

Using WMI Scripts with BitDefender Client Security

Whitepaper



1. Introduction

BitDefender Client Security is a robust and easy-to-use business security and management solution, which delivers superior proactive protection from viruses, spyware, rootkits, spam, phishing and other malware.

BitDefender Client Security comprises several features for automated network management, including Windows Management Instrumentation (WMI) scripting support.

WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM), an initiative to establish standards for accessing and sharing management information in an enterprise network. WMI is WBEM-compliant and provides integrated support for Common Information Model (CIM), the data model describing the objects that exist in a management environment.

Basically, WMI allows managing Windows workstations using scripts. WMI scripts can be run only on workstations with WMI services installed. WMI is preinstalled in Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, Windows Me, and Windows 2000.



More Information

For more details on WMI, please refer to the [Windows Management Instrumentation](#) topic on the Microsoft Developer Network (MSDN) website.

Usually, the implementation and deployment of any fully customized automated solution is an extremely challenging and complex process. To avoid the time-consuming task of researching and developing WMI scripts, BitDefender Client Security offers you an entire set of predefined templates for scripting purposes.

BitDefender Client Security enables running WMI scripts on groups of network workstations and provides scheduling capabilities to reduce the administration effort and centralize results. Thus, IT administrators can perform **network audit** (gathering of hardware and system information from workstations) and **administrative actions** remotely.

Different from other business security solutions that may include third-party software to provide WMI scripting support, BitDefender Client Security directly integrates WMI scripts into its management component, BitDefender Management Server. This results in a lower TCO and a comprehensive and easy-to-use management solution.

2. Key Benefits

Several important benefits arise from using the WMI scripts implemented in BitDefender Management Server:

Reduced Network Administration Workload and Costs

- Saves IT administrators the time they would spend to learn about and develop WMI scripts by providing over 30 predefined WMI script templates
- Reduces considerably the time spent on centralizing network audit information from all network workstations
- Enables network and security administration from a single interface through the use of the BitDefender Management Console
- Provides full automation by allowing WMI scripts to be run on groups of workstations (the Management Server integrates with Active Directory for easy and flexible group management)
- Enhances management capabilities and reduces the administration effort by allowing IT administrators to take action (remove software, restart, shutdown, log off) on network workstations remotely
- Helps reduce workstation downtime by assisting IT administrators in the troubleshooting process with preliminary information about the affected network workstations
- Helps maintain compliance with application use policies by enabling IT administrators to remotely control the applications installed and the processes running on the network workstations

Improved Network Visibility and Monitoring

- Allows performing network audit by gathering:
 - hardware information
 - system and software information
 - Windows user accounts information
 - disk and file system information
- Provides quick and easy access to information by centralizing the results of each script.

3. Available WMI Script Templates

BitDefender Client Security allows creating WMI scripts based on predefined WMI script templates. The following table displays all 32 WMI script templates currently available, grouped by their use:

<i>Category</i>	<i>Available Script Templates</i>
Hardware Information (6 script templates)	List CPU Info
	List MB (motherboard) Settings
	List Video Info
	List monitor settings
	List network adapter values
	List power management info
System and Software Information (11 script templates)	Operating System
	Get system info
	Get Last SP Installed
	Enumerate Startup Programs
	List Installed Software
	List Hotfix
	Current Processes
	List Services
	List WMI Settings
	List startup info
List startup menu	
Windows User Accounts Information (4 script templates)	List current users
	List local users
	List Domain and Workgroup info
	List logon session info
Disk and File Systems Information (5 script templates)	Current Shares
	Free Disk Space
	List Logical Disk Info
	Enumerate memory
	Enumerate pagefile

<i>Category</i>	<i>Available Script Templates</i>
Administrative Actions (6 script templates)	Computer restart
	Computer shutdown
	Log off user
	Remove Software
	Kill Process
	Run program

You can find a detailed description of each WMI script template in the [appendix](#).



Operating System Restrictions

To run the following WMI scripts on Windows Server 2003 or 64-bit Windows operating systems, you must first install the **Windows Installer Provider (MSI provider)**, as it does not come preinstalled on default installations.

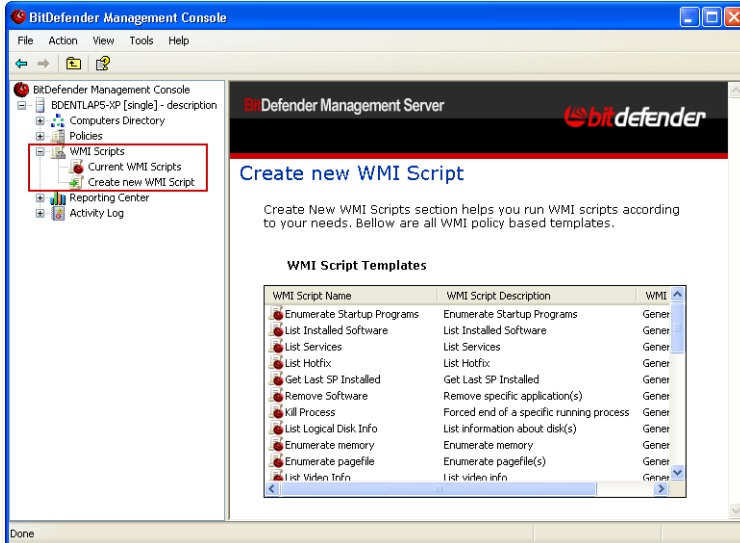
- Enumerate startup programs
- List installed software
- Get system info

This provider is included on the Windows installation CD as an optional Windows component and can be installed using the Control Panel. For more information, please refer to the following topics on the Microsoft Developer Network (MSDN) website:

- [Operating System Availability of WMI Components](#)
- [Windows Installer Provider](#)

4. Operation

IT administrators create WMI scripts using the dedicated snap-in from the BitDefender Management Console.



WMI Scripts Snap-In

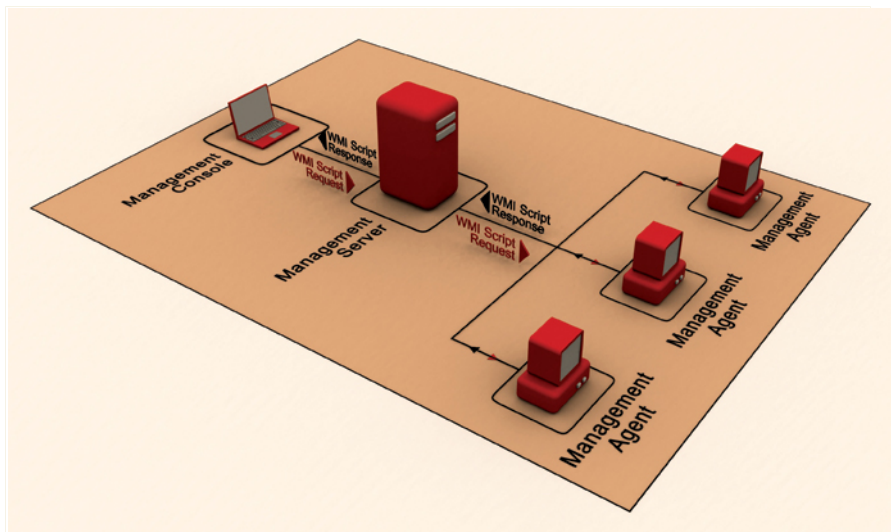
The WMI scripts can be run on any WMI-enabled workstation managed by BitDefender Management Server.

These are the stages of the script creation and execution process:

1. In the management console, the IT administrator creates a WMI script using the WMI script template appropriate to the task to be performed. In most cases, the script is created immediately, without having to configure any settings.
2. The IT administrator assigns the WMI script to run on specific client workstations or groups of client workstations. The script can be scheduled to run one time only or on a regular basis.
3. During the server-agent communication session, BitDefender Management Server sends the script request to the BitDefender Management Agent installed on the assigned client workstations.
4. BitDefender Management Agent runs the script immediately or as scheduled.

5. After the script is executed, BitDefender Management Agent sends the results to BitDefender Management Server.
6. The IT administrator can check the results in the management console.

The diagram below illustrates how WMI scripts operate in BitDefender Client Security.



Operation Diagram

5. Examples

Here are two examples of tasks that can be accomplished using the WMI scripts provided by BitDefender Client Security:

- Gathering Information about Client Workstations
- Application Control

5.1. Gathering Information about Client Workstations

WMI scripts can be successfully used in the troubleshooting process. The IT administrator can remotely run specific WMI scripts to obtain preliminary information about client workstations having issues. Based on this information, the IT administrator can better assess the problem and find potential quick fixes.

The **Get system info** script, for example, provides useful information about client workstations, such as:

- operating system information
- system name, model and manufacturer
- total RAM memory
- processor
- BIOS version

Client: VDANCIU, Ip: 10.10.17.51	
Operating systems	
Index:	1.
Operating System name:	Microsoft Windows XP Professional C:\WINDOWS\Device\Harddisk0\Partition2
Version:	5.1.2600
Service pack:	2.0
Operating system manufacturer:	Microsoft Corporation
Windows Directory:	C:\WINDOWS
Locale:	0409
Available physical memory:	1.4 GB
Total virtual memory:	2.0 GB
Available virtual memory:	1.9 GB
Memory stored in paging files:	3.4 GB
Systems	
System name:s	VDANCIU
System manufacturer:	Dell Computer Corporation
System model:	Dimension 4600i
Time zone:	180
Total physical memory:	2.0 GB
Processors	
System type:	0
Processor:	x86 Family 15 Model 2 Stepping 9
BIOS	
BIOS version:	DELL - 7

Get System Info

5.2. Application Control

A number of WMI scripts help maintain compliance with the organization's policies regarding the use of applications. Using only the BitDefender Management Console, the IT administrator can easily find out what software is installed on client workstations and remove any undesired application.

Step 1 - Verifying Installed Applications

The **List Installed Software** script can be used to obtain the list of applications installed on client workstations with the Windows installer. Once the script is executed, the IT administrator can check the results in the management console.

The image below provides an example of such results for a client workstation. In this example, **Generic Application** is an undesired application that should be removed.

Index	Caption	Description	Version	Install date
1.	Compatibility Pack for the 2007 Office system	Compatibility Pack for the 2007 Office system	12.0.6215.1000	20080614
2.	Generic Application	Used as example	1.6.0.50	20070917
3.	MSXML 4.0 SP2 (KB936181)	MSXML 4.0 SP2 (KB936181)	4.20.9848.0	20070913
4.	Microsoft .NET Framework 3.0 Service Pack 1	Microsoft .NET Framework 3.0 Service Pack 1	3.1.21022	20071214
5.	Apple Software Update	Apple Software Update	2.1.0.110	20080625
6.	Microsoft .NET Framework 2.0 Service Pack 1	Microsoft .NET Framework 2.0 Service Pack 1	2.1.21022	20071214
7.	Microsoft Office XP Professional with FrontPage	Microsoft Office XP Professional with FrontPage	10.0.6626.0	20070912
8.	QuickTime	QuickTime	7.4.0.91	20080206
9.	BitDefender Management Agent	BitDefender Management Agent	3.0.2	20080807
10.	Microsoft Virtual PC 2007	Microsoft Virtual PC 2007	6.0.156.0	20070914
11.	Software Update for Web Folders	Software Update for Web Folders	9.60.6715.0	20070912
12.	Adobe Photoshop CS2	Adobe Photoshop CS2	9.0	20070913
13.	MSXML 4.0 SP2 (KB927978)	MSXML 4.0 SP2 (KB927978)		
14.	MSXML 6.0 Parser (KB933579)	MSXML 6.0 Parser (KB933579)	6.10.1200.0	20070913
15.	MSXML 6.0 Parser	MSXML 6.0 Parser		
16.	Windows Presentation Foundation	Windows Presentation Foundation	3.0.6920.0	20071119
17.	Adobe Acrobat 7.0 Professional	Adobe Acrobat 7.0 Professional	7.1.0	20080516
18.	TortoiseSVN 1.4.8.12137 (32 bit)	TortoiseSVN 1.4.8.12137 (32 bit)	1.4.12137	20070913

List Installed Software



Other Useful Scripts

Two other scripts can provide additional information about the software installed on client workstations:

- **List startup menu** retrieves the applications that have shortcuts in the Start menu.
- **Current Processes** provides information about the processes currently running on client workstations.

Step 2 - Removing Installed Applications

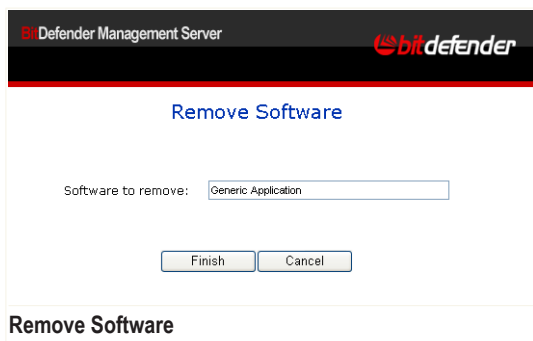
If an application installed on a client workstation does not comply with the application use policies, it can be easily removed using the **Remove Software** script. This script makes use of the **Add or Remove Software** applet in the Control Panel to remove applications installed on client workstations.

Here are a few examples of application types that can be remotely removed using this script:

- antivirus
- peer-to-peer
- chat
- multimedia
- games

The IT administrator only has to provide the application name (as displayed in **Add or Remove Programs** or by the **List Installed Software** script) and run the script on the respective workstation. The application will be removed from the client workstation, without any user intervention.

In the previous example, **Generic Application** was an undesired application. To remove it, the IT administrator must provide the same name as the one retrieved by the **List Installed Software** script.



Appendix. Description of WMI Script Templates

This appendix provides a detailed description of the available WMI script templates.

Computer restart

Restarts client workstations.

Computer shutdown

Shuts down client workstations.

Current Processes

Provides information on the processes currently running on client workstations.

Current Shares

Provides information about the existing shares on client workstations.

Enumerate memory

Provides the size of the physical (RAM) memory installed in client workstations.

Enumerate pagefile

Provides information about the virtual memory (the page file) available on client workstations. This includes:

- the location and size of the page file
- the initial and the maximum size

Enumerate Startup Programs

Provides information about the programs that run on client workstations at startup.

Free Disk Space

Provides the list of the logical disks on client workstations and the available disk space on each of them.

Get Last SP Installed

Provides the version of the Windows Service Pack installed on client workstations.

Get system info

Provides useful information about client workstations. This includes:

- operating system information
- system name, model and manufacturer
- total RAM memory
- processor
- BIOS version

Kill Process

Ends a specific process running on client workstations. The **Current Processes** script can be used to obtain the list of running processes.

List CPU Info

Provides various information about the processor of client workstations. This includes:

- processor name and ID
- description
- manufacturer
- clock speed

List current users

Lists the users currently logged on to client workstations.

List Domain and Workgroup info

Provides information on the domain or workgroup client workstations are part of.

List Hotfix

Provides information about the Microsoft and Windows hotfixes installed on client workstations.

List Installed Software

Provides the list of software installed on client workstations with the Windows installer.

List local users

Provides information about the local Windows user accounts configured on client workstations.

List Logical Disk Info

Provides information about the logical disks (floppy drive, hard-disk drives, CD-ROM drive etc) on client workstations. This includes:

- name (label)
- description
- free disk space
- size

List logon session info

Provides information regarding the logon session on client workstations.

List MB Settings

Provides information about the motherboard of client workstations. This includes:

- name
- manufacturer
- serial number

List monitor settings

Provides information about the monitor of client workstations. This includes:

- monitor type
- manufacturer
- physical dimensions

List network adapter values

Provides detailed information about the network adapters installed in client workstations. This includes:

- adapter type
- manufacturer
- MAC and network address

List power management info

Provides power management information about client workstations.

List Services

Provides various information regarding the services running on client workstations. This includes:

- service name and display name
- state (stopped / running)
- start mode (auto / manual / disabled)
- description

List startup info

Provides information on the startup of client workstations.

List startup menu

Lists the program shortcuts from the Start menu of client workstations. The entries are grouped by user.

List Video Info

Provides various information regarding the video display of client workstations. This includes:

- video adapter name and type
- graphics memory
- resolution
- driver name and version
- minimum and maximum refresh rates

List WMI Settings

Provides information about the WMI settings of client workstations.

Log off user

Logs off the current user logged on to client workstations.

Operating System

Provides useful information about the operating system running on client workstations. This includes:

- operating system and version
- registered user
- serial number
- installation time

Remove Software

Removes a specific application installed on client workstations. The script can be used to remove any application that appears in the **Add or Remove Programs** applet in the Control Panel.

Run program

Runs a specific application on client workstations. The application can be located on the target workstation or on the personal computer of the IT administrator.