Global Information Assurance Certification Paper

Patch Management with Microsoft Windows Update Services

GCWN Version 5.0

Option 1 – Solving a Windows Problem

Cody Ray

Date, 2004

Summary

The objective of this paper is to introduce Windows Update Services (WUS), a new solution from Microsoft that assists in patch management. The paper will discuss how WUS compares to other Microsoft patch management solutions and describe scenarios where WUS might be better suited. The paper will explain how to install WUS, how to configure WUS and how to avoid some common pitfalls. In conclusion, the paper will describe some needed improvements for future releases of WUS and critic Microsoft's future security outlook.

Let me begin with a question, "What is the main complaint about Microsoft products, especially their operating systems?" Most likely your answer will revolve closely around the issues of stability and vulnerabilities, which in most cases go hand in hand. It is known by most personnel in the IT industry and certainly by security practitioners involved with computing systems that software programmers are not perfect. In fact, until recently most programmers were never taught the basics of secure programming nor were they expected or encouraged to program with security in mind. Recent events such as those reported by CERT (www.us-cert.gov) demonstrate the never ending struggle to keep systems patched against the latest vulnerabilities and debilitating viruses. CERT is an organization built to help identify computer system vulnerabilities and manage them through alerts, communication and publication through various means including an extensive list of common vulnerabilities known as the CVE (Common Vulnerabilities and Exposures List) located at http://cve.mitre.org/. The list below illustrates CERT's Current Activity Table as of December 10, 2004.

W32/Sober - http://www.us-cert.gov/current/current_activity.html#w32/sober

W32/MyDoom - http://www.us-cert.gov/current/current_activity.html#w32/mydoom

W32/Bagle Revisted - http://www.us-cert.gov/current/current_activity.html#w32/bagle

Exploit for Microsoft GDI+ JPEG Parser - http://www.us-cert.gov/current/current_activity.html#gdi

W32/Sasser - http://www.us-cert.gov/current/current_activity.html#sasser

Exploitation of Outlook Express MHTML Cross-Domain Scripting Vulnerability - http://www.us-cert.gov/current/current_activity.html#mhtml

Internet Explorer HTML Elements Vulnerability - http://www.us-cert.gov/cas/techalerts/TA04-336A.html

It is obvious that the computer industry has yet to solve the problem of poor coding. It should also be obvious that law enforcement, new laws and anti-virus companies don't have the ability to control the creative mind of an individual or

an individual's actions when it comes to malware programming and distribution. To suggest that certain bills have the ability to guide young, creative and rebellious brains from creating code that harms others simply because of certain punishments is ridiculous. The hacker culture is such that the ability to break through or defy what is expected is exactly the point. Therefore, to a certain extent these steps have further challenged the individuals out there to come up with more creative, destructive and hard to trace methods.

In a controversial paper coauthored by a former employee of @Stake Corporation (recently acquired by Symantec Corporation), Dan Geer, states that the Microsoft dominate presence in the American economy was a threat to America's security. He states that their faulty software undermines ongoing security efforts to minimize the threat of malware, hackers and cyberterrorism. Mr. Geer was fired shortly after @Stake discovered the existence of the paper. This argument is not so far fetched when you consider that Microsoft probably has a presence in every business in America and that they manage probably 90% of all major commercially available software packages. It is also safe to say that most Internet users browse the Web with Internet Explorer, Microsoft's inheritably insecure web browser. In fact, it has been suggested by some security organizations to drop Internet Explorer all together and use an alternative browser such as Opera or the increasingly popular Mozilla Firefox (www.mozilla.org). Paul Boutin asked the question, "Are the Browser Wars Back?" in a recent article written for Slate (http://slate.msn.com). In closing he says this, "Internet Explorer is used by 95 percent of the world. Firefox's fan base adds up to 2 or 3 percent at most. Which browser do you think the Russian hackers are busily trying to break into again?" Microsoft must make an effort to secure their software and they must be willing to actively pursue a solution to better manage patches and security vulnerabilities. As it turns out Microsoft is taking the first steps toward this end.

Microsoft, as a company, finally heard the voices from the community and decided to act by creating a new initiative. Bill Gates, the chairman of Microsoft, announced this new initiative that would focus on security and stability within the Microsoft suite of products, on January 15, 2002 via a company wide e-mail (http://news.com.com/2009-1001-817210.html?legacy=cnet). One such step taken by the company to accomplish this monumental task was to create a better software update process for all of its products. It is rather obvious that when you create a majority of the software that runs the world's computers you are going to have a lot of patches and vulnerabilities discovered throughout the life cycle of the products. Therefore, this was not an easy task to undertake. Microsoft's first step was to recreate the already popular Windows Update Service they offer online through ActiveX controls and establish a more comprehensive approach. This new approach, using their latest Windows Update software now at version five, allows for an Express Install or a Custom Install process. The Express Install process displays all the high priority updates and automatically downloads and installs them with one click of the mouse, while the Custom Install displays high priority updates and optional updates which include software and hardware updates and even includes an optional beta software release offering.

This new offering from Microsoft has come a long way in helping the average user to better secure their computers and offers an intuitive approach to solving one of the basic problems of security, patch management. However, this approach doesn't quite meet the need for large IT infrastructures and large corporations. It would not be very efficient for IT personnel to visit each workstation and server in an organization whenever the latest vulnerability patch for Windows is released. It would also not be efficient to visit the Windows Update website, manually updating each computer. Microsoft addresses these issues in a myriad of different ways. First, Microsoft allows you to schedule a time for automatic updates via its Windows Update client (which is downloaded via ActiveX controls when first visiting the Windows Update website). When an update is available, the client can allow you to choose when to download this update, allowing for an automated installation. In turn, the client may be configured for a complete manual installation. In automatic mode a scheduled time is configured for downloading the update(s), installing and even automatic rebooting of the system. In manual mode you determine when you want to download the updates, install them and reboot the system with user intervention. This seems to be a step closer to a solution, but again large corporations and IT infrastructures may still find this to be an issue because it seems to not quite centralize the process under a control mechanism.

Microsoft understands the needs of its larger partners and corporations and has provided much more granular, centralized, yet wider scaled solutions for patch management and overall housecleaning of its products. This is why, in March of 2004, Bill Gates announced products to help unify the patch management process and provide better solutions for IT management. In March, Mr. Gates announced the availability of SUS (Software Update Service) and SMS 2003 (System Management Server 2003) in Microsoft's Executive E-mail section of their corporate website (http://www.microsoft.com/mscorp/execmail/2004/03-31security.asp). He also mentioned in this announcement Microsoft's move to monthly patch releases in order to improve manageability and scheduling for IT management. Since this announcement, WUS (Windows Update Services) has been released in beta form and expands upon the offerings of SUS. SMS has also been updated with its first service pack release.

This gives us three options, available via Microsoft, to assist in tackling the ever increasing threat of vulnerable software. However, I am focusing only on patch management and will quickly narrow my discussion specifically to WUS.

First, the word "management" in patch management is key when comparing the first solution, Windows Update (via the Microsoft website) because there really isn't any management involved. Sure, you can configure your desktops and servers to auto-update via the website and you may even want to push down a common schedule for this to occur via group policy, but it hardly allows you to pick and choose what gets updated. This creates a problem when trying to properly test the updates applied within your existing applications. You could certainly establish a testing environment and run updates just for that

environment. You may also choose to block access to the Microsoft Windows Update website except for your testing machines, but there is a far better way to manage testing scenarios.

Secondly, SMS provides a comprehensive solution, but also is much more difficult to start using and requires a lot of training and time to learn the workings of the product. In addition, we are simply focusing on patches and updates, not full system management and control. If you are looking simply for a patch management solution, SMS is just too large a beast and far more expensive a solution to bring into the organization. Microsoft has outlined the differences in fact between SUS 1.0 SP1 and SMS 2003 (WUS had not been released at the time of this report) in an easy to view table format below.

Capability	SUS 1.0 with Service Pack 1	SMS 2003
Supported Platforms for Content	Windows 2000, Windows Server 2003, Windows XP	Windows NT 4.0, Windows 2000, Windows Server 2003, Windows XP, Windows 98
Supported Content Types	Only security and security rollup patches, critical updates, and Service Packs for the above platforms	All patches, Service Packs, and updates for the above platforms. Also supports patch, update, and application installations for Microsoft and other applications.
Targeting Content to Systems	No	Yes
Network Bandwidth Optimization	Yes, for patch deployment	Yes, for patch deployment and server synchronization
Patch Distribution Control	Basic	Advanced
Patch Installation and Scheduling Flexibility	Controlled by administrator (automatic) or user (manual)	Administrator-controlled with granular scheduling capabilities
Patch Installation Status Reporting	Limited: Client installation history and server-based installation logs	Installation status, result, and compliance details
Deployment Planning	Not applicable	Yes
Inventory Management	Not applicable	Yes

Compliance Checking	Not applicable	Yes

http://www.microsoft.com/technet/security/guidance/secmod193.mspx#ECAA

In a later article, Microsoft mentioned the following differences or improvements of WUS over SUS 1.0:

- Update additional Microsoft Products (Windows, Office, Exchange, SQL Server and MSDE)
- Improve administrative control over the update management process
- Minimize network bandwidth utilization and impact of network issues
- Deliver status reporting capabilities
- Optimize the end user experience
- Improve ease and flexibility of system implementation
- Increase administrator productivity

In addition to the advances listed above, WUS also uses Microsoft's BITS technology which allows for the downloading of updates in the background while using bandwidth that is not being used by other applications, thereby not effecting workflow or responsiveness. BITS also has the ability to resume downloads or continue processing a download while the system is down and unavailable (this includes a reboot of the system). To further increase the performance over the network BITS implements binary delta compression technology to help those large updates along.

I believe we can now agree that for patch management WUS fits our needs quite nicely. Let's get started using WUS and its patch management features! You may obtain WUS at the following website http://www.microsoft.com/windowsserversystem/wus/trial.mspx. In order to download the product, you must first agree to the open evaluation agreement and obtain or use an existing Microsoft Passport credential. Once downloaded you simply double click on the packaged executable and follow the wizard installation.

The server requirements are not stringent enough to warrant a dedicated server for WUS, however, I do not recommend installing it on an existing server currently running a website. There are conflicts in doing this that I will discuss shortly. Microsoft recommends for 500 clients or less the following profile:

Requirement	Minimum	Recommended
CPU	300 MHz	1 GHz or faster
RAM	256 MB	1 GB
Database	WMSDE/MSDE	WMSDE/MSDE

Microsoft recommends for 500 clients or more the following profile:

Requirement	Minimum	Recommended
CPU	1 GHz or faster	2 GHz or faster
RAM	1 GB	1 GB
Database	SQL Server 2000 SP3a	SQL Server 2000 SP3a

In addition to the list above there is a minimum requirement of 6 GB free space within the volume where WUS will store its repository of updates and 30 GB is recommended. The volume must be NTFS formatted and 2 GB of free space is needed just to install WUS and a database. Yes, a database is required to run WUS, but Microsoft gives you a few choices as long as you stay with their products. Microsoft allows you to run Windows SQL Server 2000 Desktop Engine (WMSDE) which ships with WUS, SQL Server 2000 Desktop Engine (MSDE) which limits you to 2 GB and of course SQL Server 2000. You will need to have MDAC 2.6 SP2 installed in order to run it on Windows 2000. Be sure to verify that the proper version of MSxml2.dll is one of the following versions:

Msxml2.dll - version 8.30.8709.0
Msxml2r.dll - version 8.1.7502.0

You must also run the latest Microsoft .NET Framework (Version 1.1 SP1) Internet Explorer 6.0 SP1 and Internet Information Services (IIS) version 5 or greater. You may obtain the free packages from Microsoft's website or visit the newly formed WUS Wiki website located at http://wus.editme.com/WUSBeforeYouInstall.

Referring to my previous statement in regard to an existing website or an existing SUS installation, WUS will attempt to install and bind to port 80, but if it is unable to bind to this port because it is in use, WUS will install on port 8530. My recommendation is to avoid installing it on an existing web server that is serving pages other than SUS and if you are upgrading to WUS from an existing SUS server, I recommend installing to port 8530, running the SUS to WUS migration utility and removing your existing SUS site, replacing it with your new WUS site. Running over a port other than port 80 introduces problems that may be easily avoided. For instance, there is an issue regarding the SUS client and the way that it self-updates. Another instance concerns group policy and the need for you to configure the port used by WUS within the client configuration settings as published by group policy. Microsoft has workarounds for these trivial issues but it is simply easier to run WUS over port 80. If you must install WUS on port 8530 Microsoft suggests you install a simple website listening on port 80. This can be the default website as WUS only requires two virtual directories for self-client update purposes. Once this is complete run the following program from a command line to finish the setup process:

cscript WUS install drive}:\Program Files\Microsoft Windows Update Services\Setup\InstallSelfUpdateOnPort80.vbs

Refer to the Microsoft WUS Deployment Guide for group policy settings that may be applicable for your environment. Keep in mind that the WUS server itself must

synchronize with Microsoft's Update servers over port 80 and 443. Figure 1 is a screenshot of the new WUS console after connecting and logging into the webpage over port 80. Make note that you must access the WUS admin console using Internet Explorer as other browsers are not supported. The screenshot was taken before an initial synchronization was performed.

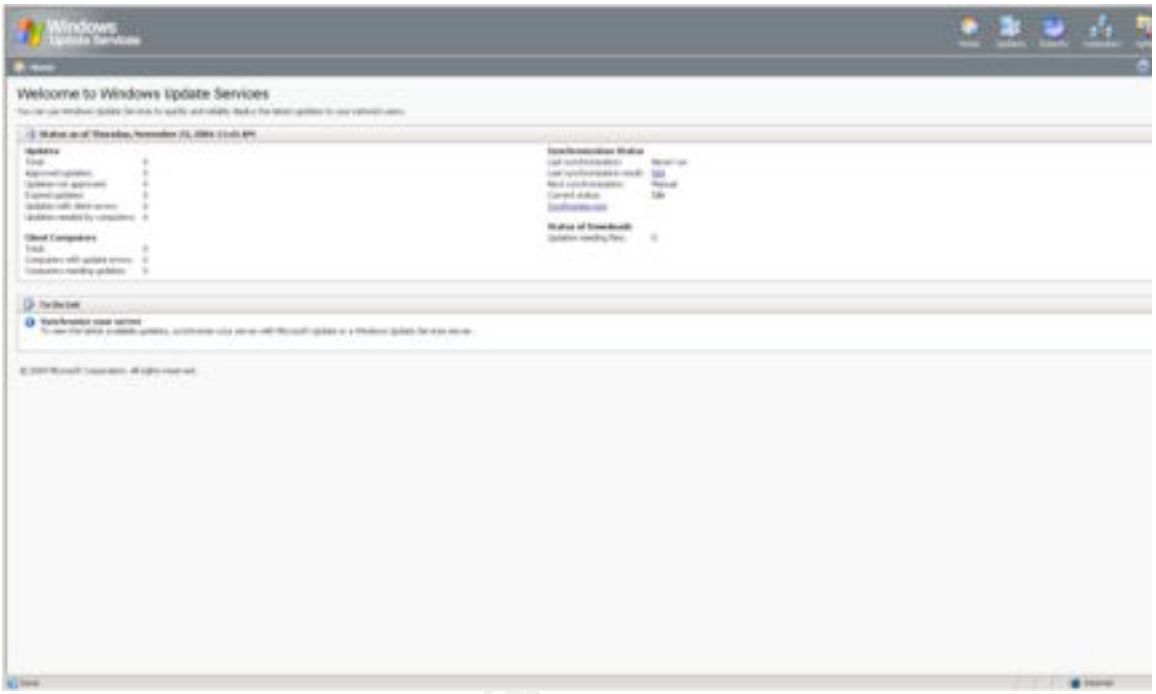

Figure 1

Further considerations must be made concerning the way you decide to deploy WUS. You can opt to deploy it in simple mode, which is to say it is the only WUS server on your network and synchronizes directly with Microsoft's Update servers. Or, you may opt for a more complex "chain" mode approach that allows other WUS "child" servers to synchronize against the "parent" WUS server within your organization. In a chain mode installation there must be only one parent which all child servers sync with. This parent server must have access to the Internet to allow for downloaded updates, but the child servers do not need access. In addition, with the newly added functionality of server groups or "target groups" within WUS, you may choose to create a child WUS server only for a particular group or branch office site, thereby reducing Internet bandwidth and/or updates to a particular sector of the network. WUS does not transfer target groups from the parent server to the child servers. WUS also does not transfer approved update information from a parent server to child servers. In a chained environment the downstream servers must always synchronize from an upstream server. Microsoft's recommendation for a WUS hierarchy is to not exceed three levels. The reason for this is simple. As each update comes into the WUS server connected to the Internet, that update must be passed down to the child server directly below it in the chain. This update is then passed from the first child server downstream to the subsequent child servers. Microsoft has tested a five deep server hierarchy with success, but suggests that bandwidth and

synchronization latency can occur and deployment of such a hierarchy is not recommended.

WUS offers four types of bandwidth control mechanisms to allow you to shape WUS around your network capacity needs. The first method is called “deferred downloads”. This method allows WUS to download metadata (the list of updates) to the server without downloading the update itself. You may then approve or disapprove an update before it is stored on your system giving you greater storage management and bandwidth management. Upon approving an update WUS will download all the necessary files for deployment. In a chained WUS installation the child servers are automatically configured for deferred downloads. This configuration cannot be changed; however, the child servers can be configured to download the metadata and the updates at the same time. If an update is approved from a child server that has not been approved by the parent server, a request is sent that triggers the parent to send the update to the child. The update is then deployed by the child server. Keep in mind that update information is not transferred from parent to child so the parent still has that particular update marked as not downloaded even though it is on the file system and was downloaded for the child server. In this case, the parent will simply not perform the download of the update again but will rather use the existing file. In conjunction with deferred downloads, there is an option to detect updates. The client reports to the WUS server and determines if it needs an update based on the metadata table. If the client needs an update, it triggers a request to the WUS server and the WUS server is then able to report which client(s) need an update. The administrator of the system may then approve the update. Only then is the data for the update actually downloaded. This saves on storage and bandwidth by limiting updates only to client requests. This type of detection downloading can be illustrated by visiting the reporting section of WUS. This is discussed later in the paper in regards to the Status of Updates report.

The second way WUS helps to improve bandwidth utilization is through express installation files. This type of update scenario requires more storage space on your WUS server and more bandwidth utilization on the Internet connection. However, express installation limits the amount of bandwidth utilization on the local area network. This scenario is controlled by the WUS client itself. In regards to deferred updates, the client requests an update from the WUS server and the server sends the update to the client, but only sends the files necessary to complete the requirements of that particular client. Client machines may have different levels of updates and may not require on a binary level the full update but rather only pieces of the update to fulfill the necessary requirements. However, when a second client requests the same update and again has different requirements, the WUS server must make a connection to the Internet to obtain the update if the necessary pieces are not yet stored on the WUS system. Express installation files address this need by downloading the full update and all of its differing pieces. The trade off is obviously storage, but Microsoft has calculated that express installation files save bandwidth over time as the amount of clients with software update variants increases allowing for a decrease in WUS Internet updates required to fulfill client requests. In a simple

standalone installation, when you have configured WUS not to store updates locally, you cannot implement express installation files.

The third option for WUS to improve bandwidth usage is by implementing its import/export feature. If there is a WUS server that does not have access to a parent WUS server or the Internet, updates may be downloaded from a separate WUS server and then exported to media. This media may then be transported to the disconnect WUS server and imported.

Before we discuss the fourth and final option for controlling bandwidth which is language filtering, let's address a few other issues.
Migrating from a SUS to WUS server is fairly easy and is discussed in great detail within Microsoft's WUS deployment documentation. As I mentioned previously, if you install WUS onto a server that is already hosting SUS on port 80, WUS will be installed and begin listening on port 8530. It is simple enough to remove SUS using Add/Remove Programs or removing the directories manually from the Information Services console. But what if you already have a collected history of downloaded content from Microsoft sitting on your hard drive ready to be deployed? Must you remove SUS and download all that content again to populate your WUS server? The answer is no. Microsoft has included a SUS to WUS migration utility that can move these files for you. I will review one scenario commonly practiced by my organization, which is to migrate local content and approvals from SUS and map approvals to the All Computers target group on WUS. If you wish to review further examples or scenarios please refer to the references list following the conclusion of this paper.

In order to move approvals and updates from SUS to WUS you must use the *WUSUTIL.EXE* utility. This program is located where you installed WUS in the Program Files\Microsoft Windows Update Services\Tools directory. You must be a member of the local Administrators group on the WUS server in order to import approvals or content. Open a command prompt window and change your directory to the location of the *WUSUTIL.EXE* utility. At the command line type:

WUSUTIL.EXE migratesus /content <path to the local SUS content> /approvals <SUS server name> /log <file name>.

Insert your appropriate parameters where I have enclosed the text with < > brackets. You may now safely delete your SUS directory and remove the SUS website from IIS. **Note:** The *WUSUTUIL.EXE* tool can only be run on a 32-bit platform.

Once you access your new WUS installation you may begin setting up target groups that allow you to actively control server updates. This will help manage the roles of each server in your infrastructure. There are two default target groups created upon initial installation. The first group is the All Computers group which contains all the computers managed by the WUS service. The second group is the Unassigned Computers group which contains all computers not assigned to a custom created group. Target groups allow for different

updates to be applied to selected computers, thereby creating an environment for administrators to easily test a certain update without effecting the entire environment. This can be accomplished by using Group Policy and Organization Units with Active Directory, but I have found it to be easier to manage within the new WUS console view allowing for a birds eye view of the groups created and the computers that are assigned to them. This eliminates the need to investigate and open multiple policy windows to determine the automatic updates policy for each OU (Organizational Unit). This is not to say that Group Policy doesn't play an important part in the update process. Figure 2 displays the Creating Groups window under the Computers menu.

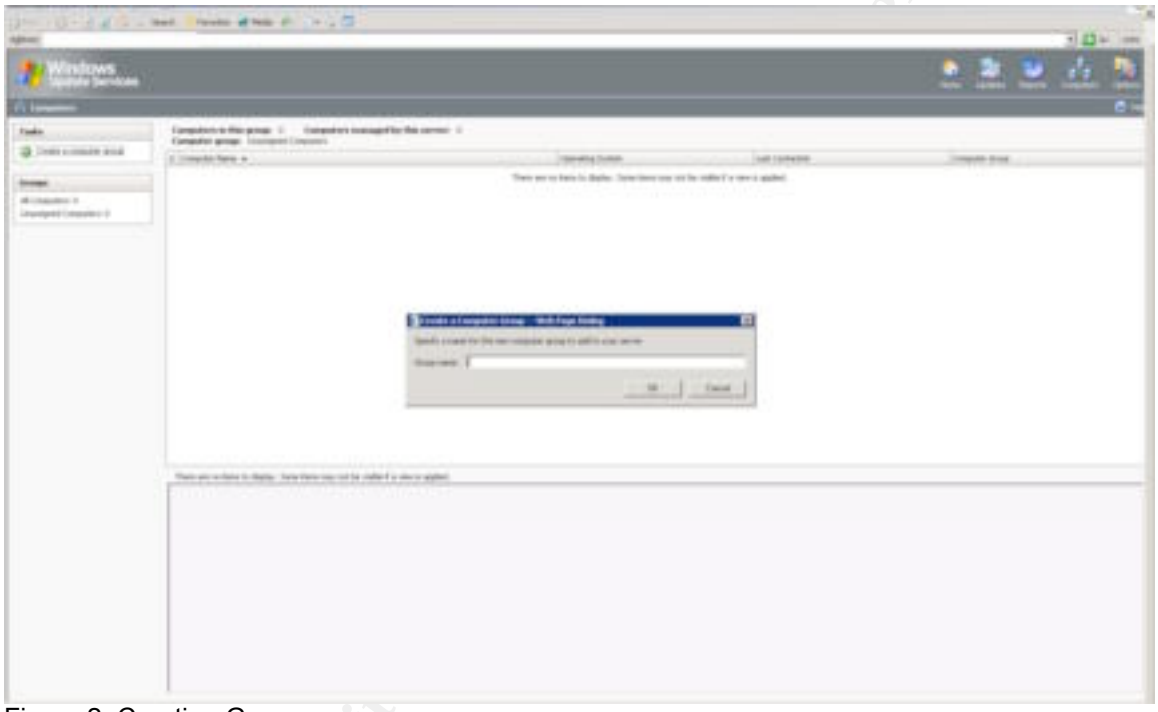

Figure 2: Creating Groups

Group policy can be configured to help with the deployment of updates by creating a standard configuration for the WUS client per OU. This is accomplished by configuring the WUS Administrative Template in group policy found in Windows XP SP2 clients and clients that have already been updated with the latest client via WUS. The template is located in the %windir%\inf directory. This client adds a few options not present in the previous SUS client. One such option ties into the target group spectrum and addresses server-side and client-side target group membership. Server-side target group membership is assigned at the WUS console and client-side target group membership is assigned through Group Policy using the WUS template. When group policy is processed the machine will assign itself to the group you specified. This group cannot be created by the client but must be created previously through the WUS console.

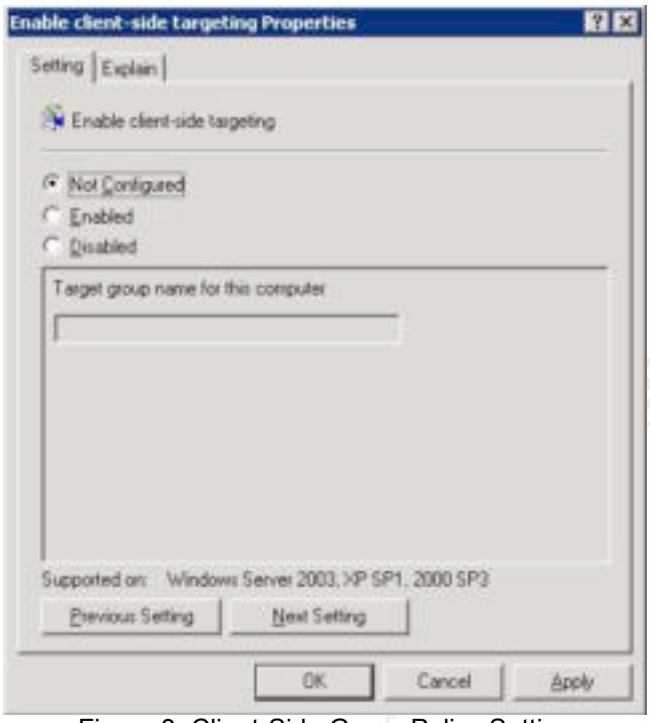

Figure 3: Client-Side Group Policy Setting

An interesting aspect of the target group installation, not covered in the documentation that I can find, is the auto discovery mode or population of computer names into the target group listing. After installing WUS I found myself anxious to get started and created my custom groups. I created groups called IIS Servers, Database Servers, Management Servers and Central File Servers. This gave me six groups (including the two default groups) but no computers to move into these groups could be found. After revisiting this issue a day later I found that the listing had populated with computers on my domain. I can only assume that the auto discovery performed is much like that of Microsoft's SMS product which doesn't automatically populate its listing either, but rather performs an exhaustive check of the network and nodes located on it before reporting back to the administrator. Once the target group list is populated under the All Computers group you may begin moving the systems to their prospective groups by highlighting the system name and clicking on the left menu item labeled Move Selected Computer. A drop down box will appear allowing you to assign that system to your custom group. It turns out that this feature just requires a little time and patience.

Upon completing your computer assignments to their appropriate target groups it is time to move on to some of the WUS settings in order to tweak your installation. By clicking on the Options button and then the Synchronization Options button you are presented with the Products and Classifications settings. When you click the Change button you are presented with a variety of Windows versions, Office versions and Exchange versions. Choose the settings you would like and move on to the Update classifications section and click on the Change button. Here you may choose to update/download Critical Updates,

Development Kits, Drivers, Feature Packs, Guidance, Security Updates, Service Packs, Tools, Update Rollups, Updates and Connectors. Each option corresponds to a description explaining what each classification contains. Critical updates are defined as updates that address a critical but non-security related bug. Development kits are software packages that assist in building applications, such as an editor or compiler. Drivers are software pieces that are necessary to control software packages or the operating system. Feature packs are additions to an existing package that provide additional functionality and are usually included later in that products next full release. The guidance classification is rather unique in that it provides scripts and sample code to help administer, deploy or use Microsoft products. At times it can be very difficult to find just the right script for the job at hand. If a script is found, the script is usually not provided by Microsoft and is not sanctioned by them. These particular updates are a welcome sight indeed. The security updates are ones that help to increase the security of a particular product and they usually address a publicly announced vulnerability. These updates are rated by Microsoft as critical, important, moderate, or low. Service packs are new to WUS and provide the latest cumulative updates for a particular package. Windows XP SP2 can be deployed via WUS and is a great example of a rather large service pack that has the ability to be deployed successfully through WUS. Tools are simply smaller applications that may help with a specific Microsoft application problem. Update rollups are almost like smaller service packs. They don't contain a cumulative set of hot fixes, but rather a specific set of updates targeted for a specific application. General updates are for non-security, non-critical bug fixes and connector(s) updates are pieces of software used to make connections between programs and/or other systems. Figure 4 below displays the Add/Remove Classification screen within the Synchronization Options.

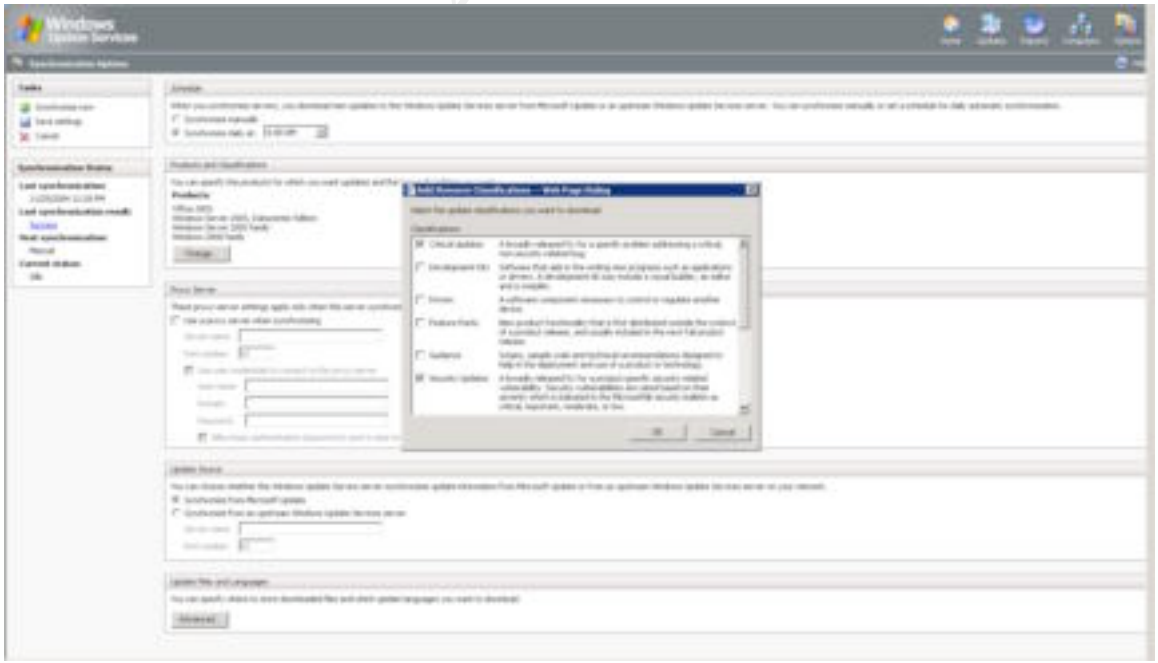

Figure 4: Products and Classifications Screen

Once you complete these settings, WUS must perform an additional synchronization in order to include the additions. Other settings available on this page include when to synchronize, proxy server settings, update source (in the case that you would like to receive updates from an upstream WUS server instead of Microsoft), where to store downloaded files and which languages you would like to download.

This brings us back to our last option for bandwidth conservation. The ability to choose which languages to download is easily one of my favorite options. WUS is able to filter updates as well as assign systems to custom groups. This helps to further organize patches and limit the downloading of unnecessary patches which in turn, assists in the further limitation of bandwidth. I especially found this useful as I did not require updates for all languages. I only require English so I am able to filter out other language packs with a simple click of the mouse. Also, I no longer am required to filter out unneeded language pack patches in the meta-list as I did in SUS. Figure 5 illustrates the filtering window for selecting language locale.

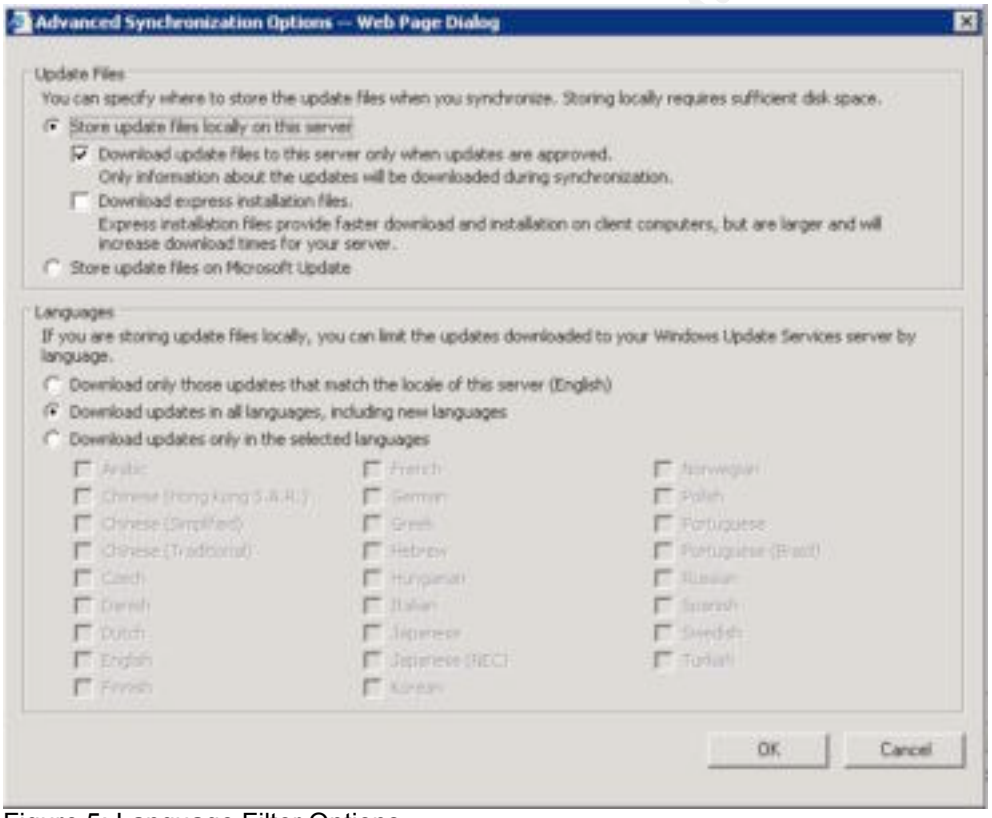

Figure 5: Language Filter Options

The Reports button ties everything together and displays on what has been installed, what is needed to be installed, what has failed and when the report status was last updated. Under the Status of Updates section you may select a specific update and drill down to view all of the target groups associated with that update. From this screen you may click an update on the list to view details, status and revision history for the update.

Clicking on a selected target group will drill down further to display an Approval setting and a Deadline setting. The Approval setting determines if the update was approved for installation or simply for detect only. The Deadline setting determines if there is an installation deadline set for that particular update. You may print the report out by clicking the *Print report* icon on the left hand side of the screen. According to Microsoft's WUS Online Help, "This will print out the status of an update by computer if you have expanded the update in the list of updates. However, you cannot print the dialog box that appears when you click an update on the list."

The Synchronization Results report displays the following sections: Last Synchronization, Synchronization Summary, Errors, New Updates, Revised Updates and Expired Updates. The Synchronization Summary section displays a total numeric value for new updates, revised updates, expired updates and errors. The Errors section displays all errors with a date field, the error that occurred and an update ID to help troubleshoot the cause of the error. The New Updates section displays the newly available updates sorted by title, product, and classification available to WUS. The Revised Updates section displays updates that Microsoft has republished for deployment. This occurs when Microsoft finds an additional bug to the update or an inconsistency in compliance to the previous update. The Expired Updates section displays updates that are no longer valid for deployment. This may be due to a now available rollup package, a service pack or a revised update that Microsoft has deemed more appropriate to deploy in your production environment.

The Settings Summary is a report outlining all the available settings in WUS and your currently selected options. This is a great page to go to when you want to double check all of your global settings or if you can't remember what option you set for a particular function and simply want to review. This allows you to visit one page rather than digging through the entire application searching for that particular section. You may also choose to print this page out for a record in case of a disaster scenario or for future WUS deployments to keep the same settings from a previous installation.

Windows Update Services makes a giant leap into patch management for Microsoft products. The software is free to use and is suitable for both large corporations with its scalability, but yet is intuitive enough for small businesses. Microsoft has taken the first step to securing its software in a manageable way in hopes of stabilizing its customers and silencing its critics. I, for one, am encouraged by Microsoft's bold steps in regard to their security initiative and hope to see improvements to WUS in the near future that will further enhance an already outstanding product. Future enhancements may include support for third party product updates, delegation of administrative privileges for tasks such as approving updates, scheduled reboots and more advanced reporting mechanisms.

References

1. Microsoft Windows Update Services Online Help
2. Deploying Microsoft Windows Update Services – http://www.microsoft.com/windowsserversystem/wus/deployment.mspx
3. Security Wire Digest - http://infosecuritymag.techtarget.com/ss/0,295812,sid6_iss125,00.html
4. Slate – http://slate.msn.com/id/2103152/
5. WUS Wiki - http://wus.editme.com/
6. SUSserver Forums - http://forums.susserver.com/index.php?showforum=11
7. Security Guidance - http://www.microsoft.com/technet/security/guidance/secmod193.mspx#ECAA