



**AIDAN FINN**

27/09/2006

# Microsoft WSUS 3.0

*Automated Patching – The First Step To Secure Your Network*

## *Abstract*

This whitepaper will discuss the importance of maintaining patch deployment, strategies and how to utilise Microsoft's Windows Server Update Services 3.0 as a solution. This whitepaper is based on the beta release of the product.

---

## Table of Contents

---

Table of Contents.....	2
Introduction.....	3
Alternative Solutions.....	4
Introducing WSUS 3.0.....	5
WSUS 3.0 Features.....	5
Requirements .....	5
Deployment Scenarios .....	7
A Small Network .....	7
Medium Network with Independent Control.....	8
Medium/Large Single Infrastructure .....	9
Networks with No Connectivity .....	10
Upgrading WSUS 2.0 .....	10
Installing WSUS 3.0.....	11
The WSUS 3.0 Configuration Wizard .....	17
The WSUS 3.0 Administration Console.....	24
Configuring WSUS Clients.....	36
The Approval Process .....	36
Installation Configuration .....	36
Summary.....	38

---

## Introduction

---

When people think about IT security, they think about firewalls and antivirus. Firewalls are important but only go so far as to protect your network against a direct attack. A firewall will only prevent illegitimate forms of traffic from the internet. It doesn't stop traffic on legitimate ports or downloads. Firewall defences have been compared to eggs: hard on the outside but soft on the inside. Anti-virus will only protect you against known threats. Many organisations have made the mistake of thinking that firewalls combined with antivirus will give them a complete defence against threats. That's a nice wish but it's not true.

Consider the SQL Slammer virus that hit the Internet in early 2003. Within minutes of its release it crippled networks worldwide. How did this work? Surely people had firewalls in place? Yes they did. Was the antivirus up to date? Yes it was. The problem was that once it could easily get past the firewall and it was unknown to antivirus vendors. It also took advantage of a known flaw in Microsoft's products that Microsoft had previously released a patch for. In fact they released the patch several months before hand and those organisations that had deployed it were protected against the virus. Microsoft had already released a free to use product called SUS that serviced the Windows product range but few had heard of it. In fact, few had any implemented process for regularly testing and deploying Microsoft updates.

In late 2003 a new virus started to cripple networks. Microsoft Blaster took advantage of a flaw in the RPC service. Surely in the time that had passed people had learned their lessons about keeping their machines up to date? It appeared that most had not. Microsoft had previously released an update to protect their products but few had deployed it.

Since this time Microsoft has spent much time campaigning and trying to raise customer awareness about the need to regularly test and deploy updates. A replacement for SUS called WSUS (2.0) was released. WSUS, again a free to use product, services all of the Microsoft product range and makes it easier for administrators or security officers to test and deploy updates on a production network.

My experience working on client sites and speaking with administrators is that both the awareness of this problem/solution and adoption of WSUS have been minimal. Many large organisation and government agencies do not maintain patch updates. This is either because they are not aware the solution exists, despites Microsoft's efforts, or because they do not sufficiently understand the problem.

With this document I aim to show how you can manage updating your entire Microsoft network with minimal manual effort by using WSUS 3.0.

---

## Alternative Solutions

---

It would be wrong for me to continue as if WSUS 3.0 was the only solution to this problem. Microsoft WSUS (which will likely be referred to as WSUS 2.0) is available at the moment and is an excellent product. It is lightweight so it can be run on a virtual machine. It is simple to use and highly scalable.

Microsoft also provides the ability to deploy updates using 2 free to download feature packs for Systems Management Server 2003. I have tried this solution but I must say that while it is very flexible and powerful, I find it to be very labour intensive to use and manage. However, I am a fan of using it the feature pack to audit and report on patch deployment success. Microsoft do state that this is their solution for large networks. Remember, Microsoft think of a large network as being something with 10,000+ managed computers.

Microsoft will be releasing the successor to SMS 2003 next year called System Centre Configuration Manager 2007. SCCM 2007 has built in functionality for deploying software updates to Microsoft products. It is extendable just like WSUS and it is a huge improvement over SMS 2003 software updates. It offers powerful scheduling, targeting and is more efficient to use than SMS 2003 if you make use of templates. However, I am left thinking that for most organisations, WSUS may still be a better solution.

A famous third party solution is HFNetChkPro. This product must be purchased. It has been around since the days of Windows NT and is very mature. Many of its customers prefer it over the free solutions from Microsoft. HFNetChkPro offers built in support for updating non-Microsoft products which does give it a distinct advantage.

Given the available options why do I still stick with WSUS? Well, it's lightweight, free, easy to use and highly scalable. Given that it is so lightweight, I choose to run it on a virtual machine, this saving on hardware costs and possible operating system costs if I use Windows 2003 R2 Enterprise as the host. Microsoft also intends to make it the basis of all of their deployment solutions. What do I mean? Consider all of the products you have that must have updates... Email antivirus/anti-spam updates, anti-spyware updates, server/desktop antivirus updates, etc. Microsoft have stated that it is their intention to use WSUS as their update mechanism for their products. This means that products such as Forefront Security for Exchange, Microsoft Antivirus, and Defender all will update via WSUS. A single update mechanism that is controlled via group policy will simplify the network and reduce the amount of configuration, maintenance and troubleshooting. In my opinion, this makes WSUS the natural choice.

---

## Introducing WSUS 3.0

---

As I am writing this document, WSUS 3.0 has just gone into public beta. If it will progress like WSUS 2.0 did, then any lessons we learn during the beta process will hold true for the RTM version.

### WSUS 3.0 Features

Naturally, a new version means new features. Here's a quick breakdown of what to expect:

- WSUS 3.0 introduces an MMC snap-in for managing your WSUS infrastructure.
- A post-setup wizard will guide an administrator through most of the necessary configuration.
- The logs are more detailed. A MOM management pack is available.
- Automated email notifications can be enabled for new updates.
- A cleanup wizard allows you to clean out obsolete data.
- Upgrading to WSUS 3.0 is a simple in place installation, a vast improvement over SUS to WSUS 2.0.
- Update checks can happen up to once per hour, an improvement over once per day.
- A granular rule system for automated approval has been introduced. You now could automatically approve updates for certain products or maybe even severity levels.
- You can grant someone the ability to have "Read only reporting", e.g. to a non-technical security officer or auditor.
- Many servers can be managed from your single administration console. This is important for anyone managing lots of WSUS servers.
- WSUS 3.0 can be clustered, possibly important in large, security critical environments.
- A WSUS 3.0 server can be switched from replica to autonomous mode without needing to uninstall. This adds flexibility to your infrastructure.
- Clients can be a member of numerous targeting groups, reflecting how the real world works.
- There is support for running WSUS 3.0 on x64 Windows.
- A branch office can download a subset of languages from the master WSUS server.
- A branch office can download metadata (approvals, etc) from the central WSUS server but download updates directly from Microsoft, e.g. if the branch has limited WAN bandwidth but generous Internet bandwidth.

### Requirements

#### WSUS Servers

- Windows Server 2003 Service Pack 1 or Windows Server "Longhorn" Beta 2
- Microsoft Internet Information Services (IIS) 6.0 or later

- 
- Background Intelligent Transfer service (BITS) 2.0 or later
  - Windows Installer 3.1 or later
  - Microsoft .NET Framework 2.0

#### *Optional Prerequisites*

- Microsoft Management Console 3.0
- SQL Server 2005 Service Pack 1
- Microsoft Report Viewer Redistributable 2005

#### **WSUS Client Computers**

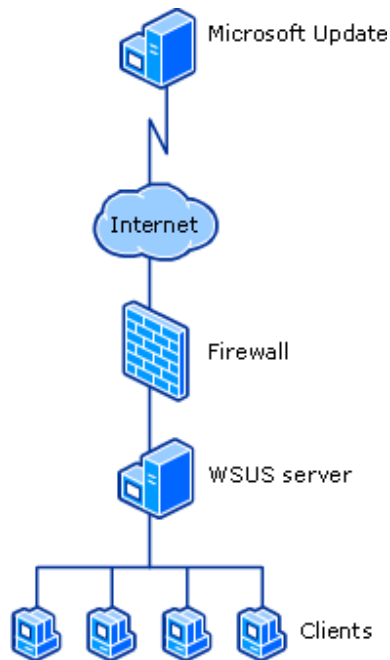
- Windows Vista Beta 2
- Windows Server 2003 (any edition)
- Windows XP
- Windows 2000 with Service Pack 4.

---

## Deployment Scenarios

Microsoft's aim was for WSUS and WSUS 3.0 to be deployable in all sorts of organizations or networks whether they are small, medium, huge, LAN, WAN or disconnected.

### A Small Network

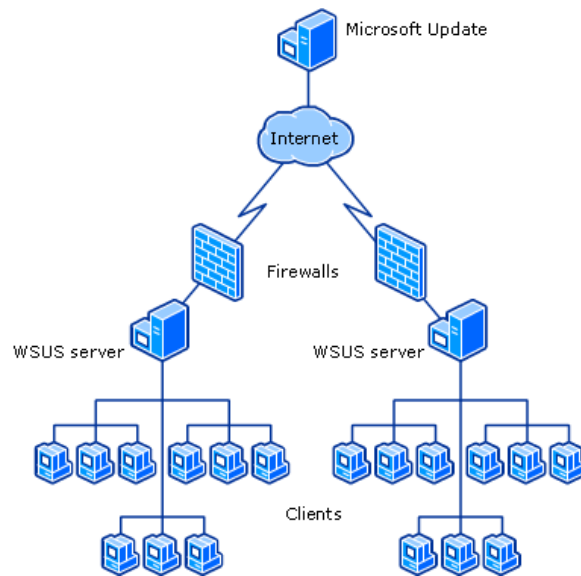


Microsoft's definition of small is a lot different to most. For Microsoft 200 computers is a small deployment. In this scenario, a single WSUS server downloads updates directly from Microsoft. Administration is easy with a single point of administration.

*Note: For this size of network, I've successfully run WSUS 2.0 on Microsoft Virtual Server 2005 virtual machine.*

---

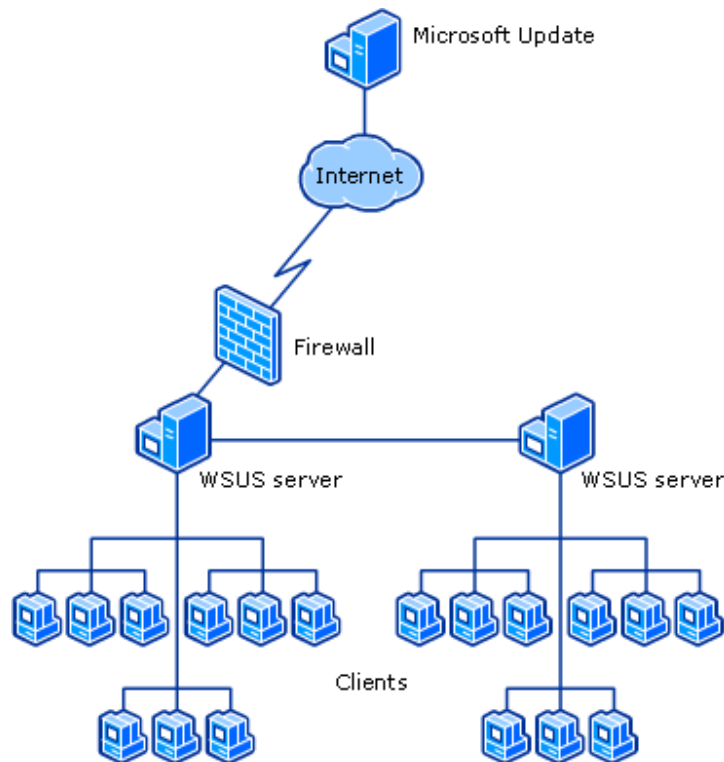
## Medium Network with Independent Control



In this scenario, each WSUS server directly updates from Microsoft. Administration is carried out on two WSUS servers, this doubling the amount of administrative effort. While not efficient, it may be required where internal politics are a factor or where there is no or limited connectivity between sites.

---

## Medium/Large Single Infrastructure



This is the best deployment solution where there is a single security policy. It is efficient because:

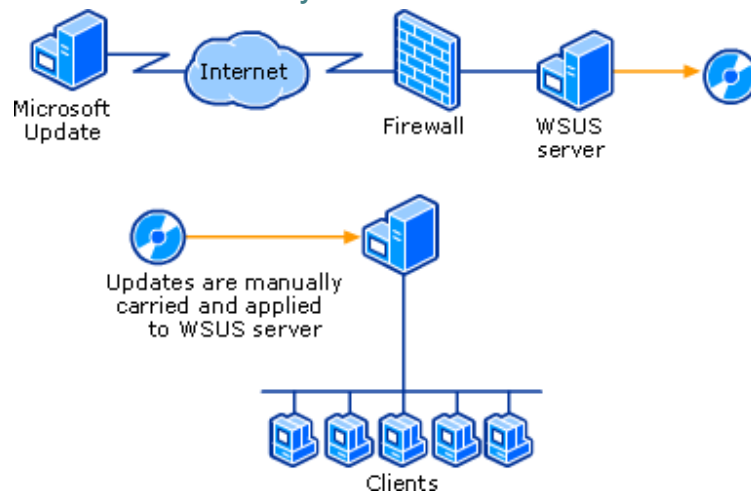
- The internet connection is used only once to download updates.
- Administrative effort is minimised; all administration, i.e. update testing/approval, is performed at the WSUS server that is the point of entry.

WSUS clients have the location of their WSUS server configured by an Active Directory site-linked Group Policy Object. This means that if client A travels from site 1 to site 2, it will access download updates from the WSUS server in Site 2 instead across the WAN.

In this diagram, Site A is the root and Site B has a downstream server. There may be a scenario where you want centralized management of Site B but it has (1) limited connectivity to site A and (2) good connectivity to the Internet. In this scenario, it is possible to configure Site B to download only metadata and the approval list from Site A. All approved updates will be downloaded directly from Microsoft over the Internet.

---

## Networks with No Connectivity



This scenario is likely to include DMZ's (although Microsoft would like us to drop that concept) and special secure networks that may be found in government agencies or organisations with sensitive materials that cannot be placed on the WAN.

Updates are tested, approved and downloaded. They are exported onto CD and then uploaded onto another WSUS server for distribution to clients on the disconnected network.

## Upgrading WSUS 2.0

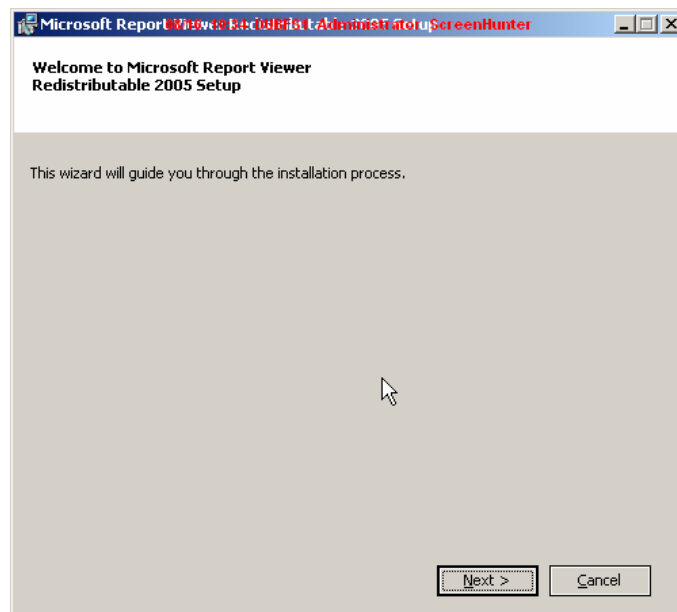
The upgrade process from WSUS 2.0 to 3.0 is seamless; good news to anyone who upgraded from SUS to WSUS 2.0. An in-place upgrade from WSUS 2.0 to 3.0 will maintain all settings and approvals.

To upgrade a hierarchy of WSUS 2.0 servers, start at the root server and work your way down. WSUS 2.0 can synchronise from WSUS 3.0. WSUS 3.0 *cannot* synchronise from WSUS 2.0.

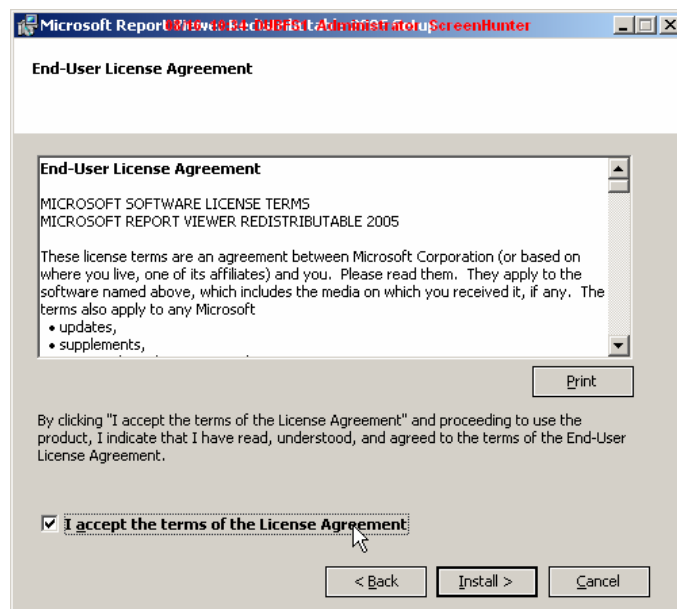
---

## Installing WSUS 3.0

You need to ensure each of the Windows prerequisites (see above) is installed. One of the other prerequisites is the Microsoft Report Viewer.



Start the report viewer installation.

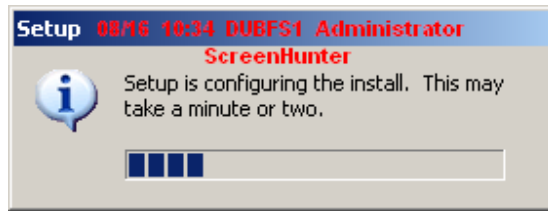


Agree to the EULA.

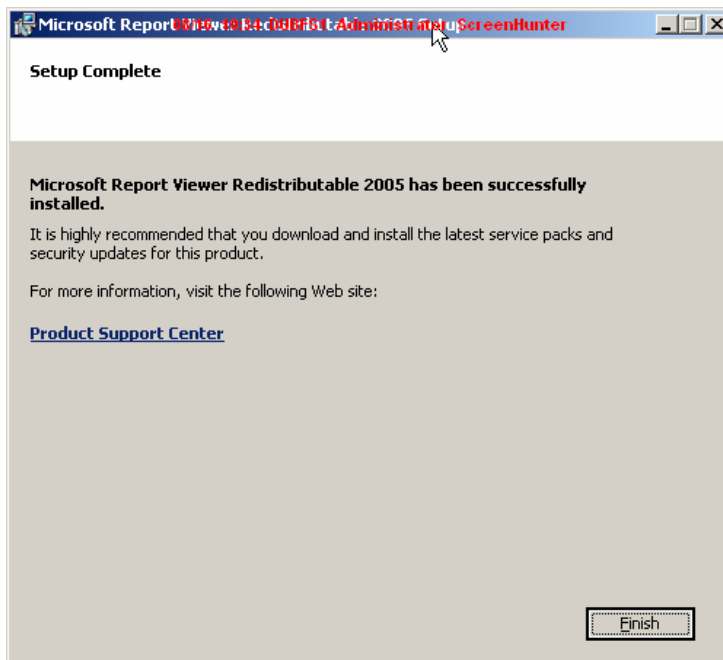
Microsoft WSUS 3.0

Copyright Aidan Finn 2006

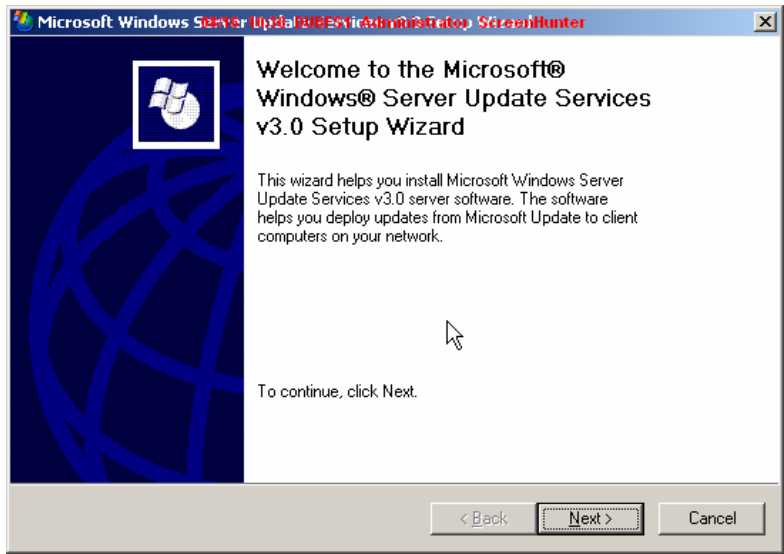
<http://joelway.spaces.live.com/>



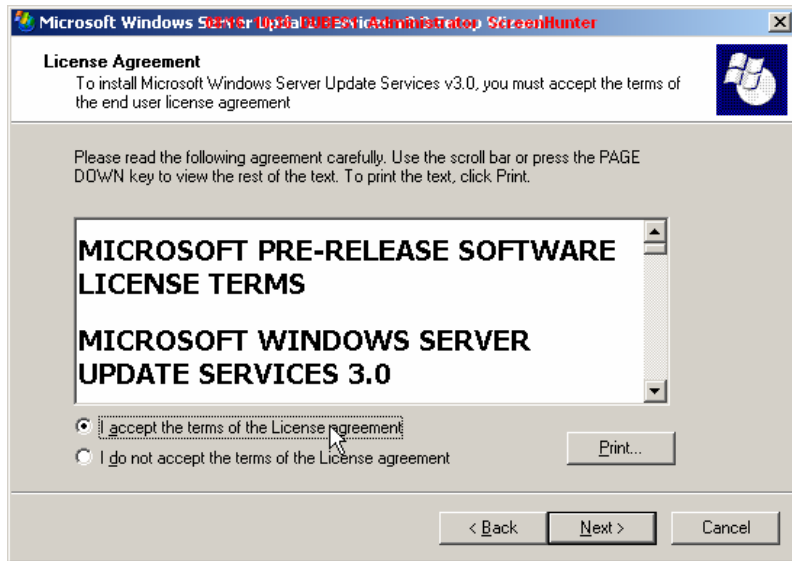
The installation will start.



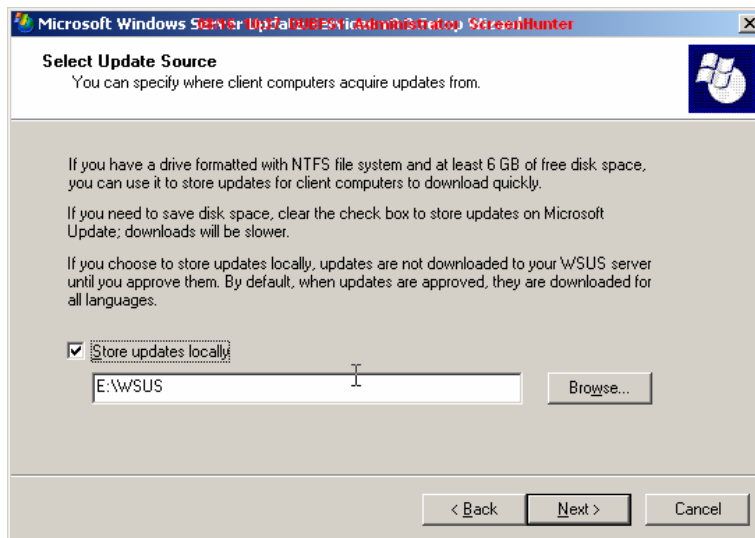
As you can see, it's a simple install. Next you will start the installation of WSUS 3.0. You'll need to download that.



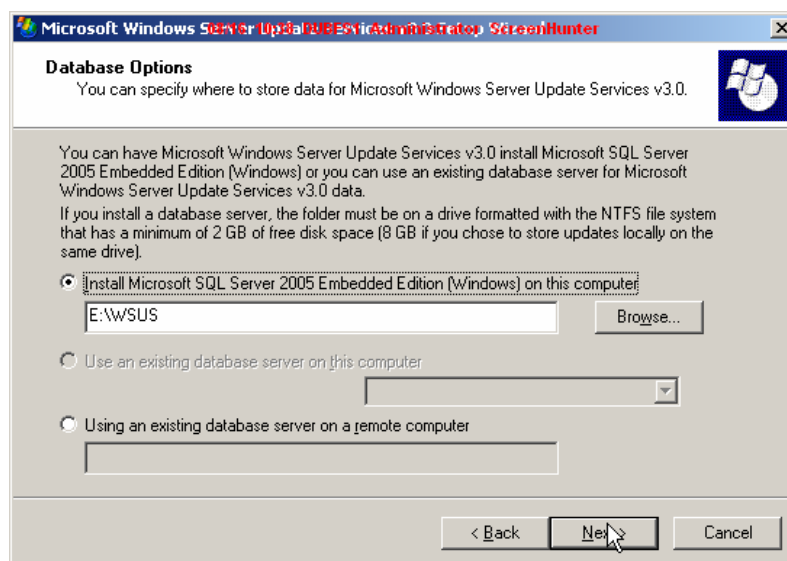
Start the installer.



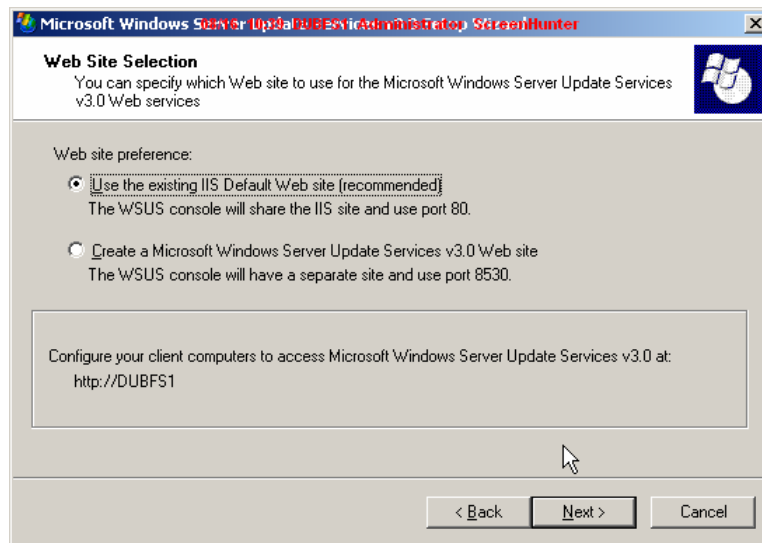
Agree to the EULA.



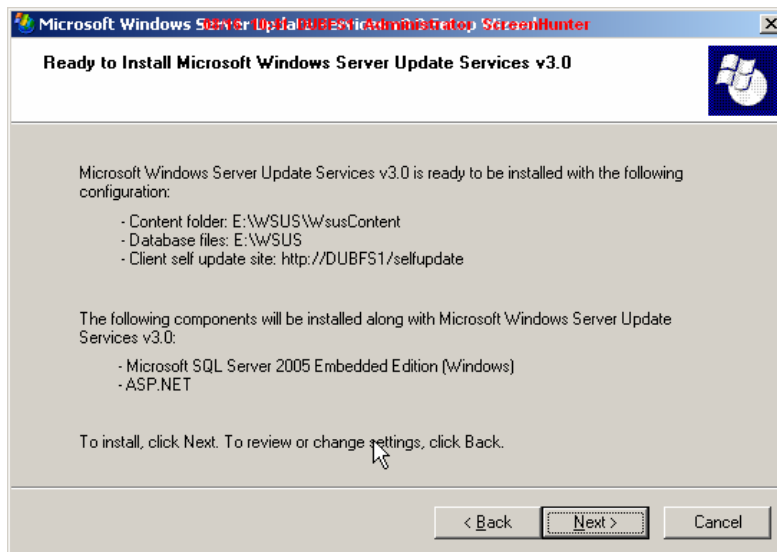
Your first decision is where to store the updates. I can't see 30GB ever being used up. My current WSUS 2.0 server is using less than 10GB.



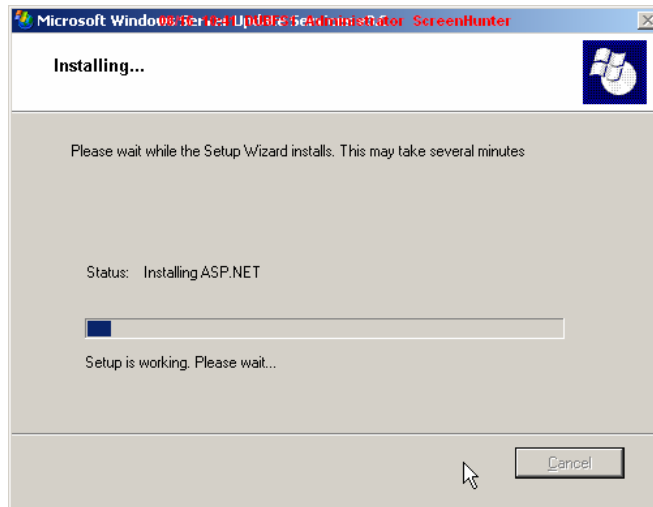
You now need to choose how you will set up your SQL database for the WSUS data. In this example I've used SQL 2005 Embedded Edition. It's like MSDE and supplied with WSUS. You could use another dedicated SQL database but I'm a "keep it simple" person so I like the built in option.



Anyone familiar with WSUS 2.0 will know this screen. What port do you want to run WSUS on? If your WSUS server runs another website then you should choose 8530. Again, I'm simple and I want a port I can remember. I'd recommend a VM for the WSUS installation so I won't have any other applications running on WSUS server. So I choose the default port of 80.



Click on <Next> when you are ready to start the installation.



At this point you can go get some coffee.

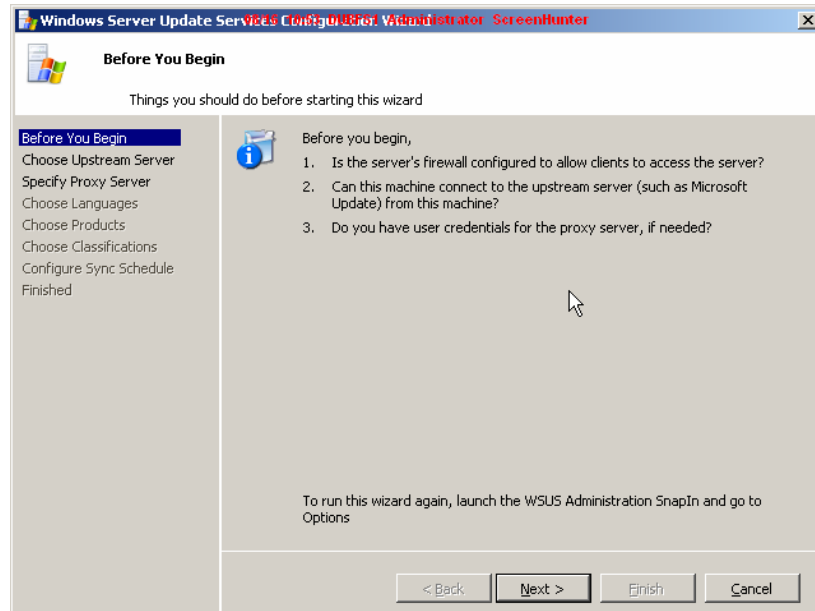


As the French say, "Voilà!" WSUS is now installed and ready to be configured. Note you have an option to configure WSUS from a wizard. This is new and welcome. You don't have to go bounding from one page to the next on a web interface to configure it any longer.

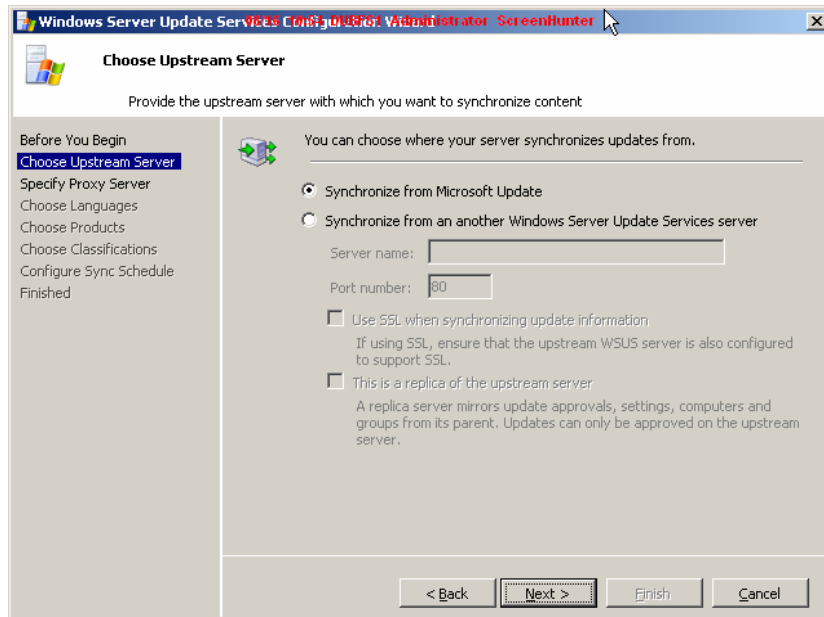
---

## The WSUS 3.0 Configuration Wizard

---



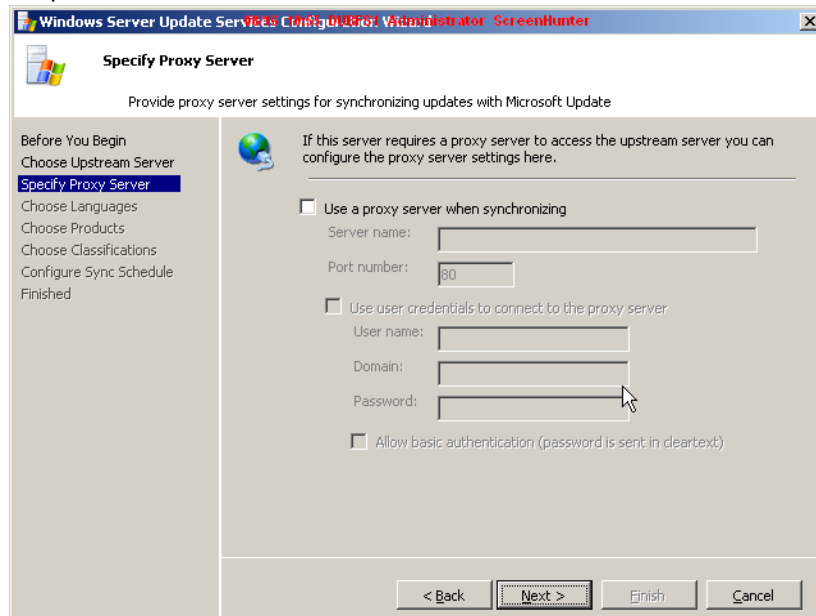
Microsoft wants you to check a few things first. Make sure your website port (80 in this case) can be accessed by WSUS clients. This is vital if you run Windows Firewall. Make sure your WSUS server has connectivity to Microsoft or to a possible upstream server so updates can be downloaded. Finally, if this is the entry/root WSUS server then make sure you have credentials for the proxy if required. I always recommend dedicated service accounts for simpler diagnostics and to limit damage if passwords get leaked.



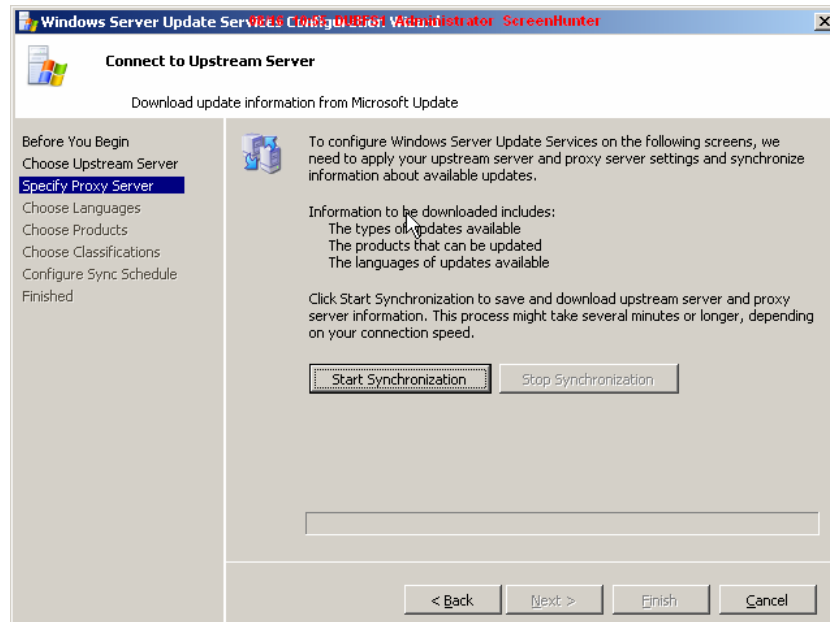
Here's your chance to decide if this server will be a downstream server (gets updates from an upstream WSUS server on your network) or will be the root WSUS server.

If this is a downstream server:

- You can choose to use SSL if the upstream server requires it.
- Make this a replica of the upstream server. This is how you can centralise management to your upstream or root servers.

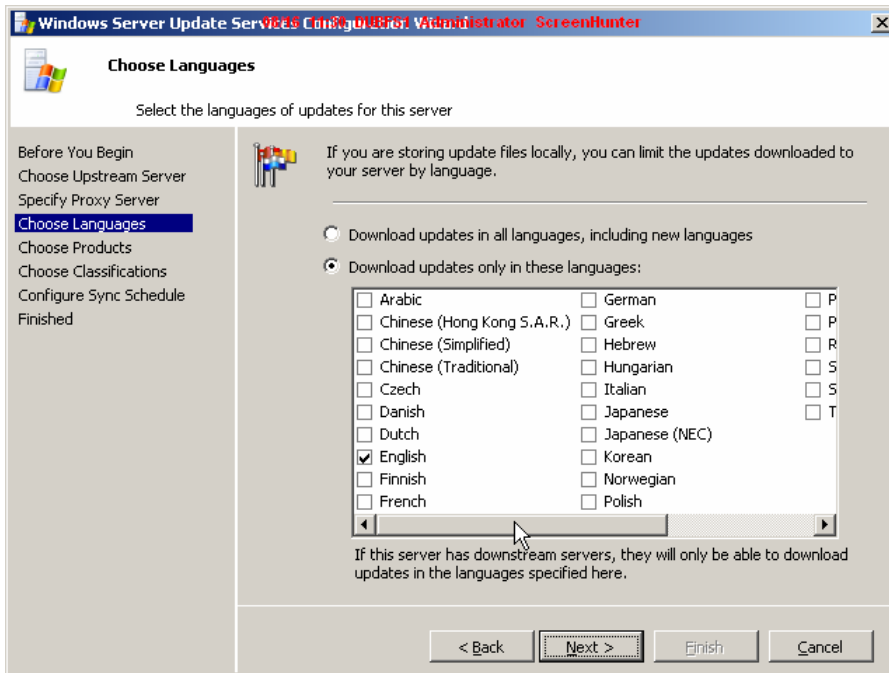


Enter any required credentials to enable your new WSUS server to get through a proxy. Please do not use your user account or an administrator account. That's a really bad idea. Use a dedicated service account.

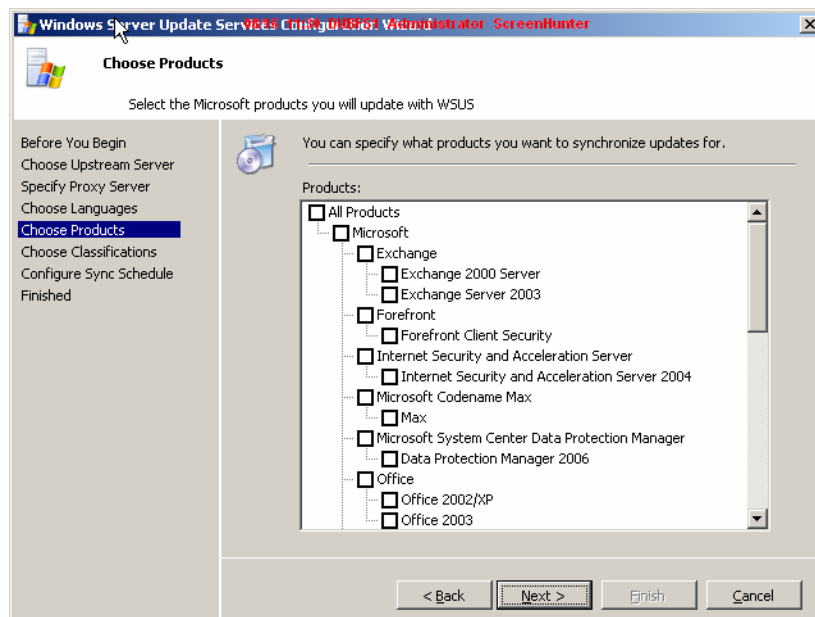


You can now start your initial synchronisation. This will only download the necessary information to complete the wizard. It will not download an updates or metadata about any updates. Note that it only intends to download information about:

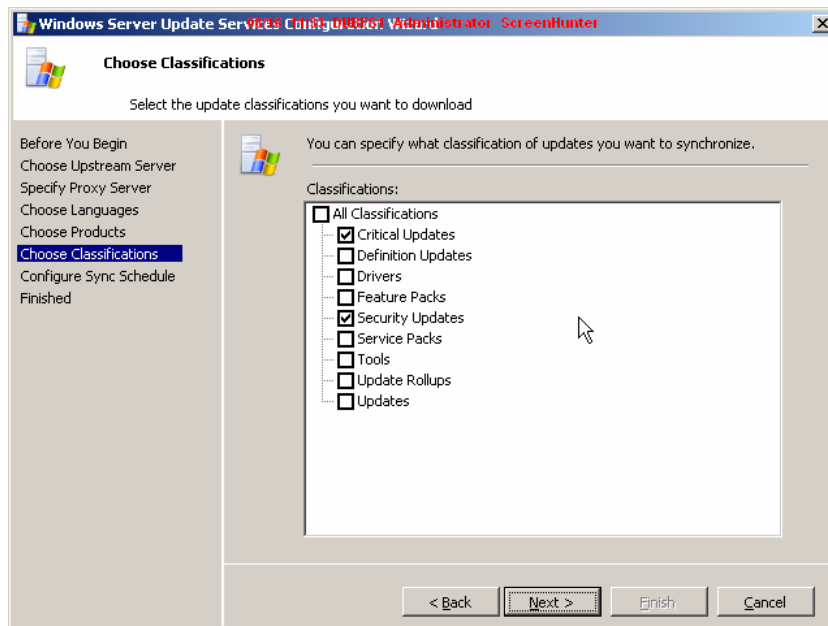
- The types of updates available, e.g. critical, important, etc.
- The products WSUS can update.
- The languages that WSUS can download updates for.



Pick and choose the languages you want to download updates for here.

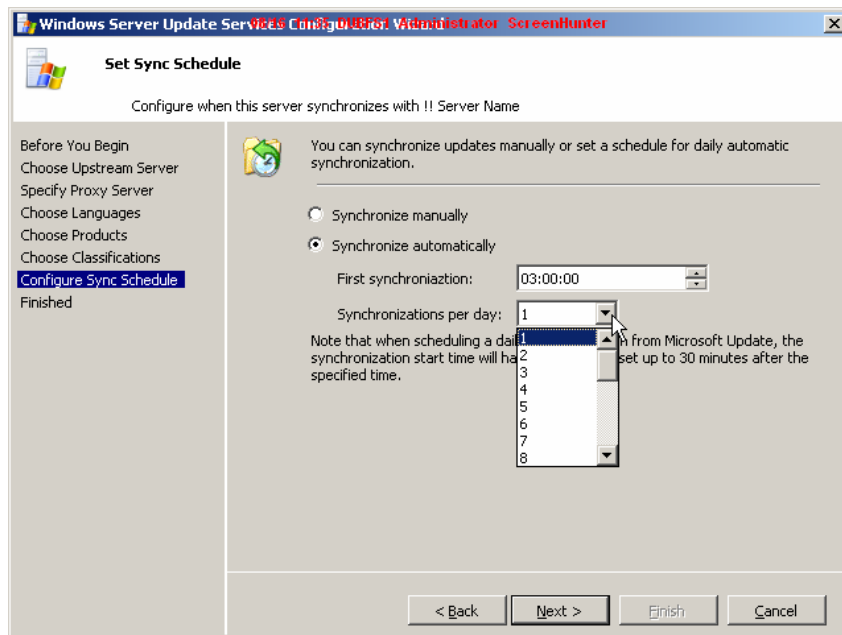


This screen allows us to pick what products on our network we wish to update via WSUS. I'd highly recommend that you only pick those products you have. It'll save you a lot of administrative effort later on instead of being lazy now and choosing "All Products".

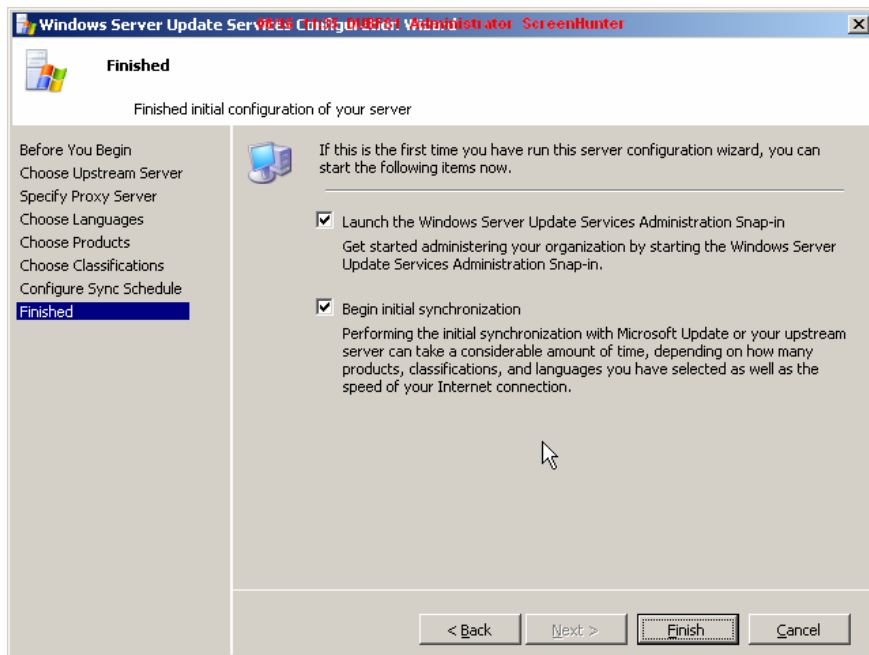


You can choose with types of update you want to download. Be careful of downloading service packs. Firstly, they can be huge and take an eternity to replicate across a WAN with limited bandwidth. I had a lot of problems with replicating Windows 2003 Service Pack 1 to our WSUS 2.0 servers when it came out. We have 16 sites replicating with one central server and the central site WAN link was bottlenecked. This caused each of the sites to fail the download so we had to suspend replication for all but one each night until all were replicated. Secondly, you don't want to risk a service pack being accidentally approved when you haven't tested it. Imagine your surprise if something like Windows Firewall appeared on all of your machines (as with XP Service Pack 2) and you weren't ready for it. That would be a P45/Pink Slip generating event.

Be careful of downloading updates too. It may conflict with any SMS feature packs you have from the likes of HP or Dell.



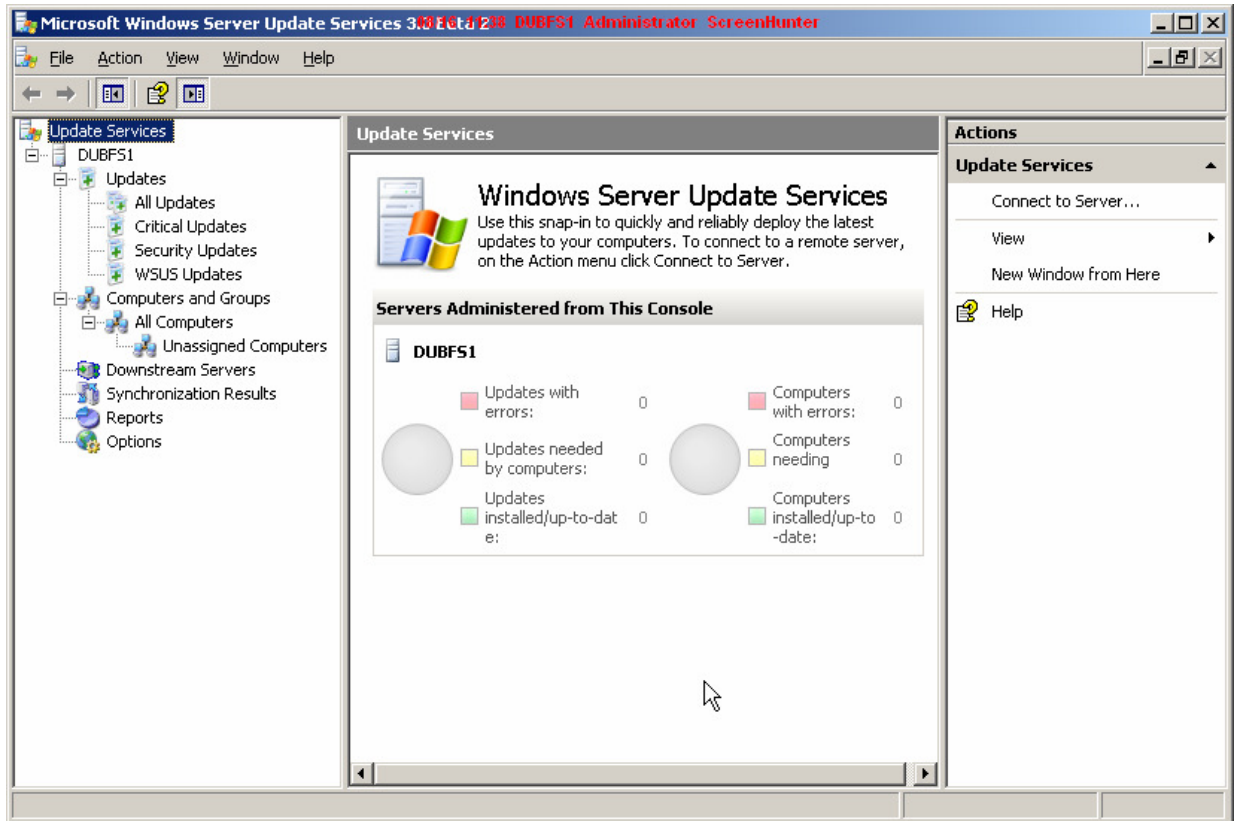
You now can configure your replication. We have the historical “choose a time of day” option here. But we also have something new. Microsoft has put in an addition option to check for updates every X hours during the day. This is probably in case they have to release an emergency patch for a critical zero day exploit. If it’s not going to place much of a load on the network then I would recommend setting this to every 1 hour.



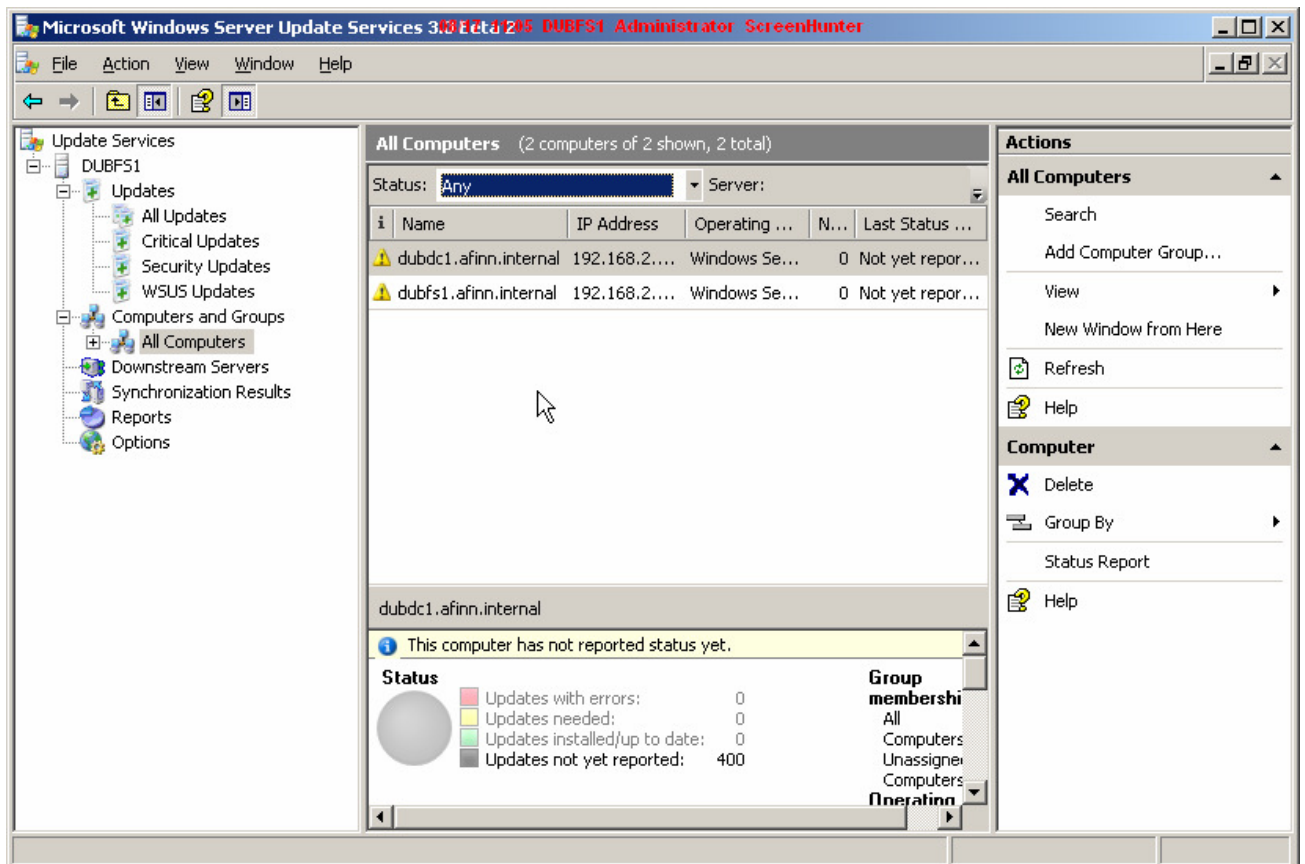
We are now nearing the end of the wizard. All of the wizard configurations are complete. We can now kick off an initial synchronisation to download update metadata. This will consist of descriptions of each available update in our selection. We can then deny or approve each update. Approval will lead to the update being downloaded from Microsoft.

The second option will start the new administrative console which is an MMC snap-in instead of the traditional web interface we have had with SUS and WSUS 2.0. Note that the old web interface is not present in Beta 1 of WSUS 3.0. I assume it is gone forever to be replaced by the MMC interface.

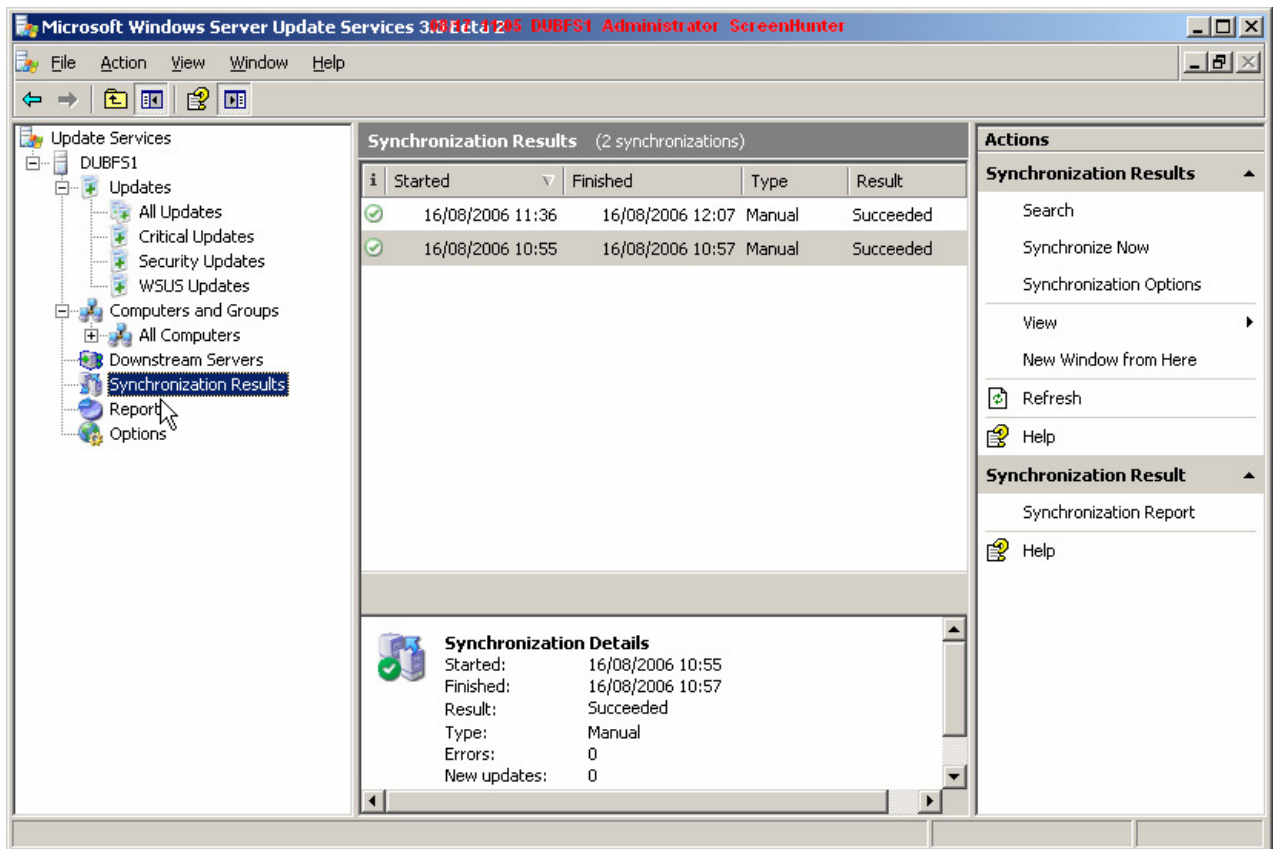
## The WSUS 3.0 Administration Console



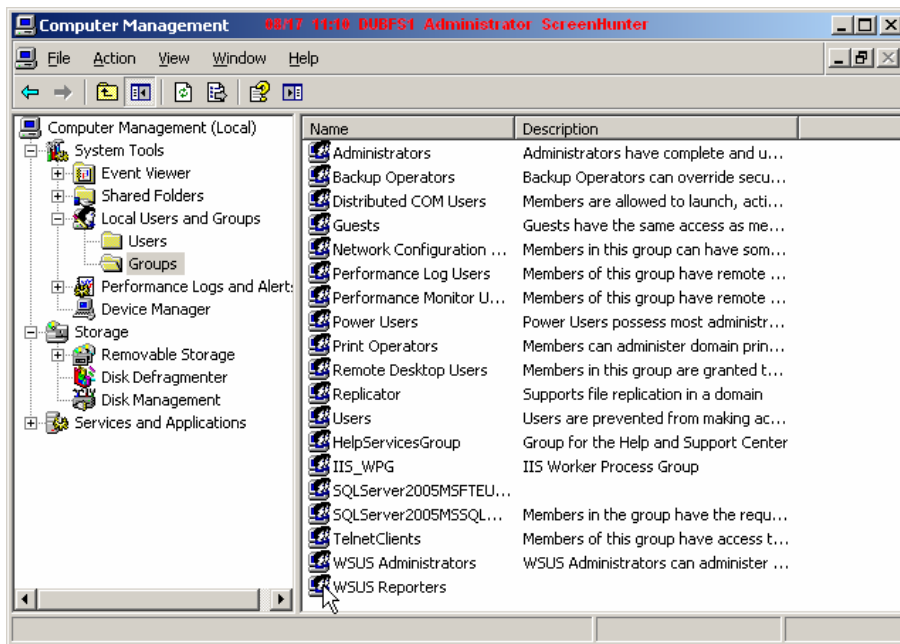
This is the new administration interface for WSUS. It's an MMC 3 snap-in so you'll need to update MMC on your administrative PC's. Anyone new to MMC 3 will notice that the centre pane is capable of doing a lot more and there is a context sensitive Actions pane. The Actions pane shows the stuff you get when you right click on something.



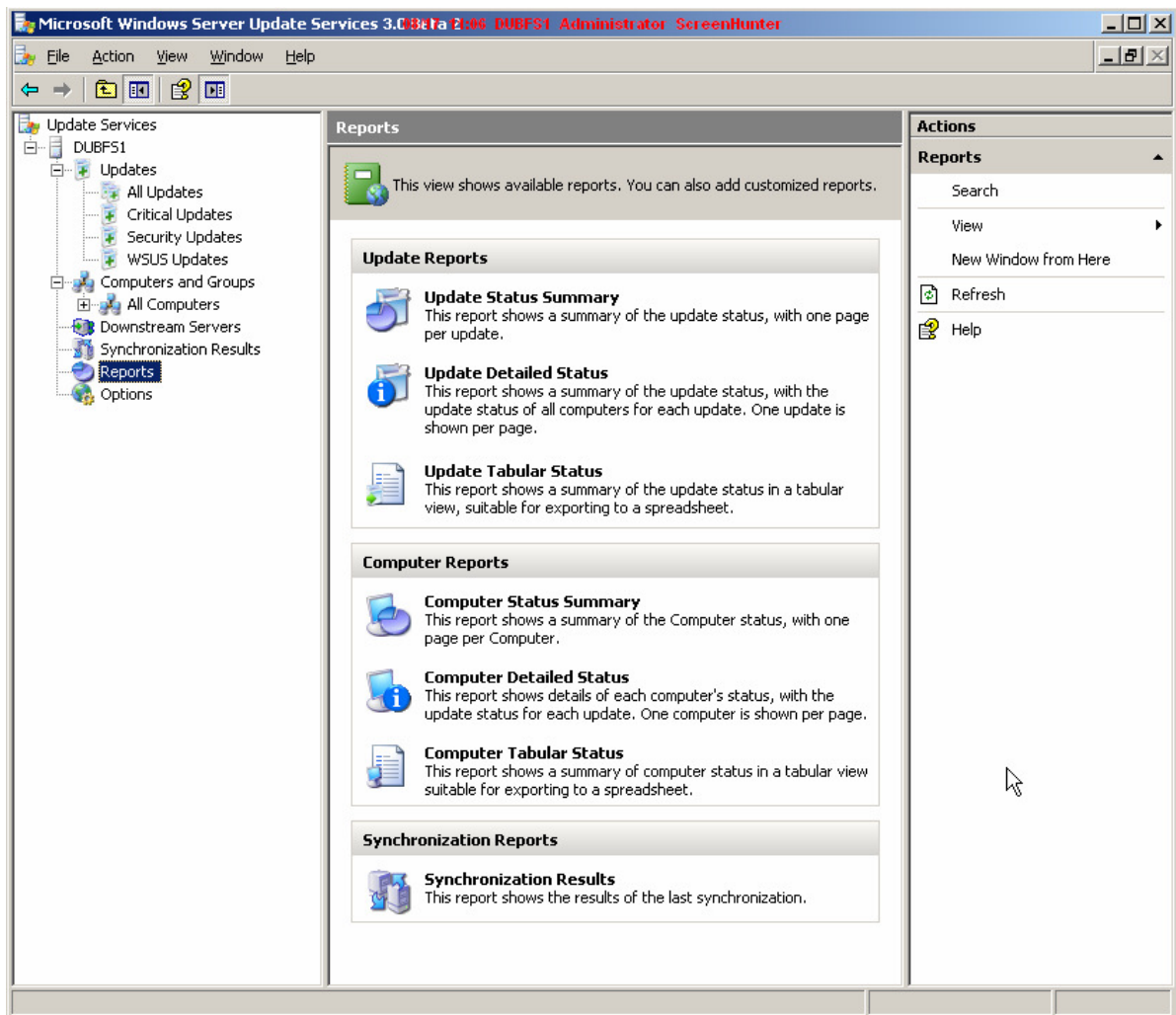
All Computers is selected above. This is a quick way of checking the deployment status of updates. You can change the selection in the dropdown box to different status types. This will present a different list of computers. You can double click on a computer to launch Report Viewer for more information.



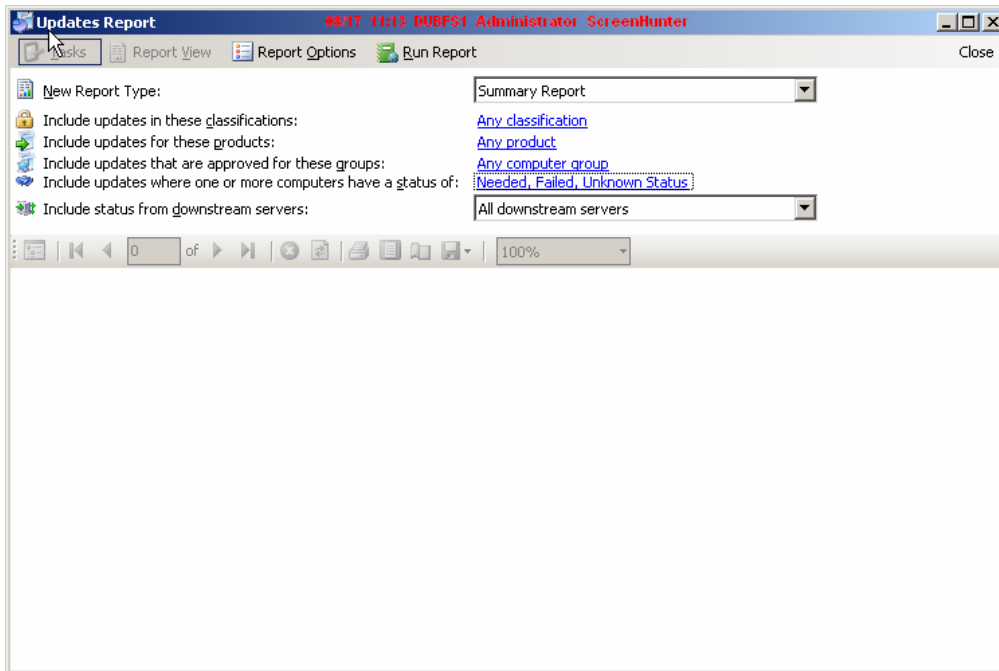
Synchronisation Results shows you just that ... the results of synchronisation. It keeps a history.



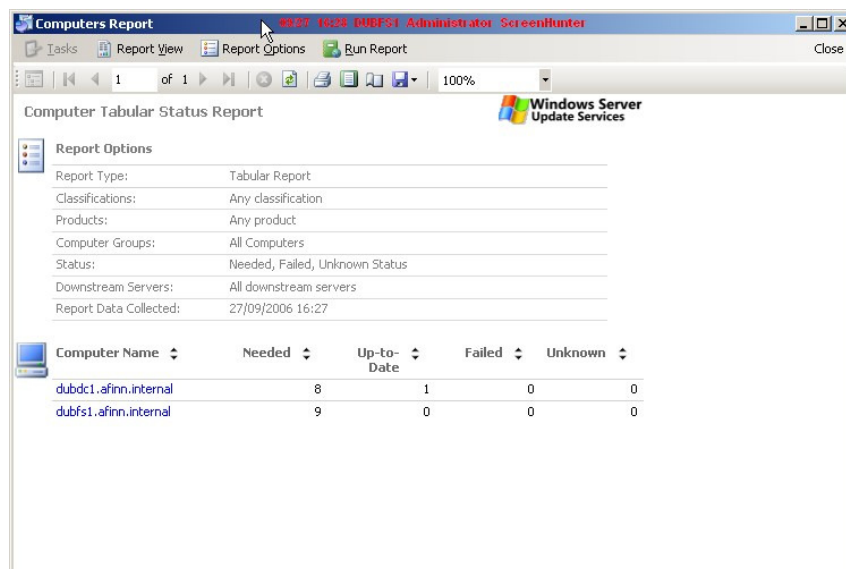
I've jumped out of WSUS here to show you two new groups on the WSUS server. WSUS Administrators have the right to fully manage WSUS. WSUS Reporters is new ... it gives you the right to give selected people (auditors, management, security officers) the ability to run read only reports from WSUS.



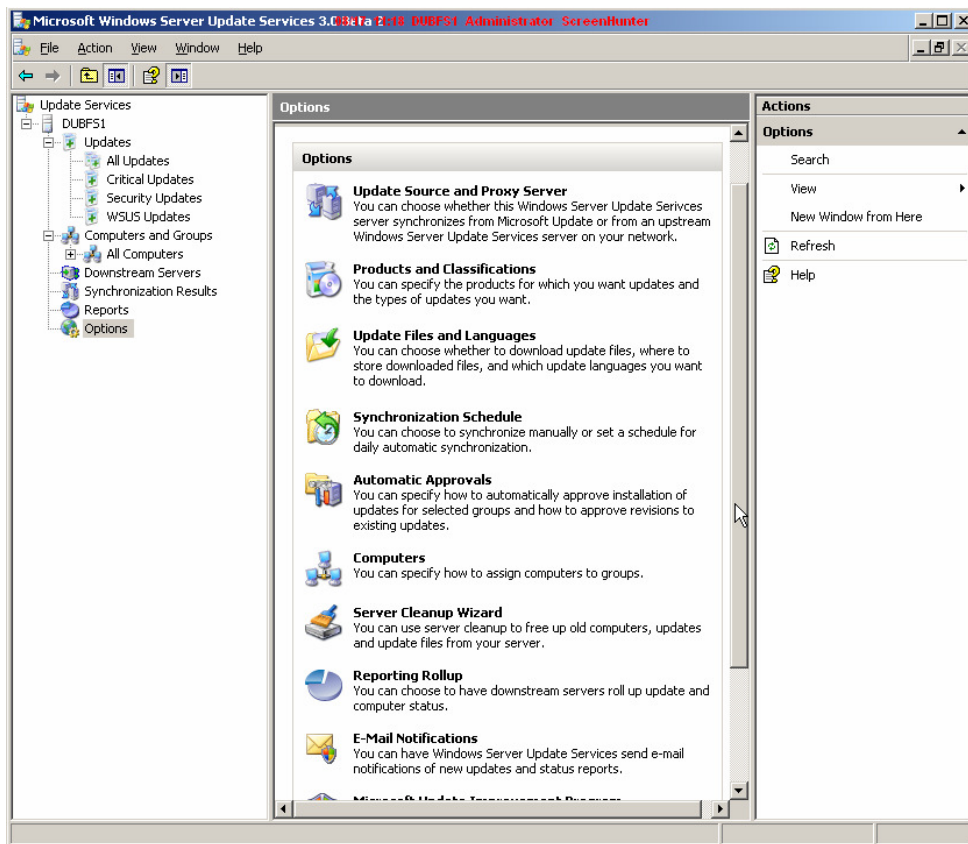
Here we can see the various reports that are available. Clicking one will kick off Report Viewer.



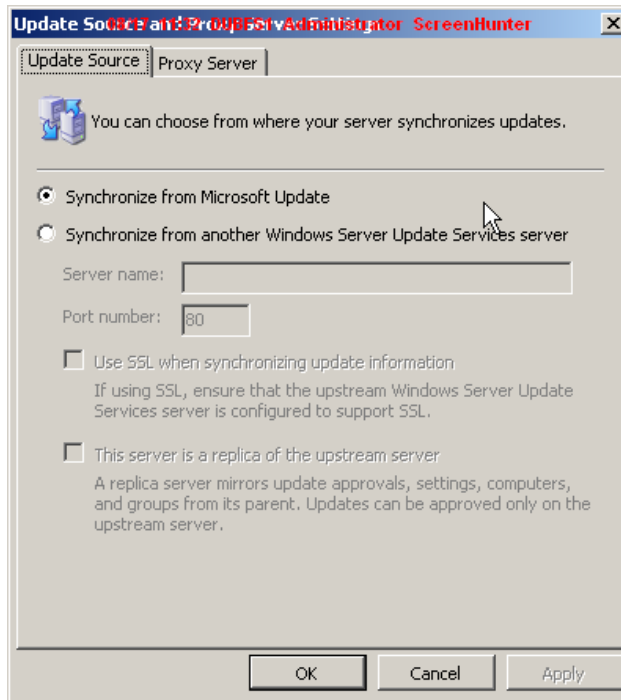
Report Viewer is running and you can see it's kept the look and feel of SQL Reporting Services. Selecting one of the items in blue text or the drop down box allows you to configure the query that will make up the report. Note that your report will include data from downstream servers, emphasizing the idea of centralised management.



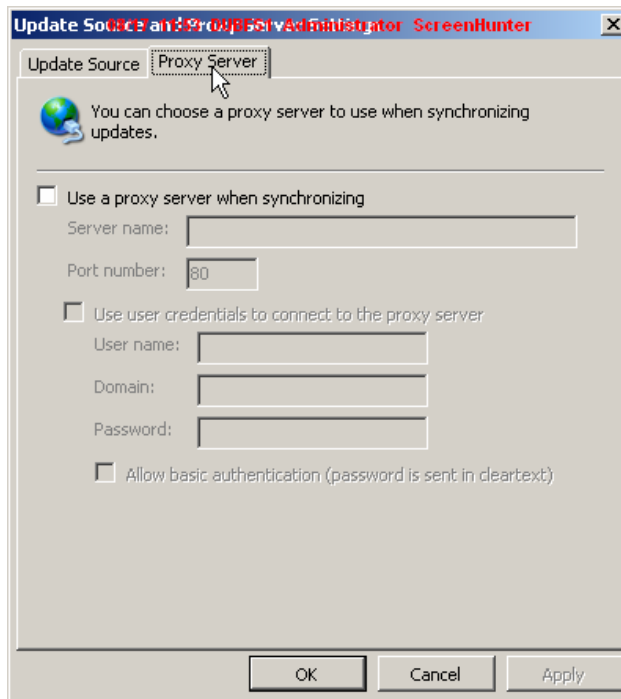
Here's a final report showing some computers that still need to be updated.



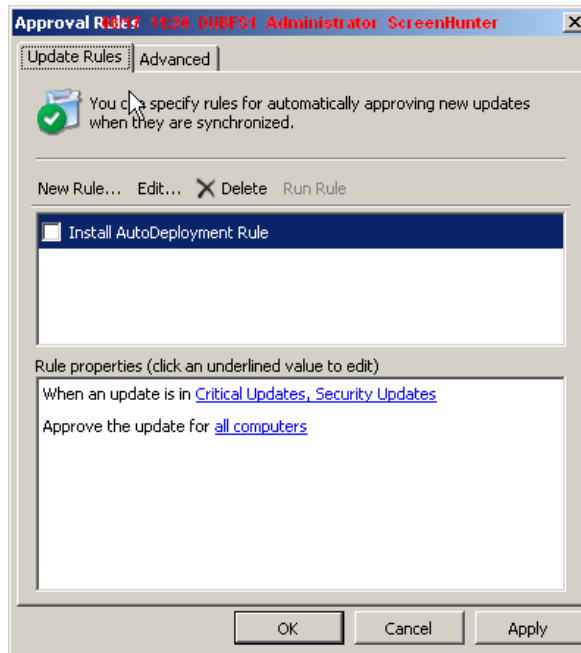
You don't need to run the configuration wizard again to modify the configuration of WSUS 3.0. Everything is under "Options".



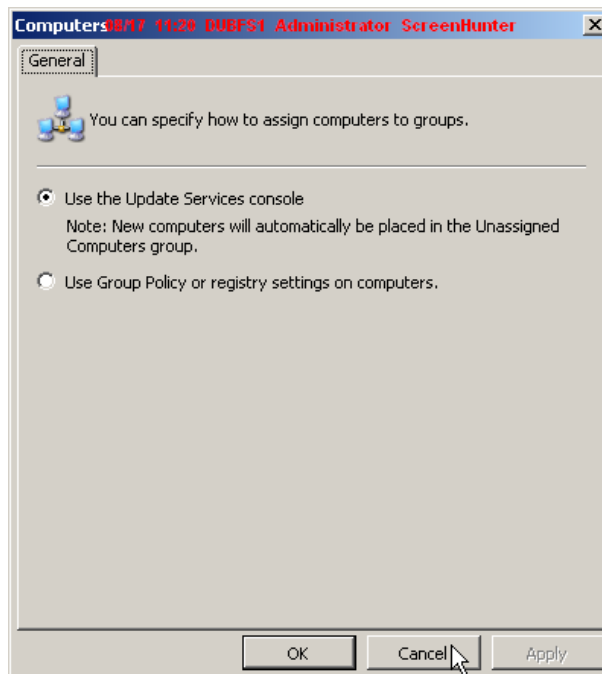
Under “Update Source and Proxy Server” we can switch a server from directly updating from Microsoft to an upstream server and vice versa.



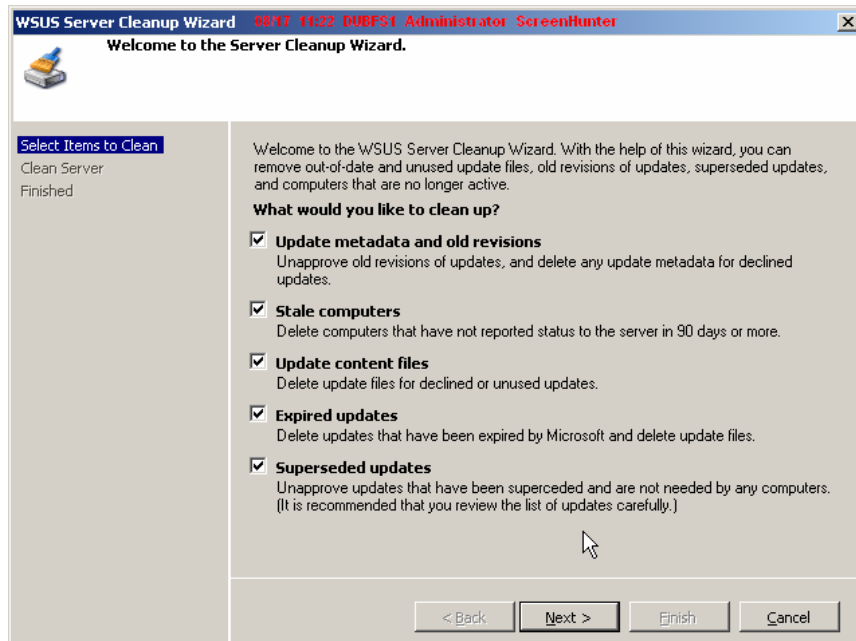
You can also modify the proxy settings.



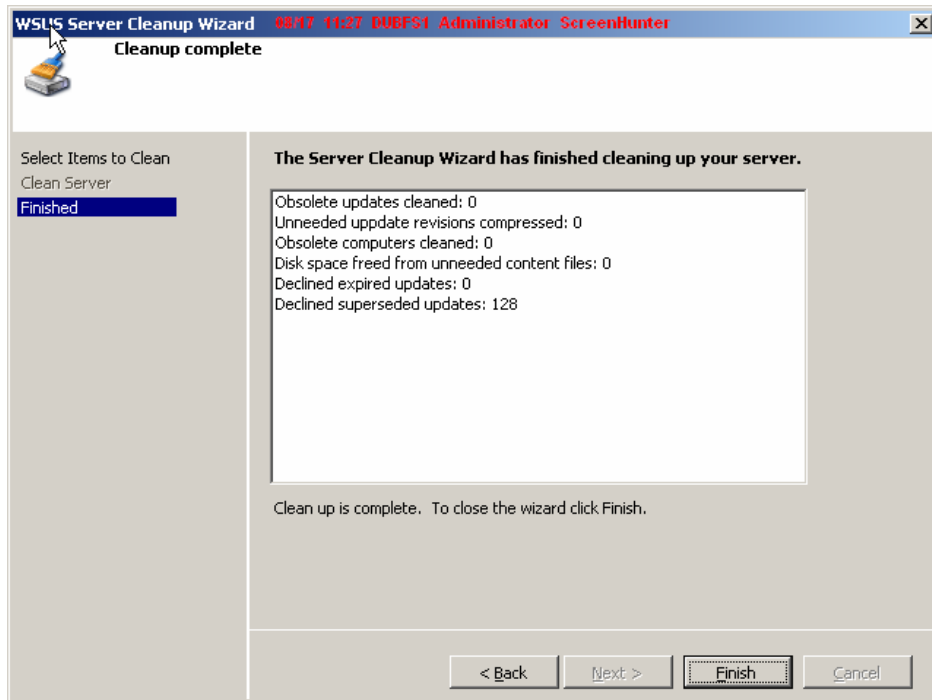
Approval Rules allows us to automatically change the approval status of updates as they are downloaded. It is rule based so it is very granular, an improvement over the inflexible system in SUS and WSUS 2.0.



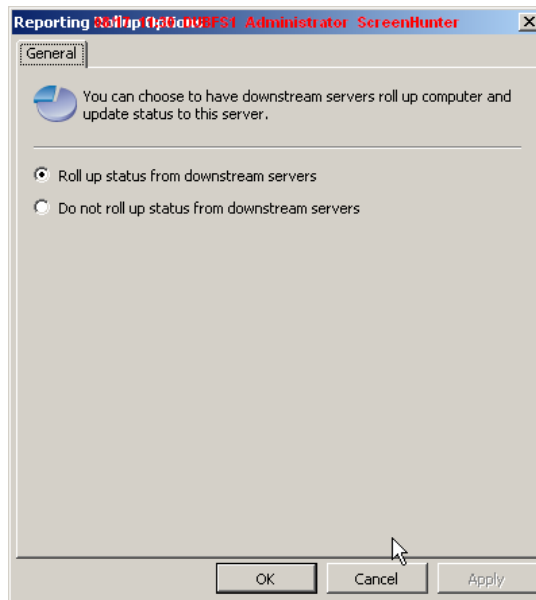
WSUS uses groups so you can target updates differently. This is very important because it allows you to set up a pilot group of computers on your live network. You can test deploy updates to this group to make sure everything is OK before deploying all updates to all computers. This screen allows you to configure how this is done. For a small pilot group, I think I'd be happier using the WSUS console. For widespread use of WSUS groups, I'd use group policy to configure group membership.



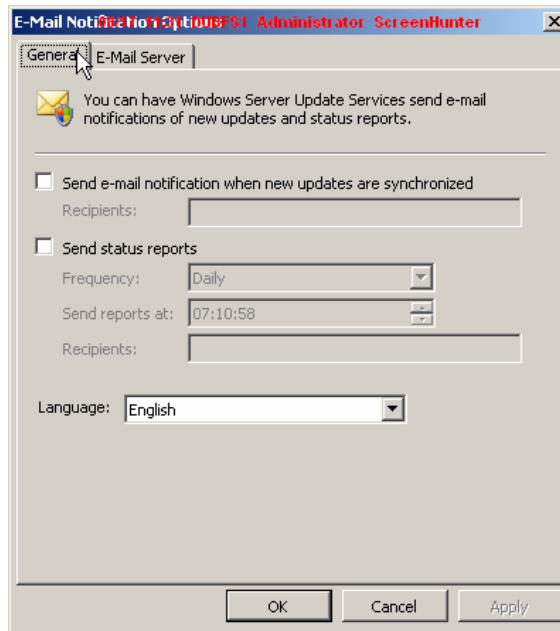
This is a nice addition. The Cleanup Wizard allows us to purge old information from the WSUS database with a minimum of fuss.



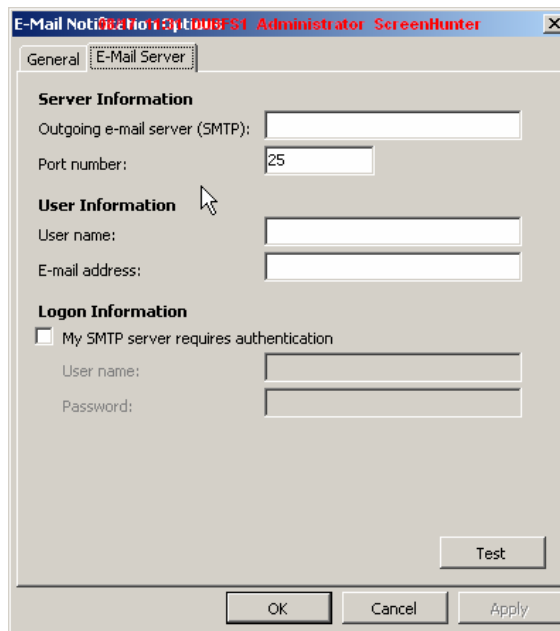
I ran the wizard on a brand new WSUS server and was able to clean out 128 updates. I'd highly recommend that you run this one pretty frequently on all of your WSUS servers.



This option will allow you centralised WSUS server to gather data from downstream servers to enable centralised reporting. Do this if at all possible to save yourself some administrative effort when it comes to reporting.



WSUS 3.0 has a basic notification engine. Ideally you'll want to be using MOM/SCOM 2007/SCE 2007 for advanced monitoring. WSUS 3.0 will send you notifications when new updates are downloaded and status reports for at a time and frequency of your choosing.



In this second tab you can configure the SMTP connection for sending notifications.

---

## Configuring WSUS Clients

---

When I say clients, I mean both servers and end user computers. I am an advocate of using WSUS to update servers. I've heard way too many clients say "we don't trust it, we update server by hand". Here's what I have noted. Yes, they do not trust automated updates but they do not have any evidence for that mistrust. And no, they do not update those servers by hand. These are usually the people who ignore warnings about critical updates and end up being crippled or shut down by the likes of SQL Slammer or Blaster. I can say, hand on heart, that I trust WSUS to update my end user computers and servers ... after I have tested the updates. I started using SUS and WSUS in 2003 and have never had a deployment or patch problem on a production network.

How do I configure my update mechanism? There are two aspects.

### The Approval Process

I have been lucky enough to use a separate and dedicated test environment with its own ADSL internet link. One that network was placed a replica of a domain controller from the live network. Key Windows systems were duplicated on the network. Who ever was on call the week of any updates had the responsibility of approving updates on the test network and monitoring the status of the systems. In this time we would also monitor IT news sources as usually for anything out of the ordinary. If everything went OK, we went through change control to deploy the updates to the live network.

If I did not have a dedicated test network then I would do this. I would build some sample virtual machines on either Microsoft Virtual Server or VMware Server (both free products). I would assign those machines to a WSUS group for pilot deployment. In WSUS I would approve updates for this pilot group and monitor the machines and the IT news sources. If everything was OK I would then push the updates out to all other machines.

### Installation Configuration

I do my entire installation configuration by group policy. Anyone without Active Directory can edit the registry to get the same effect. I'm not going to go through each and every setting because Microsoft's documentation (with WSUS and in the GPO object) does that better than I ever can.

I have 4 levels of group policy object:

- The top level will configure global settings such as how frequently to check for updates, etc.
- An end user machine policy (desktops and laptops) will configure Automatic Updates to download updates and start the installation at 03:00, every day. A missed schedule will

---

force the installation to start 1 minute after the next start up. Reboots will not be automatic but will prompt the user giving them a choice to ignore. Reminders to reboot will be every 30 minutes. Non-administrators will be notified of updates being available for installation (so they can kick them off early if they choose) and will be able to install updates when shutting down.

- Servers are configured differently due to their importance. Servers will automatically update at 03:00 on Saturday morning. This gives the maximum amount of possible time for recovery should something go wrong. Non-administrators will *not* be notified of updates (bad for Terminal Servers). The option to install updates will be available in the shutdown menu.
- If I have WSUS servers in multiple sites then I create and link a site policy to configure the location of the WSUS server for each Active Directory site.

I may choose to add a 5<sup>th</sup> policy for selected key servers, e.g. cluster nodes. A few machines may need to be updated manually. In this case I configure them to download updates and to only allow a manual installation.

There is one setting that I am still on the fence on. There is an option to allow accelerated installation of updates that do not require a reboot, i.e. they install as soon as they are downloaded. I certainly would not allow this on servers. I might allow it on desktops but usually don't. I find update installations can slow down PC's and the fewer helpdesk calls saying "my PC is slow" that I get, the better.

---

## Summary

---

Given the options that are out there, including free ones such as WSUS 3.0, there is no excuse for an organization not to be using an automated solution for deploying updates.

WSUS 3.0 already appears to be a “killer application” that will be an improvement over the successful WSUS 2.0. I would encourage anyone to start investigating this technology now and to start planning for the future.