GFI White Paper

Patch management with GFI LanGuard™ and Microsoft WSUS

A cost-effective and easy solution
for network-wide patch management

This white paper provides an overview of how to use GFI LanGuard and Microsoft Windows Software Update Services (WSUS) to keep your network automatically updated with the latest security patches.

GFI®

Contents

Introduction

Patch management is an essential network administration task. It consists of scanning machines on the network for missing patches and deploying those patches as soon as they become available. Failure to do so makes a network doubly vulnerable – not only is the vulnerability there, but it has now also been publicized, making it more likely to be exploited by malicious users, hackers and virus writers.

Time and again, however, countless administrators fail to apply the right patches leading to worms which exploit security vulnerabilities in Microsoft operating systems. One such notorious case was Zotob, the August 2005 worm that spread by exploiting known vulnerabilities in unpatched Microsoft SQL 2000-based computers. Until recently, the main reason for this was because installing patches was a cumbersome and daunting job. Yet with the advent of sophisticated automatic patch management tools, this scenario can be eliminated.

This white paper provides an overview of how any network administrator uses GFI LanGuard and Microsoft Windows Software Update Services (WSUS) to keep the network updated with minimal effort.

WSUS and GFI LanGuard

What is GFI LanGuard?

GFI LanGuard is a security scanner that checks your network for possible security vulnerabilities by scanning your entire network for missing security patches, service packs, open shares, open ports, unused user accounts and more. Its powerful reporting allows you to easily lock down your network against hackers. GFI LanGuard can also remotely deploy missing patches and service packs in applications and operating system.

What is Windows Software Update Services (WSUS)?

Microsoft WSUS is a free patch management tool provided by Microsoft to help network administrators deploy the latest Microsoft product updates to Microsoft Windows Server 2000, Windows server 2003 and Windows XP operating systems. In addition, WSUS allows information technology administrators to easily deploy security and other update patches to Microsoft applications including Microsoft Office XP, Microsoft Office 2003, Microsoft Exchange 2003 as well as Microsoft SQL Server 2000.

By using Microsoft WSUS, administrators can fully manage the distribution of patches that are released through Microsoft Update to computers in their network. In simple terms, Microsoft WSUS is a version of Microsoft Update that you can run on your network. Instead of each workstation having to connect to the Internet to update Windows, each workstation connects to the Microsoft WSUS Server instead and updates from there. In addition, a WSUS (Master/ Upstream) server can be the update source for other WSUS servers within the organization. Thus, the WSUS (Master/Upstream2) Server alone requires access to the public Internet as it connects to Windows Update.

By connecting to Windows Update, Microsoft WSUS Server provides notification of critical updates as well as performing automatic distribution of those updates to your workstations and servers. Microsoft WSUS server gives the administrator more control over updates: The administrator can test and approve updates from the public Windows Update site before deployment on the corporate intranet. Deployment takes place on a schedule created by the administrator. Information on updates is first downloaded into the database. When a WSUS client reports that it needs an update, WSUS decides that on the next synchronization cycle, it'll download the update.

WSUS is a development based on Software Update Services (SUS) and it builds on the features of SUS by providing:

- Increased bandwidth efficiency: Exploits bandwidth efficiency through the Background Intelligent Transfer Service (BITS) 2.0
- Multi-lingual support: Includes additional language support for customers worldwide
- Configurable deployment options: Allows the administrator to specify the required update action by selecting an option out of Install, Remove Update, Detect–only or Decline

- Data migration and import/export features
- Database options: Allows the administrator to select the WSUS database where update information and WSUS server settings are to be stored
- Reporting capabilities: Allows the administrator to monitor the update activity
- Update suitability check: Allows the administrator to estimate how many computers need to be updated. A 'Detect-Only' action determines if an update is suitable for each computer before proceeding to patch deployment
- Update targeting: Allows the administrator to configure which computers need to be updated
- More updates and automated download capabilities: Automatic update, enables both server and client computers to receive updates for Microsoft operating systems and applications from Microsoft Update or from a source server running WSUS (i.e. a Master/Upstream server).

What are the advantages of using GFI LanGuard and Microsoft WSUS server together?

Microsoft WSUS server is a good solution for pushing out Microsoft patches. It supports all Windows XP, 2000/2003 operating system patches, including those for applications that are part of the operating system such as IIS and Internet Explorer. Additionally it supports patches for Microsoft Office XP/2003 applications, Microsoft Exchange 2003 and Microsoft SQL Server 2000.

However, Microsoft WSUS does not offer the following features that are provided by GFI LanGuard:

- Deployment of patches to ISA server machines
- Deployment of patches to machines running Windows NT
- Deployment of third party software patches and software

Therefore, GFI LanGuard and Microsoft WSUS jointly make a perfect combination to keep Windows machines up-to-date, including Microsoft application patches and service packs, and third party software and software patches.

How to set up patch management on your network

Step 1: Installing Microsoft WSUS server

Microsoft WSUS was designed to act as an automated server that works in the background rather than a desktop-based scanning tool. Once it is set up, the patch management process is automated.

Hardware and Software requirements

WSUS Server hardware requirements:

- 1 GHz processor or higher
- 1 GB RAM
- A minimum of 1 GB free space is required for the system partition
- A minimum of 6 GB free space are required for the volume where WSUS stores content (30 GB are recommended).

NOTE: Both the system partition and the partition on which you install WSUS must be formatted with the NTFS file system.

WSUS Server software requirements:

- Windows Server 2000 (SP 3 or higher) or Windows Server 2003 operating system
- Microsoft Internet Information Services (IIS) 5.0
- Background Intelligent Transfer Service (BITS) 2.0
- Database software that is 100% compatible with Microsoft SQL (e.g. MicrosoftDE 2000)

» Microsoft Internet Explorer 6.0 Service Pack 1 or higher

» Microsoft .NET Framework Version 1.1 Redistributable Package

» Microsoft .NET Framework 1.1 Service Pack 1.

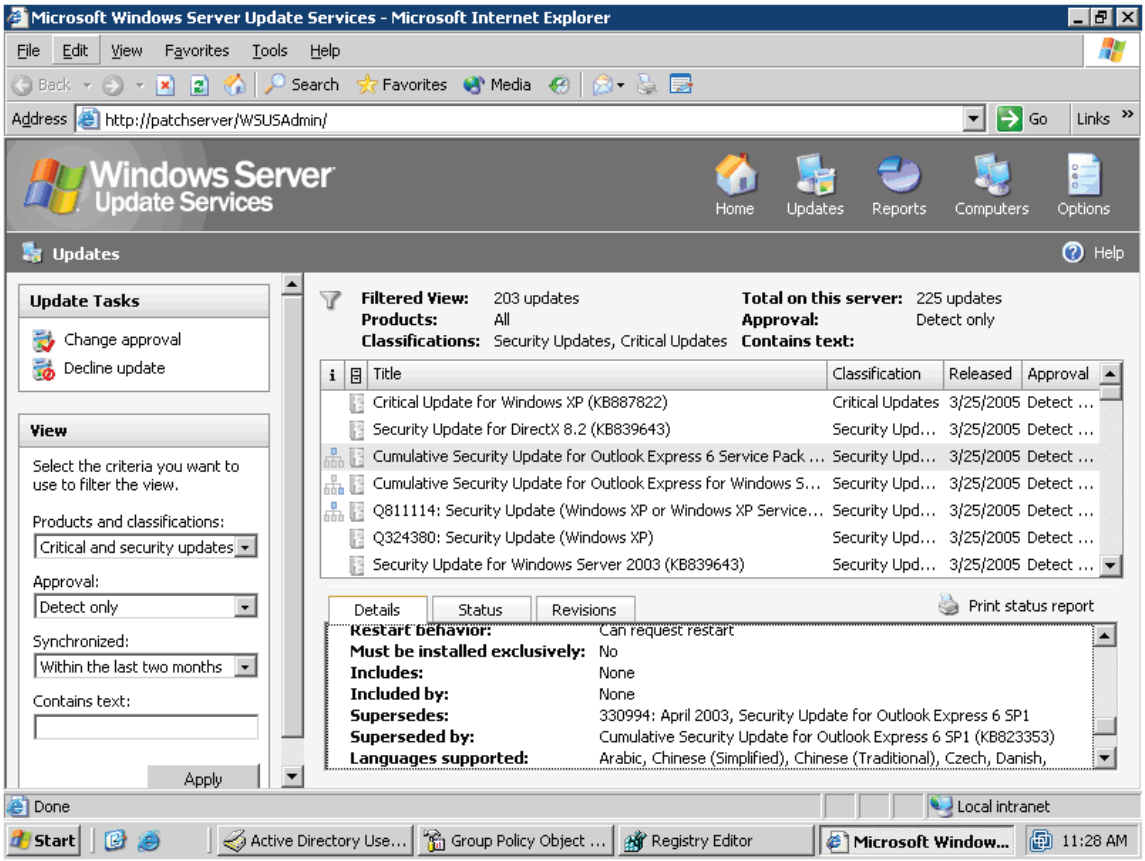
WSUS client software requirements:

» Windows Server 2000 (SP 3 or higher), Windows XP or Windows Server 2003 operating system.

Once WSUS is installed (requires IIS), you should configure it to check for updates. It is also important to ensure that workstations and servers have either Windows 2000 SP3, Windows XP SP1/SP2 or Windows 2003 installed, or that they have the Microsoft WSUS client installed. (Windows NT is not supported). The WSUS client can easily be pushed out by using Group Policy that is provided by the 'deploy custom software' feature of GFI LanGuard Group Policy should be used again to configure the client workstations to get their automatic updates from your WSUS server. This procedure is also explained in more detail in the documents accompanying Microsoft WSUS.

Administering the Microsoft WSUS server

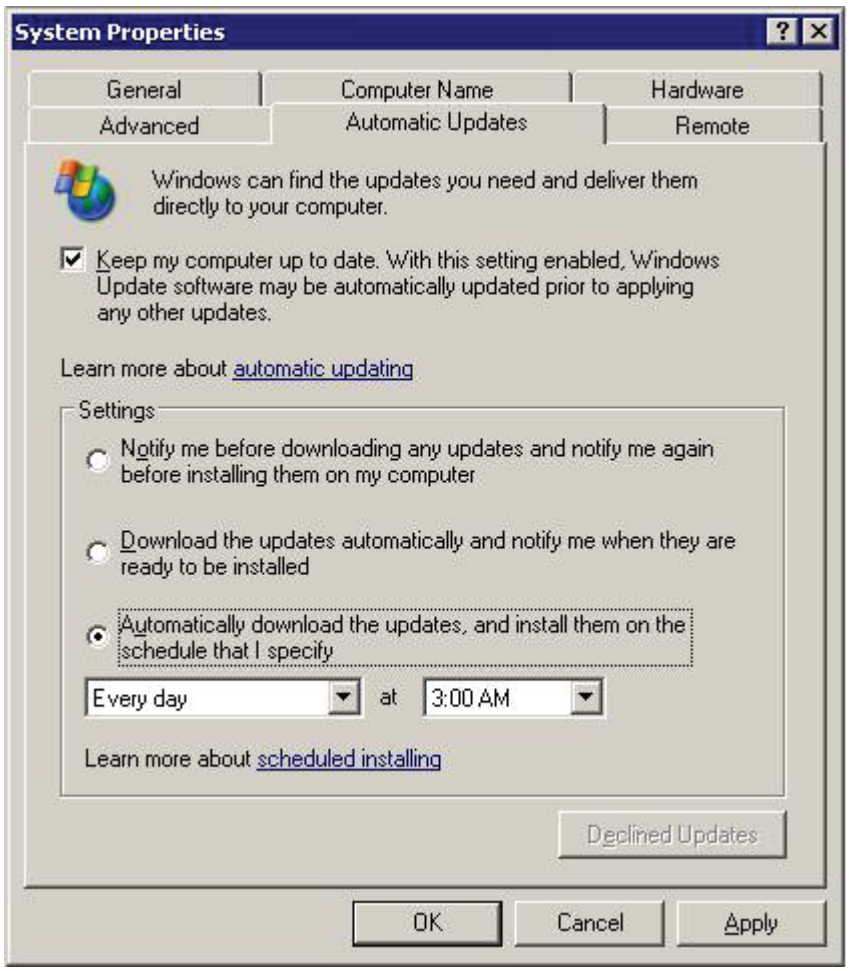
The administration of Microsoft WSUS server is all web-based, allowing you to administer it remotely. The Microsoft WSUS server downloads all available updates automatically and notifies you of new updates. New updates can be approved for deployment or rejected, ensuring that the administrator still has full control over what gets installed on your network. The approval interface is very similar to updating a single machine using Windows Update.



Approving updates via the Microsoft WSUS server administration interface

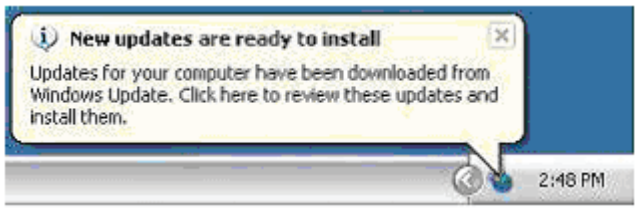
The Microsoft WSUS client

Once you have installed both Microsoft WSUS server and the Microsoft WSUS client, all updates are pushed out automatically. As an administrator, you can configure how and when this should happen. You can also allow the user to have some sort of control over this process, if you wish. The screenshot below shows the options available. Of course, these options can be locked using Group Policy.



Automatic updates control panel with options

After you have configured the Microsoft WSUS client, patches are deployed automatically. The user is notified that updates are ready to install through a message in the task bar (see image below).



User gets feedback that updates are about to be installed

Step 2: Patch management with GFI LanGuard

Once Microsoft WSUS server is operational on your network, you need to install GFI LanGuard to perform the following patch management tasks:

- Deployment of Microsoft application patches and service packs for Microsoft Office, Microsoft SQL Server 2000, Microsoft Exchange 2003 Server and Microsoft ISA Server
- Checking that missing patches and service packs are installed and issuing an HTML report about this
- Deployment of patches to machines running Windows NT
- Deployment of third party software patches (can also be used to deploy virus signature updates)
- Immediate deployment of a particular patch in the event of emergency; waiting for WSUS to perform the update would not be possible.

Scanning for missing patches with GFI LanGuard

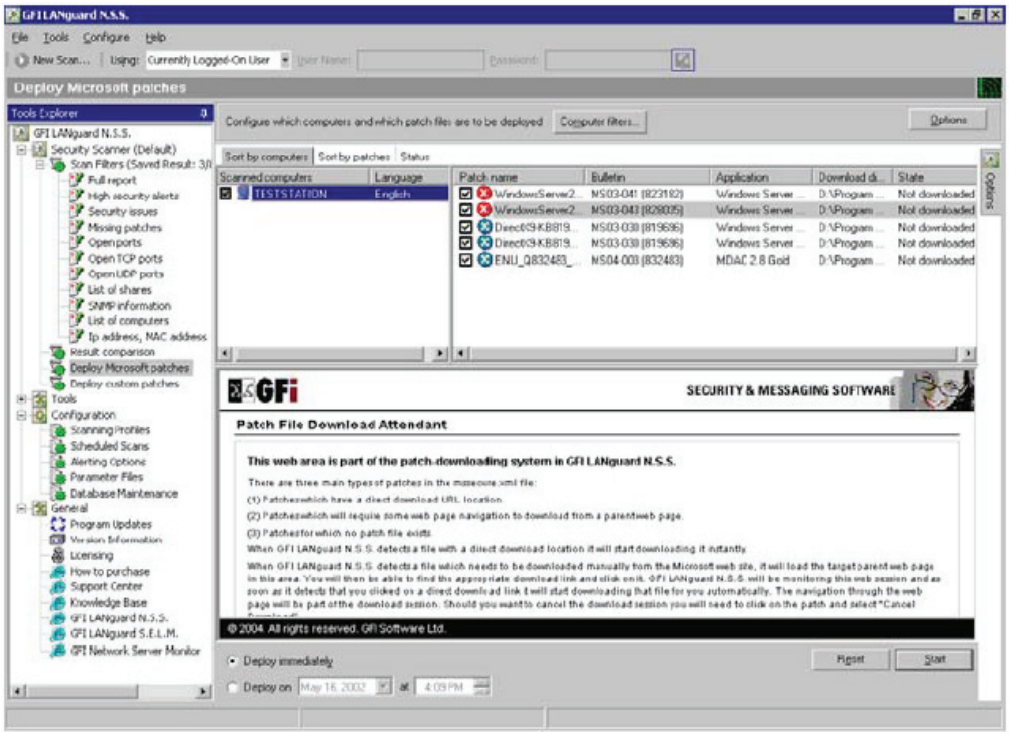
Once you have your patch management in place, it is important to regularly scan your network to check that all patches and service packs have been deployed by Microsoft WSUS. GFI LanGuard quickly scans your network and lists all missing patches and service packs under the Alerts node.

To scan your network, enter the IP range directly at the top of the scanner interface, or use the Scan Wizard (accessed from the File drop-down menu) to specify which computers to scan. You can scan domains, specific computers and an entire IP range. Click Finish to start the scanning process. You'll see each machine appear in the left-hand pane as it is found by GFI LanGuard. The right-hand pane provides detailed progress information.

Once the network scan is complete, missing patches and service packs are detailed under the Vulnerabilities node. If Microsoft WSUS is updating all client machines correctly, you should only see missing patches for third party software or operating systems and applications patches not supported by WSUS such as Windows NT and ISA Server patches.

GFI LanGuard NSS displays missing patches

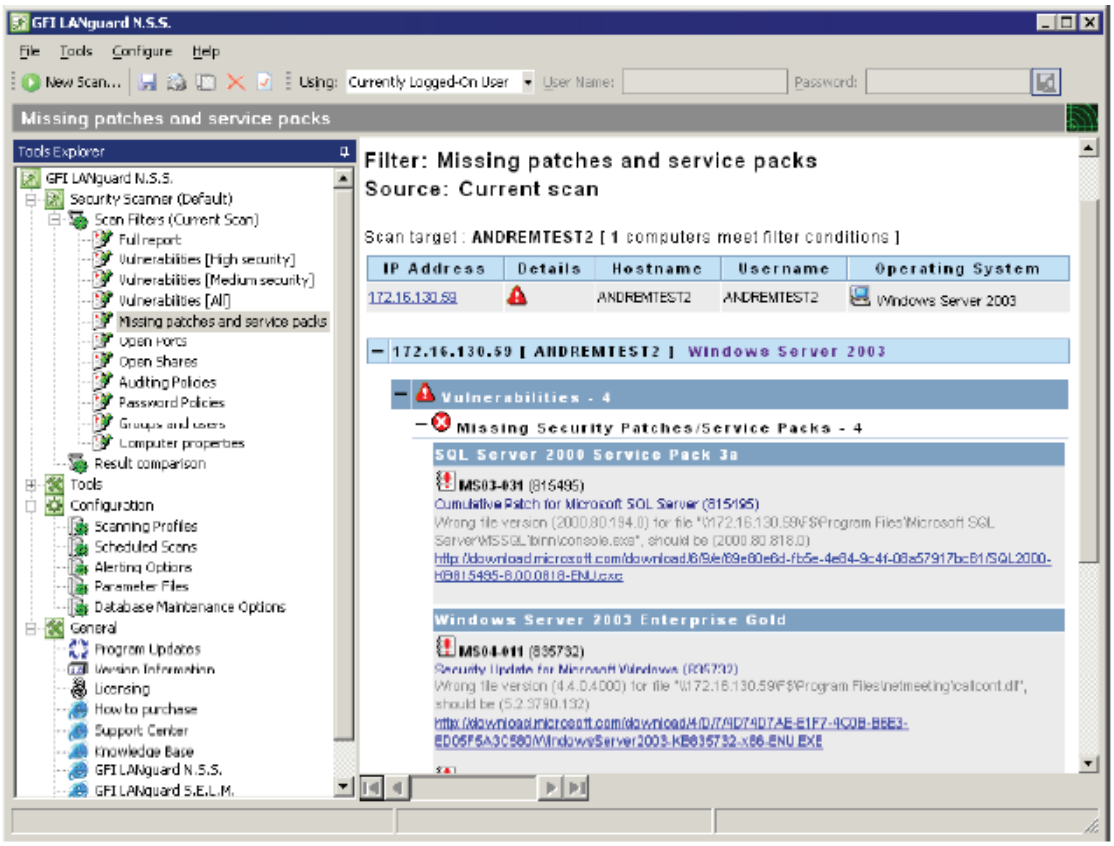
Right-clicking on a patch or a service pack allows you to deploy the missing service pack or patch to that computer or all computers. The Deploy Patches node, shown in the screenshot, allows you to easily specify which patches to push out and to which computers.



Deploying patches

Step 3: Reporting

Once you have scanned your network, you can also create a concise report that lists all missing patches and service packs. To generate the missing patches report, go on File > Filters > Missing Patches



The GFI LanGuard missing patches/service packs report

Conclusion

Microsoft WSUS Server is perfect for Windows XP/2000/2003 operating system patch management. In addition, it can efficiently manage patches for Microsoft Office XP/2003, Microsoft Exchange 2003 and Microsoft SQL Server 2000. Although you can use a patch management product instead, using Microsoft WSUS Server saves you time in the long run: Once set up, it is easy to keep your network up-to-date. Coupled with the fact that Microsoft WSUS Server is free, this makes for an easy decision. However, Microsoft WSUS Server does not perform all/complete patch management. It neither deploys patches to ISA Servers and Windows NT operating system nor does it support updates for third party software. You must therefore use a patch management tool in addition to Microsoft WSUS Server to keep your machines completely up-to-date.

GFI LanGuard in tandem with Microsoft WSUS offers all the features found in more expensive patch management solutions at a minimal cost. Most patch management solutions range from $1,500 for a 100-machine license to $8,000 and more for a 500-machine license. The combination of GFI LanGuard N.S.S. and Microsoft WSUS allows you to update operating systems using Microsoft WSUS (Windows 2000, XP, .NET, IIS, IE, Windows Media) and service packs, Microsoft application patches (Word, Excel, Outlook,etc..), Windows NT patches and third party software using GFI LanGuard.

The combined solution of GFI LanGuard and Microsoft WSUS is not only more powerful and flexible, it is also much more cost-effective: Microsoft WSUS is free and GFI LanGuard licenses start from as little as $495 for 32 IPs. For more information on GFI LanGuard and to download your copy, please visit: http://www.gfi.com/lannetscan/.

About GFI

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SME) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com