



BITDEFENDER BUSINESS SOLUTIONS

Using WMI to Enhance Network Visibility
and Streamline Operational Management

Solution Brief

TABLE OF CONTENTS

1. Introduction	4
2. Windows Management Instrumentation (WMI) Technology Explained	4
3. Five Reasons To Integrate Antimalware Security With Network Audit And Systems Management	5
4. Bitdefender's Network Auditing Explained	7
5. Collecting Network Auditing Data	8
6. Bitdefender's Network Tasks Explained	13
7. Conclusions	20
Appendix: Description Of Network Task Templates	21

1. INTRODUCTION

Many IT departments are expected to maintain business operations effectively, but often with limited resources, leaving little time to implement proactive processes and procedures to minimize their exposure to threats. Small and Medium Businesses (SMB's) are even further restricted by strict budget requirements and IT tasks are often fulfilled by someone in a dual role with little in-depth knowledge.

With so many business and IT requirements to be met, overstretched IT staff find it hard to implement and maintain both security solutions and manage the network. The solution to this problem is to assist IT staff in simplifying and automating repetitive manual tasks, helping to improve the overall security of the network and aid in compliance reporting.

As a company grows, the addition of new employees, systems, and office applications also increases the complexity of an organization's network. The addition of each new desktop, laptop or server must be managed by existing IT staff, reducing the ability to maintain control and complicates efforts to visualize what is really happening in the network. To be proactive, and to work smarter, IT departments must ensure they have simple and effective tools that can help automate repetitive and manual IT tasks, in addition to providing better visibility of the devices and applications needed to maintain their business. Automated tools can quickly expose security holes – such as unauthorized use of rogue applications or unknown devices running services - that further expose an organization to potential security risks including data leakage, malware infections and virus outbreaks.

2. WINDOWS MANAGEMENT INSTRUMENTATION (WMI) TECHNOLOGY EXPLAINED

Windows Management Instrumentation (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.

WMI allows network administrator to remotely manage Windows servers and workstations deployed throughout their network using industry standard scripts. WMI Scripts can only be run on workstations with WMI services installed. WMI is preinstalled with Windows 7, Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, Windows Me, and Windows 2000.

To alleviate this burden on SMB IT resources, BitDefender Business Solutions has integrated several features for automated network management to provide maximum value to its customers. One such feature is support for WMI scripting.

Typically, 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 Tasks, BitDefender offers over 30 predefined templates that use the WMI scripting standard.

The BitDefender Management Server is unique among Corporate Antimalware solutions in that it directly integrates WMI Scripts into its management component, resulting in a lower Total Cost of Ownership (TCO) than other solutions due to a comprehensive and easy-to-use interface. It can be configured to run WMI Scripts on groups of network workstations and provide scheduling capabilities to reduce the administration and network workload and centralize the results for reporting. Thus, IT administrators can perform network audit (gathering of hardware and system information from Windows workstations and Servers) and administrative actions remotely.

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

3. FIVE REASONS TO INTEGRATE ANTIMALWARE SECURITY WITH NETWORK AUDIT AND SYSTEMS MANAGEMENT

Many businesses may not have the resources to invest in a specialized asset management application, but most have the need to be aware of installed software within their network to ensure security, compliancy to financial audits, and governmental or industry mandates.

To help address this problem, BitDefender's Centralized Management Console can be configured to collect information on systems deployed within the network at daily intervals to provide IT managers with historical and up-to-date inventory audit reports that allow visibility into networked assets as well as fulfill internal or external audit requirements.

Integrated Network Audit and System Management allow companies to:

1. Simplify network management and reduce the manual compliance reporting burden
2. Automate network audit data collection for inventory and change reporting
3. Ensure compliancy with software licenses and identify unauthorized applications
4. Reduce overhead for managing a separate inventory system and agents on endpoints
5. Identify HW/SW that does not meet an organizations policy requirements

1. SIMPLIFY NETWORK MANAGEMENT AND REDUCE THE MANUAL COMPLIANCE REPORTING BURDEN

The BitDefender Management Server enables IT staff to do more in less time by executing remote Network Tasks via a simple, wizard-driven interface. It provides a step-by-step configuration of all the necessary scripting parameters, with immediate or scheduled execution on selected computers or on computer groups within the network.

The Network Tasks can manage remotely installed applications and running processes or services, the Windows Update process, or defining access to local USB removable media. These configuration management changes can be applied on-masse automatically to selected Windows systems within the network, freeing up IT staff for other, more important and less menial responsibilities.

2. AUTOMATE NETWORK AUDIT DATA COLLECTION FOR INVENTORY AND CHANGE REPORTING

Regulatory compliance and internal financial reporting requirements are driving the need for automated network auditing and reporting in many organizations. Some of the common regulatory compliance reporting requirements were issued by Payment Card Industry (PCI), Health Insurance portability and Accountability Act (HIPAA), Sabanes-Oxley (SOX) or many other financial authorities.

The Network Audit features found in the BitDefender Centralized Management console take advantage of the WMI script capability by enabling IT administrators to create software and hardware configuration snapshots. The collected software and hardware information is available on-demand for each Windows desktop or server running the WMI service, with different report configurations to highlight the different aspects of the deployment.

The remotely collected data will provide IT staff on-demand, and always up-to-date, inventory and audit reports – conveniently together with reports on the organization’s security posture.

3. ENSURE COMPLIANCY WITH SOFTWARE LICENSES AND IDENTIFY UNAUTHORIZED APPLICATIONS

Unauthorized and rogue applications installed or executed by users after downloading from the Internet are a constant security concern to most network administrators. Many of these applications can remain unnoticed until there is an imminent threat to business operations, such as causing network outages congested with high levels of unknown traffic, or a compromise to the systems on the network is detected. Many employees using these rogue applications are unaware of the security risk caused by their actions, or the risk to the business as a whole. Rogue applications may exploit malicious code inside organization’s network and expose confidential data to cyber criminals.

With full visibility into all Windows compatible software within an organization’s network, administrators can proactively track compliancy of legitimately purchased software and unauthorized applications, which can then be used as evidence for financial auditing and reduce the risk of legal action or concerns for unauthorized, pirated applications.

4. REDUCING THE NEED FOR A SEPARATE INVENTORY APPLICATION AND MULTIPLE ENDPOINT AGENTS

Small and Medium Businesses can directly benefit from BitDefender’s integrated approach to corporate antimalware and network management by reducing the need for multiple specialized applications, in addition to reducing the number of agents already deployed on workstations and servers deployed throughout the network.

The auditing feature used by WMI does not require an inventory agent on the endpoint, resulting in minimal system memory or performance impact on each endpoint during the scheduled data collection process.

5. IDENTIFY HW/SW THAT DOES NOT MEET AN ORGANIZATIONS POLICY REQUIREMENTS

Custom auditing reports can provide even more configurable reports for specific needs based on a predefined list of hardware or software criteria.

Identifying outdated hardware to be replaced, planning to upgrade physical memory to meet new office application's requirements, or simply checking all the workstations have sufficient remaining disk space.

Identifying specific software within the network is also easy by simply establishing a query by application's name and version (e.g. Microsoft Office or Outlook). Finding and reporting workstations with specific applications installed is easy by defining a software query criteria.

4. BITDEFENDER'S NETWORK AUDITING EXPLAINED

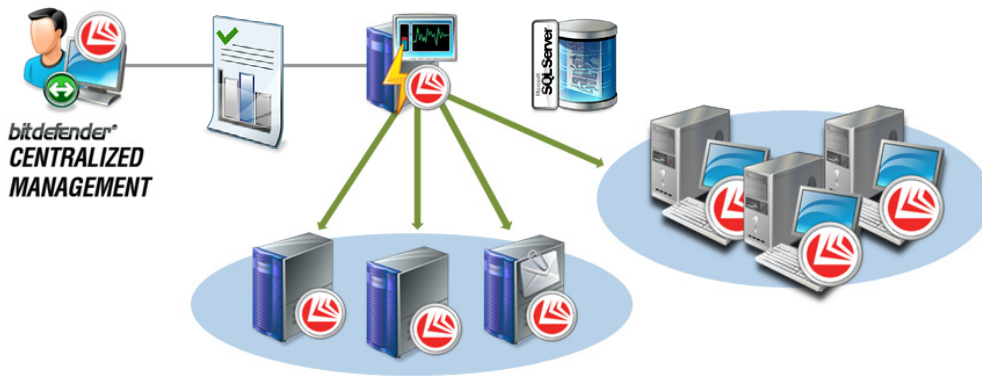
The Network Auditing feature in BitDefender's Management Console uses integrated WMI Scripting to allow IT administrators the ability to perform hardware and software configuration snapshots of the Windows systems deployed within their network. The remotely collected data provides IT administrators with an on-demand, up-to-date inventory and audit reporting capability – conveniently together with malware reports reflecting the organization's overall security posture.

This chapter explains how the BitDefender Network Audit feature collects the auditing data from the organization's network and generates four different types of reports either directly from the collected data or based on the data stored into database;

1. **Snapshot Report Wizard**, to view the current software and hardware configurations
2. **Historical Reports** allow for the tracking of all installed or uninstalled software - within a predefined time period - for full visibility into any changes once a baseline has been defined.
3. **Comparison Reports** show the differential between two points in time with historical information to facilitate change management requirements on all installed or uninstalled software within the network. Due to parameters required for the comparison report, it cannot be automatically generated and emailed at a pre-scheduled interval.
4. **Custom Reports** include all the most common parameters for: CPU type and speed; disk drives, file system and remaining space; Operating System and specific Service Packs; Motherboard manufacturers, serial number and version; Virtual memory page file's size and location; Physical memory; and Installed Software by name and version (e.g. Microsoft Office or Outlook).

5. COLLECTING NETWORK AUDITING DATA

Before the Network Auditing feature can be used for audit reporting, it must first be configured to collect the auditing data from the Windows systems deployed within the network. Snapshot reports can quickly gather data and the progress can be monitored during the data collection process with information on how many endpoints were interegated. For optimized performance in larger networks, the auditing reports cannot be generated using live data from the network; instead the data must be collected into Management Server's auditing database prior to generating reports.



Once the initial data has been collected, the data collector can be configured to run daily - or less frequently on smaller networks - to update both software and hardware details within the Management Server’s auditing database. The software auditing snapshots are stored for historical change management reports to track all installed or uninstalled software within the network (within a specific time period). Hardware details can be reported for the current snapshot status, but not as historical reports.

Administrators have also an option for archiving the auditing data into local or remote device for historical reporting purposes while the auditing database would remain lean and more responsive during the generation of reports.

5.1 PORT WIZARD 1: SNAPSHOT REPORT

Status Report for Installed Software				
Report Details				
This report lists installed software detected on specified day grouped by Application Name, Computer IP				
Name	Network Audit Status Report for Installed Software			
Report Date	2011-03-09			
Generated for	10.10.15.101; 169.254.128.13; 169.254.76.145; 192.168.0.10; 192.1...			
Report Data				
Application Name	Computer IP	Version	Install Date	Uninstall line
7-Zip 9.20	192.168.0.125	9.20.00.0	2011-02-28	MsiExec.exe /I{23170F69-40C1-2701-0920-000001000000}
	192.168.0.180	9.20.00.0	2011-03-01	MsiExec.exe /I{23170F69-40C1-2701-0920-000001000000}
Adobe AIR	192.168.0.180	2.5.1.17730	2011-02-25	MsiExec.exe /I{46C045BF-2B3F-4BC4-8E4C-00E0CF8BD9DB}
	192.168.0.60	2.5.1.17730	2011-03-09	MsiExec.exe /I{46C045BF-2B3F-4BC4-8E4C-00E0CF8BD9DB}

Snapshot reports are used to generate reports for listing the current software and hardware configurations for single endpoints or groups of systems deployed within the network. The report can be generated for a specific, predefined report, such as the Operating System report in the example seen below.

5.2 REPORT WIZARD 2: HISTORICAL REPORT

The Historical Report is used to generate reports for installed or removed hardware or software with details grouped by computer (IP), application’s name or change action taken (i.e. install or uninstall application).

The example report below has been generated to group auditing data based on IP address and the actions taken specifically for that system. The report can be used to review installed applications each month and take actions to identify and uninstall rogue or unauthorized applications from the organization's network. Many organizations are required track software changes and generate reports to comply with internal security policy or regulatory requirements, so the information contained within the report must be detailed enough to identify applications down to the specific version and the endpoint on which the application was installed during the reporting period.

Historical Report for Installed Software							bitdefender
Report Details							
This report lists all actions taken on installed software grouped by Final State (Present / Absent), Day, Application Name, Computer IP							
Name	Network Audit Historical Report						
Report Date	2011-03-01 to 2011-03-11						
Generated for	<input type="checkbox"/> 10.10.0.10; 10.10.0.100; 10.10.0.15; 10.10.0.17; 10.10.0.18; 10.10.0.19; 10.10.0.2; 10.10.0.20; 10.10.0.21; 10.10.0.22; 10.10.0.23; 10.10.0.25; 10.10.0.32; 10.1...						
Report Data							
State	Day	Application Name	Computer IP	Version	Install Date	Uninstall line	
Absent	2011-03-01	BitDefender Business Client	10.10.100.153	3.5.1.0	2011-02-23	MsExec.exe /I{EB4766BC-1967-41A5-80A7-3B1E8733C4F6}	
	2011-03-07	BitDefender Business Client	10.10.100.166	3.5.1.0	2011-02-23	MsExec.exe /I{EB4766BC-1967-41A5-80A7-3B1E8733C4F6}	
	2011-03-11	BitDefender Business Client	10.10.100.167	3.5.1.0	2011-02-23	MsExec.exe /I{EB4766BC-1967-41A5-80A7-3B1E8733C4F6}	
Present	2011-03-01	BitDefender Business Client	10.10.100.153	3.5.1.0	2011-02-28	MsExec.exe /I{EB4766BC-1967-41A5-80A7-3B1E8733C4F6}	
	2011-03-02	Adobe AIR	10.10.100.149	2.5.1.17730	2011-03-01	MsExec.exe /I{46C045BF-2B3F-4BC4-8E4C-00E0CF8DD9DB}	
	2011-03-02	Adobe Download Manager	10.10.100.149	1.6.2.99	Unknown	"C:\Program Files\NOS\bin\getPins\Uninst_Adobe.exe" /s	


5.3 REPORT WIZARD 3: COMPARISON REPORTS

The Comparison Report is wizard-driven and can be used to generate reports to highlight only the changes made during two different points in time and can be grouped by computer (IP), application's name or change action taken (i.e. install or uninstall application). The example report below has been generated to group auditing data based on the computer (IP).

Comparison Report for Installed Software							bitdefender
Report Details							
This report lists all applications by comparing what was present on 2011-03-02 versus 2011-03-11 grouped by Computer IP, Day, Final State (Present / Installed), Application Name							
Name	Network Audit Comparison Report						
Report Date	2011-03-02 versus 2011-03-11						
Generated for	<input type="checkbox"/> 10.10.0.10; 10.10.0.100; 10.10.0.15; 10.10.0.17; 10.10.0.18; 10.10.0.19; 10.10.0.2; 10.10.0.20; 10.10.0.21; 10.10.0.22; 10.10.0.23; 10.10.0.25; 10.10.0.32; 10.1...						
Report Data							
Computer IP	Day	State	Application Name	Version	Install Date	Uninstall line	
10.10.100.139	2011-03-02	Installed	Conduit Engine		2011-03-09	C:\PROGRAM-1\CONDUIT-1\ConduitEngine\Uninstall.exe	
	2011-03-02	Removed	Roblox		2011-03-10	"C:\Program Files\Roblox\Versions\version-e0247ad93e84259\Roblox.exe" /uninstall -altuser	
	2011-03-02	Removed	Softonic-Eng7 Toolbar	6.2.3.0	2011-03-09	C:\PROGRAM-1\SOFTON-1\UNWISE EXE /U C:\PROGRAM-1\SOFTON-1\INSTALL LOG	
	2011-03-02	Installed	Winamp	5.601	2011-03-09	"C:\Program Files\Winamp\UninstWA.exe"	
	2011-03-02	Installed	Winamp Toolbar		2011-03-09	"C:\Program Files\Winamp\Toolbar\uninstall.exe"	
10.10.100.167	2011-03-02	Installed	Winamp	5.601	2011-03-09	"C:\Program Files\Winamp\UninstWA.exe"	

5.4 REPORT WIZARD 4: QUERY-BASED CUSTOM REPORTS

The Custom Report wizard is used to define a query for reports containing specific software or hardware parameters. The query may contain one or more most commonly used parameters, including CPU type, speed and single/dual cores; disk drives, file system and remaining space; Operating System and specific Service Packs; Motherboard manufacturers, serial number and version; Virtual memory page file's size and location; Physical memory; Installed Software by name and version (e.g. Microsoft Office or Outlook). The example report below has been generated for RAM Memory Usage that exceeds 1000 MB (i.e. 1 GB). Such information could be used to identify computers with sufficient memory to install a new operating system, or to run applications that require at least 1 GB RAM memory.

Network Audit Custom Report				
				
Report Details				
Name	raport 1			
Report Date	2011-03-09			
Generated for	10.10.15.101 ; 169.254.128.13 ; 169.254.76.145 ; 192.168.0.10 ; 192.168.0.101 ; 192.168.0.102 ; 192.168.0....			
Filters	Memory Usage OS	RAM OS Name	> Contains	1,00 GB XP
Report Data				
Computer IP	Install Date	OS Name	SP	RAM
192.168.0.101	2009-12-02	Microsoft Windows XP Professional	3	1.94 GB
192.168.0.113	2009-12-21	Microsoft Windows XP Professional	3	3.21 GB
192.168.0.161	2010-06-17	Microsoft Windows XP Professional	3	1.95 GB
192.168.0.179	2010-02-11	Microsoft Windows XP Professional	3	2.75 GB
192.168.0.19	2009-05-22	Microsoft Windows XP Professional	2	2.00 GB

6. BITDEFENDER'S NETWORK TASKS EXPLAINED

Security and network administration can be more effectively managed from a single interface through the use of the BitDefender Management Console. This integrated functionality helps to minimize the time spent by IT administrators on menial tasks by centralizing basic Windows management tasks for workstations and servers deployed throughout the network.

IT staff can now do more in less time and fewer resources using BitDefender's simple wizard-driven interface to automate the scheduling and execution of Tasks run on groups of systems. The Management Server also integrates with Active Directory and allows for easy and flexible management without the need to recreate the user and group structure already embedded in the network.

The Network Tasks features in the Management Console can reduce the administration effort by allowing IT staff to take direct action (such as uninstall software, restart or shutdown a system, and log off users) remotely without the need for physical access to the system. In turn the Network Tasks also help make the systems more secure and compliant with security policy by remotely modifying system configurations and locking down settings – such as disabling Windows autorun and restricting USB storage device usage in the network.

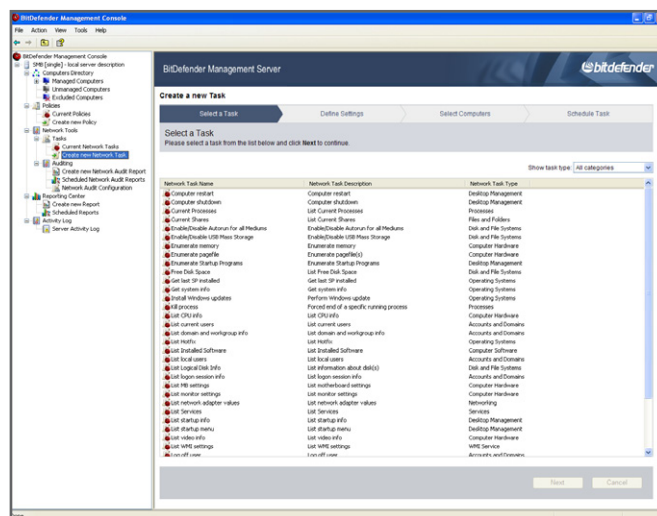
Finally, three examples of Network Management Tasks are explained in detail to demonstrate

what can be accomplished by using BitDefender:

1. Gathering Information about Windows Endpoints (Server or Workstation)
2. Application Visibility and Control
3. Making Your Network More Secure

6.1 RUNNING WIZARD-BASED NETWORK TASKS

IT administrators run Tasks from the Network Tasks section found in the BitDefender Management Console.



Wizard-Based Network Tasks in the Management Console

The Tasks 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 Task using the Task 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 Task 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 agent-server 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.

6.2 NETWORK TASK TEMPLATES

BitDefender allows the creation of Network Tasks based on predefined templates that are based on pre-written and tested Tasks. The following table displays all 37 Network Task templates currently available, grouped by their use:

Administrative Actions <i>12 Task Templates</i>	System and Software Info <i>15 script templates</i>	Disk and Hardware Info <i>10 script templates</i>
Computer Restart Computer Shutdown Enable/Disable Autoruns Enable/Disable USB Mass Storage Install Windows Updates Kill Process Log off User Remote Desktop Connection Remove Software Run Program Send Message Windows Automatic Updates	Operating System Get System Info Get Last Service Pack Installed Enumerate All Startup Programs List Installed Software List Hotfixes List Current Processes List Services List WMI Settings List Startup Info List Startup Menu List Current Users List Local Users List Domain and Workgroup Info List Logon Session Info	Current Shares Free Disk Space List Logical Disk Info Enumerate Memory Enumerate Virtual Memory List CPU Info List Motherboard Settings List Video Info List Monitor Settings List Network Adapter Values

Predefined Network Tasks Available in v3.5

6.3 EXAMPLE 1: GATHERING INFORMATION ABOUT ENDPOINTS

Tasks can be successfully used in the troubleshooting process. The IT administrator can remotely run specific Tasks 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

Operating systems	
Operating System name:	Microsoft Windows XP Professional
Version:	5.1.2600
Service pack:	3.0
Operating system manufacturer:	Microsoft Corporation
Configuration:	Stand-alone workstation
Build type:	Multiprocessor Frecc
Registered owner:	Cosmin
Registered organization:	BITDefender
Product ID:	76487-OEM-0011903-00102
Original install date:	2009-10-12 13:50:22
Windows directory:	E:\WINDOWS
System directory:	E:\WINDOWS\system32
Boot device:	\Device\HarddiskVolume3
Locale:	en-us;English (United States)
Time zone:	(GMT+02:00) Minsk
Total physical memory:	1.99 GB
Available physical memory:	1.07 GB
Total virtual memory:	2.00 GB
Available virtual memory:	1.96 GB
Memory stored in paging files:	3.33 GB
Systems	
System name:	SMB

The “Get System Info” script returns valuable information about each endpoint

6.4 EXAMPLE 2: APPLICATION CONTROL ON ENDPOINTS

A number of Tasks 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 undesired applications.

STEP 1 - VERIFYING INSTALLED APPLICATIONS

To verify what applications are installed on client workstations, the IT administrator can use the List installed software task. This task can be used to obtain the list of all the applications installed on client workstations, including Microsoft and Windows updates.

Once the task is executed, the IT administrator can check the results in the Current Network Tasks pane by double-clicking the task. The image below provides an example of the results gathered for a client workstation.

ID	Name	Description	Uninstall command line	Status	Date
7.	Name: Microsoft Internationalized Domain Names Mitigation APIs	Description: Microsoft Internationalized Domain Names Mitigation APIs	Uninstall command line: N/A	N/A	2010-03-01
8.	Name: Windows Internet Explorer 7	Description: Windows Internet Explorer 7	Uninstall command line: N/A	20070813.185237	2010-03-01
9.	Name: Security Update for Windows XP (KB2079403)	Description: Security Update for Windows XP (KB2079403)	Uninstall command line: N/A	1	2010-08-11
10.	Name: Security Update for Windows XP (KB2115168)	Description: Security Update for Windows XP (KB2115168)	Uninstall command line: N/A	1	2010-08-11
11.	Name: Security Update for Windows XP (KB2121546)	Description: Security Update for Windows XP (KB2121546)	Uninstall command line: N/A	1	2010-09-16
12.	Name: Update for Windows XP (KB2141007)	Description: Update for Windows XP (KB2141007)	Uninstall command line: N/A	1	2010-09-16
13.	Name: Hotfix for Windows XP (KB2158563)	Description: Hotfix for Windows XP (KB2158563)	Uninstall command line: N/A	1	2010-09-30
14.	Name: Security Update for Windows XP (KB2160329)	Description: Security Update for Windows XP (KB2160329)	Uninstall command line: N/A	1	2010-08-11
15.	Name: Security Update for Windows Internet Explorer 7 (KB2183461)	Description: Security Update for Windows Internet Explorer 7 (KB2183461)	Uninstall command line: N/A	1	2010-08-11

Example of “List of Installed Software” detected on endpoint

TIP: OTHER USEFUL SCRIPTS

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

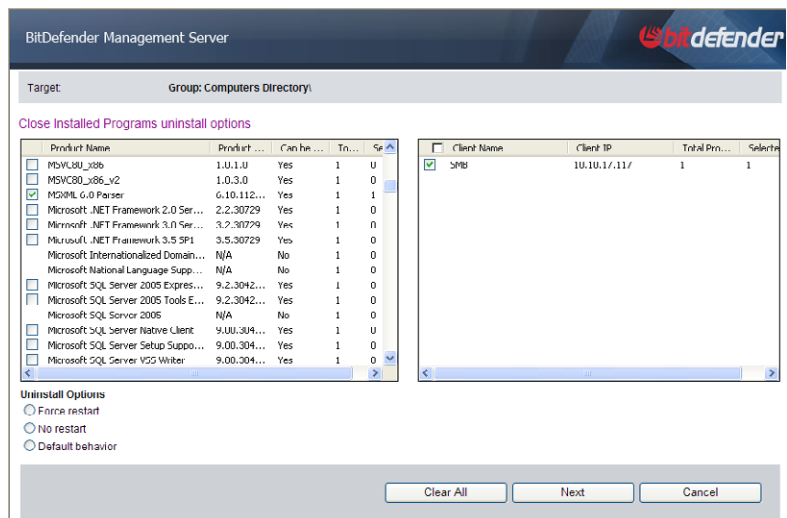
- List startup menu retrieves the applications that have shortcuts in the Start menu.
- Current Processes provides information about the processes currently running on client workstations.

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 from the results section of the List Installed Software task. Here are a few examples of application types that can be removed remotely:

- Third-party Antivirus solutions
- VoIP and chat applications
- P2P
- Multimedia and games

In order to remove an application, the IT administrator must click the link above the results table.



Example of Installed Programs Selected for Removal

Two tables are displayed here:

- The left-side table displays all applications installed on the client workstations the script has run on.
- The right-side table displays all client workstations on which a selected application is installed.

It takes a few easy steps to remove an undesired application:

1. Select the application from the list.
2. To remove the application from all the workstations it is installed on, select the check box in the Client name column header. To remove it from specific workstations, only select the corresponding check boxes.

3. Select a restart option. A computer restart may be required to completely remove the selected application.
4. Click Uninstall and then OK to remove the application from the selected computers.

A Run program Task is automatically created and assigned to the selected computers so that the application is removed. Application removal will not require user intervention.

Once the script is executed, the IT administrator can check the results to see if the script ran successfully in the Current Network Task pane by double-clicking the script.

6.5 EXAMPLE 3: INCREASING YOUR NETWORK SECURITY

Computer worms are increasingly using USB storage devices and the Windows autorun feature to spread through networks. This was the case with the recent Downadup worm, also known as Conficker or Kido, which is estimated to have infected millions of business network computers.

Note: Autorun enables automatic detection and reading of new media connected to the computer. Such media includes USB flash drives, network shares, CDs, DVDs and other. This Windows feature can be used to automatically execute malicious code as soon as an infected medium is connected to the computer.

To help IT administrators counter these network vulnerabilities, BitDefender Client

Security provides the following Tasks:

- Enable/Disable Autorun - to remotely control autorun for all drives on managed computers.

The screenshot shows the BitDefender Management Server interface. At the top, it says 'BitDefender Management Server' and 'bitdefender'. Below that, there's a 'Create a new Task' section with a progress bar showing four steps: 'Select a Task', 'Define Settings', 'Select Computers', and 'Schedule Task'. The 'Define Settings' step is currently active. Underneath, it says 'Define Task Settings' and 'Please define the task settings below and click Next to continue.' There are two radio button options: 'Enable Autorun' (which is selected) and 'Disable Autorun'. A note below says 'Note: The changes will take place after the system is restarted.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

- Enable/Disable USB Mass Storage - to remotely allow or block the use of USB storage devices on managed computers.

The screenshot shows the BitDefender Management Server interface. At the top, it says 'BitDefender Management Server' and 'bitdefender'. Below that, there's a 'Create a new Task' section with a progress bar showing four steps: 'Select a Task', 'Define Settings', 'Select Computers', and 'Schedule Task'. The 'Define Settings' step is currently active. Underneath, it says 'Define Task Settings' and 'Please define the task settings below and click Next to continue.' There are two radio button options: 'Enable USB Mass Storage' (which is selected) and 'Disable USB Mass Storage'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

IT administrators can run these Tasks on all managed computers to completely disable autorun and USB storage devices in the network. Afterwards, these Tasks can be run as needed to temporarily enable autorun and USB storage devices on specific managed computers or groups.

7. CONCLUSIONS

Unique for both SMB and corporate networks, BitDefender combines antimalware protection with remote audit and system management using WMI (Windows Management Instrumentation) technology, allowing network administrators to gain an additional layer of visibility and protection to help them identify and eliminate gaps within their network. With the addition of enhanced visibility and improved manageability, BitDefender's Business Solutions go beyond traditional corporate antimalware solutions to protect critical services such as email messaging systems, desktop clients and servers from attacks - whether the threats originate from outside or within the organization.

About BitDefender®

BitDefender is the creator of one of the industry's fastest and most effective lines of internationally certified security software. Since its inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe - giving them the peace of mind of knowing that their digital experiences will be secure. BitDefender solutions are distributed by a global network of value-added distribution and reseller partners in more than 100 countries worldwide. More information about BitDefender and its products are available at the company's security solutions press room. Additionally, BitDefender's www.malwarecity.com provides background and the latest updates on security threats helping users stay informed in the everyday battle against malware.

About BitDefender® Business Solutions

Companies can protect their business systems from attack by using BitDefender's ability to detect and prevent known and zero-day threats, ensure compliance to corporate security policies and manage them effectively with fewer IT resources. Combined with integrated audit and system management, BitDefender's Business Solutions protect corporate networks and streamline IT operations with centrally managed, multi-platform Endpoint, Server and Gateway security solutions.

Simple to deploy and easy to manage, BitDefender's Business Security solutions provide visibility into an organization's network security posture, in addition to streamlining critical IT management related tasks. The Centralized Management consolidates traditional corporate antimalware functionality with wizard-driven Network Tools that simplifies mass remote configuration management and network-wide auditing of Windows-based desktops and servers.

Download Trial Versions of BitDefender Business Solutions at www.bitdefender.com/business

APPENDIX: DESCRIPTION OF NETWORK TASK TEMPLATES

This appendix provides a detailed description of the available Network Task 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.

Enable/Disable Autorun for All Drives – Enables or disables the Windows Autorun feature for all drives on client workstations. Autorun enables automatic detection and reading of new media.

Enable/Disable USB Mass Storage – Enables or disables USB storage devices on client workstations. Such devices include USB memory sticks (flash pens) and MP3 players.

Enumerate All Startup Programs – Provides information about all the programs that run on client workstations at startup.

Enumerate (Physical RAM) Memory – Provides the size of the physical (RAM) memory installed in client workstations.

Enumerate (Virtual Memory) Pagefile – Provides information about the virtual memory (the page file) available on client workstations, including: the location and size of the page file, and initial/maximum size.

Enumerate Startup Programs – Provides information about the programs installed using the Windows installer 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 information about client workstations, including: operating system information, system name, model and manufacturer, total RAM memory, processor, BIOS version.

Install Windows Updates – Helps you identify the Windows updates available for client workstations and install all or specific Windows updates on client workstations.

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 details about the processor of client workstations, including: 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 all software and Microsoft and Windows updates installed on client workstations. An uninstall command line is provided for each application or update installed with the Windows installer. You can remove an application using this command line with a Run Program script.

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, including: name (label), description, free disk space, size.

List Logon Session Info – Provides details regarding the logon session on client workstations.

List Motherboard Settings – Provides information about the motherboard (MB) of client workstations, including: name, manufacturer, and serial number.

List Monitor Settings – Provides information about the monitor of client workstations, including: monitor type, manufacturer and physical dimensions.

List Network Adapter Values – Provides detailed information about the network adapters installed in client workstations, including: adapter type, manufacturer, MAC and network address

List Services – Provides information regarding the services running on client workstations, including: service name and display name, state (stopped / running), start mode (automatic / 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 detailed information regarding the video display of client workstations, including: video adapter name and type, graphics memory, resolution, driver name and version, and minimum/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, including: operating system and version, registered user, serial number, and installation time.

Remote Desktop Connection – Changes the Windows settings on client workstations in order to allow or block incoming remote connections through Remote Desktop Connection.

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 local machine (where the BitDefender Management Console is installed).

Send Message – Sends a message to the user logged on client workstations. For Windows 2000 workstations, the script uses the net send command and requires the Messenger service to be started (default setting). For other Windows workstations, the script uses the msg command and requires the Terminal Services service to be started (default setting).

Windows Automatic Updating – Configures Windows Automatic Updates on client workstations. Windows Automatic Updates helps users keep their operating system up-to-date.