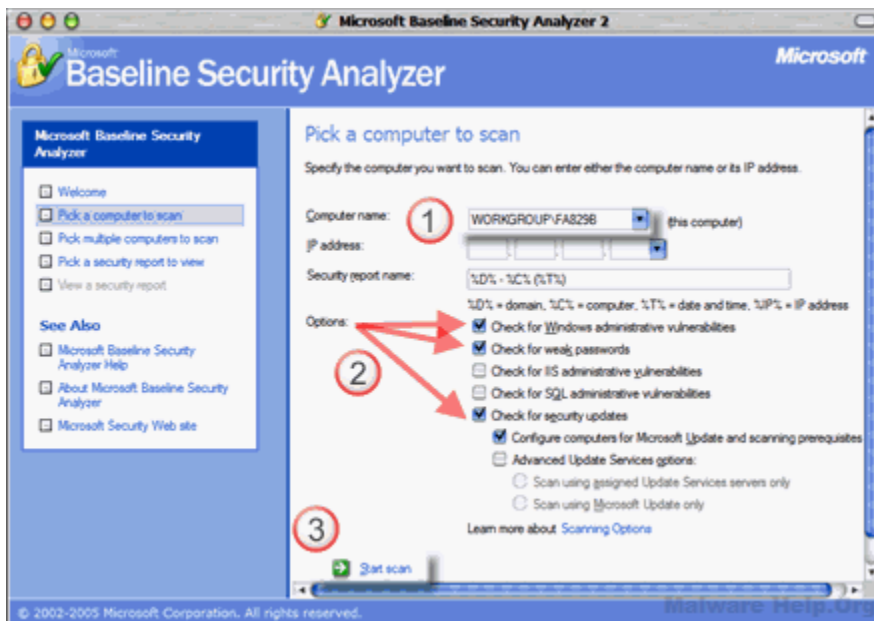
Scanning your System

Download and Install Microsoft Baseline Analyzer (MBSA) from [Microsoft](#).

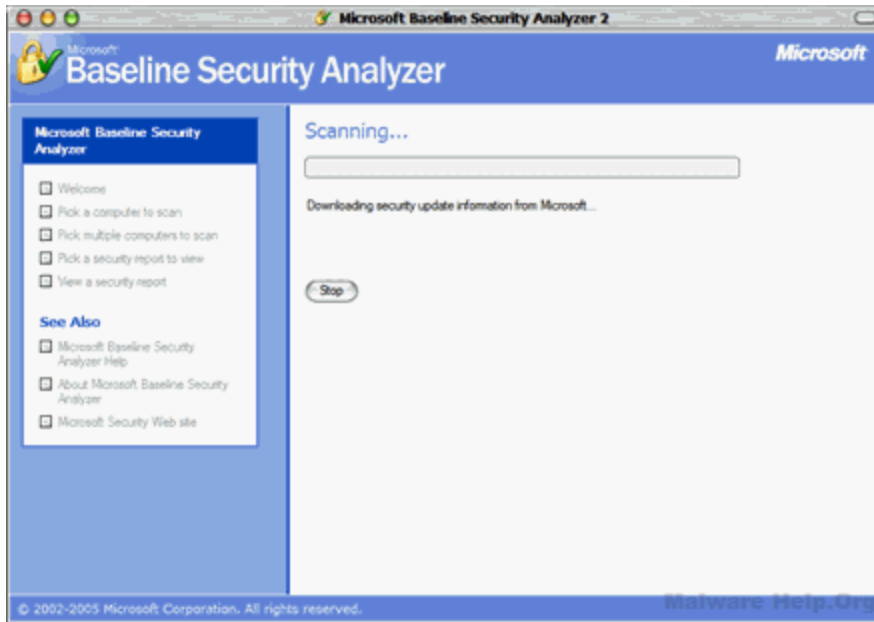
Double click to open MBSA. Click "**Scan a computer**".



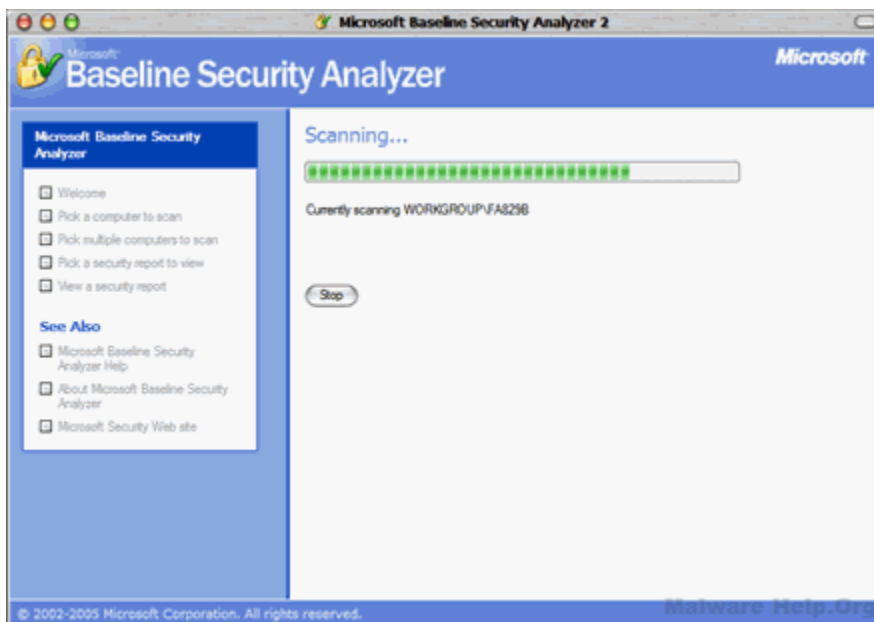
If you are scanning the local computer, it will be pre-selected for scanning. You can also choose to scan another computer if you are in a network by selecting its name or its IP address. Make sure the options "Check for Windows Administrative vulnerabilities", "Check for weak passwords" and "Check for security updates" are checked. You can uncheck the options "Check for IIS vulnerabilities" and "Check for SQL vulnerabilities", if you don't have them installed.



MBSA is downloading the list of latest security catalogue in the form of a signed .cab file from Microsoft.



MBSA is scanning the selected computer.



Once the scan is complete, the results are shown in a nicely organized report that has details of "What was scanned", "Result details" and "How to correct this". Note if any products are not found to be installed on scanned machines, the associated product checks will not be performed and will not be reflected in this report.



How to interpret the MBSA scan reports

MBSA displays different icons in the report score columns depending on whether a vulnerability was found on the scanned machine.

For the *administrative vulnerability checks*, a red X is used when a critical check failed (for example, a user has a blank password). A yellow X is used when a non-critical check failed (for example, an account has a password that does not expire). A green checkmark is used when a check passes (that is, no issue was found for that particular check). A blue asterisk is used for best practice checks (for example, checking if auditing is enabled), and a blue asterisk informational icon is used for checks that simply provide information about the computer being scanned (for example, the operating system version of the scanned computer).

For the *security update checks*, a red X is used when MBSA confirms that a security update is missing from the scanned computer. A yellow X is used for warning messages (for example, the computer does not have the latest service pack or update rollup), and a blue star is used for informational messages indicating that an update is not available to the computer because it has not been approved on the Update Services server. Scores cannot be changed or reassigned for system configuration checks. [MBSA 2.0 Frequently Asked Questions](#)

Security Update Checks









Security Update Scan Results		Malware Help.Org
Score	Issue	Result
	Windows Security Updates	2 service packs or update rollups are missing. What was scanned Result details How to correct this
	Office Security Updates	No security updates are missing. What was scanned Result details

This check determines which available service packs and security updates for pre-determined MS products are not installed on the scanned computer. MBSA will report missing updates marked as critical security updates in Microsoft Update for the following products:

- Microsoft Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003
- Internet Information Server (IIS) 4.0, IIS 5.0, IIS 6.0
- SQL Server 7.0, SQL Server 2000 (including Microsoft Data Engine 1.0 and 2000)
- Internet Explorer 5.01 and later
- Windows Media Player 6.4 and later

- Exchange Server 5.5, Exchange Server 2000, Exchange Server 2003 (including Exchange Admin Tools)
- Microsoft Data Access Components (MDAC) 2.5, MDAC 2.6, MDAC 2.7, MDAC 2.8
- Microsoft Virtual Machine (VM)
- MSXML 2.5, MSXML 2.6, MSXML 3.0, MSXML 4.0
- Content Management Server 2001, Content Management Server 2002
- Commerce Server 2000, Commerce Server 2002
- BizTalk® Server 2000, BizTalk Server 2002, BizTalk Server 2004
- SNA Server 4.0, Host Integration Server 2000, Host Integration Server 2004
- Microsoft Office

Windows Checks

Windows Scan Results		Malware Help.Org
Administrative Vulnerabilities		
Score	Issue	Result
	Restrict Anonymous	Computer is running with RestrictAnonymous = 0. This level allows basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security. What was scanned How to correct this
	Automatic Updates	Automatic Updates are managed through Group Policy on this computer. What was scanned
	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows.
	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
	Autologon	This check was skipped because the computer is not joined to a domain. What was scanned
	Password Expiration	This check was skipped because the computer is not joined to a domain. What was scanned



The following checks are performed by MBSA:

- Check for account password expiration
- Check for file system type on hard drives
- Check if Auto Logon feature is enabled
- Check if Guest account is enabled
- Check the RestrictAnonymous registry key settings
- Check the number of local Administrator accounts
- Check for blank or simple local user account passwords
- Check if unnecessary services are running List the shares present on the computer
- Check if Windows auditing is enabled
- Check the Windows version running on the scanned computer
- Check if Internet Connection Firewall is enabled
- Check if Automatic Updates is enabled
- Check if incomplete updates require the computer to be restarted

The MBSA also provides additional system information about unnecessary services, Windows shares, Windows version etc.

Additional System Information		
Score	Issue	Result
	Auditing	This check was skipped because the computer is not joined to a domain. What was scanned How to correct this
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	No shares are present on your computer. What was scanned
	Windows Version	Computer is running Windows 2000 or greater. What was scanned

Desktop Application Checks

Desktop Application Scan Results		
Administrative Vulnerabilities		
Score	Issue	Result
	IE Zones	Internet Explorer zones do not have secure settings for some users. What was scanned Result details How to correct this
	Macro Security	4 Microsoft Office product(s) are installed. No issues were found. What was scanned Result details

MBSA performs the following checks:

- List the Internet Explorer security zone settings for each local user
- Check if Internet Explorer Enhanced Security Configuration is enabled for Administrators
- Check if Internet Explorer Enhanced Security Configuration is enabled for non-Administrators

- List the Office products security zone settings for each local user

With each vulnerability found, MBSA will also tell you how to fix it. Click on the "**Result details**" link on the report.

Internet Explorer zones do not have secure settings for some users.

Result Details

Some or all of the user settings for the following zones are below the recommended level.

Score	User	Zone	Level	Recommended Level
✗	FA829B\Shanmuga	Internet	Medium (Custom)	Medium

In this instance, clicking on the "**result details**" pops up another window with details of vulnerabilities found for Internet Explorer. Clicking on the provided link opens another Window, which shows the exact individual options which are not set to the recommended settings.

Some or all of the user settings for this zone are below the recommended level.

Result Details

Internet zone

Score	Setting	Current	Recommended
✗	Download signed ActiveX controls	Enable	Prompt
✗	Download unsigned ActiveX controls	Enable	Disable
✗	Initialize and script ActiveX controls not marked as safe	Prompt	Disable

Clicking on **How to correct this** opens an IE Window with the recommended solution with step-by-step instructions.

Solution

Use the recommended Internet Explorer zone settings in the scan report.

Instructions

To select the recommended Internet Explorer zone settings

1. Start Internet Explorer.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Security** tab, click each content zone, and then click **Default Level** to set the recommended security level. If **Default Level** is not enabled, you can re-enable it by changing the position of the security level slider.

Once you have gone through the report and fixed all the vulnerabilities, rerun **MBSA** to check that there are no more vulnerabilities exists in your system.