



Deploying Microsoft Windows Server Update Services

Microsoft Corporation

Author: Susan Norwood

Editor: Craig Liebendorfer

Abstract

This paper describes how to deploy Microsoft® Windows Server™ Update Services (WSUS) 3.0. You will find a comprehensive description of how WSUS functions, as well as descriptions of WSUS scalability and bandwidth management features. This paper also offers step-by-step procedures for installation and configuration of the WSUS server. You will read how to update and configure Automatic Updates on client workstations and servers that will be updated by WSUS. Also included are steps for setting up a WSUS server on an isolated segment of your network and manually importing updates.

Microsoft®

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Deploying Microsoft Windows Server Update Services 3.0	11
Introduction to Deploying Windows Server Update Services 3.0	12
Design the WSUS 3.0 Deployment.....	12
Choose a Type of WSUS Deployment.....	12
Simple WSUS deployment.....	13
Using computer groups.....	14
WSUS server hierarchies.....	15
Networks disconnected from the Internet	16
Branch offices with low-bandwidth connections	17
Network load balancing clusters.....	17
Support for "roaming" clients.....	18
Choose a WSUS Management Style	19
Centralized management.....	19
Distributed management.....	21
Choose the Database Used for WSUS 3.0	21
Selecting a database	22
Database authentication, instance, and database name	23
Determine Where to Store WSUS Updates	23
Local storage.....	23
Remote storage.....	24
Determine Bandwidth Options to Use.....	25
Deferring the download of updates.....	25
Filtering updates	26
Using express installation files	27
Background Intelligent Transfer Service.....	28
Determine WSUS Capacity Requirements.....	29
Install the WSUS 3.0 Server.....	30
Configure the Network	31
Configure the Proxy Server.....	31

Configure the Firewall	32
Installation of Required Software	33
Windows Server 2003	33
Windows Server "Longhorn"	33
Configure IIS	34
Configuring IIS 7.0	35
Client self-update	35
Using the WSUS custom Web site	35
Accessing WSUS on a custom port	36
Using host headers	36
Migrate from WSUS 2.0 to WSUS 3.0	37
Before upgrading from WSUS 2.0 to WSUS 3.0	37
Migrating a Remote SQL Server Installation from WSUS 2.0 to WSUS 3.0	37
After upgrading	38
Run WSUS 3.0 Server Setup	38
Before you begin	39
Installing WSUS	40
Install the WSUS 3.0 Administration Console	44
Supported operating systems for console-only installation	44
Software prerequisites for console-only installation	44
Install the console	45
Access the WSUS administration console	46
Configure the WSUS 3.0 Server	46
Using the WSUS 3.0 Configuration Wizard	47
Choose the upstream server	48
Specify the proxy server	49
Connect to the upstream server	50
Choose update languages	51
Choose update products	52
Choose update classifications	53
Configure the synchronization schedule	55
Configuring WSUS from the administration console	56
Access the WSUS 3.0 Administration Console	56
Synchronize the WSUS 3.0 Server	56

Advanced Synchronization Options	57
Update storage options	57
Deferred downloads options.....	58
Express installation files options.....	58
Filtering updates options	59
Set Up E-Mail Notifications.....	59
Personalize the WSUS Display	61
Set Up a Hierarchy of WSUS Servers.....	63
Create Replica Servers	63
Enable reporting rollup from replica servers	64
Create the Computer Groups	64
Setting up computer groups	65
Step 1: Specify how to assign computers to computer groups	65
Step 2: Create computer groups	65
Step 3: Move the computers	66
Approve WSUS 3.0 Updates	66
Verify Deployment of Updates.....	67
Secure WSUS 3.0 Deployment	68
Hardening your Windows Server 2003 running WSUS	68
Adding authentication for chained WSUS Servers in an Active Directory environment	68
Step 1: Create an authentication list	69
Step 2: Disable anonymous access to the WSUS server.....	69
Securing WSUS with the Secure Sockets Layer Protocol	70
Limitations of WSUS SSL deployments.....	70
Configuring SSL on the WSUS server.....	71
Configuring SSL on client computers	72
Configuring SSL for downstream WSUS servers.....	73
Further reading about SSL.....	73
Update and Configure the Automatic Updates Client	74
Client Requirements.....	75
Update Client	75
Automatic Updates client self-update feature	75

Determine a Method to Configure Clients	76
Configure Clients Using Group Policy.....	77
Load the WSUS Administrative Template.....	78
Configure Automatic Updates	79
Specify intranet Microsoft Update service location.....	79
Enable client-side targeting.....	80
Reschedule Automatic Updates scheduled installations	81
No auto-restart for scheduled Automatic Update installation options.....	81
Automatic Update detection frequency.....	82
Allow Automatic Update immediate installation.....	83
Delay restart for scheduled installations	83
Reprompt for restart with scheduled installations.....	84
Allow non-administrators to receive update notifications.....	84
Allow signed content from the intranet Microsoft update service location	85
Remove links and access to Windows Update	85
Disable access to Windows Update	86
Configure Clients in a Non-Active Directory Environment.....	87
Editing the Local Group Policy object.....	87
Using the registry editor	87
Automatic Update configuration options	89
Automatic Updates scenarios.....	93
RescheduleWaitTime.....	93
Example 1: Installation must occur immediately following system startup	94
Example 2: Installations must occur fifteen minutes after the Automatic Updates service starts.....	94
NoAutoRebootWithLoggedOnUsers.....	95
Example 1: Non-administrator user on a workstation	96
Example 2: Non-administrator user on a server	97
Summary of behavior for NoAutoRebootWithLoggedOnUsers settings	97
Interaction with other settings	99
Manipulate Client Behavior Using Command-line Options	100
Detectnow Option	100
Resetauthorization Option.....	100
Client Behavior with Update Deadlines.....	101
Expired and unexpired deadlines	101
Deadlines and updates that require restarts	101
WSUS updates and deadlines	102

Set Up a Disconnected Network (Import and Export the Updates)	102
Step 1: Matching Advanced Options.....	103
Step 2: Copying Updates from the File System.....	104
Step 3: Copying Metadata from the Database	105
Importing Updates to Replica Servers	107
Import metadata to a replica server	107
Appendix A: Unattended Installations	108
Appendix B: Configure Remote SQL	110
Remote SQL limitations	111
Database requirements.....	111
Step 1: Install SQL Server 2005 Service Pack 1 on the back-end computer	112
Step 2: Check administrative permissions on SQL Server	113
Step 3: Install WSUS on the front-end computer	114
Appendix C: Configure WSUS for Network Load Balancing	115
Step 1: Configure remote SQL	115
Step 2: Set up the other front-end WSUS servers	116
Step 3: Configure the front-end WSUS servers	116
Step 4: Set up a DFS share	116
Step 5: Configure IIS on the front-end WSUS servers	118
Step 6: Move the local content directory on the first front-end WSUS server to the DFS share.....	119
Step 7: Configure the NLB	119
Step 8: Test the WSUS NLB configuration	120
Step 9: Configure WSUS clients to sync from the DFS share	120
Appendix D: Configure WSUS for Roaming Clients	121
Step 1: Identify the servers to use as WSUS servers.....	121
Step 2: Set up the host names on the DNS server.....	121
Step 3: Set up the DNS server for netmask ordering and round robin	122
Step 4: Configure the WSUS servers	122
Step 5: Configure WSUS clients to use the same host name.....	122
Appendix E: List of Security Settings	123
Windows Server 2003.....	123
Audit policy.....	123
Security options.....	124

Event log settings	136
System services	138
TCP/IP hardening	144
IIS security configuration	146
Enable general IIS error messages.....	146
Enable additional IIS logging options	146
Remove header extensions	147
SQL Server 2005	147
SQL registry permissions.....	147
Stored procedures	148
Appendix F: Prerequisites Schema.....	150
Prerequisites Schema	151
Example	151
Appendix G: Detect the Version of WSUS	152
Versioning in SUS 1.0	152
Versioning in WSUS 2.0.....	153
WSUS 3.0 pre-release candidate versions	153
WSUS 3.0 Release Candidate 1 and later versions.....	153

Deploying Microsoft Windows Server Update Services 3.0

This guide describes how to deploy Microsoft® Windows® Server™ Update Services (WSUS) 3.0. You will find a comprehensive description of how WSUS functions, as well as descriptions of WSUS scalability and bandwidth management features. This guide also offers step-by-step procedures for installation and configuration of the WSUS server. You will read how to update and configure Automatic Updates on client workstations and servers that will be updated by WSUS. Also included are steps for setting up a WSUS server on an isolated segment of your network and manually importing updates, as well as steps for configuring WSUS for network load balancing.



Note

A downloadable copy of this document is available at the [Windows Server](http://go.microsoft.com/fwlink/?LinkId=86416) (<http://go.microsoft.com/fwlink/?LinkId=86416>).

In this guide

- [Introduction to Deploying Windows Server Update Services 3.0](#)
- [Design the WSUS 3.0 Deployment](#)
- [Install the WSUS 3.0 Server](#)
- [Configure the WSUS 3.0 Server](#)
- [Update and Configure the Automatic Updates Client](#)
- [Set Up a Disconnected Network \(Import and Export the Updates\)](#)
- [Appendix A: Unattended Installations](#)
- [Appendix B: Configure Remote SQL](#)
- [Appendix C: Configure WSUS for Network Load Balancing](#)
- [Appendix D: Configure WSUS for Roaming Clients](#)
- [Appendix E: List of Security Settings](#)
- [Appendix F: Prerequisites Schema](#)
- [Appendix G: Detect the Version of WSUS](#)

Introduction to Deploying Windows Server Update Services 3.0

This guide describes how to deploy Microsoft® Windows® Server Update Services (WSUS) 3.0. Begin your WSUS deployment by reading about how WSUS functions, its general requirements, and its features for scalability and bandwidth management. Read how to choose a network and database configuration for your WSUS 3.0 installation in [Design the WSUS 3.0 Deployment](#). Next, read how to install and configure the WSUS server in the section [Install the WSUS 3.0 Server](#). Then read how to configure Automatic Updates on client workstations and servers that will be updated by WSUS in [Update and Configure the Automatic Updates Client](#).

Design the WSUS 3.0 Deployment

The first step in deploying WSUS 3.0 is to design the server configuration. The following sections describe various aspects of deployment design—from a simple configuration with a single server to a configuration with multiple WSUS servers. Some of the considerations to take into account are connection bandwidth (for both Internet connections and LAN or WAN connections), network configuration, and different language requirements.

In this guide

- [Choose a Type of WSUS Deployment](#)
- [Choose a WSUS Management Style](#)
- [Choose the Database Used for WSUS 3.0](#)
- [Determine Where to Store WSUS Updates](#)
- [Determine Bandwidth Options to Use](#)
- [Determine WSUS Capacity Requirements](#)

Choose a Type of WSUS Deployment

This section describes the basic features of all WSUS deployments. Use this section to familiarize yourself with simple deployments with a single WSUS server, as well as more complex scenarios, such as a WSUS server hierarchy or a WSUS server on an isolated

network segment. This section also explains how to target different sets of updates to different groups of computers.

Simple WSUS deployment

The most basic WSUS deployment consists of a server inside the corporate firewall that serves client computers on a private intranet, as shown in the "Simple WSUS Deployment" illustration below. The WSUS server connects to Microsoft Update to download updates. This is known as *synchronization*. During synchronization, WSUS determines if any new updates have been made available since the last time you synchronized. If it is your first time synchronizing WSUS, all updates are made available for download.



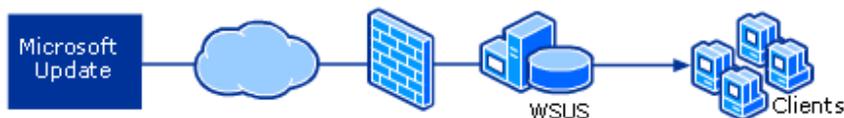
Note

Initial synchronization can take over an hour. All synchronizations after that should be significantly shorter.

By default, the WSUS server uses port 80 for HTTP protocol and port 443 for HTTPS protocol to obtain updates from Microsoft. If there is a corporate firewall between your network and the Internet, you will have to open these ports on the server that communicates directly to Microsoft Update. If you are planning to use custom ports for this communication, you will have to open those ports instead.

You can configure multiple WSUS servers to synchronize with a parent WSUS server. Chaining WSUS servers together is discussed later in this guide.

Simple WSUS Deployment



Automatic Updates is the client component of WSUS. Automatic Updates must use the port assigned to the WSUS Web site in Microsoft Internet Information Services (IIS). If there are no Web sites running on the server where you install WSUS, you can use the default Web site or a custom Web site. If you set up WSUS on the default Web site, WSUS listens for Automatic Updates on port 80. If you use a custom Web site, WSUS listens on port 8530. Alternate port numbers cannot be specified at setup time, but can be configured afterwards.

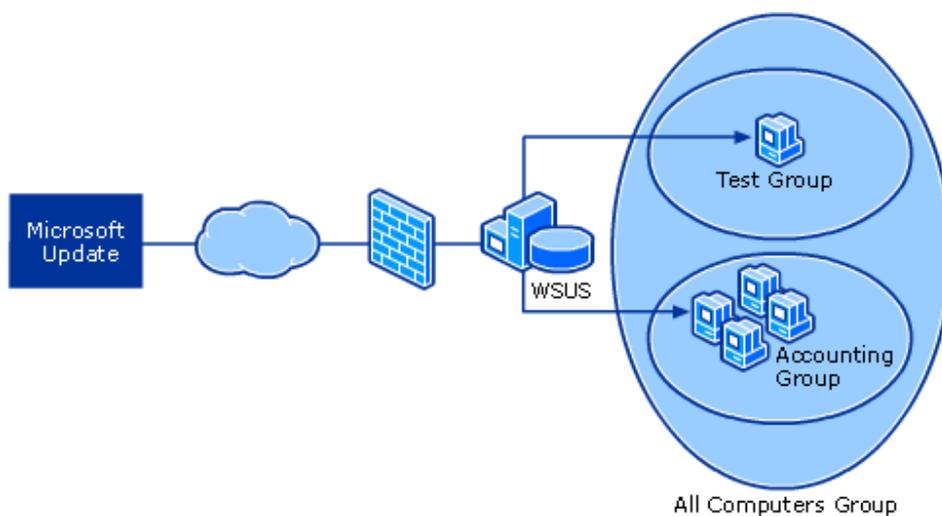
If you use the custom Web site, you must also have a Web site set up and running on port 80 to accommodate updating legacy Automatic Updates client software. If you use

the custom Web site, remember to include the port number in the URL when you configure Automatic Updates to point to the WSUS server. Other issues to consider when using a custom port for the WSUS Web site are discussed in "Using the WSUS custom Web site" in [Configure IIS](#) later in this guide.

Using computer groups

Computer groups are an important part of WSUS deployments, even a basic deployment. Computer groups enable you to target updates to specific computers. There are two default computer groups: All Computers and Unassigned Computers. By default, when each client computer initially contacts the WSUS server, the server adds it to both these groups.

Simple WSUS Deployment with Computer Groups



You can move computers from the Unassigned Computers group to a group you create. You cannot remove computers from the All Computers group. The All Computers group enables you to target updates to every computer on your network regardless of group membership. The Unassigned Computers group permits you to target only computers that have not yet been assigned group membership.

One benefit of creating computer groups is that it enables you to test updates. The "Simple WSUS Deployment with Computer Groups" illustration depicts two custom groups named Test and Accounting, as well as the All Computers group. The Test group contains a small number of computers representative of all the computers contained in the Accounting group. Updates are approved first for the Test group. If the testing goes

well, you can roll out the updates to the Accounting group. There is no limit to the number of custom groups you can create. There are instructions for creating custom computer groups in [Create the Computer Groups](#) later in this guide.

 **Note**

Do not use WSUS to distribute updates to client computers that are not licensed for your organization. The WSUS license agreement specifically disallows this.

WSUS server hierarchies

You can create complex hierarchies of WSUS servers. Since you can synchronize one WSUS server with another WSUS server instead of with Microsoft Update, you need to have only a single WSUS server that is connected to Microsoft Update. When you link WSUS servers together, there is an *upstream* WSUS server and a *downstream* WSUS server, as shown in the "WSUS Server Hierarchy" illustration below.

There are two ways to link WSUS servers together:

Autonomous mode: An upstream WSUS server shares updates with its downstream server or servers during synchronization, but not update approval status or computer group information. Downstream WSUS servers must be administered separately. Autonomous servers can also synchronize updates for a set of languages that is a subset of the set synchronized by their upstream server.

Replica mode: An upstream WSUS server shares updates, approval status, and computer groups with its downstream server or servers. Downstream replica servers inherit update approvals and cannot be administered apart from their upstream WSUS server.

For more information see [Choose a WSUS Management Style](#).

WSUS Server Hierarchy



This type of configuration is useful for many types of deployment. You might use it to download updates once from the Internet and then distribute those updates to branch offices with downstream servers, saving bandwidth on your Internet connection. You might use it to scale WSUS in a large organization with more client computers than one

WSUS server can manage. You might also use it to move updates closer to where they will be deployed.

Three levels is the recommended limit to a WSUS server hierarchy. This is because each level adds additional lag time to propagate updates throughout the chain. Theoretically there is no limit to how deep you can go, but only deployments with a hierarchy five levels deep have been tested.

The downstream server must always synchronize to an upstream server, as in the "WSUS Server Hierarchy" illustration above. This keeps synchronizations traveling downstream. If you attempt to synchronize an upstream server to a downstream server, you effectively create a closed loop, which is not supported. You can find step-by-step instructions for synchronizing WSUS servers in [Set Up a Hierarchy of WSUS Servers](#) later in this guide.

When you set up a WSUS server hierarchy, you should point Automatic Updates on all WSUS servers to the farthest downstream WSUS server in the hierarchy. This shields the entire chain from server-to-server protocol-breaking changes, because the downstream WSUS server can be used to update the broken upstream WSUS servers via Automatic Updates.



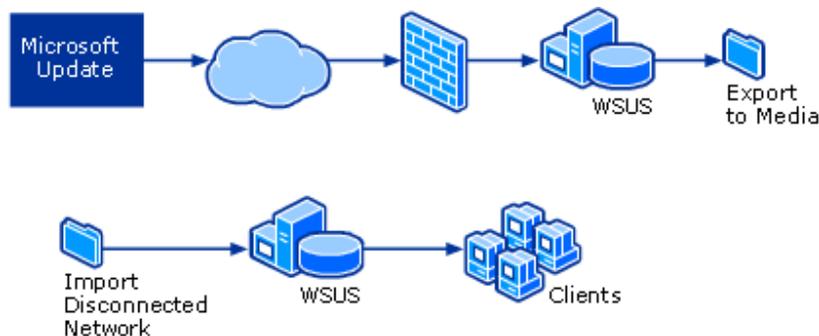
Important

If you have multiple downstream servers, you should not configure them to synchronize updates and roll up results at the same time of day. Downstream servers roll up information to their upstream server immediately after they synchronize. This may cause a high load on the upstream server, resulting in rollup failures. You must configure different downstream servers to synchronize at different times of day.

Networks disconnected from the Internet

It is unnecessary for your entire network to be connected to the Internet in order for you to use WSUS. If you have a network segment that is not connected to the Internet, consider deploying WSUS as shown in the "Distributing Updates on an Isolated Segment" illustration below. In this example, you create a WSUS server that is connected to the Internet but isolated from the intranet. After you download updates to this server, you can export the updates to media, hand-carry the media to disconnected WSUS servers, and import the updates.

Distributing Updates on an Isolated Segment



Exporting and importing is also appropriate for organizations that have high-cost or low-bandwidth links to the Internet. Even with all the bandwidth-saving options described later in this guide, downloading enough updates for all Microsoft products throughout an organization can be bandwidth-intensive. Importing and exporting updates enables organizations to download updates once and distribute by using inexpensive media. See [Set Up a Disconnected Network \(Import and Export the Updates\)](#) for more information about how to export and import updates.

Branch offices with low-bandwidth connections

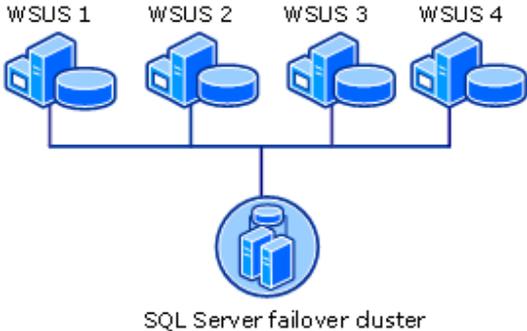
In many organizations, branch offices have low-bandwidth connections to the central office but high-bandwidth connections to the Internet. In this case you may want to configure downstream WSUS servers to get information about which updates to install from the central WSUS server, but download the updates themselves from Microsoft Update. For information about how to set up this kind of configuration, see [Advanced Synchronization Options](#).

Network load balancing clusters

Network load balancing increases the reliability and performance of your WSUS network. You can set up multiple WSUS servers that share a single SQL Server 2005 failover cluster, as in the "Network Load Balancing with a SQL Server Failover Cluster" illustration below. (Note that for this configuration you must use a full SQL Server 2005 installation, not the Windows Internal Database installation provided by WSUS.) You can also have all the WSUS servers use a DFS share to store their content. See [Appendix C: Configure](#)

[WSUS for Network Load Balancing](#) for more information about configuring WSUS and SQL Server for network load balancing.

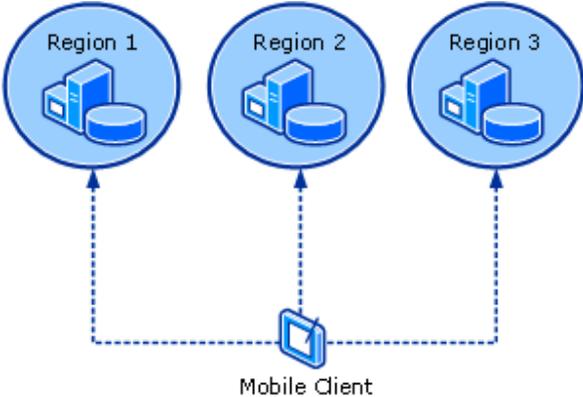
Network Load Balancing with a SQL Server Failover Cluster



Support for "roaming" clients

If you have many mobile users who log on to your network from different sites, you may want to use the following configuration to allow them to update their computers from the closest WSUS server. In this configuration, shown in the "Roaming Clients Using Different WSUS Servers" illustration below, there is one WSUS server per region, and each region is a DNS subnet. All clients are pointed to the same WSUS server name, which resolves in each subnet to the nearest WSUS server. See [Appendix D: Configure WSUS for Roaming Clients](#) for more information about how to configure DNS to support roaming clients.

Roaming Clients Using Different WSUS Servers



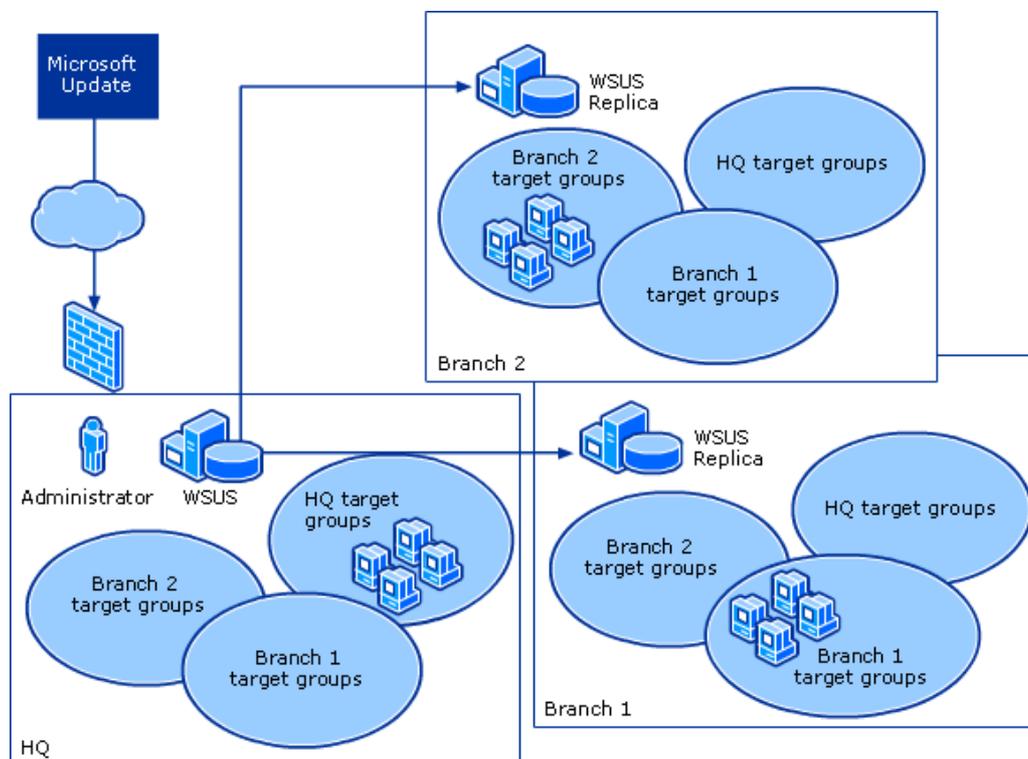
Choose a WSUS Management Style

WSUS supports deployments in both central and distributed management models. These management models enable you to manage your update distribution solution in the way that makes the most sense for your organization. You do not have to use a single management model throughout your organization. It is perfectly acceptable for a single organization to have a centrally managed WSUS deployment serving some computers, and one or more independently managed WSUS deployments serving other computers.

Centralized management

Centrally managed WSUS servers utilize replica servers. Replica servers are not administered separately, and are used only to distribute approvals, groups, and updates. The approvals and targeting groups you create on the master server are replicated throughout the entire organization, as shown in the "WSUS Centralized Management (Replica Servers)" illustration below. Remember that computer group membership is not distributed throughout the replica group, only the computer groups themselves. In other words, you always have to load client computers into computer groups.

WSUS Centralized Management (Replica Servers)



It is possible that not all the sites in your organization require the same computer groups. The important thing is to create enough computer groups on the administered server to satisfy the needs of the rest of the organization. Computers at different sites can be moved into a group appropriate for the site. Meanwhile, computer groups inappropriate for a particular site simply remain empty. All update approvals, like computer groups, must be created on the master server. For step-by-step instructions, see [Create Replica Servers](#) later in this guide.

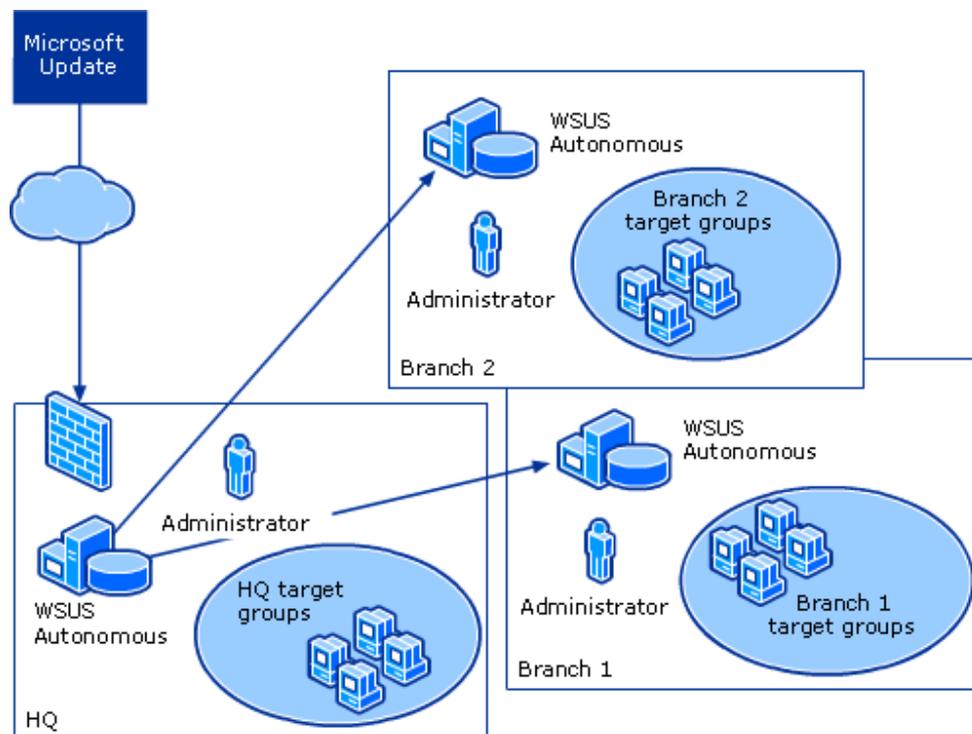
Note

If you change language options, Microsoft recommends that you manually move the changes between the centrally managed WSUS server and its replica servers. Changing language options on the centrally managed server alone might result in a mismatch between the number of updates that are approved on the central server and the number of updates approved on the replica servers.

Distributed management

Distributed management offers you full control over approvals and computer groups for the WSUS server, as shown in the "WSUS Distributed Management" illustration below. With the distributed management model, you typically have an administrator at each site, who takes care of deciding in what languages to synchronize updates, creating computer groups, assigning computers to groups, testing and approving updates, and ensuring that the correct updates are installed on the right computer groups. Distributed management is the default installation option for all WSUS installations.

WSUS Distributed Management



Choose the Database Used for WSUS 3.0

You do not need to be a database administrator or purchase database software to use WSUS. WSUS 3.0 will install Windows Internal Database if you choose to install a minimal version of SQL Server. This version of SQL Server is designed to require very

little management by the WSUS administrator. (If you already have Windows Internal Database installed, WSUS will use that.) Of course, if you want more control over the database, you can also use the full version of SQL Server with WSUS.

The WSUS database stores the following types of information:

- WSUS server configuration information
- Metadata that describes each update
- Information about client computers, updates, and client interaction with updates

You should not attempt to manage WSUS by accessing data directly in the database. Manage WSUS manually by using the WSUS console, or programmatically by calling WSUS APIs.

Each WSUS server requires its own database. If there are multiple WSUS servers in your environment, you must have multiple WSUS databases. WSUS does not support storing multiple WSUS databases on a SQL Server instance. The only exception is the case of a network load balanced cluster using a SQL Server failover cluster, as described in [Appendix C: Configure WSUS for Network Load Balancing](#).

Selecting a database

Use the following information to determine what database software is right for your organization. Once you have made a selection, see if there are any additional tasks you need to complete to set up the database software to work with WSUS. You can use database software that is 100-percent compatible with Microsoft SQL. There are two options that have been tested extensively for use with WSUS:

- Windows Internal Database ships with WSUS 3.0. This version of SQL Server does not have a user interface or tools. Administrators are meant to interact with these products through WSUS.
- Microsoft SQL Server 2005 is the full-featured database software from Microsoft. WSUS 3.0 requires SQL Server 2005 with Service Pack 1. If you use the full version of SQL Server, the SQL Server administrator should enable the *nested triggers* option in SQL Server. Do this before the WSUS administrator installs WSUS and specifies the database during the setup process. WSUS Setup enables the *recursive triggers* option, which is a database-specific option; however, it does not enable the *nested triggers* option, which is a server global option.

WSUS does support running database software on a computer separate from WSUS, but there are some restrictions. See [Appendix B: Configure Remote SQL](#) for more information.

Database authentication, instance, and database name

You cannot use SQL authentication with WSUS, which supports only Windows authentication. If you choose Windows Internal Database for the WSUS database, WSUS Setup creates an instance of SQL Server named `server\MICROSOFT##SSEE`, where `server` is the name of the computer. With either database option, WSUS Setup creates a database named SUSDB. The name of this database is not configurable.

In most cases each WSUS server will use a different SQL Server instance. One exception is the network load balancing configuration, in which multiple WSUS servers use a clustered SQL Server instance. For more information about this configuration and how to set it up, see [Appendix C: Configure WSUS for Network Load Balancing](#).

Determine Where to Store WSUS Updates

Although metadata that describes updates is stored in the WSUS database, the updates themselves are not. Updates are divided into two parts: a metadata part that describes the update, and the files required to install the update on a computer. Update metadata includes the end-user license agreement (EULA) and is typically much smaller than the size of the actual update.

You have two choices for update locations. You can store updates on the local WSUS server, or you can store updates on Microsoft Update. There is a configuration using shared update storage for network load balanced clusters, described in [Appendix C: Configure WSUS for Network Load Balancing](#). The result for either option is outlined in the following sections. If you have multiple WSUS servers chained together, each WSUS server in the chain may choose its own update storage options. These options are selected during the setup process, but can also be changed after installing WSUS. See [Advanced Synchronization Options](#) for step-by-step procedures.

Local storage

You can store update files locally on the WSUS server. This saves bandwidth on your Internet connection because client computers download updates directly from the WSUS server. This option requires enough disk space to store the updates you intend to download. There is a minimum requirement of 20 GB of hard disk space to store updates locally, but 30 GB is recommended. Local storage is the default option.

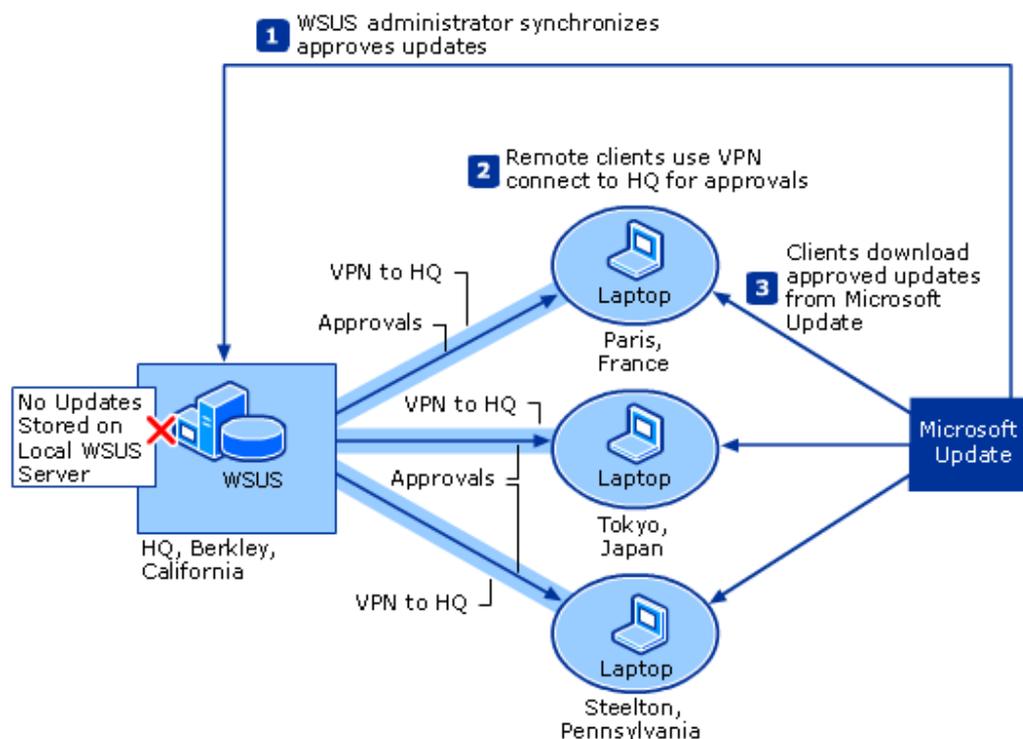
 **Note**

The 30 GB recommendation is only an estimate based on a number of variables, such as the number of updates released by Microsoft for any given product, how many products and update languages are selected, and whether standard update files or express updates are to be downloaded. Although 30 GB should work for most customers, your particular situation might require more than 30 GB of disk space.

Remote storage

If you want, you can store update files remotely on Microsoft servers. WSUS enables you to use Microsoft Update for the distribution of approved updates throughout your organization. This is particularly useful if most of the client computers connect to the WSUS server over a slow WAN connection but have high-bandwidth connections to the Internet, or if there are only a small number of client computers.

Clients Downloading Approved Updates from Microsoft Update



In this scenario WSUS is configured so that client computers download updates from Microsoft Update. When you synchronize the WSUS server with Microsoft Update, you get only the update metadata describing the updates. The files that install updates on client computers are not stored on the WSUS server.

Updates are still approved on the WSUS server, but each client connects to the Internet to download the approved updates from Microsoft servers. These are the same servers Microsoft uses to distribute updates to the public. Although your clients obtain updates from Microsoft over the Internet, you still make the decisions about which updates are approved for distribution. The advantage of this scenario is faster downloads for distributed clients and network bandwidth savings for your organization.

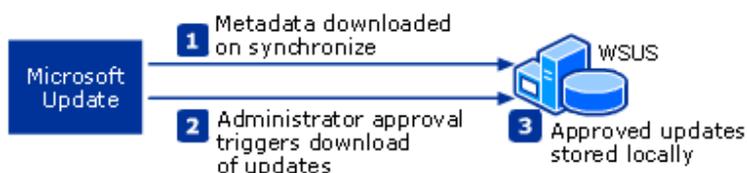
Determine Bandwidth Options to Use

WSUS allows you to shape the deployment to fit your organization's bandwidth needs. The decisions you make about how to synchronize with Microsoft Update have a dramatic effect on the efficient use of bandwidth. Read the following sections to understand WSUS features for managing bandwidth.

Deferring the download of updates

WSUS enables you to download update metadata before downloading the update itself. With deferred download, updates are downloaded only after the update has been approved, which saves bandwidth and WSUS server disk space. You can test the files prior to deploying them on your network, and client computers download the updates from the intranet. Microsoft recommends deferring the download of updates (the default WSUS configuration), since it makes optimal use of network bandwidth and disk space.

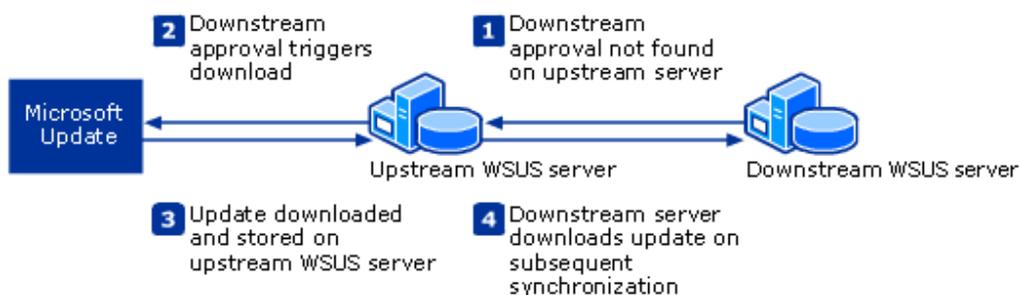
Deferred Downloads of Updates



If you have a chain of WSUS servers, it is recommended that you do not chain them too deeply, for the following reasons:

- In a chain of WSUS servers, WSUS automatically sets all downstream servers to use the deferred download option that is selected on the highest upstream server—in other words, the server that is directly connected to Microsoft Update. However, you may change this configuration (for example, to keep an upstream server doing full synchronization, while downstream servers defer their downloads).
- If you have deferred downloads enabled and a downstream server requests an update that has not been approved on the upstream server, the downstream server's request triggers a download on the upstream server. The downstream server then downloads the content on a subsequent synchronization, as shown in the "Deferred Downloads Using Multiple WSUS Servers" illustration. If you have a deep hierarchy of WSUS servers using deferred downloads, there is greater potential for delay as content is requested, downloaded, and then passed down the chain.

Deferred Downloads Using Multiple WSUS Servers



If you chose to store updates locally during the WSUS setup process, deferred downloads are enabled by default. You can change this option manually. See [Advanced Synchronization Options](#) for step-by-step procedures.

Filtering updates

WSUS allows you to choose only the updates your organization requires during synchronizations. You can filter synchronizations by language, product, and classification of update.

In a chain of WSUS servers, WSUS automatically sets all downstream servers to use the update filtering options that are selected on the server directly connected to Microsoft Update. You can change this configuration to get a subset of languages on a downstream server, or you can defer the download of updates. Deferring downloads is described in [Deferring the Download of Updates](#).

By default WSUS downloads Critical and Security Updates for all Windows products in every language, as well as Office updates and Windows Defender virus definitions. Microsoft recommends that you limit languages to the ones you actually use in order to conserve bandwidth and disk space. To change language options, or to change product and update classification options, see [Using the WSUS 3.0 Configuration Wizard](#).

Using express installation files

You can use express installation files to limit the bandwidth consumed on your local network, at the cost of bandwidth consumption on your Internet connection and disk space. By default WSUS does not use express installation files. To understand the tradeoff, you first have to understand how WSUS updates client computers.

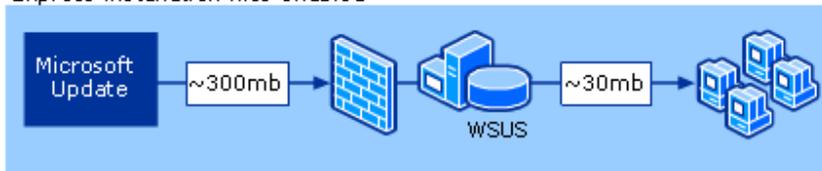
Updates typically consist of new versions of files that already exist on the computer being updated. On a binary level these existing files might not differ very much from updated versions. The express installation files feature is a way of identifying the exact bytes that change between different versions of files, creating and distributing updates that include just these differences, and then merging the original file with the update on the client computer. Sometimes this is called *delta delivery* because it downloads only the difference, or delta, between two versions of a file.

When you distribute updates this way, there is an initial investment in bandwidth. Express installation files are larger than the updates they are meant to distribute. This is because the express installation file must contain all the possible variations of each file it is meant to update.

The upper part of the "Express Installation Files Feature" illustration shows an update being distributed with express installation files; the lower part of the illustration shows the same update being distributed without using express installation files. Notice that with express installation files enabled, you incur an initial download three times the size of the update. However, this cost is mitigated by the reduced amount of bandwidth required to update client computers on the corporate network. With express installation files disabled, your initial download of updates is smaller, but the full size of the download must then be distributed to each of the clients on your corporate network.

Express Installation Files Feature

Express installation files enabled



Express installation files disabled



The file sizes in the "Express Installation Files Feature" illustration are for illustrative purposes only. Each update and express installation file varies in size, depending on what files need to be updated. Further, the size of each file actually distributed to clients by using express installation files varies depending upon the state of the computer being updated.

Important

Express installation files are often larger than the updates they are meant to distribute. On the other hand, it is always less expensive to distribute updates within a network using express installation files than to distribute full update files.

Not all updates are good candidates for distribution using express installation files. If you select this option, you obtain express installation files for any updates being distributed this way. If you are not storing updates locally, you cannot use the express installation files feature. By default, WSUS does not use express installation files. To enable this option, see [Advanced Synchronization Options](#).

Background Intelligent Transfer Service

WSUS uses the Background Intelligent Transfer Service 2.0 (BITS) protocol for all its file-transfer tasks, including downloads to clients and server synchronizations. BITS is a Microsoft technology that allows programs to download files by using spare bandwidth. BITS maintains file transfers through network disconnections and computer restarts. For more information about BITS, see the BITS documentation on the [MSDN site](#) at <http://go.microsoft.com/fwlink/?LinkId=79389>.

Determine WSUS Capacity Requirements

Hardware and database software requirements are driven by the number of client computers being updated in your organization. The following tables offer guidelines for server hardware and database software, based on the number of client computers being serviced. A WSUS server using the recommended hardware can support a maximum number of 20,000 clients. Both the system partition and the partition on which you install WSUS must be formatted with the NTFS file system.

Important

WSUS 3.0 cannot be installed on a compressed drive. Please check that the drive you choose is not compressed.

Minimum hardware recommendations

Hardware	Low-end 500 or fewer clients	Typical 500–3,000 clients	High-end 3,000–20,000 clients, or rollup of 30,000 clients	Super high-end 10,000 clients, or rollup of 100,000 clients
CPU	1 GHz	1.5 GHz or faster	3 GHz hyper threaded processor, x64 hardware	3 GHz hyper threaded dual processor
Graphics card	16 MB hardware accelerated PCI/AGP video card capable of 1-24*86*16bpp			
RAM	1 GB	2 GB	2 GB	4 GB
Page file	At least 1.5 times physical memory			

Hardware	Low-end 500 or fewer clients	Typical 500–3,000 clients	High-end 3,000–20,000 clients, or rollup of 30,000 clients	Super high-end 10,000 clients, or rollup of 100,000 clients
I/O subsystem	Fast ATA/IDE 100 hard disk or equivalent SCSI drives	Fast ATA/IDE 100 hard disk or equivalent SCSI drives	Fast ATA/IDE 100 hard disk or equivalent SCSI drives	Fast ATA/IDE 100 hard disk or equivalent SCSI drives
Network card	10 MB	100 MB	1 GB	1 GB
Hard drive— system partition	1 GB	1 GB	1 GB	1 GB
Hard drive— content storage	20 GB	30 GB	30 GB	30 GB
Hard drive— SQL Server installation	2 GB	2 GB	2 GB	2 GB

 **Note**

These guidelines assume that WSUS clients are synchronizing with the server every eight hours (for the high-end configuration) or every two hours (for the super high-end configuration). If they synchronize more often, there will be a corresponding increment in the server load. For example, if clients synchronize twice a day, the load will be twice as much as if they synchronize once a day.

 **Note**

Increasing the number of languages will also increase the load. Supporting five languages rather than one language will approximately double the size of the content directory.

Install the WSUS 3.0 Server

After designing the WSUS deployment, you are ready to install the WSUS server component. Use the five topics listed below to prepare the computer and the network

environment for WSUS. Check hardware and software requirements (as noted in the [Determine WSUS Capacity Requirements](#) section above). Install the required software, including database software (as noted in the [Installation of Required Software](#) section below). If you want to create a custom Web site or install WSUS on a computer that already has a Web site, see the IIS section. If you have a firewall or proxy server, see the firewall section to ensure that WSUS has access to updates on the Internet. After you have completed preparations, you can install and configure the WSUS server.

**Note**

It is not possible to upgrade from Microsoft Software Update Services (SUS) to WSUS 3.0. You must uninstall SUS before installing WSUS 3.0. If you are doing a migration from WSUS 2.0 to WSUS 3.0, see the section on migrating WSUS.

In this guide

- [Configure the Network](#)
- [Installation of Required Software](#)
- [Configure IIS](#)
- [Migrate from WSUS 2.0 to WSUS 3.0](#)
- [Run WSUS 3.0 Server Setup](#)
- [Install the WSUS 3.0 Administration Console](#)

Configure the Network

Before you start to install WSUS, you should make sure that your network is configured to work with WSUS. You should check two areas in particular: the proxy server (if your network uses a proxy server to communicate with the Internet) and the corporate firewall

Configure the Proxy Server

When you configure the root WSUS server on your network, you need to know whether there will be a proxy server between the WSUS server and the Internet. If you do, you will need to check the following issues before starting to install WSUS:

- Protocols supported by the proxy server. WSUS will communicate with Microsoft Update via HTTP and SSL, so the proxy server must support both protocols.

- The authentication method used by the proxy server (basic authentication or Windows authentication).

Configure the Firewall

If there is a corporate firewall between WSUS and the Internet, you might need to configure the firewall to ensure that WSUS can obtain updates.

To configure the firewall

- To obtain updates from Microsoft Update, the WSUS server uses port 80 for HTTP protocol and port 443 for HTTPS protocol. This is not configurable.
- If your organization does not allow those ports and protocols to be open to all addresses, you can restrict access to the following domains so WSUS and Automatic Updates can communicate with Microsoft Update:
 - <http://windowsupdate.microsoft.com>
 - http://*.windowsupdate.microsoft.com
 - https://*.windowsupdate.microsoft.com
 - http://*.update.microsoft.com
 - https://*.update.microsoft.com
 - http://*.windowsupdate.com
 - <http://download.windowsupdate.com>
 - <http://download.microsoft.com>
 - http://*.download.windowsupdate.com
 - <http://test.stats.update.microsoft.com>
 - <http://ntservicepack.microsoft.com>



Note

The steps for configuring the firewall are meant for a corporate firewall positioned between WSUS and the Internet. Because WSUS initiates all its network traffic, there is no need to configure Windows Firewall on the WSUS server.

Although the connection between Microsoft Update and WSUS requires ports 80 and 443 to be open, you can configure multiple WSUS servers to synchronize with a custom port.

Installation of Required Software

The following is a list of required software for each operating system that supports WSUS 3.0. Ensure that the WSUS server meets this list of requirements before running WSUS Setup. If any of these updates requires restarting the computer when installation is completed, you should restart your server before installing WSUS.

Windows Server 2003

The following software is required for running WSUS on Windows Server 2003 Service Pack 1:

- Microsoft Internet Information Services (IIS) 6.0. For information about configuring IIS, see [Configure IIS](#).
- [Microsoft .NET Framework Version 2.0 Redistributable Package](#), available on the Microsoft Download Center (<http://go.microsoft.com/fwlink/?LinkId=68935>). For 64-bit platforms, go to [Microsoft .NET Framework Version 2.0 Redistributable Package](#) (<http://go.microsoft.com/fwlink/?LinkId=70637>).
- [Microsoft Management Console 3.0 for Windows Server 2003 \(KB907265\)](#), available on the Microsoft Download Center (<http://go.microsoft.com/fwlink/?LinkId=70412>). For 64-bit platforms, go to [Microsoft Management Console 3.0 for Windows Server 2003 x64 Edition](#) (<http://go.microsoft.com/fwlink/?LinkId=70638>).
- [Microsoft Report Viewer Redistributable 2005](#), available on the Microsoft Download Center (<http://go.microsoft.com/fwlink/?LinkId=70410>).

Windows Server "Longhorn"

The following software is required for running WSUS on Windows Server® Code Name "Longhorn":

- Microsoft Internet Information Services (IIS) 7.0. For information on configuring IIS, see [Configure IIS](#).
- [Microsoft Report Viewer Redistributable 2005](#), available on the Microsoft Download Center (<http://go.microsoft.com/fwlink/?LinkId=70410>).

Configure IIS

Before installing WSUS, make sure you have Internet Information Services (IIS) installed. By default, WSUS uses the default Web site in IIS. WSUS Setup also gives you the option of creating a Web site on a custom port.

If the IIS service (W3SVC) is stopped during WSUS installation, WSUS Setup starts the service. Likewise, if you install WSUS to the default Web site and the site is stopped, WSUS Setup starts it.

To install IIS 6.0 on Windows Server 2003

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. In the **Components** list, select **Application Server**. Click **Details** and make sure that ASP.NET is selected
4. Click **OK**, click **Next**, and then follow the instructions on the screen.



Note

If this machine has been upgraded from Windows 2000, it may have the IIS 5.0 Isolation mode turned on. This must be turned off before installing WSUS 3.0.

To install IIS 7.0 on Windows Server "Longhorn"

1. Start the Server Manager (click **Start**, click **Run**, and then type **CompMgmtLauncher**).
2. In the tree view, select **Roles**, then in the **Roles** pane click **Add Roles**.
3. In the **Add Roles Wizard**, click **Select Server Roles**, select the **Web Service (IIS)** check box, click **Next**, and then click **Next** again.

At this time you may see a message box **Add features required for Web Server (IIS)?** Click **Add Required Features**.

4. In the **Select Role Services** window, make sure that the following services are selected:
 - **Common HTTP Features** (including **Static Content**)
 - **ASP.NET, ISAPI Extensions**, and **ISAPI Features** (under **Application Development**)
 - **Windows Authentication** (under **Security**)

- **IIS Metabase Compatibility** (under **Management Tools**, expand **IIS 6 Management Compatibility**)
5. Click **Next**, and then review your selections.
 6. Click **Install**.

Configuring IIS 7.0

After installing IIS 7.0 on Windows Server "Longhorn", you will need to update the IIS configuration file.

1. Open the IIS configuration file: `%WINDIR%\system32\inetsrv\applicationhost.config`
2. In the `<system.webServer><modules>` tag, remove `<add name="CustomErrorModule">`, if it is present.
3. In the `<system.webServer><modules>` tag, add `<remove name="CustomErrorModule">`.

The resulting tag should look like this:

```
<system.webServer>
<modules>
<remove name="CustomErrorModule">
</modules>
</system.webServer>
```

Client self-update

WSUS uses IIS to update most client computers automatically to WSUS-compatible Automatic Updates software. To accomplish this, WSUS Setup creates a virtual directory named Selfupdate under the Web site running on port 80 of the WSUS server. This virtual directory, called the self-update tree, contains the WSUS-compatible Automatic Updates software.

Using the WSUS custom Web site

If you configure WSUS on a custom port, you must have a Web site running on port 80. The Web site on port 80 does not have to be dedicated to WSUS. In fact, WSUS uses the site on port 80 only to host the self-update tree.

Malicious programs can target port 80 for HTTP traffic. If WSUS is using a custom port, you can temporarily shut down port 80 throughout your network, but still be able to distribute updates to combat malicious programs.

If you already have a Web site on the computer where you intend to install WSUS, you should use the setup option for creating a custom Web site. This option puts the WSUS Web site on port 8530. This port is not configurable.

 **Note**

If you change the WSUS port number after WSUS installation, you must manually restart the IIS service.

Accessing WSUS on a custom port

If WSUS is using a custom port to communicate with clients, you must use a custom URL to access the WSUS Web service. Use the following instructions to configure WSUS when it is running on port 8530.

- Include a custom port number in the URL directing the client computer to the WSUS server (for example, `http://WSUSServerName:portnumber`).
- For more information about pointing client computers to the WSUS server, see [Determine a Method to Configure Clients](#) later in this guide.
- If you set up any WSUS servers downstream from a server that uses a custom port number, you must enter the custom port number when configuring the source server settings on the downstream WSUS server.
- You can find instructions for connecting a downstream WSUS server to an upstream WSUS server in [Set Up a Hierarchy of WSUS Servers](#).

Using host headers

If you decide to use host headers, you should run the **configuressl** command after configuring WSUS. If you do not do so, WSUS Reporters may not be able to access the WSUS server.

 **Note**

If you assign host header values to the default Web site, you might interfere with Windows® SharePoint® Services and Exchange functionality.

To run the **configuress1** command

1. Open a command window.
2. Navigate to the WSUS Tools directory:

```
cdWSUSInstallDi\Tools
```

where WSUSInstallDir is the directory in which WSUS is installed.

3. Type the following command:

Wsusutil configuressl



Note

The **configuressl** command sets both the host header name and the server certificate name.

Migrate from WSUS 2.0 to WSUS 3.0

The WSUS 3.0 installation program will migrate all WSUS 2.0 settings to WSUS 3.0. Furthermore, if the installation program finds any SQL Server database other than SQL Server 2005 Service Pack 1 (or SQL Server 2005 Service Pack 2 for Windows Server "Longhorn"), it will back up the existing database, install Windows® Internal Database, and migrate the database to it.

Before upgrading from WSUS 2.0 to WSUS 3.0

You should make sure that your WSUS 2.0 installation is in good working order before upgrading.

1. Check for recent errors in the event logs, problems with synchronization between downstream servers and upstream servers, or problems with clients not reporting. Make sure that these issues have been resolved before continuing.
2. You may want to run DBCC CHECKDB to ensure that the WSUS database is correctly indexed. For more information about CHECKDB, see DBCC CHECKDB (<http://go.microsoft.com/fwlink/?LinkId=???>).
3. Back up the WSUS database.

Migrating a Remote SQL Server Installation from WSUS 2.0 to WSUS 3.0

If you have installed WSUS 2.0 on one computer and the SQL Server database on another, you must uninstall WSUS 2.0 from the database server before upgrading to WSUS 3.0.

 **Note**

Please make sure that your WSUS 2.0 database is not corrupt before upgrading.

 **To migrate WSUS 2.0 to WSUS 3.0 with a remote SQL Server installation**

1. Uninstall WSUS 2.0 from the back-end computer. Do not choose to delete the database.
2. Install WSUS 3.0 on the front-end computer.

The [Windows Server Update Services 3.0 Operations Guide](#)

(<http://go.microsoft.com/fwlink/?LinkId=81072>) includes other types of migration documentation, such as migrating from Windows Internal Database to Microsoft SQL Server.

After upgrading

It is a good idea to reindex the database after you upgrade. For more information about reindexing the database, see Appendix I: Database Maintenance in the WSUS 3.0 Operations Guide.

Run WSUS 3.0 Server Setup

After reviewing the previous topics, you are ready to install WSUS. You must log on with an account that is a member of the local Administrators group. Only members of the local Administrators group can install WSUS.

If you want to perform an unattended installation, see [Appendix A: Unattended Installations](#) later in this guide.

 **Important**

Be sure to read the WSUS Release Notes. Release notes often contain important late-breaking information about the release. Look for the WSUS Release Notes in the following location:

```
<WSUSInstallationDrive>:\Program Files\Microsoft Windows Server Update Services\Documentation\En\
```

**Note**

The latest version of WSUS setup is available on the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=74472) for Windows Server Update Services at <http://go.microsoft.com/fwlink/?LinkId=74472>.

Before you begin

Before you start WSUS Setup, you should make sure that the root of the drive where WSUS stores updates has certain permissions. WSUS Setup does not modify permissions on the root drive where you store updates, but this drive may not have appropriate permissions set. For example, security tools may have been used to strip away default permissions from the disk before the installation of WSUS. To manage this problem, use the following procedure to check the drive and directories where updates are stored to ensure permissions are set correctly.

▶ To check permissions on the drive and directories where updates are stored

1. Double-click **My Computer**, right-click the drive where updates are stored, and then click **Sharing and Security**.
2. Ensure that the drive has read permissions for the built-in Users group or **NT Authority\Network Service**.
3. Ensure that the root folder on the drive also has read permissions for **NT Authority\Network Service**.
4. Ensure that the content directory itself (usually `<drivename>:\WSUS\WsusContent`) has read permissions for **NT Authority\Network Service**. These permissions should have been set by the installation program.

The default Web site needs to allow anonymous access (that is, read access) by the IUSER_servername account. Some applications, notably Windows SharePoint Services, will remove anonymous access.

▶ To check for anonymous access to the default Web site

1. Go to the Internet Information Services (IIS) Manager, click the server name, click **Web Sites**, and then right-click the WSUS Web site.
2. In the context menu select **Permissions**.
3. In the Security tab you should see the **Internet Guest Account** listing.

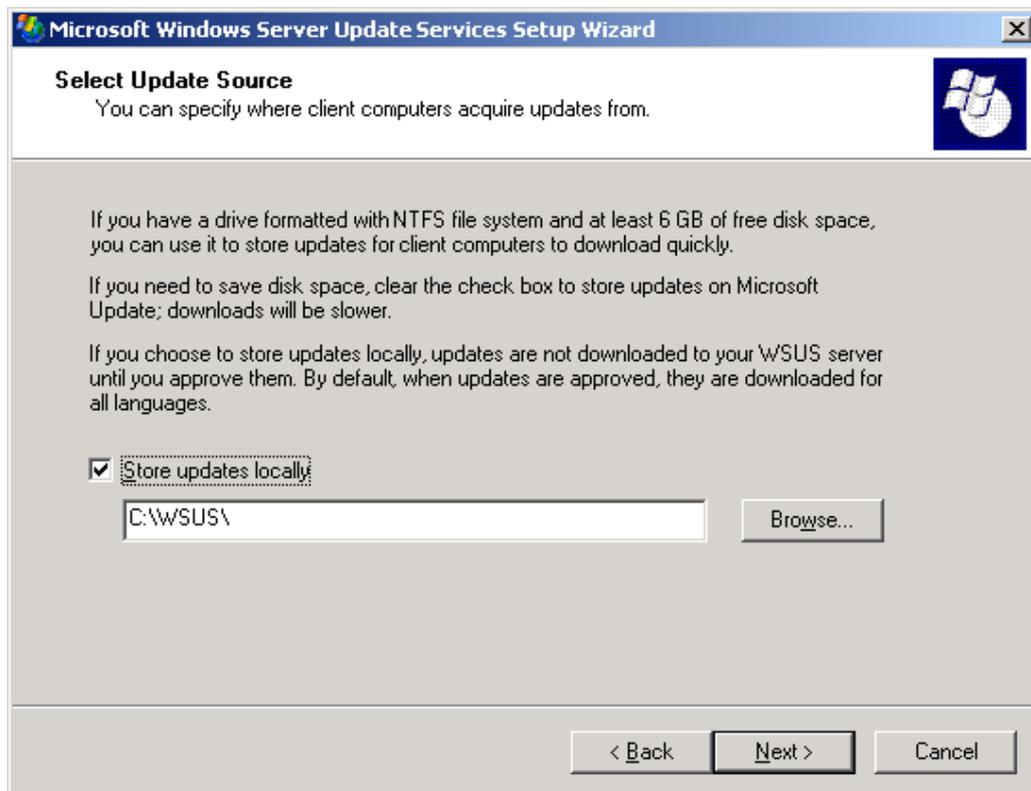
4. If you do not see this account, you will need to add it.
5. Add a user account named IUSR_*serverName* to the local machine, where *serverName* is the name of the server.
6. Give this account the following permissions: Read & Execute, List Folder Contents, and Read. You should deny write access to this account.
7. Return to IIS Manager, right-click the WSUS Web site, and then click **Permissions**.
8. Add the newly-created user to this Web site.

For more information about allowing anonymous access to Web sites, see [Allowing Anonymous Access to Web Sites \(IIS 6.0\)](http://go.microsoft.com/fwlink/?LinkId=75850) at <http://go.microsoft.com/fwlink/?LinkId=75850>.

Installing WSUS

To install WSUS on your server

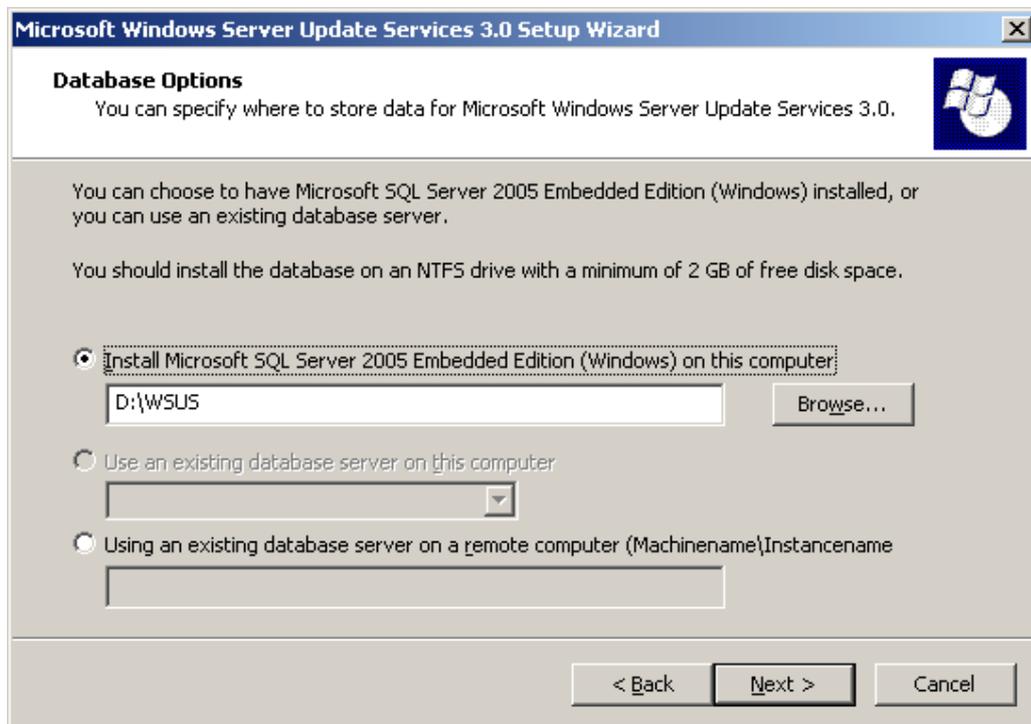
1. Double-click the installer file.
2. On the **Welcome** page, click **Next**.
3. On the **Installation Mode Selection** page, select the **Full server installation including Administration Console** check box, and then click **Next**.
4. Read the terms of the license agreement carefully. Click **I accept the terms of the License agreement**, and then click **Next**.



5. On the **Select Update Source** page, you can specify where client computers get updates. If you select the **Store updates locally** check box, updates are stored on WSUS, and you can select a location in the file system where updates should be stored. If you do not store updates locally, client computers connect to Microsoft Update to get approved updates.

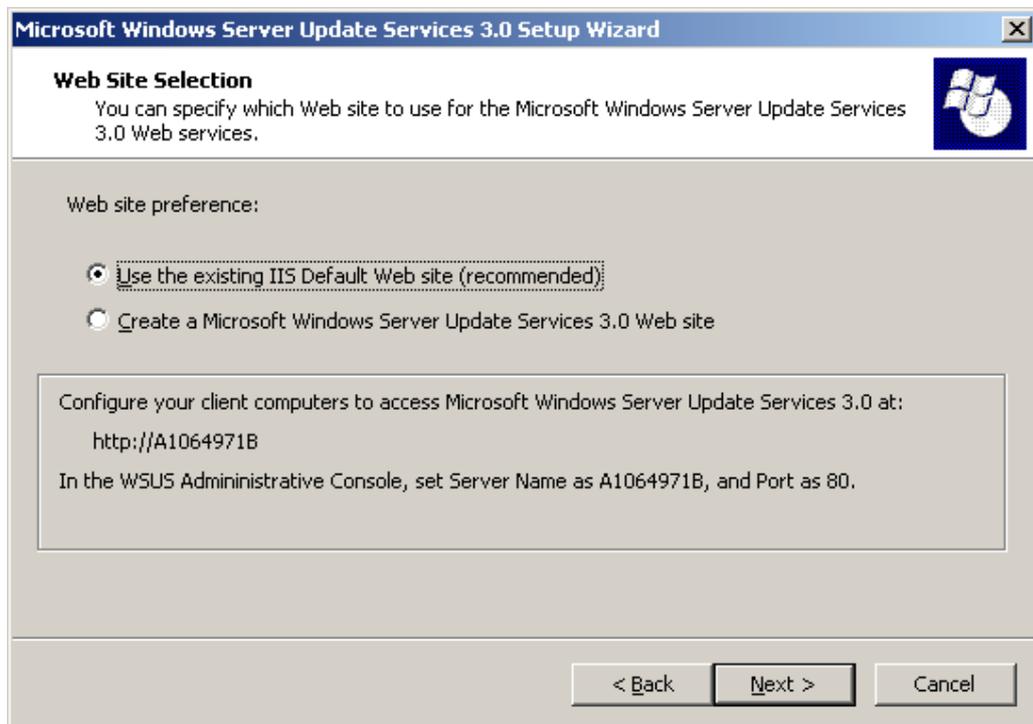
Make your selection, and then click **Next**.

For more information, see [Determine Where to Store WSUS Updates](#) earlier in this guide.



- On the **Database Options** page, you select the software used to manage the WSUS database. By default, WSUS offers to install Windows Internal Database. To accept the default setting, click **Install Microsoft SQL Server 2005 Embedded Edition (Windows) on this computer**. If you cannot use Windows Internal Database, click **Using an existing database server on this computer**, and select the instance name from the drop-down list. The instance name should appear as *<serverName>\<instanceName>*, where *serverName* is the name of the server and *instanceName* is the name of the SQL instance. Make your selection, and then click **Next**.

For more information, see [Choose the Database Used for WSUS 3.0](#) earlier in this guide.



7. On the **Web Site Selection** page, you specify the Web site that WSUS will use to point client computers to WSUS. If you wish to use the default IIS Web site on port 80, select the first option. If you already have a Web site on port 80, you can create an alternate site on port 8530 by selecting the second option. Make your selection, and then click **Next**.

For more information, see [Configure IIS](#) earlier in this guide.

8. On the **Ready to Install Windows Server Update Services** page, review your choices, and then click **Next**.
9. The final page of the installation wizard will tell you whether or not the WSUS 3.0 installation was completed successfully. The final page of the installation wizard will tell you whether or not the WSUS 3.0 installation was completed successfully. After you click **Finish** the configuration wizard will be launched.

Install the WSUS 3.0 Administration Console

After installing WSUS 3.0 on a server, you can manage WSUS 3.0 from any computer on your network, as long as the domain of that computer has a trust relationship with the domain of the server. You will need to perform a separate installation, from the same downloaded installation package, on every machine from which you want to run the WSUS 3.0 administration console.

Important

The WSUS 3.0 administration console can be used to manage any WSUS server that has a trust relationship with the administration console computer.

Supported operating systems for console-only installation

- Windows Server® Code Name "Longhorn"
- Windows Vista™
- Windows Server 2003 Service Pack 1
- Windows XP Service Pack 2

Software prerequisites for console-only installation

- [Microsoft .NET Framework Version 2.0 Redistributable Package \(x86\)](http://go.microsoft.com/fwlink/?LinkId=68935), available on the Microsoft Download Center (<http://go.microsoft.com/fwlink/?LinkId=68935>). For 64-bit platforms, go to [Microsoft .NET Framework Version 2.0 Redistributable Package \(x64\)](http://go.microsoft.com/fwlink/?LinkId=70637) (<http://go.microsoft.com/fwlink/?LinkId=70637>).
- [Microsoft Management Console 3.0 for Windows Server 2003 \(KB907265\)](http://go.microsoft.com/fwlink/?LinkId=70412), available on the Microsoft Download Center (<http://go.microsoft.com/fwlink/?LinkId=70412>). For 64-bit platforms, go to [Microsoft Management Console 3.0 for Windows Server 2003 x64 Edition \(KB907265\)](http://go.microsoft.com/fwlink/?LinkId=70638) (<http://go.microsoft.com/fwlink/?LinkId=70638>). For Windows XP Service Pack 2, go to <http://go.microsoft.com/fwlink/?LinkId=86951> (<http://go.microsoft.com/fwlink/?LinkId=86951>).

- [Microsoft Report Viewer Redistributable 2005](http://go.microsoft.com/fwlink/?LinkId=70410), available on the Microsoft Download Center (<http://go.microsoft.com/fwlink/?LinkId=70410>).

Install the console

To install the WSUS 3.0 administration console, use the same installation package you downloaded to install the WSUS server.



Note

The latest version of the WSUS setup executable is available on the [WSUS Web site](http://go.microsoft.com/fwlink/?LinkId=74472) (<http://go.microsoft.com/fwlink/?LinkId=74472>).

The console-only installation process can be run from the setup UI from the command line. For more information about command-line installation, see [Appendix A: Unattended Installations](#) later in this guide.

▶ To install the WSUS 3.0 console only from the UI

1. Double-click the installer file (WSUSSetup-x86.exe or WSUSSetup-x64.exe).
2. On the **Welcome** page, click **Next**.
3. On the **Installation Mode Selection** page, select the **Administration Console only** check box, and then click **Next**.
4. Read the terms of the license agreement carefully. Click **I accept the terms of the License Agreement**, and then click **Next**.
5. The final page of the installation wizard will tell you whether or not the WSUS 3.0 installation was completed successfully. Then click **Finish**.

▶ To install the WSUS 3.0 console only from the command line

1. Open a command window.
2. Navigate to the directory in which you saved the installation executable. (This will be either WSUSSetup-x86.exe or WSUSSetup-x64.exe.)
3. Type one of the following commands: **WSUSSetup-x86.exe CONSOLE_INSTALL=1** or **WSUSSetup-x64.exe CONSOLE_INSTALL=1**.
4. This will bring up the **Welcome** page of the installation UI. Click **Next**.
5. Read the terms of the license agreement carefully. Click **I accept the terms of the License Agreement**, and then click **Next**.

6. Wait for the installation process to finish, and then click **Finish**.

Access the WSUS administration console

You must be a member of the local Administrators group or the WSUS Administrators security group on the computer on which WSUS is installed in order to use all the features of the WSUS console. Members of the WSUS Reporters security group have read-only access to the console.

To open the WSUS administration console

1. Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Microsoft Windows Server Update Services 3.0**.
2. If you are bringing up the remote console for the first time, you will see only **Update Services** in the left pane of the console.
3. To connect to a WSUS server, in the **Actions** pane click **Connect to Server**.
4. In the **Connect To Server** dialog box, type the name of the WSUS server and the port on which you would like to connect to it.
5. If you wish to use SSL to communicate with the WSUS server, select the **Use Secure Sockets Layer (SSL) to connect to this server** check box.
6. Click **Connect** to connect to the WSUS server.
7. You may connect to as many servers as you need to manage through the console.

Configure the WSUS 3.0 Server

After installing WSUS, you are ready to configure the server. During installation, WSUS Setup created a security group called WSUS Administrators for managing WSUS. Add WSUS administrators to this group so that WSUS administrators do not have to be members of the local Administrators group to manage WSUS.

In this guide

- [Using the WSUS 3.0 Configuration Wizard](#)
- [Access the WSUS 3.0 Administration Console](#)

- [Synchronize the WSUS 3.0 Server](#)
- [Advanced Synchronization Options](#)
- [Set Up E-Mail Notifications](#)
- [Personalize the WSUS Display](#)
- [Set Up a Hierarchy of WSUS Servers](#)
- [Create Replica Servers](#)
- [Create the Computer Groups](#)
- [Approve WSUS 3.0 Updates](#)
- [Verify Deployment of Updates](#)
- [Secure WSUS 3.0 Deployment](#)

Using the WSUS 3.0 Configuration Wizard

The WSUS 3.0 configuration wizard will be run immediately after installation or at a later time. If you want to change the configuration later, you run **WSUS Server Configuration Wizard** from the **Options** page of the WSUS 3.0 Administration console. Before configuring the WSUS server, make sure you know the answers to the following questions:

1. Is the server's firewall configured to allow clients to access the server? See the [Configure the Network](#) section earlier in this document for more details.
2. Can this machine connect to the upstream server (Microsoft Update or an upstream WSUS server)?
3. If this machine is the root WSUS server (the one that connects to Microsoft Update), will it use a proxy server?
4. If a proxy server will be used, does it support both HTTP and SSL protocols?
5. Do you have the name of the proxy server and the user credentials for the proxy server?
6. Do you know the port number on which this machine will connect to the upstream server? (Although the connection between Microsoft Update and WSUS requires ports 80 and 443 to be open, you can configure a downstream WSUS server to use a custom port.)

The Configuration Wizard allows you to configure the following areas:

- [Choose the Upstream Server](#)
- [Specify the Proxy Server](#)
- [Connect to the Upstream Server](#)
- [Choose Update Languages](#)
- [Choose Update Products](#)
- [Choose Update Classifications](#)
- [Configure the Synchronization Schedule](#)



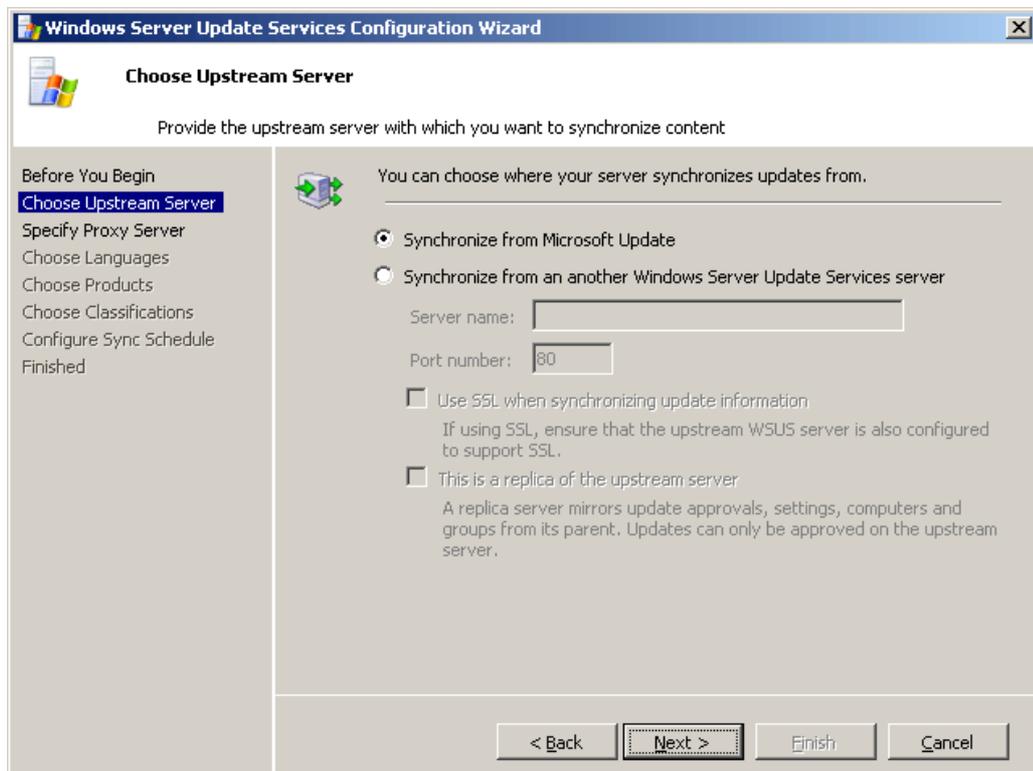
Note

You will need to configure the upstream server and proxy server before configuring the updates.

Choose the upstream server

Choose the upstream server

1. On the **Choose Upstream Server** page, select the source from which this server will get its updates (Microsoft Update or another WSUS server).
2. If you choose to synchronize from Microsoft Update, you are finished with this page. Click **Next**, or select **Specify Proxy Server** from the left pane.
3. If you choose to synchronize from another WSUS server, specify the server name and the port on which this server will communicate with the upstream server.
4. To use SSL, check the **Use SSL when synchronizing update information** check box. In that case the servers will use port 443 for synchronization. (You should make sure that both this server and the upstream server support SSL.)
5. If this is a replica server, check the **This is a replica of the upstream server** check box. (For more information about replica versus autonomous downstream servers, see the [Choose a WSUS Management Style](#) section earlier in this document.)
6. At this point you are finished with upstream server configuration. Click **Next**, or select **Specify proxy server** from the left pane.



Specify the proxy server

► Specify the proxy server

1. If you are setting up the root WSUS server that connects to Microsoft Update, you may wish to configure it to use a proxy server. On the **Specify Proxy Server** page of the configuration wizard, select the **Use a proxy server when synchronizing** check box, and then type the proxy server name and port number (port 80 by default) in the corresponding boxes.
2. If you want to connect to the proxy server by using specific user credentials, select the **Use user credentials to connect to the proxy server** check box, and then type the user name, domain, and password of the user in the corresponding boxes. If you want to enable basic authentication for the user connecting to the proxy server, select the **Allow basic authentication (password is sent in cleartext)** check box.
3. At this point you are finished with proxy server configuration. Click **Next** to go to the

Connect to Upstream Server page.

The screenshot shows the 'Specify Proxy Server' step of the 'Windows Server Update Services Configuration Wizard'. The window title is 'Windows Server Update Services Configuration Wizard'. The main heading is 'Specify Proxy Server' with a sub-heading 'Provide proxy server settings for synchronizing updates with Microsoft Update'. On the left, a navigation pane lists steps: 'Before You Begin', 'Choose Upstream Server', 'Specify Proxy Server' (highlighted), 'Choose Languages', 'Choose Products', 'Choose Classifications', 'Configure Sync Schedule', and 'Finished'. The main area contains a globe icon and the text: 'If this server requires a proxy server to access the upstream server you can configure the proxy server settings here.' There are four checkboxes: 'Use a proxy server when synchronizing' (checked), 'Use user credentials to connect to the proxy server' (unchecked), and 'Allow basic authentication (password is sent in cleartext)' (unchecked). The 'Use a proxy server when synchronizing' section has two text boxes: 'Server name:' containing 'netproxy' and 'Port number:' containing '80'. The 'Use user credentials to connect to the proxy server' section has three text boxes: 'User name:', 'Domain:', and 'Password:'. At the bottom, there are four buttons: '< Back', 'Next >' (highlighted), 'Finish', and 'Cancel'.

Important

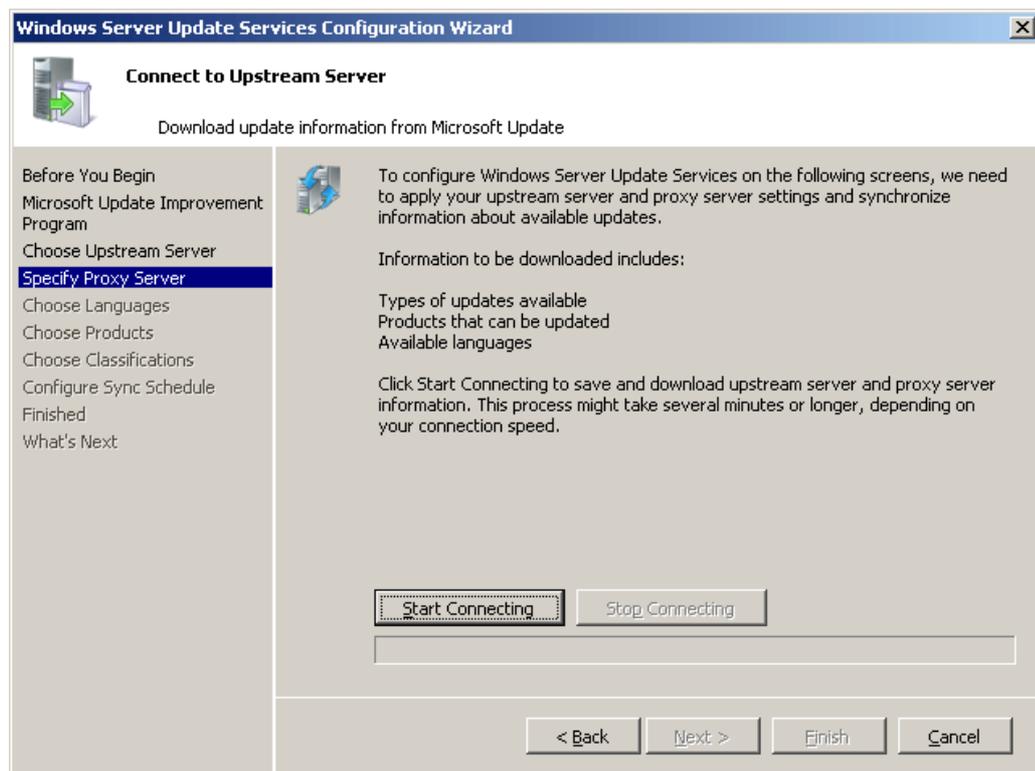
The proxy server should be configured to accept both HTTP and HTTPS resources.

Connect to the upstream server

Connect to the upstream server

1. Click the **Start Connecting** button, which will save and upload your settings and then download information about available updates, products, and classifications. This initial connection will take only a few minutes.
2. While the connection is taking place, the **Stop Connecting** button will be available. If there are problems with the connection, stop the connection, fix the problems, and restart the connection.

- After the connection has completed successfully, click **Next**. If you have chosen to store updates locally, you will go to the **Choose Languages** page, or you can select a different page from the left pane.



Note

If the connection to your upstream WSUS server (either Microsoft Update or an intranet WSUS server) fails, you will see a message at the bottom of the screen. Typically it will say something like "An HTTP error occurred." For more information, click the **Details** link.

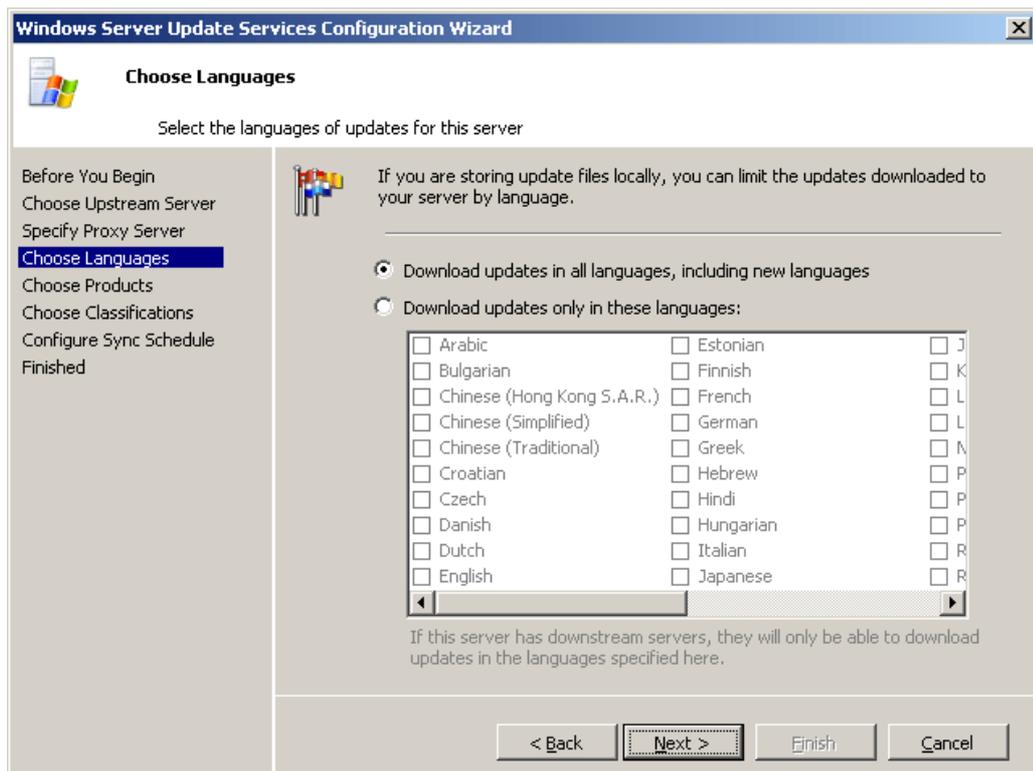
Choose update languages

Choose update languages

- The **Choose Languages** page allows you to get updates from all languages or from a subset of languages. Selecting a subset of languages will save disk space, but it is important to choose all of the languages that will be needed by all of the clients of

this WSUS server.

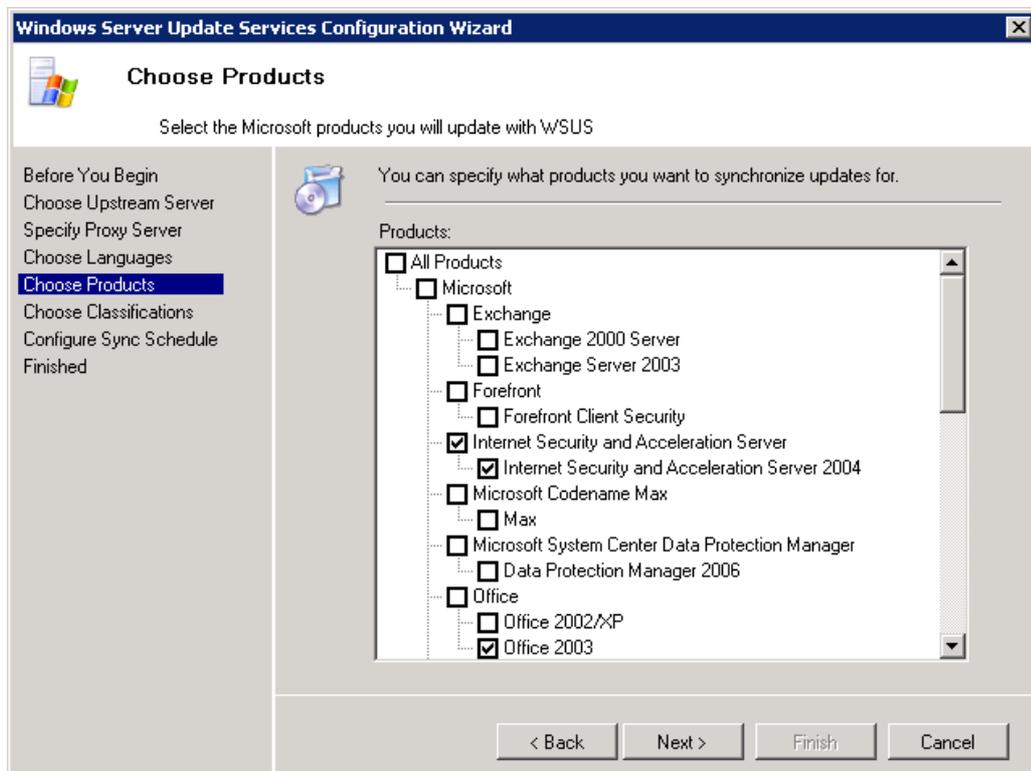
2. If you choose to not get updates for all languages, select **Download updates only in these languages**, and select the languages for which you want updates. Click **Next** to go to the **Choose Products** page, or select a different page from the left pane.



Choose update products

▶ Choose update products

1. The **Choose Products** page allows you to specify the products for which you want updates.
2. You may check product categories, such as Windows, or specific products, such as Windows Server 2003. Selecting a product category will cause all of the products under it to be selected. Click **Next** to proceed to the **Choose Classifications** page, or select a different page from the left pane.



Choose update classifications

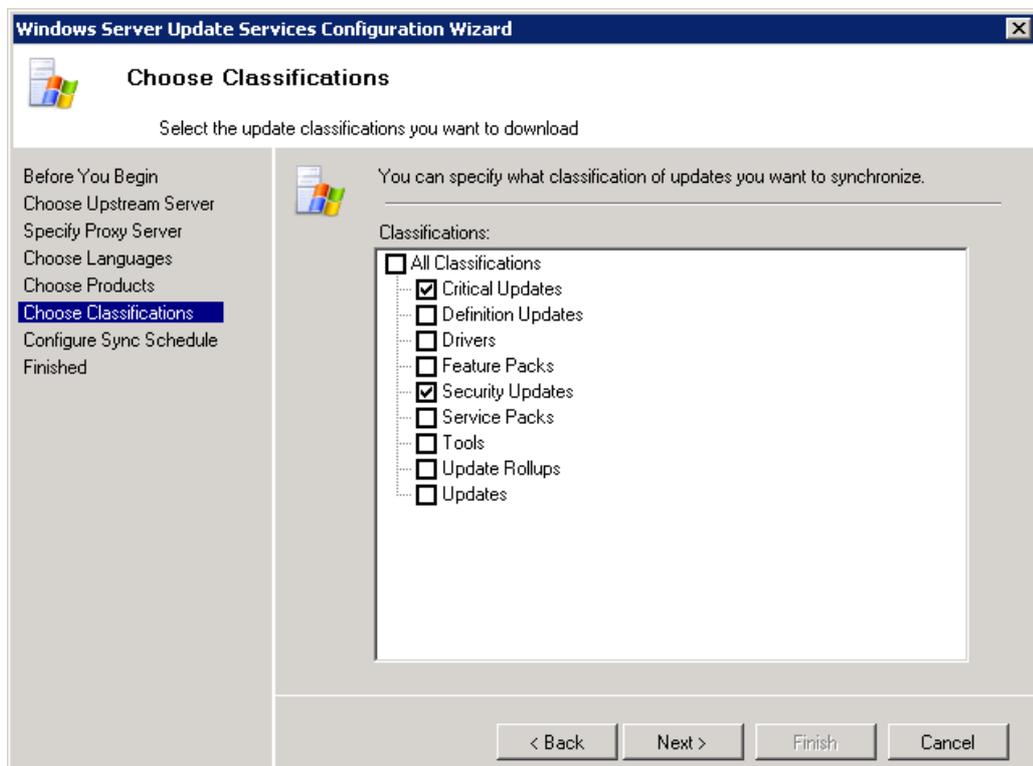
There are nine update classifications that you can use to filter the updates you get from Microsoft Updates:

- **Critical Updates:** Broadly released fixes for specific problems addressing critical, non-security related bugs.
- **Definition Updates:** Updates to virus or other definition files.
- **Drivers:** Software components designed to support new hardware.
- **Feature Packs:** New feature releases, usually rolled into products at the next release.
- **Security Updates:** Broadly released fixes for specific products, addressing security issues.

- **Service Packs:** Cumulative sets of all hotfixes, security updates, critical updates, and updates created since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features.
- **Tools:** Utilities or features that aid in accomplishing a task or set of tasks.
- **Update Rollups:** Cumulative sets of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a specific component, such as Internet Information Services (IIS).
- **Updates:** Broadly released fixes for specific problems addressing non-critical, non-security related bugs.

▶ Choose update classifications

1. The **Choose Classifications** page allows you to choose the update classifications you wish to obtain. You can choose all of the classifications or a subset of them.
2. Click **Next** to proceed to the **Configure Sync Schedule** page, or select a different page from the left pane.



Configure the synchronization schedule

▶ Configure the synchronization schedule

1. You will see the **Set Sync Schedule** page, which allows you to choose whether to perform update metadata synchronization manually or automatically.
2. If you choose to synchronize manually on this server, you will have to initiate the synchronization process from the WSUS Administration console.
3. If you choose to synchronize automatically, the WSUS server will synchronize at specified intervals. Set the time of the first synchronization and specify the number of synchronizations per day you wish this server to perform. For example, you can specify that synchronizations will start at 3:00 A.M. and that there will be four synchronizations a day. In that case, synchronizations will run every day at 3:00 A.M., 9:00 A.M., 3:00 P.M., and 9:00 P.M.

The screenshot shows the 'Set Sync Schedule' page of the Windows Server Update Services Configuration Wizard. The window title is 'Windows Server Update Services Configuration Wizard'. The page title is 'Set Sync Schedule'. Below the title, it says 'Configure when this server synchronizes with !! Server Name'. On the left side, there is a navigation pane with the following steps: 'Before You Begin', 'Choose Upstream Server', 'Specify Proxy Server', 'Choose Languages', 'Choose Products', 'Choose Classifications', 'Configure Sync Schedule' (which is highlighted in blue), and 'Finished'. The main content area has a heading 'You can synchronize updates manually or set a schedule for daily automatic synchronization.' Below this heading, there are two radio buttons: 'Synchronize manually' (which is unselected) and 'Synchronize automatically' (which is selected). Under 'Synchronize automatically', there is a text box for 'First synchronization:' containing '4:41:46 PM' and a dropdown menu for 'Synchronizations per day:' set to '2'. At the bottom of the main content area, there is a note: 'Note that when scheduling a daily synchronization from Microsoft Update, the synchronization start time will have a random offset up to 30 minutes after the specified time.' At the bottom of the wizard, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

After you have completed all of the above configuration steps, click **Finished** in the configuration wizard. If you have not already launched the WSUS Administration console, you can do so by leaving the **Launch the Windows Server Update Services Administration Snap-in** check box selected, and you can start the first synchronization by leaving the **Begin initial synchronization** check box selected.

Configuring WSUS from the administration console

It is also possible to carry out the same configuration steps outside the Configuration Wizard from the **Options** node of the WSUS Administration console. To configure or change the upstream server and proxy server settings, select **Update Source and Proxy Server**. To configure or change the product and classifications for which you want updates, select **Products and Classifications**. To update the languages for which you want updates, select **Update Files and Languages**.

Access the WSUS 3.0 Administration Console

Use the following procedure to access the WSUS administration console.

You must be a member of the local Administrators group or the WSUS Administrators group on the server on which WSUS is installed in order to use all of the features of the WSUS console. However, members of the WSUS Reporters group have read-only access to the console as well.

To open the WSUS console

- On your WSUS server, click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Microsoft Windows Server Update Services**.

Synchronize the WSUS 3.0 Server

After you select products and update classifications, you are ready to synchronize WSUS. The synchronization process involves downloading updates from Microsoft

Update or another WSUS server. WSUS determines if any new updates have been made available since the last time you synchronized. If this is the first time you are synchronizing the WSUS server, all of the metadata for updates in the product categories and classifications that you have selected are synchronized to your WSUS server.

**Note**

The first synchronization on a WSUS server will generally take a long time. You will not be able to make changes to the server's update filters (products, classifications, languages) while the server is being synchronized.

▶ To synchronize the WSUS server

1. In the WSUS Administration console, click the **Synchronizations** node.
2. In the **Actions** pane, click **Synchronize Now**.

After the synchronization finishes, you can click **Updates** in the tree view for this server to view the list of updates.

Advanced Synchronization Options

Advanced synchronization features include various options to manage bandwidth and store updates. There is a description of each of these features, including reasons why these features are useful and their limitations, in [Determine Where to Store WSUS Updates](#) and [Determine Bandwidth Options to Use](#) earlier in this guide.

Update storage options

Use the **Update Files** section to determine whether update files will be stored on WSUS or if client computers will connect to the Internet to get updates from Microsoft Update. There is a description of this feature in [Determine Where to Store WSUS Updates](#) earlier in this guide.

▶ To specify where updates are stored

1. In the left pane of the WSUS Administration console, click **Options**.
2. In **Update Files and Languages**, click the **Update Files** tab.
3. If you want to store updates in WSUS, select the **Store update files locally on this server** check box. If you want clients to connect to the Internet to get updates, then select the **Do not store updates locally; computers install**

updates from Microsoft Update check box.

Important

You can always change from storing updates on Microsoft Update to storing updates locally. However, you must make sure that the disk on which you choose to store updates has enough space for the updates. See [Determine WSUS Capacity Requirements](#) for a discussion of disk space for local storage. If there is not enough disk space to make the change, you may damage the WSUS installation.

Deferred downloads options

Use the **Update Files** section to determine if updates should be downloaded during synchronization or when the update is approved. Find a description of this feature in "Deferring the Download of Updates" in [Determine Bandwidth Options to Use](#) earlier in this guide.

To specify whether updates are downloaded during synchronization or when the update is approved

1. In the left pane of the WSUS Administration console, click **Options**.
2. In **Update Files and Languages**, click the **Update Files** tab.
3. If you want to download only metadata about the updates during synchronization, select the **Download updates to this server only when updates are approved** check box. This is the default option. If you want the update files and metadata during synchronization, clear the check box.

Express installation files options

Use the **Update Files** section to determine if express installation files should be downloaded during synchronization. Find a description of this feature in "Using Express installation files" in [Determine Bandwidth Options to Use](#) earlier in this guide.

To specify whether express installation files are downloaded during synchronization

1. In the left pane of the WSUS Administration console, click **Options**.
2. In **Update Files and Languages**, click the **Update Files** tab.
3. If you want to download express installation files, select the **Download express**

installation files check box. If you do not want to download express installation files, clear the check box.

Filtering updates options

Use the **Languages** section to select the language of the updates to synchronize. There is a description of this feature in “Filtering updates” in [Determine Bandwidth Options to Use](#) earlier in this guide.

To specify language options

1. In the left pane of the WSUS Administration console, click **Options**.
2. In **Update Files and Languages**, click the **Update Languages** tab.
3. In the **Advanced Synchronization Options** dialog box, under **Languages**, select one of the following language options, and then click **OK**.
 - **Download updates in all languages, including new languages:** This means that all languages will be downloaded during synchronization. If a new language is added, it will be automatically downloaded.
 - **Download updates only in these languages:** This means that only updates targeted to the languages you select will be downloaded during synchronization. If you choose this option, you must also choose each language you want from the list of those available.



Note

If you change language options, Microsoft recommends that you manually synchronize them between the centrally managed WSUS server and its replica servers. Changing language options on the centrally managed server alone might result in a mismatch between the number of updates that are approved on it and the number of updates approved on the replica servers.

Set Up E-Mail Notifications

The WSUS 3.0 server can be configured to send e-mail notifications of new updates and reports on the status of the WSUS network. Notifications will be sent whenever the WSUS server synchronizes new updates, and status reports can be sent daily or weekly.

Set up e-mail notifications

1. In the WSUS Administration console, click **Options** in the left pane.
2. In the center pane, click **E-Mail Notifications**.
3. Click the **General** tab.
4. If you want update notifications, select the **Send e-mail notification when new updates are synchronized** check box.
5. In the **Recipients** box, type the e-mail addresses of the people who should receive update notifications. Separate the names with semi-colons.
6. If you want status reports, select the **Send status reports** check box.
7. In the **Frequency** box, select either **Daily** or **Weekly**.
8. In the **Send reports at** box, set the time at which you want status reports to be sent.
9. In the **Recipients** box type the e-mail addresses of the people who should receive status reports, delimited by semicolons.
10. In the **Language** box, select the language in which the status reports should be sent.
11. Click **Apply** to save these settings.



Note

If both the WSUS administrative console and the WSUS server have the same settings for Daylight Savings Time adjustments, notifications will appear at the correct time. If the adjustments for Daylight Savings Time are different, then notifications will be off by the difference in the Daylight Savings Time adjustment.

Set up the e-mail server

1. Select the **E-Mail Server** tab.
2. In the **Outgoing e-mail server (SMTP)** box, type the name of your SMTP server.
3. In the **Port number** box, type the server's SMTP port (25 by default).
4. In the **Sender name** box, type the sender's e-mail display name. Generally this will be the name of the WSUS administrator.
5. In the **E-mail address** box, type the sender's e-mail address.
6. If the SMTP server requires logon information, select the **My SMTP server requires authentication** check box.

7. Enter the user name and password in the respective boxes.

**Note**

You may change authentication credentials only on a WSUS server, not from a remote administration console.

1. Click **Apply** to save this information.
2. After saving the e-mail server information, you can test your configuration by clicking **Test**. The **Event Viewer** should show any issues with sending the e-mail.

**Note**

If your e-mail notification is not working properly, one place to look is the SoftwareDistribution.log file (found in your WSUS directory, usually ...\\Program Files\\Update Services\\LogFiles). One error message that is symptomatic of incorrect SMTP configuration is the following:

```
EmailNotificationAgent.WakeupWorkerThreadProc Exception occurred when
sending email of type Summary: System.Net.Mail.SmtpException: Failure
sending mail. ---> System.IO.IOException: Unable to read data from the
transport connection: net_io_connectionclosed.
```

You should investigate your SMTP e-mail server configuration to resolve this problem.

Personalize the WSUS Display

You can configure different aspects of the way WSUS server information is displayed in the WSUS Administration console. You can display information from downstream replica servers when you view computer and update status information. You can have validation errors displayed as pop-up windows. And you can display different types of information in the computer overview's **To Do** section.

To display rollup data from downstream replica servers

1. From the WSUS Administration console, click **Options**, and then click **Personalization**.

2. On the **General** tab, select the **Include computers and status from replica downstream servers** check box.
3. Click **OK**.

 **Important**

Computer and update status will roll up from downstream replica servers only. It is not possible to get rolled-up status from a downstream autonomous server.

 **To display validation errors as pop-up windows**

1. From the WSUS Administration console, click **Options**, and then click **Personalization**.
2. On the **General** tab, select the **Show validation errors as popups** check box.
3. Click **OK**.

 **Note**

If you choose this option, errors will appear as pop-up windows and not as links in the UI.

 **To display different information in the To Do section**

1. From the WSUS Administration console, click **Options**, and then click **Personalization**.
2. On the **To Do List** tab, select one or more of the following items:
 - **Computers have not reported status for more than 30 days**
 - **WSUS updates are waiting to be approved for install**
 - **Critical updates are waiting to be approved for install**
 - **Computers have requested nonexistent computer groups**
 - **The server database is almost full**
 - **SSL is not enabled**
 - **New products and new classifications have been added in the past 30 days**
 - **Update file languages are enabled on this server, but are no longer supported by the upstream server**
3. Click **OK**.

Set Up a Hierarchy of WSUS Servers

There is a discussion of the advantages and limitations of setting up WSUS server hierarchies in "WSUS Server Hierarchies" in [Choose a Type of WSUS Deployment](#) earlier in this guide.

To connect a downstream server to an upstream server

1. In the left pane of the WSUS Administration console, click **Options**.
2. Select the **Update Source and Proxy Server** option and click the **Update Source** tab.
3. Select the **Synchronize from another Windows Server Update Services server** check box, and then type the server name and port number in the corresponding boxes.
4. If you are planning to use SSL for this connection, select the **Use SSL when synchronizing update information** check box. The port used for this connection will be 443.
5. If you want this server to be a replica of the upstream server, select the **This server is a replica of the upstream server** check box.
6. Click **OK**.

Important

When you configure a downstream server, you should make sure that the update languages it supports are a subset of the languages supported on its upstream server. If you choose a language on a downstream server that is not supported on an upstream server, you will not be able to get updates in that language. To remind you of this issue, a task will appear on the home page of the downstream server.

Create Replica Servers

A description of the benefits of creating a replica server is available in "Centralized Management" in [Choose a WSUS Management Style](#) earlier in this guide.

▶ **To create a replica group for centralized management of multiple WSUS servers**

1. Install WSUS on a computer at a site where it can be managed by an administrator. Follow the steps in [Run WSUS 3.0 Server Setup](#) in this guide.
2. Install WSUS on a computer at a remote site, in the same way as in Step 1. When you have launched the Configuration Wizard, go to the **Choose Upstream Server** page, select the **Synchronize from another Windows Server Update Services server** check box, and then enter the name of the WSUS server from step 1.
3. If you are planning to use SSL for this connection, select the **Use SSL when synchronizing update information** check box.
4. Select the **This is a replica of the upstream server** check box.
5. Repeat steps 2, 3, and 4 as necessary to add additional WSUS servers to the replica group.

Enable reporting rollup from replica servers

You can roll up computer and update status from replica servers to their upstream server.

▶ **To enable reporting rollup from replica servers**

1. In the WSUS administration console on the upstream server, click **Options**, and then **Reporting Rollup**.
2. Select the **Roll up status from replica downstream servers** check box, and then click **OK**.

Create the Computer Groups

There is a description of why you may want to use this feature, as well as a discussion of limitations and default settings, in the "Using Computer Groups" section in [Choose a Type of WSUS Deployment](#) earlier in this guide.

Setting up computer groups

Setting up computer groups is a three-step process:

1. Specify how to assign computers to computer groups. There are two options: server-side targeting and client-side targeting. With server-side targeting, you manually add each computer to its group. With client-side targeting, you automatically assign the computers by using either Group Policy or registry keys.
2. Create computer groups.
3. Move the computers into groups by using whichever method you chose in the first step.

Step 1: Specify how to assign computers to computer groups

Use the WSUS console to specify whether you are using client-side or server-side targeting.

To specify the method for assigning computers to groups

1. In the WSUS Administration console, click **Options**, and then click **Computers**. In the **Computers** dialog box, select one of the following options:
 - **Use the Update Services console.** Select this option if you want to create groups and assign computers through the WSUS console.
 - **Use Group Policy or registry settings on client computers.** Select this option if you want to create groups and assign computers using Group Policy or by editing registry settings on the client computer.
2. Click **OK** to save your settings.

Step 2: Create computer groups

Create computer groups in WSUS. The computer groups must be created on an autonomous WSUS server, whether you use client-side or server-side targeting. Computer groups cannot be created on a replica server or on a remote administration console.

To create a computer group

1. In the WSUS Administration console, click **Computers**, and then click **All**

Computers.

2. In the **Actions** pane, click **Add Computer Group**.
3. In the **Name** box, type a name for your new computer group, and then click **OK**.

Step 3: Move the computers

Use WSUS to move computers into groups, or automate this task.

▶ To move a computer to a different group by using server-side targeting

1. In the WSUS Administration console, click **Computers**, and then click the computer group of the computer you want to move.
2. In the list of computers, right-click the computer you want to move, and then click **Change Membership** in the shortcuts menu.
3. In the **Set Computer Group Membership** dialog box, click the computer group or groups to which you want to move the computer, and then click **OK**.

▶ To move a computer to a different group by using client-side targeting

- Use Group Policy or the registry to enable client-side targeting. For more information about how to configure the client computer, see [Determine a Method to Configure Clients](#). For more information about the client-side targeting setting, see the "Enable client-side targeting" section in [Configure Clients Using Group Policy](#) later in this guide.

Approve WSUS 3.0 Updates

You should approve updates to test the functionality of your WSUS deployment. There are many options for deploying updates; the procedure below covers only the basics. Use WSUS Help or the [Microsoft Windows Update Services](#) at <http://go.microsoft.com/fwlink/?LinkId=81072> to understand all your approval options.

▶ To approve multiple updates for installation

1. On the WSUS Administration console, click **Updates**, and then click **All Updates** or the classification of updates you wish to approve.

2. On the list of updates, right-click the update or updates you want to approve for installation, and then click **Approve** on the shortcuts menu.
3. In the **Approve Updates** dialog box, click the arrow next to the computer group for which you wish to approve the updates, and then click **Approved for Install**.
4. If you want to approve these updates for subgroups of this group, click the arrow again, and then click **Apply to Children**.
5. If you want to specify a deadline (that is, a time by which these updates should be installed), click the arrow again, and then click **Deadline**. You may specify a standard time (one week, one month, etc.) or a custom time.
6. Do the same for any other groups for which you would like to approve the selected updates.
7. When you have finished setting up the approvals, click **Approve**.
8. You will see the **Approval Progress** window while the updates are being approved. If there is any problem, such as a conflict among the selected updates, it will be reported here. You may click **Cancel** to exit the approval process at any time. When the approval process completes successfully, close the window.

 **Note**

If you want to install an update immediately, you can specify a deadline at the current time or in the past. You can find more information about how clients install updates with deadlines in [Client Behavior with Update Deadlines](#).

Verify Deployment of Updates

When client computers check in with the WSUS server, you can see whether updates have been deployed. By default, client computers check in with WSUS every 22 hours, but this is configurable. For more information about configuring the time when client computers check in with WSUS, see the "Automatic Update detection frequency" section in [Configure Clients Using Group Policy](#) later in this guide.

There are many different ways to see whether updates have been deployed. You can get a general view of the network's update status by clicking the name of the WSUS server in the left pane of the WSUS Administration console. The center pane provides a general view of the status of all the computers that report to this WSUS server, and of all the updates known to this server. You can find more information by clicking the status. Similarly, if you would like to look at the status of different updates, you can click the

Updates node in the left pane; if you would like to look at the status of different computers and groups, you can click the **Computers** node in the left pane.

You can print reports on any of the above categories, or on individual computers or updates, by clicking the item for which you want a report and then clicking **Status Report** in the **Actions** pane. You may also set up summary reports by clicking the **Reports** node in the left pane and then customizing one of the summary reports listed there.

Secure WSUS 3.0 Deployment

This guide includes three ways to enhance the security of your WSUS server:

- Recommendations for hardening your WSUS server.
- Recommendations for adding authentication between chained WSUS servers in an Active Directory environment.
- Recommendations for implementing the Secure Sockets Layer protocol on WSUS.

Hardening your Windows Server 2003 running WSUS

You can find recommended settings for hardening your WSUS server in [Appendix E: List of Security Settings](#). These recommendations include hardening a number of Windows Server components, as well as IIS 6.0 and SQL Server 2005.

Adding authentication for chained WSUS Servers in an Active Directory environment

You can add authentication for server-to-server synchronization.

There are some limitations to enabling authentication. Any WSUS server you want to authenticate must be in an Active Directory environment. If the WSUS servers are in different forests, there has to be trust between forests for this authentication method to succeed.

Enabling authentication is a two-step process:

1. Create a list of downstream WSUS servers allowed to authenticate with this WSUS server, and add this list to a web.config file.

2. In IIS, disable anonymous access to the WSUS server.

With completion of these two steps, only the downstream computers listed can synchronize with the WSUS server. Each of these steps is detailed below.

Step 1: Create an authentication list

WSUS setup creates a configuration file that enables you to add an explicit list of computers that have access to WSUS. You can find this file in the file system of the WSUS server at:

%ProgramFiles%\Update Services\WebServices\serversyncwebservice\Web.config

Use the `<authorization>` element to define an authentication list. You must add the `<authorization>` element below the `<configuration>` and `<system.web>` elements.

Consider the example below:

```
<configuration>
  <system.web>
    <authorization>
      <allow users="domain\computer_name,domain\computer_name" />
      <deny users="domain\computer_name,domain\computer_name" />
    </authorization>
  </system.web>
</configuration>
```

Within the opening and closing `<authorization>` tags, you specify a list of computers that are allowed a connection to the Web service. You must enter these computers as `domain\computer_name`. If you want multiple computers, use a comma to separate the names. You can also specify an explicit list of computers that are denied access. Order in this list is important, as the evaluation stops with the first item that applies to the user. If the `<allow users>` element is absent or empty, all servers are allowed.

The XML schema for this list can be found on the [MSDN Web site](http://go.microsoft.com/fwlink/?LinkId=47691) at <http://go.microsoft.com/fwlink/?LinkId=47691>.

Step 2: Disable anonymous access to the WSUS server

The next step is to configure IIS to disable anonymous access to the ServerSyncWebService virtual directory and enable Integrated Windows authentication.

To configure IIS to disable anonymous access and enable Integrated Windows authentication for the WSUS ServerSyncWebService

1. On the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then

click **Internet Information Services (IIS) Manager**.

2. Expand the local computer node.
3. Expand the WSUS Web site node
4. Right-click **ServerSyncWebService**, and then click **Properties**.
5. On the **Directory Security** tab, under **Authentication and access control**, click **Edit**.
6. In the **Authentication Methods** dialog box, clear the **Enable anonymous access** check box, and then select the **Integrated Windows authentication** check box.
7. Click **OK** twice.

Securing WSUS with the Secure Sockets Layer Protocol

You can use the Secure Sockets Layer (SSL) protocol to secure your WSUS deployment. WSUS uses SSL to allow client computers and downstream WSUS servers to authenticate the WSUS server. WSUS also uses SSL to encrypt the metadata passed between clients and downstream WSUS servers. Note that WSUS uses SSL only for metadata, not for content. This is also the way Microsoft Update distributes updates.

Updates consist of two parts: the metadata that describes the update, and the files to install the update on a computer. Microsoft mitigates the risk of sending update files over an unencrypted channel by signing each update. In addition to signing each update, a hash is computed and sent with the metadata for each update. When an update is downloaded, WSUS checks the digital signature and hash. If the update has been altered, it is not installed.

Limitations of WSUS SSL deployments

There are two limiting issues that administrators considering WSUS SSL deployments need to take into account.

1. Securing your WSUS deployment with SSL increases the workload of the server. You should plan for about a 10 percent loss of performance because of the additional cost of encrypting all the metadata sent over the network.

2. If you are using remote SQL, the connection between the WSUS server and the server running the database is not secured with SSL. If the database connection must be secured, consider the following recommendations:
 - Put the database on the WSUS server (the default WSUS configuration).
 - Put the remote server running SQL and the WSUS server on a private network.
 - Deploy Internet Protocol security (IPsec) on your network to secure network traffic. The [Overview of IPsec Deployment](http://go.microsoft.com/fwlink/?LinkId=45154) page on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=45154> offers guidance about how to deploy IPsec in your environment.

Configuring SSL on the WSUS server

The most important thing to remember when configuring the WSUS server to use SSL is that WSUS requires two ports in this configuration: one for encrypted metadata using HTTPS and one for HTTP. When you configure IIS to use SSL, keep the following points in mind:

- You cannot set up the entire WSUS Web site to *require* SSL. This would mean that all traffic to the WSUS site would have to be encrypted, but WSUS encrypts only update metadata. If a client computer or another WSUS server attempts to get update files from WSUS on the HTTPS port, the transfer will fail.

To keep the WSUS Web site as secure as possible, require SSL only for the following virtual roots:

- SimpleAuthWebService
- DSSAuthWebService
- ServerSyncWebService
- APIRemoting30
- ClientWebService

To keep WSUS functioning, you should not require SSL for the following virtual roots:

- Content
 - Inventory
 - ReportingWebService
 - SelfUpdate
- On the WSUS server, run the command:

wsusutil configuressl *certificateName*

where *certificateName* is the DNS name of the WSUS server. For example, if clients will connect to `https://myWSUSServer`, then *certificateName* should be `myWSUSServer`. If clients will connect to `https://myWSUSServer.myDomain.com`, then *certificateName* should be `myWSUSServer.myDomain.com`.

- The certificate of the certification authority must be imported into either the local computer's Trusted Root CA store or the Windows Server Update Service's Trusted Root CA store on downstream WSUS servers. If the certificate is imported only to the Local User's Trusted Root CA store, the downstream WSUS server will not be authenticated on the upstream server. For more information about SSL certificates, see [How to implement SSL in IIS \(KB 299875\)](http://go.microsoft.com/fwlink/?LinkId=86176) (<http://go.microsoft.com/fwlink/?LinkId=86176>).
- You must import the certificate to all the computers that will communicate with the server, including all clients, downstream servers, and computers running the administration console remotely. Again, the certificate should be imported into the local computer's Trusted Root CA store or the Windows Server Update Service's Trusted Root CA store.
- You can use any port you like when you configure IIS to use SSL. However, the port you set up for SSL determines the port that WSUS uses for clear HTTP. Consider the following examples:
 - If you use the industry standard port of 443 for HTTPS traffic, then WSUS uses port 80 for clear HTTP traffic, which is the industry standard for HTTP.
 - If you use any other port for HTTPS traffic, WSUS assumes that clear HTTP traffic should be sent over the port that numerically precedes the port for HTTPS. For example, if you use port 8531 for HTTPS, WSUS uses 8530 for HTTP.

Configuring SSL on client computers

There are two important caveats when configuring client computers:

- You must include a URL for a secure port on which the WSUS server is listening. Because you cannot require SSL on the server, the only way to ensure that client computers use a secure channel is to make sure they use a URL that specifies HTTPS. If you are using any port other than 443 for SSL, you must include that port in the URL, too.

For example, `https://<ssl-servername>` specifies a WSUS server that is using port 443 for HTTPS; however, while `https://<ssl-servername>:3051` specifies a WSUS server that is using a custom SSL port of 3051.

For more information about how to point client computers to the WSUS server, see "Specify intranet Microsoft Update service location" in [Configure Clients Using Group Policy](#) later in this guide.

- The certificate on client computers has to be imported into either the Local Computer's Trusted Root CA store or Automatic Update Service's Trusted Root CA store. If the certificate is imported only to the Local User's Trusted Root CA store, Automatic Updates will fail server authentication.
- Your client computers must trust the certificate you bind to the WSUS server in IIS. Depending upon the type of certificate you are using, you may have to set up a service to enable the clients to trust the certificate bound to the WSUS server. For more information, see "Further reading about SSL" later in this section.

Configuring SSL for downstream WSUS servers

The following instructions are for configuring a downstream server to synchronize to an upstream server that is using SSL.

To synchronize a downstream server to an upstream server that is using SSL

1. In the WSUS Administration snap-in, click **Options**, and then click **Update Source and Proxy Server**.
2. In the **Update Source** box, select **Synchronize from another Windows Server Update Services server** check box, type the name of the upstream server and the port number it uses for SSL connections, and then select the **Use SSL when synchronizing update information** check box.
3. Click **OK** to save the settings.

Further reading about SSL

Setting up a Certification Authority (CA), binding a certificate to the WSUS Web site, and then bootstrapping client computers to trust the certificate on the WSUS Web site are complex administrative tasks. The step-by-step procedures for each task are beyond the scope of this guide.

However, several articles on the subject are available. For more information and instructions about how to install certificates and set up your environment, see the following pages on the Microsoft Web site.

- The [Windows Server 2003 PKI Operations Guide](http://go.microsoft.com/fwlink/?LinkId=83159) (<http://go.microsoft.com/fwlink/?LinkId=83159>) provides a guide for administrators about how to configure and operate a Windows Certification Authority.
- [How to Set Up SSL on a Web Server](http://go.microsoft.com/fwlink/?LinkId=41454) (<http://go.microsoft.com/fwlink/?LinkId=41454>) offers step-by-step instructions for setting up SSL on a Web site.
- [Certificate Autoenrollment in Windows Server 2003](http://go.microsoft.com/fwlink/?LinkId=17801) (<http://go.microsoft.com/fwlink/?LinkId=17801>) offers instructions about how to automatically enroll client computers running Windows XP in Windows Server 2003 Enterprise environments integrated with Active Directory.
- [Advanced Certificate Enrollment and Management](http://go.microsoft.com/fwlink/?LinkId=83160) (<http://go.microsoft.com/fwlink/?LinkId=83160>) offers guidance about how to automatically enroll client computers in other environments.

Update and Configure the Automatic Updates Client

After planning the deployment, and installing and configuring the WSUS server, you are ready to work with the client computers. You can use Group Policy or the registry to configure Automatic Updates. Configuring Automatic Updates involves pointing the client computers to the WSUS server, making sure that the Automatic Updates software is up to date, and configuring any additional environment settings.

In this guide

- [Client Requirements](#)
- [Update Client](#)
- [Determine a Method to Configure Clients](#)
- [Manipulate Client Behavior Using Command-line Options](#)
- [Client Behavior with Update Deadlines](#)

Client Requirements

Automatic Updates is the WSUS client software. Other than a network connection, Automatic Updates requires no particular hardware configuration. It can be used with WSUS on any computer that runs any of the following operating systems:

- Windows Vista
- Windows Server "Longhorn"
- Microsoft Windows Server 2003, any edition
- Microsoft Windows XP Professional SP 2
- Microsoft Windows 2000 Professional with Service Pack 4 (SP4), Windows 2000 Server with SP3 or SP4, or Windows 2000 Advanced Server with SP3 or SP4

Update Client

WSUS requires the WSUS client, a version of Automatic Updates compatible with WSUS. Computers running Windows XP with Service Pack 2 and Windows Vista already have the WSUS client installed.

Automatic Updates client self-update feature

Each time Automatic Updates checks the public Web site or internal server for updates, it also checks for updates to itself. This means that most versions of Automatic Updates can be pointed to the public Windows Update site and they will automatically self-update. You can also use the WSUS server to self-update the client software. For specifics, see the "Client self-update" section in [Configure IIS](#) earlier in this guide.

The self-updating client software is available on the following operating systems:

- Windows Vista
- Windows Server "Longhorn"
- Windows Server 2003
- Windows XP with Service Pack 2
- Windows 2000 with Service Pack 3 or Service Pack 4

Determine a Method to Configure Clients

How best to configure Automatic Updates and WSUS environment options depends upon your network environment. In an Active Directory environment, you would use Group Policy. In a non-Active Directory environment, you might use the Local Group Policy object or edit the registry directly.

Administrator-defined configuration options driven by Group Policy—whether set with Group Policy in an Active Directory environment or via the registry or Local Group Policy object—always take precedence over user-defined options. When you use administrative policies to configure Automatic Updates, the Automatic Updates user interface is disabled on the target computer.

If you configure Automatic Updates to notify the user of updates that are ready to be downloaded, it sends the notification to the System log and to a logged-on administrator of the computer. You can use Group Policy to enable non-administrators to get this message. If no user with administrator credentials is logged on and you have not enabled non-administrators to get notifications, Automatic Updates waits for an administrator to log on before offering the notification.

By default every 22 hours, minus a random offset, Automatic Updates polls the WSUS server for approved updates; if any new updates need to be installed, they are downloaded. The amount of time between each detection cycle can be manipulated from 1 to 22 hours by using Group Policy.

You can manipulate the notification options as follows:

- If Automatic Updates is configured to notify the user of updates that are ready to be installed, the notification is sent to the System log and to the notification area of the client computer.
- When a user with appropriate credentials clicks the notification-area icon, Automatic Updates displays the available updates to install. In this case, a user with the appropriate credentials is either a logged-on administrator or a non-administrator granted appropriate credentials by means of Group Policy. The user must then click **Install**, so the installation can proceed. A message appears if the update requires the computer to be restarted to complete the update. If a restart is requested, Automatic Updates cannot detect additional updates until the computer is restarted.

If Automatic Updates is configured to install updates on a set schedule, applicable updates are downloaded and marked as ready to install. Automatic Updates notifies

users having appropriate credentials via a notification-area icon, and an event is logged in the System log. This indicates that the user can install updates.

At the scheduled day and time, Automatic Updates installs the update and restarts the computer (if necessary), even if there is no local administrator logged on. If a local administrator is logged on and the computer requires a restart, Automatic Updates displays a warning and a countdown for when the computer will restart. Otherwise, the installation occurs in the background.

If it is required to restart the computer, and any user is logged on, a similar countdown dialog box is displayed, warning the logged-on user about the impending restart. You can manipulate computer restarts with Group Policy.

After the new updates are downloaded, Automatic Updates polls the WSUS server again for the list of approved packages to confirm that the packages it downloaded are still valid and approved. This means that, if a WSUS administrator removes updates from the list of approved updates while Automatic Updates is downloading updates, only the updates that are still approved are actually installed.

In this guide

[Configure Clients Using Group Policy](#)

[Configure Clients in a Non-Active Directory Environment](#)

Configure Clients Using Group Policy

When you configure the Group Policy settings for WSUS, you should use a Group Policy object (GPO) linked to an Active Directory container appropriate for your environment. Microsoft does not recommend editing the Default Domain or Default Domain Controller GPOs to add WSUS settings.

In a simple environment, you link the GPO with the WSUS settings to the domain. In more complex environments, you might have multiple GPOs linked to several organizational units (OUs), so that you can set different WSUS policy settings on different types of computer.

After you set up a client computer, it will take a few minutes before it appears on the **Computers** page in the WSUS console. For client computers configured with an Active Directory-based GPO, it will take about 20 minutes after Group Policy refreshes (that is, applies any new settings to the client computer). By default, Group Policy refreshes in the background every 90 minutes, with a random offset of 0–30 minutes.

 **Note**

If you want to refresh Group Policy sooner, you can go to a command prompt on the client computer and type: **gpupdate /force**.

Load the WSUS Administrative Template

Before you can set any Group Policy options for WSUS, you must ensure that the latest administrative template has been loaded on the computer used to administer Group Policy. The administrative template with WSUS settings is named `wuau.adm`. Although there are additional Group Policy settings related to the Windows Update Web site, all the new Group Policy settings for WSUS are contained within the `wuau.adm` file.

If the computer you are using to configure Group Policy has the latest version of `wuau.adm`, you do not need to load the file to configure settings. The new version of `wuau.adm` is available on Windows XP with Service Pack 2. Administrative template files are stored by default in the `%windir%\Inf` directory.

 **Important**

You can find the correct version of `wuau.adm` on any computer that has the WSUS-compatible Automatic Updates installed. You can use the old version of `wuau.adm` to point Automatic Updates to the WSUS server in order to self-update for the first time. After Automatic Updates self-updates, the new `wuau.adm` file appears in the `%windir%\Inf` folder.

If the computer you are using to configure Group Policy does not have the latest version of `wuau.adm`, you must first load it by using the following procedure.

 **Note**

You can start the Group Policy editor by clicking **Start**, then **Run**, then typing **gpedit.msc**.

 **To add the WSUS Administrative Template**

1. In the Group Policy Object Editor, click either of the **Administrative Templates** nodes.
2. On the **Action** menu, click **Add/Remove Templates**.
3. Click **Add**.
4. In the **Policy Templates** dialog box, select **wuau.adm**, and then click **Open**.
5. In the **Add/Remove Templates** dialog box, click **Close**.

Configure Automatic Updates

The settings for this policy enable you to configure how Automatic Updates works. You must specify that Automatic Updates download updates from the WSUS server rather than from Windows Update.

▶ To configure the behavior of Automatic Updates

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **Configure Automatic Updates**.
3. Click **Enabled** and select one of the following options:
 - **Notify for download and notify for install.** This option notifies a logged-on administrative user before the download and before the installation of the updates.
 - **Auto download and notify for install.** This option automatically begins downloading updates and then notifies a logged-on administrative user before installing the updates.
 - **Auto download and schedule the install.** If Automatic Updates is configured to perform a scheduled installation, you must also set the day and time for the recurring scheduled installation.
 - **Allow local admin to choose setting.** With this option, the local administrators are allowed to use Automatic Updates in Control Panel to select a configuration option of their choice. For example, they can choose their own scheduled installation time. Local administrators are not allowed to disable Automatic Updates.
4. Click **OK**.

Specify intranet Microsoft Update service location

The settings for this policy enable you to specify a WSUS server that Automatic Updates will contact for updates. You must enable this policy in order for Automatic Updates to download updates from the WSUS server.

Enter the WSUS server HTTP(S) URL twice, so that the server specified for updates is also used for reporting client events. For example, type **http(s)://servername** in both boxes, where *servername* is the name of the server. Both URLs are required.

To redirect Automatic Updates to a WSUS server

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **Specify Intranet Microsoft update service location**.
3. Click **Enabled** and type the HTTP(S) URL of the same WSUS server in the **Set the intranet update service for detecting updates** box and in the **Set the intranet statistics server** box. For example, type **http(s)://servername** in both boxes, where *servername* is the name of the server. If the port is not 80 for HTTP or 443 for HTTPS, you should add the port number:
https://servername:portnumber.
4. Click **OK**.

Enable client-side targeting

This policy enables client computers to add themselves to target computer groups on the WSUS server, when Automatic Updates is redirected to a WSUS server.

If the status is set to **Enabled**, this computer will identify itself as a member of a particular computer group when it sends information to the WSUS server, which uses it to determine which updates should be deployed to this computer. This setting indicates to the WSUS server which group the client computer should use. You must actually create the group on the WSUS server.

If the status is set to **Disabled** or **Not Configured**, no computer group information will be sent to WSUS.

To enable client-side targeting

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **Enable client-side targeting**.
3. Click **Enabled**, and then type the name of the computer group to which you want to add this computer in the **Target group name for this computer box**.

4. Click **OK**.

Reschedule Automatic Updates scheduled installations

This policy specifies the amount of time that Automatic Updates should wait after system startup before proceeding with a scheduled installation that did not take place earlier.

If the status is set to **Enabled**, a missed installation will occur the specified number of minutes after the computer is next started.

If the status is set to **Disabled**, a missed installation will occur with the next scheduled installation.

If the status is set to **Not Configured**, a missed installation will occur one minute after the next time the computer is started.

This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the [Configure Automatic Updates](#) policy is disabled, this policy has no effect.

To reschedule Automatic Update scheduled installation

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **Reschedule Automatic Update scheduled installations**, click **Enabled**, and type the number of minutes to wait.
3. Click **OK**.

No auto-restart for scheduled Automatic Update installation options

This policy specifies that, to complete a scheduled installation, Automatic Updates will wait for the computer to be restarted instead of causing the computer to restart automatically.

If the status is set to **Enabled**, Automatic Updates will not restart a computer automatically during a scheduled installation if a user is logged on to the computer. Instead, Automatic Updates will notify the user to restart the computer in order to

complete the installation. Be aware that Automatic Updates will not be able to detect future updates until the restart occurs.

If the status is set to **Disabled** or **Not Configured**, Automatic Updates will notify the user that the computer will automatically restart in five minutes to complete the installation. This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the [Configure Automatic Updates](#) policy is disabled, this policy has no effect.



Note

This policy setting does not allow non-administrative Terminal Services users to restart the remote computer where they are logged on. This is because, by default, non-administrative Terminal Services users do not have computer restart privileges.

▶ To prevent auto-restart for scheduled Automatic Update installation options

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **No auto-restart for scheduled Automatic Update installation options**, and click **Enabled**.
3. Click **OK**.

Automatic Update detection frequency

This policy specifies the number of hours that Windows will wait before checking for available updates. The exact wait time is determined by using the number of hours specified minus a random value between 0 and 20 percent of that number. For example, if this policy is used to specify a 20-hour detection frequency, then all computers to which this policy is applied will check for updates anywhere between 16 and 20 hours.

If the status is set to **Enabled**, Automatic Updates will check for available updates at the specified interval.

If the status is set to **Disabled** or **Not Configured**, Automatic Updates will check for available updates at the default interval of 22 hours.

▶ To set Automatic Update detection frequency

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click

Windows Update.

2. In the details pane, click **Automatic Update detection frequency**, click **Enabled**, and type the number of hours for the detection interval.
3. Click **OK**.

Allow Automatic Update immediate installation

This policy specifies whether Automatic Updates should automatically install certain updates that neither interrupt Windows services nor restart Windows.

If the status is set to **Enabled**, Automatic Updates will immediately install these updates after they have been downloaded and are ready to install.

If the status is set to **Disabled**, such updates will not be installed immediately.

To allow Automatic Update immediate installation

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **Allow Automatic Update immediate installation**, and click **Enabled**.
3. Click **OK**.

Delay restart for scheduled installations

This policy specifies the amount of time that Automatic Updates should wait before proceeding with a scheduled restart.

If the status is set to **Enabled**, a scheduled restart will occur the specified number of minutes after the installation is finished.

If the status is set to **Disabled** or **Not Configured**, the default wait time is five minutes.

To delay restart for scheduled installations

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.

2. In the details pane, click **Delay restart for scheduled installations**, click **Enabled**, and type the number of minutes to wait.
3. Click **OK**.

Reprompt for restart with scheduled installations

This policy setting specifies the amount of time that Automatic Updates should wait before prompting the user again for a scheduled restart.

If the status is set to **Enabled**, a scheduled restart will occur the specified number of minutes after the prompt for restart was dismissed.

If the status is set to **Disabled** or **Not Configured**, the default interval is 10 minutes.

To reprompt for restart with scheduled installations

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **Re-prompt for restart with scheduled installations**, click **Enabled**, and type the number of minutes to wait before restarting.
3. Click **OK**.

Allow non-administrators to receive update notifications

This policy specifies whether logged-on non-administrative users will receive update notifications. If Automatic Updates is configured (by policy or locally) to notify the user either before downloading and installation or only before installation, these notifications will be offered to any user, administrator, or non-administrator who is logged on to the computer.

If the status is set to **Enabled**, Automatic Updates will include non-administrators when determining which logged-on user should receive notification.

If the status is set to **Disabled** or **Not Configured**, Automatic Updates will notify only logged-on administrators.

▶ **To allow non-administrators to receive update notifications**

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **Allow non-administrators to receive update notifications**, and click **Enabled**.
3. Click **OK**.



Note

This policy setting does not allow non-administrative Terminal Services users to restart the remote computer where they are logged in. This is because, by default, non-administrative Terminal Services users do not have computer restart privileges.

Allow signed content from the intranet Microsoft update service location

If this policy setting is enabled, Automatic Updates receives signed third-party updates from the Windows Server Update Services server. If this policy is not enabled, users will be able to get updates only from Microsoft.

▶ **To allow signed content from the intranet Microsoft Update service location**

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, click **Allow signed content from intranet Microsoft update service location**, and click **Enabled**.
3. Click **OK**.

Remove links and access to Windows Update

If this policy setting is enabled, Automatic Updates receives updates from the WSUS server. Users who have this policy setting enabled cannot get updates from a Windows Update Web site that you have not approved. If this policy setting is not enabled, the **Windows Update** icon remains on the **Start** menu; local administrators will be able to visit the Windows Update Web site, from which they could install unapproved software.

This happens even if you have specified that Automatic Updates must get approved updates from your WSUS server. In Windows Vista, this setting will gray out the **Check for updates** option in the **Windows Update** application.

▶ **To remove links and access to Windows Update**

1. In the Group Policy Object Editor, expand **User Configuration**, expand **Administrative Templates**, and then click **Start Menu and Taskbar**.
2. In the details pane, click **Remove links and access to Windows Update**, and click **Enabled**.
3. Click **OK**.

Disable access to Windows Update

If this policy setting is enabled, all Windows Update features are removed. It blocks access to the Microsoft Update and Windows Update Web sites, and in Windows Vista will gray out the **Check for updates** option in the **Windows Update** application. The machine will not get automatic updates directly from Windows Update or Microsoft Update, but it can still get updates from a WSUS server. This setting overrides the user settings **Remove links and access to Windows Update** and **Remove access to use all Windows Update features**.

▶ **To disable access to Windows Update**

1. In the Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, expand **Internet Communication Management**, and then click **Internet Communication settings**.
2. In the details pane, click **Turn off access to all Windows Update features**, and click **Enabled**.
3. Click **OK**.

Configure Clients in a Non-Active Directory Environment

In a non-Active Directory environment, you can configure Automatic Updates by using any of the following methods:

- Using Group Policy Object Editor and editing the Local Group Policy object
- Editing the registry directly by using the registry editor (Regedit.exe)

Editing the Local Group Policy object

For a listing of the entries and the values to set, see [Configure Clients Using Group Policy](#) earlier in this guide.

Using the registry editor

Administrators who do not wish to use Group Policy may set up client computers using the registry. Registry entries for the WSUS server are located in the following subkey:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate.

The keys and their value ranges are listed in the following table.

Windows Update registry keys

Entry name	Data type	Values
AcceptTrustedPublisherCerts	Reg_DWORD	Range = 1 0 1 = Enabled. The WSUS server will distribute signed third-party updates if available. 0 = Disabled. The WSUS server will not distribute third-party updates.

Entry name	Data type	Values
ElevateNonAdmins	Reg_DWORD	Range = 1 0 1 = Users in the Users security group are allowed to approve or disapprove updates. 0 = Only users in the Administrators user group can approve or disapprove updates.
TargetGroup	Reg_SZ	Name of the computer group to which the computer belongs, used to implement client-side targeting (for example, "TestServers.") This policy is paired with TargetGroupEnabled .
TargetGroupEnabled	Reg_DWORD	Range = 1 0 1 = Use client-side targeting. 0 = Do not use client-side targeting. This policy is paired with TargetGroup .
WUServer	Reg_SZ	HTTP(S) URL of the WSUS server used by Automatic Updates and (by default) API callers. This policy is paired with WUStatusServer ; both must be set to the same value in order for them to be valid.

Entry name	Data type	Values
WUStatusServer	Reg_SZ	The HTTP(S) URL of the server to which reporting information will be sent for client computers that use the WSUS server configured by the WUStatusServer key. This policy is paired with WUStatusServer ; both must be set to the same value in order for them to be valid.
DisableWindowsUpdateAccess	Reg_DWORD	Range = 1 0 1 = Disables access to Windows Update. 0 = Enables access to Windows Update.

Automatic Update configuration options

The registry entries for Automatic Update configuration options are located in the following subkey:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

The keys and their value ranges are listed in the following table.

Automatic Updates Configuration Registry Keys

Entry name	Data type	Value range and meanings
AUOptions	Reg_DWORD	Range = 2 3 4 5 2 = Notify before download. 3 = Automatically download and notify of installation. 4 = Automatically download and schedule installation. (Only valid if values exist for ScheduledInstallDay and ScheduledInstallTime .) 5 = Automatic Updates is required, but end users can configure it.
AutoInstallMinorUpdates	Reg_DWORD	Range = 0 1 0 = Treat minor updates as other updates are treated. 1 = Silently install minor updates.
DetectionFrequency	Reg_DWORD	Range = n, where n = time in hours (1–22). Time between detection cycles.
DetectionFrequencyEnabled	Reg_DWORD	Range = 0 1 1 = Enable DetectionFrequency. 0 = Disable custom DetectionFrequency (use default value of 22 hours).

Entry name	Data type	Value range and meanings
NoAutoRebootWithLoggedOnUsers	Reg_DWORD	Range = 0 1 1 = Logged-on user gets to choose whether or not to restart his or her computer. 0 = Automatic Updates notifies user that the computer will restart in 5 minutes.
NoAutoUpdate	Reg_DWORD	Range = 0 1 0 = Enable Automatic Updates. 1 = Disable Automatic Updates.
RebootRelaunchTimeout	Reg_DWORD	Range = n, where n = time in minutes (1–1,440). Time between prompting again for a scheduled restart.
RebootRelaunchTimeoutEnabled	Reg_DWORD	Range = 0 1 1 = Enable RebootRelaunchTimeout 0 = Disable custom RebootRelaunchTimeout (use default value of 10 minutes)
RebootWarningTimeout	Reg_DWORD	Range = n, where n = time in minutes (1–30). Length, in minutes, of the restart warning countdown, after installing updates with a deadline or scheduled updates.

Entry name	Data type	Value range and meanings
RebootWarningTimeoutEnabled	Reg_DWORD	Range = 0 1 1 = Enable RebootWarningTimeout 0 = Disable custom RebootWarningTimeout (use default value of 5 minutes)
RescheduleWaitTime	Reg_DWORD	Range = n, where n = time in minutes (1–60). Time, in minutes, that Automatic Updates should wait at startup before applying updates from a missed scheduled installation time. Note that this policy applies only to scheduled installations, not deadlines. Updates whose deadlines have expired should always be installed as soon as possible.
RescheduleWaitTimeEnabled	Reg_DWORD	Range = 0 1 1 = Enable RescheduleWaitTime 0 = Disable RescheduleWaitTime (attempt the missed installation during the next scheduled installation time).
ScheduledInstallDay	Reg_DWORD	Range = 0 1 2 3 4 5 6 7 0 = Every day. 1 through 7 = The days of the week from Sunday (1) to Saturday (7). (Only valid if AUOptions = 4.)

Entry name	Data type	Value range and meanings
ScheduledInstallTime	Reg_DWORD	Range = n, where n = the time of day in 24-hour format (0–23).
UseWUserver	Reg_DWORD	Range = 0 1 1 = This machine gets its updates from a WSUS server. 0 = This machine gets its updates from Microsoft Update. The WUserver value is not respected unless this key is set.

Automatic Updates scenarios

The following scenarios illustrate specific issues

RescheduleWaitTime

If a scheduled installation is missed (because the client computer was turned off) and **RescheduleWaitTime** is not set to a value between 1 and 60, Automatic Updates waits until the next scheduled day and time to perform the installation. If a scheduled installation is missed and **RescheduleWaitTime** is set to a value between 1 and 60, then Automatic Updates reschedules the installation to occur at the Automatic Updates service start time plus the number of minutes specified in **RescheduleWaitTime**.

There are 3 basic rules for this feature:

1. When a scheduled installation is missed, it will be rescheduled for the system startup time plus the value of **RescheduleWaitTime**.
2. Changes in the scheduled installation day and time via the Control Panel or Group Policy are respected over the rescheduled time.
3. The rescheduled time has precedence over the next calculated scheduled day and time if the “next calculated scheduled day and time” is later than the rescheduled time. The “next calculated scheduled day and time” is calculated as follows:

- a. When Automatic Updates starts, it uses the currently set schedule to calculate the “next calculated scheduled day and time”.
- b. The resulting day and time value is then compared to the **ScheduledInstallDate**.
- c. If the values are different, Automatic Updates performs the following actions:
 - sets a new “next calculated scheduled day and time” within Automatic Updates.
 - writes this new “next calculated scheduled day and time” to the **ScheduledInstallDate** registry key.
 - logs an event stating the new scheduled installation day and time.

The following examples show the use of the **RescheduleWaitTime** value.

Example 1: Installation must occur immediately following system startup

This example shows the consequences of **RescheduleWaitTime** set to 1.

1. Update installations are scheduled to occur every day at 3:00 A.M.
2. The **RescheduleWaitTime** registry value is set to 1.
3. Automatic Updates finds an update, downloads it, and is ready to install it at 3:00 A.M.
4. The logged-on user does not see the “ready to install” prompt because the user does not have administrative privileges on the computer.
5. The user shuts down the computer.
6. The user restarts on the computer after the scheduled time has passed.
7. When Automatic Updates starts, it recognizes that it missed its previously set scheduled installation time and that **RescheduleWaitTime** is set to 1. It therefore logs an event with the new scheduled time (one minute after the current time).
8. If no one logs on before the newly scheduled time (1 minute interval) the installation begins. Since no one is logged on, there is no delay and no notification. If the update requires it, Automatic Updates will restart the computer.
9. The user logs on to the updated computer.

Example 2: Installations must occur fifteen minutes after the Automatic Updates service starts

This example shows the consequences of **RescheduleWaitTime** set to 15.

1. Update installations are scheduled to occur every day at 3:00 A.M.
2. The local administrator of the client computer sets the RescheduleWaitTime registry value to 15.
3. Automatic Updates finds an update, downloads it, and is ready to install it at 3:00 A.M.
4. The local administrator ignores the prompt to install the update.
5. The local administrator shuts down the computer.
6. The local administrator restarts on the computer after the scheduled time has passed.
7. When Automatic Updates starts, it recognizes that it missed its previously set scheduled install time, and that **RescheduleWaitTime** is set to 15. It therefore logs an event with the new scheduled time (fifteen minutes after the current time).
8. The local administrator logs on before the newly-scheduled time.
9. After Automatic Updates has been running for 15 minutes, it starts the scheduled installation.
10. The local administrator is notified five minutes before installation begins by the countdown timer.
11. The timer expires and the installation proceeds.

NoAutoRebootWithLoggedOnUsers

To prevent Automatic Updates from restarting a computer while users are logged on, the administrator can create the NoAutoRebootWithLoggedOnUsers registry value in s. The value is a DWORD and must be either 0 (false) or 1 (true). If this value is changed while the computer is in a restart pending state, it will not take effect until the next time an update requires a restart.

When the admin creates and sets the **NoAutoRebootWithLoggedOnUsers** registry key to 1, the restart countdown dialog that pops up for the logged on user (active and inactive) will change in the following ways:

Users with administrator credentials	Users without administrator credentials
The No button will be active.	The No button will be inactive.

Users with administrator credentials	Users without administrator credentials
The Yes button will be active if the logged-on user is the only administrator logged on at the time the restart dialog appears.	The Yes button will now be active only if the logged-on user is the only non-administrator logged on at the time the restart dialog appears. However, the Yes button will be inactive if the user's local security policy prohibits restarting.
The restart countdown progress bar and the text underneath the progress bar will not display.	The restart countdown progress bar and the text underneath the progress bar will not display.

Example 1: Non-administrator user on a workstation

In this scenario the network has been set up with the following conditions:

- Updates are scheduled to be installed every day at 3:00 A.M.
- Users must run as non-administrative users.
- **NoAutoRebootWithLoggedOnUsers** is set to 1.
- The user is assigned **Shut down the system** privileges via Group Policy.

Resulting client behavior:

1. Automatic Updates detects and downloads an update and sets the scheduled installation time to 3:00 A.M.
2. The logged on non-administrative user leaves the workstation locked at the end of the day.
3. The scheduled installation starts At 3:00 A.M.
4. This update requires a restart, so Automatic Updates pops up a dialog to the user's locked session saying that a restart is required.
5. At 9:00 A.M. the user unlocks the workstation and sees the restart prompt.
6. The user is unable to click **No** to dismiss the dialog, but can click **Yes** because no other users are logged on to the workstation. There is no timeout, so the user can accept the prompt to restart at a convenient time.

Example 2: Non-administrator user on a server

In this scenario the network has been set up with the following conditions:

- By default, users who do not have administrative privileges are not allowed to restart Windows Servers. This is enforced by the local security policies.
- Multiple non-administrator users are logged on at the time the scheduled installation begins.
- The installation requires that the computer be restarted.

Resulting client behavior:

1. Users are notified of the installation.
2. When the installation requires a restart, all logged-on users are notified that the computer must be restarted.
3. Event ID 21 is written to the system event log:
4. Non-administrator users are not allowed to dismiss the dialog by clicking **No**.
5. Since non-administrator users do not have permissions to restart the server, the **Yes** button is also disabled.
6. If new users log on, they also receive the notification that the server needs to restart.

Every time a user logs off, Automatic Updates tests to see if there are any users still logged on.

When there are no logged-on users (therefore no opportunity for user data loss), Automatic Updates writes Event ID 22 to the system event log as shown below, and begins the restart procedure.

Summary of behavior for NoAutoRebootWithLoggedOnUsers settings

The following table shows the difference in behavior with **NoAutoRebootWithLoggedOnUsers** enabled (set to 1) or disabled/not configured (not set to 1).

Scenario following a scheduled installation	With NoAutoRebootWithLoggedOnUsers enabled	With NoAutoRebootWithLoggedOnUsers disabled or not configured
No users logged on	Automatic restart immediately following installation	Automatic restart immediately following installation
Single user with administrative privileges	Restart notification allows user to start or postpone restart. This notification does not have a countdown timer. Therefore the user must initiate the system restart.	Restart notification allows user to start or postpone restart. This notification has a 5 minute countdown timer. When the timer expires, the automatic restart begins.
Single user with restart privileges but no other administrative privileges	Restart notification that allows user to initiate the restart but not to postpone it. This notification does not have a countdown timer. Therefore the user must initiate the system restart.	Restart notification that allows user to initiate the restart but not to postpone it. This notification has a 5-minute countdown timer. When the timer expires, the automatic restart begins.
Single non-administrator without restart privilege	Restart notification that does not allow the user to initiate the restart or postpone it. This notification does not have a countdown timer. Therefore the user must wait for an authorized user to initiate the system restart.	Restart notification that does not allow the user to initiate the restart or postpone it. This notification has a 5-minute countdown timer. When the timer expires, the automatic restart begins.
Administrator while other users are logged on	Restart notification that does not allow the user to initiate the restart but does allow the user to postpone it. This notification does not have a countdown timer. Therefore the user must initiate the system restart.	Restart notification that does not allow the user to initiate the restart but does allow the user to postpone it. This notification has a 5 minute countdown timer. When the timer expires, the automatic restart begins.

Scenario following a scheduled installation	With NoAutoRebootWithLoggedOnUsers enabled	With NoAutoRebootWithLoggedOnUsers disabled or not configured
Non-administrator with restart privilege while other users are logged on	Restart notification that does not allow the user to initiate the restart or postpone it. This notification does not have a countdown timer. Therefore the user must initiate the system restart.	Restart notification that does not allow the user to initiate the restart or postpone it. This notification has a 5 minute countdown timer. When the timer expires, the automatic restart begins.
Non-administrator without restart privilege while other users are logged on	Restart notification that does not allow the user to initiate the restart or postpone it. This notification does not have a countdown timer. Therefore, the user must wait for an authorized user to initiate the system restart.	Restart notification that does not allow the user to initiate the restart or postpone it. This notification has a 5 minute countdown timer. When the timer expires, the automatic restart begins.

Note: After all users log off, Automatic Updates will restart the computer to complete the installation of the update.

Interaction with other settings

If the “Remove access to use all Windows Update features” setting (**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate\DisableWindowsUpdateAccess**) is enabled, Automatic Updates will not notify that logged-on user. It makes a local administrator appear as a non-administrator, so that user will not be able to install updates. When this policy is enabled, the Automatic Updates service still runs, and scheduled installations will still occur if they were configured to run.

If the “Remove links and access to Windows Update” Group Policy setting (**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWindowsUpdate**) is enabled, then Automatic Updates will continue to get updates from the WSUS server. Users with this policy set will not be able to get updates that the WSUS administrator has not approved on the WSUS server. If this policy is not enabled, the Microsoft Update icon will remain on the Start menu; local administrators will be able to visit the Microsoft Update Web site and install software that the WSUS administrator has not approved. This happens even if you have specified that Automatic

Updates should get approved updates from the WSUS server. In Windows Vista, enabling this setting will gray out the **Check for updates** option in the **Windows Update** application.

The above settings can be overridden by the **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\DisableWindowsUpdateAccess** setting.

Manipulate Client Behavior Using Command-line Options

There are two documented command-line options used for manipulating Automatic Updates behavior. These options are helpful for testing and troubleshooting client computers. For comprehensive troubleshooting information for problems with both the WSUS server and client computers, see the [Microsoft Windows Server Update Services](http://go.microsoft.com/fwlink/?LinkId=81072) at <http://go.microsoft.com/fwlink/?LinkId=81072>.

Detectnow Option

Because waiting for detection to start can be a time-consuming process, an option has been added to allow you to initiate detection right away. On one of the computers with the new Automatic Update client installed, run the following command at the command prompt:

```
wuauclt.exe /detectnow
```

Resetauthorization Option

WSUS uses a cookie on client computers to store various types of information, including computer group membership when client-side targeting is used. By default, this cookie expires an hour after WSUS creates it. If you are using client-side targeting and change group membership, use this option in combination with **detectnow** to expire the cookie, initiate detection, and have WSUS update computer group membership.

Note that when combining parameters, you can use them only in the order specified as follows:

```
wuauclt.exe /resetauthorization /detectnow
```

Client Behavior with Update Deadlines

You can specify a deadline when you approve an update or set of updates on the WSUS server. Setting a deadline will cause clients to install the update at a specific time, but there are a number of different situations, depending on whether the deadline has expired, whether there are other updates in the queue for the client to install, and whether the update (or another update in the queue) requires a restart.

Expired and unexpired deadlines

If the client contacts the server after the update deadline has passed, it will try to install the update as soon as possible. WSUS administrators can set update deadlines to a date in the past in order to have clients install the update immediately.

If the deadline has not passed, the client will download the update and install it the next time an install occurs. For example, if the client downloads an update with a deadline of 6:00 A.M., and the scheduled installation time is 3:00 A.M., the update will be installed at 3:00 A.M. Likewise, if a user starts an install before a (downloaded) update's deadline, the update will be installed.

Deadlines and updates that require restarts

Updates that have deadlines and require restarts will cause a forced restart at the time of the deadline, no matter when the update was actually installed. For example, if an update with a 6:00 A.M. deadline was downloaded and installed at 3:00 A.M., but the computer was not restarted at that time, it will be restarted at 6:00 A.M.

Moreover, if the computer is pending restart (because another update requiring a restart was installed, but the computer was not restarted), and an update with a deadline is installed, the computer will be restarted. The following is an example of client behavior with an unexpired deadline:

1. Update 1, which has no deadline but requires restart, is installed at 1:00 A.M., and the computer is not restarted.
2. Update 2, which has a deadline of 6:00 A.M. and does not require restart, is downloaded and installed at 3:00 A.M.
3. The computer is restarted at 6:00 A.M. (the deadline of Update 2).

The following is an example of client behavior with an expired deadline:

1. Update 1, which has no deadline but requires restart, is installed at 2:00 A.M., and the computer is not restarted.
2. Update 2, which has a deadline of 1:00 A.M. and does not require restart, is downloaded and installed at 3:00 A.M.
3. The computer is restarted after Update 2 is installed, at 3:00 A.M. (the first possible restart time).

WSUS updates and deadlines

A WSUS update (an update that is required in order for WSUS to continue functioning correctly) has installation priority over other kinds of update. If an update with a deadline is blocked by a WSUS update, the deadline will apply to the WSUS update, as in the following sequence of events:

1. Update 1, which is a WSUS update with a deadline of 6:00 A.M., and Update 2, which is a non-WSUS update with a deadline of 2:00 A.M., are both downloaded at 1 A.M.
2. The next scheduled install is at 3:00 A.M.
3. The install of Update 1 starts at 2:00 A.M.

If the deadline of a blocked update has expired, the WSUS update that is blocking it will be installed immediately.

Set Up a Disconnected Network (Import and Export the Updates)

Managing WSUS on a disconnected network involves exporting updates and metadata from a WSUS server on a connected network and then importing them to the WSUS server on the disconnected network. There is a conceptual discussion of this feature in the "Networks Disconnected from the Internet" section in [Choose a Type of WSUS Deployment](#) earlier in this guide.

There are three steps to exporting and then importing updates:

1. Make sure that the options for express installation files and update languages on the exporting server are compatible with the settings on the importing server. This ensures that you collect the updates you intend to distribute.

2. Copy updates from the file system of the export server to the file system of the import server.
3. Export update metadata from the database on the export server, and import it into the database on the import server. The last section explains how to import exported updates to a replica server.

In this guide

- [Step 1: Matching Advanced Options](#)
- [Step 2: Copying Updates from the File System](#)
- [Step 3: Copying Metadata from the Database](#)
- [Importing Updates to Replica Servers](#)

Step 1: Matching Advanced Options

Make sure that the options for express installation files and languages on the exporting server match the settings on the importing server. For example, if you did not select the option for express installation files on the exporting server but did have the express installation file option selected on the importing server, you would not be able to distribute updates by using express installation files, because none were synchronized by the exporting server. A mismatch of language settings can have a similar effect.

You do not have to concern yourself with matching the settings for schedule, products and classifications, source, or proxy server. The setting for deferred download of updates has no effect on the importing server. If you are using the option for deferred downloads on the exporting server, you must approve the updates so they can be downloaded before taking the next step, which is migrating updates to the importing server.

To ensure that express installation and language options on the exporting server match settings on the importing server

1. In the WSUS Administration snap-in of the exporting server, click the **Options** node in the left pane, and then click **Update Files and Languages**.
2. In the **Update Files** tab, check the setting for **Download express installation files**.
3. In the **Update Languages** tab, check the settings for the update languages.
4. In the WSUS Administration snap-in of the importing server, click the **Options** node in the left pane, and then click **Update Files and Languages**.

5. Make sure the settings for **Download express installation files** and **Languages** options match the selections on the exporting server.

For more information about these options, see the topics "Using Express Installation Files" and "Filtering Updates" in [Determine Bandwidth Options to Use](#) earlier in this guide.

Step 2: Copying Updates from the File System

Copy updates from the file system of the exporting server to the file system of the importing server. The procedures described below use the Windows Backup or Restore Wizard, but you can use any utility you like, including xcopy. The object is to copy updates from the file system on the exporting server to the files system of the importing server. When you copy files to the importing server, you must maintain the folder structure for all folders under the content directory. Make sure that the updates appear in the folder on the importing server that has been designated to store updates; this designation is typically made during the setup process. You should also consider using an incremental backup system to limit the amount of data you need to move each time you refresh the server on the disconnected network.

To back up updates from file system of the exporting server to a file

1. On your exporting WSUS server, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **ntbackup**. The **Backup or Restore Wizard** starts by default, unless it is disabled. You can use this wizard or click the link to work in **Advanced Mode** and use the following steps.
3. Click the **Backup** tab, and then select the folder where updates are stored on the exporting server. By default, WSUS stores updates at *WSUSInstallationDrive\WSUS\WSUSContent*, where *WSUSInstallationDrive* is the drive on which WSUS is installed.
4. In the **Backup media or file name** box, type a path and file name for the backup (.bkf) file.
5. Click **Start Backup**. The **Backup Job Information** dialog box appears.
6. Click **Advanced**. Under **Backup Type**, click **Incremental**.
7. From the **Backup Job Information** dialog box, click **Start Backup** to start the

backup operation.

8. Copy the backup file you just created to the importing server.

▶ **To restore updates from a file to the file system of the importing server**

1. On your importing WSUS server, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **ntbackup**. The **Backup or Restore Wizard** starts by default, unless it is disabled. You can use this wizard or click the link to work in **Advanced Mode** and use the following steps.
3. Click the **Restore and Manage Media** tab, and select the backup file you created on the exporting server. If the file does not appear, right-click **File**, and then click **Catalog File** to add the location of the file.
4. In the **Restore files to** box, click **Alternate location**. This option preserves the folder structure of the updates; all folders and subfolders will appear in the folder you designate. You must maintain the directory structure for all folders under `\WSUSContent`.
5. Under **Alternate location**, specify the folder where updates are stored on the importing server. By default, WSUS stores updates at `WSUSInstallationDrive\WSUS\WSUSContent\`, where *WSUSInstallationDrive* is the drive on which WSUS is installed. Updates must appear in the folder on the importing server designated to hold updates; this is typically done during installation.
6. Click **Start Restore**. When the **Confirm Restore** dialog box appears, click **OK** to start the restore operation.

Step 3: Copying Metadata from the Database

Export update metadata from the database on the exporting server and import it into the database on the importing server using the WSUSUtil.exe utility program. For more information about this utility, see "Managing WSUS 3.0 from the Command Line", in the [Windows Server Update Services 3.0 Operations Guide](http://go.microsoft.com/fwlink/?LinkId=81072) at <http://go.microsoft.com/fwlink/?LinkId=81072>.

 **Note**

You must be a member of the local Administrators group on the WSUS server to export or import metadata; both operations can be run only on a WSUS server.

You should copy updates to a directory on the importing server before you import metadata. If WSUS finds metadata for an update that is not in the file system, the WSUS console shows that the update failed to be downloaded. This type of problem can be fixed by copying the update to a directory on the importing server and then deploying the update again.

Although you can use incremental backups to move update files to the importing server, you cannot move update metadata incrementally. WSUSutil.exe exports all the metadata in the WSUS database during the export operation.

 **Important**

Never import exported data from a source that you do not trust. Importing content from a source you do not trust might compromise the security of your WSUS server.

 **Note**

During the import or export process, the Update Service, the Windows NT service that underpins the WSUS application, is shut down.

 **To export metadata from the database of the exporting server**

1. At the command prompt on the exporting server, navigate to the folder that contains WSUSutil.exe (usually ...\\Program Files\\Update Services\\Tools).
2. Type the following:

```
wsusutil.exe exportpackagename logfile
```

For example:

```
wsusutil.exe export export.cab export.log
```

The package (.cab file) and log file name must be unique. WSUSutil.exe creates these two files as it exports metadata from the WSUS database.

3. Move the export package you just created to the importing server.

 **To import metadata to the database of the importing server**

1. At the command prompt on the importing server, navigate to the directory that contains WSUSutil.exe (usually ...\\Program Files\\Update Services\\Tools).

2. Type the following:

```
wsusutil.exe import packagename logfile
```

For example:

```
wsusutil.exe import export.cab import.log
```

WSUSUtil.exe imports the metadata from the exporting server and creates a log file of the operation.



Note

It can take 3–4 hours for the database to validate content that has just been imported.

Importing Updates to Replica Servers

In some situations, you may need to import updates or metadata to a replica server. For example, you may wish to speed up the initial synchronization by copying the updates to the replica server. To copy update content to a replica server, you may use the same steps described in [Step 2: Copying Updates from the File System](#). However, because metadata is not ordinarily kept on the replica server, you must temporarily turn off the replica setting on the server, import the metadata, and then turn it on again.

Import metadata to a replica server

To import metadata to a replica server

1. In the WSUS Administration snap-in, go to **Options**, then select **Update Source and Proxy Server**.
2. On the **Update Source** tab, clear the **This server is a replica server of the upstream server** check box, and then click **OK** to save the setting.
3. Follow the procedures for exporting and importing metadata described in [Step 3: Copying Metadata from the Database](#).
4. After completing the import, go back to the **Update Source** tab of the **Update Source and Proxy Server** page, and then select the **This server is a replica server of the upstream server** check box. Click **OK** to save the setting.

Appendix A: Unattended Installations

You can use command-line parameters to run WSUS Setup in unattended mode. When running this way, WSUS Setup does not display a user interface (UI). If you need to troubleshoot the setup process, use the log files, which you can find at the following location:

WSUSInstallationDrive:\Program Files\Microsoft Windows Server Update Services\LogFiles\

Use command-line parameters from a command prompt.

Type the following command:

WSUSSetup.exe /*command-line parameter property=value*

where *command-line parameter* is a command-line parameter from the WSUS Setup command-line parameters table, where *property* is a property from the WSUS Setup properties table, and where *value* is the actual value of the property being passed to WSUS. Both tables are included below.

If you need to pass a value to WSUS Setup, use the property name, an equals sign ("="), and its value. Properties are always paired with values. For example, if you wanted WSUS Setup to install silently and set the WSUS Content Directory to the D:\WSUS directory, you would use the following syntax:

WSUSSetup.exe /q CONTENT_DIR=D:\WSUS

If you need help with WSUSutil.exe, you can use the **/help** command to display the list of command-line parameters:

WSUSSetup.exe /help

WSUS setup command-line parameters

Option	Description
/q	Perform silent installation.
/u	Uninstall the product. Also uninstalls the Windows Internal Database instance if it is installed.

Option	Description
/p	Prerequisite check only. Does not install the product, but inspects the system and reports any prerequisites that are missing.
/?, /h	Display command-line parameters and their descriptions.
/g	Upgrade from the 2.0 version of WSUS. The only valid parameter with this option is /q (silent installation). The only valid property with this option is DEFAULT_WEBSITE.

WSUS setup properties

Property	Description
CONTENT_LOCAL	0=content hosted locally, 1=host on Microsoft Update
CONTENT_DIR	Path to content directory. Default is <i>WSUSInstallationDrive\WSUS\WSUSContent</i> , where <i>WSUSInstallationDrive</i> is the local drive with the largest amount of free space.
WYUKON_DATA_DIR	Path to Windows Internal Database data directory.
SQLINSTANCE_NAME	The name should appear in the format <i>ServerName\SQLInstanceName</i> . If the database instance is on the local machine, use the %COMPUTERNAME% environment variable. If an existing instance is not present, the default is %COMPUTERNAME%\WSUS.
DEFAULT_WEBSITE	0=port 8530, 1=port 80
PREREQ_CHECK_LOG	Path and file name for log file
CONSOLE_INSTALL	0=install the WSUS server, 1=install console only
ENABLE_INVENTORY	0=do not install inventory features, 1=install inventory features

Property	Description
DELETE_DATABASE	0=retain database, 1=remove database
DELETE_CONTENT	0=retain content files, 1=remove content files
DELETE_LOGS	0=retain log files, 1=remove log files (used with the /u install switch).
CREATE_DATABASE	0=use current database, 1=create database
PROGRESS_WINDOW_HANDLE	Window handle to return MSI progress messages
MU_ROLLUP	1=join Microsoft Update Improvement Program, 0=don't join
FRONTEND_SETUP	1=do not write the content location to the database, 0=write the content location to the database (for NLB)

Appendix B: Configure Remote SQL

WSUS offers limited support for running database software on a computer that is separate from the computer where the rest of WSUS is installed. This section offers step-by-step instructions for how to install WSUS in this configuration.

Setting up WSUS for remote SQL is a three-step process:

1. Install and configure SQL Server 2005 on the back-end server.
2. Check that the administrator who is going to install WSUS 3.0 also has permissions on SQL Server
3. Install WSUS 3.0 on the front-end computer, and configure it to use the database on the back-end computer.



Note

For a remote SQL installation on WSUS 3.0, you install WSUS on the front-end computer only. You do not need to install WSUS on the back-end computer.

Remote SQL limitations

- You cannot use a server configured as a domain controller for the back end of the remote SQL pair.
- You must not be running Terminal Server on the computer that will be the front end server of a remote SQL installation.
- You must use at least Microsoft SQL Server 2005 Service Pack 1 (available on the [Microsoft Download Center](http://go.microsoft.com/fwlink/?LinkId=66143) (<http://go.microsoft.com/fwlink/?LinkId=66143>) for database software on the back-end computer if that computer is running Windows Server 2003, and SQL Server 2005 Service Pack 2 if it is running Windows Server® Code Name "Longhorn".
- Both the front-end and the back-end computers must be joined to an Active Directory domain, otherwise, if they are in different domains, you must establish cross-domain trust between the domains before running WSUS setup.
- If you already have WSUS 2.0 installed in a remote SQL configuration and wish to upgrade to WSUS 3.0, you should uninstall WSUS 2.0 (using **Add or Remove Programs** in Control Panel) on the back-end computer while ensuring that the existing database remains intact. Then you should install SQL Server 2005 Service Pack 1 and upgrade the existing database. Finally, you should install WSUS 3.0 on the front-end computer.

Database requirements

WSUS 3.0 requires SQL Server 2005 with Service Pack 1 on Windows Server 2003 and SQL Server 2005 Service Pack 2 on Windows Server "Longhorn". If you use the full version of SQL Server, the SQL Server administrator should first verify that the nested triggers option on SQL Server is turned on. Do this before setting up the WSUS database.

You cannot use SQL authentication. WSUS supports only Windows authentication. WSUS Setup creates a database named SUSDB. For more information about what is stored in the WSUS database or how it functions, see [Choose the Database Used for WSUS 3.0](#) earlier in this guide.

Step 1: Install SQL Server 2005 Service Pack 1 on the back-end computer

Install a SQL Server 2005 database on the back-end computer and enable remote connections. You may use a named instance or the default instance for the WSUS database.

► Set Up Remote SQL Connections

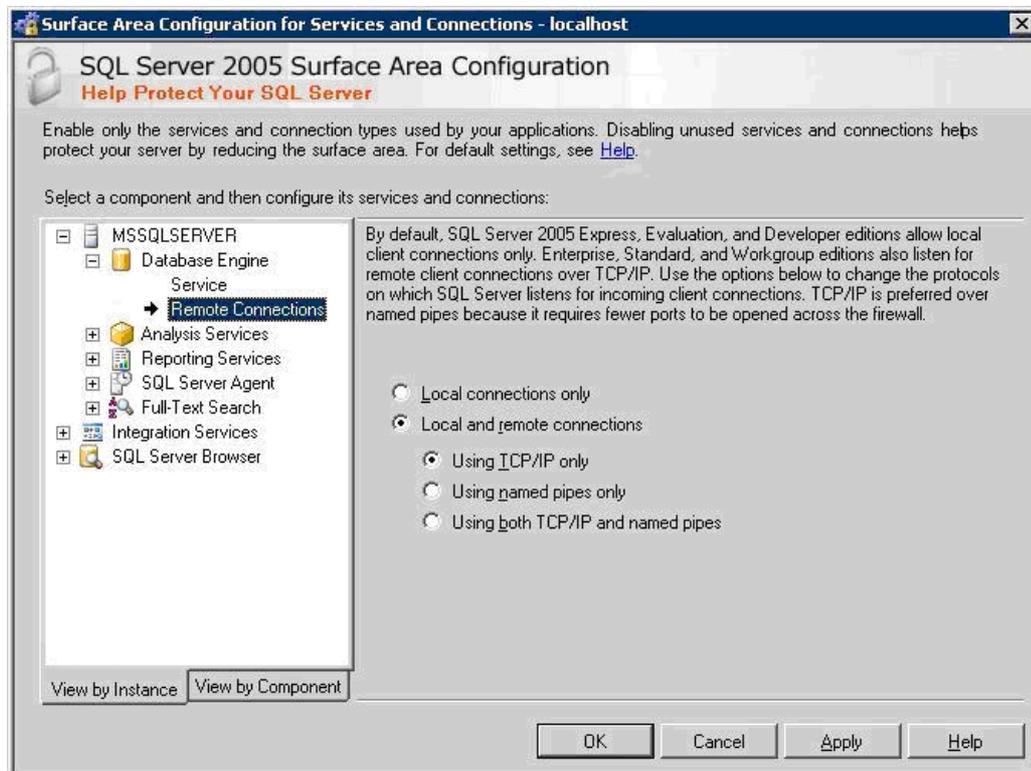
1. Click **Start**, point at **All Programs**, point at **SQL Server 2005**, point at **Configuration Tools**, and select **SQL Server Surface Area Configuration**.
2. Choose **Surface Configuration for Services and Connections**.



► Enable Remote SQL Connections

1. In the left window, click the **Remote Connections** node.
2. Select **Local and remote connections** and then select **Using TCP/IP only**.

3. Click **OK** to save the settings.



If you plan to run the SQL Server service remotely under a domain account, you will need to register a service principal name (SPN) for this server. For more information about adding an SPN, please see [How to make sure that you are using Kerberos authentication when you create a remote connection to an instance of SQL Server 2005](http://go.microsoft.com/fwlink/?LinkId=85942) (<http://go.microsoft.com/fwlink/?LinkId=85942>).

Important

Running the SQL Server service under a local non-system account is not supported.

Step 2: Check administrative permissions on SQL Server

You should make sure that the person who is going to install WSUS 3.0 on the front-end computer has administrative permissions on SQL Server.

▶ **To ensure administrative permissions on SQL Server**

1. Start **SQL Server Management Studio** (click **Start**, click **Run**, and then type **sqlwb**).
2. Connect to the SQL Engine on the server where SQL Server 2005 was installed in Step 1.
3. Select the **Security** node and then select **Logins**.
4. The right pane will show a list of the accounts that have database access. Check that the person who is going to install WSUS 3.0 on the front-end computer has an account in this list.
5. If the account does not exist, then right-click the **Logins** node, select **New Login**, and add the account.
6. Set up this account for the roles needed to set up the WSUS 3.0 database. The roles are either **dbcreator** plus **diskadmin**, or **sysadmin**. Accounts belonging to the local Administrators group have the **sysadmin** role by default.

Step 3: Install WSUS on the front-end computer

Now install WSUS on the front-end computer. This server will need access to the Internet or to another WSUS server to obtain updates. You need to prepare this computer with all the prerequisites for a normal WSUS installation, except for database software.

Run WSUS Setup from the command line, using the

SQLINSTANCE_NAME=servername\instancename command-line option, where *servername* is the name of the remote computer, and *instancename* is the name of the SQL Server instance that you will use for WSUS. This option installs WSUS as the front end of a remote SQL pair and installs the database setup portion of the WSUS setup process on the remote machine.

▶ **To install WSUS on the front-end computer**

1. At the command prompt, navigate to the folder containing the WSUS Setup program, and type:
WSUSSetup.exe SQLINSTANCE_NAME=servername\instancename
2. You will see the **Welcome** page of the installation wizard. Continue installing WSUS as in the procedure given in [Run WSUS 3.0 Server Setup](#).

 **Note**

After you have completed the WSUS 3.0 installation, you can delete the SQL Server account set up in Step 2, if you wish to do so.

Appendix C: Configure WSUS for Network Load Balancing

Network load balancing (NLB) is a strategy that can keep networks running even if one (or more) servers go offline. It can be used in conjunction with WSUS, but requires special steps at setup time.

You should set up WSUS for NLB after configuring your SQL Server 2005 database as a failover cluster. For more information about how to set up SQL Server 2005 as a failover cluster, see [How to: Create a New SQL Server 2005 Failover Cluster](http://go.microsoft.com/fwlink/?LinkId=76490) at <http://go.microsoft.com/fwlink/?LinkId=76490>. However, you should set up WSUS before configuring the NLB cluster. For more information about how to set up an NLB cluster, see [Network Load Balancing Clusters](http://go.microsoft.com/fwlink/?LinkId=76491) at <http://go.microsoft.com/fwlink/?LinkId=76491>.

 **Note**

None of the servers taking part in the cluster should be a front-end domain controller.

 **Important**

The maximum number of front-end WSUS servers per database instance is four.

Step 1: Configure remote SQL

You should configure WSUS for remote SQL according to the procedure given in [Appendix B: Configure Remote SQL](#) earlier in this guide.

When you have finished this step, you will have the back-end SQL machine set up, as well as one of the front-end WSUS server machines. In the next step you will set up the other front-end WSUS servers.

Step 2: Set up the other front-end WSUS servers

In this step you will install WSUS on the other front-end WSUS servers without creating the database.

▶ To install WSUS on the front-end computer

1. At the command prompt, navigate to the folder containing the WSUS Setup program, and type:

```
WSUSSetup.exe /q FRONTEND_SETUP=1  
SQLINSTANCE_NAME=server\instance CREATE_DATABASE=0
```

2. You will see the **Welcome** page of the installation wizard. Continue installing WSUS as in the procedure given in [Run WSUS 3.0 Server Setup](#).



Note

If you are using the default SQL instance, leave the instance name blank. For example, if you are using the default instance on a server named MySQLServer, SQLINSTANCE_NAME should be MySQLServer.

Step 3: Configure the front-end WSUS servers

All the front-end WSUS servers should use a proxy server and should authenticate by means of the same user name and password. You can configure this in the WSUS administration console.

▶ To configure the proxy server on WSUS front-end servers

1. In the WSUS administration console, select **Options**, then **Update Source and Proxy Server**.
2. Select the **Proxy Server** tab, then enter the proxy server name, port, user name, domain, and password, then click **OK**.
3. Repeat this procedure on all the front-end WSUS servers.

Step 4: Set up a DFS share

You should create a single file location that is available to all the front-end WSUS servers. Even if you do not store updates locally, you will need a location for End User

License Agreement files. You may wish to do so by storing them on a Distributed File System share.

 **Note**

It is not necessary to use a DFS share with an NLB cluster. You can use a standard network share, and you can ensure redundancy by storing updates on a RAID controller.

This step explains how to set up DFS on one of the servers in your cluster on a Windows Server 2003 server.

 **To set up a DFS share**

1. Go to **Start**, point at **All Programs**, point at **Administrative Tools**, and click **Distributed File System**.
2. You will see the **Distributed File System** management console. Right-click the **Distributed File System** node in the left pane and click **New Root** in the shortcut menu.
3. You will see the **New Root Wizard**. Click **Next**.
4. In the **Root Type** screen, select **Stand-alone root** as the type of root, and click **Next**.
5. In the **Host Server** screen, type the name of the host server for the DFS root or search for it with **Browse**, and then click **Next**.
6. In the **Root Name** screen, type the name of the DFS root, and then click **Next**.
7. In the **Root Share** screen, select the folder that will serve as the share, or create a new one. Click **Next**.
8. In the last screen of the wizard, review your selections before clicking **Finish**.
9. You will see an error message if the Distributed File System service has not yet been started on the server. You can start it at this time.
10. Make sure that the domain account of each of the front-end WSUS servers has change permissions on the root folder of this share. That is, if there is a WSUS server installed locally on the computer that has the DFS share, the Network Service account should have change permissions on the root folder. In addition, the user account of the administrator who will run the **movecontent** command (in Step 5) should also have change permissions. For each of the remote WSUS servers, the *domain/computer* account (where domain is the name of the domain and computer is the name of the computer) should have change permissions on

the root folder of the share.

**Note**

For more information about setting permissions on DFS shares, see [KB 308568](http://go.microsoft.com/fwlink/?LinkId=86550), "How To Set File Permissions for Shares in DFS Replica Sets to Apply to All Replicas" (<http://go.microsoft.com/fwlink/?LinkId=86550>).

Step 5: Configure IIS on the front-end WSUS servers

In order to access the updates on the DFS share, the front-end WSUS servers must have IIS configured to allow remote access.

▶ To configure IIS for remote access on the front-end WSUS servers

1. On each of the servers, go to **Start**, point at **All Programs**, point at **Administrative Tools**, and click **Internet Information Services (IIS) Manager**.
2. You will see the **Internet Information Services (IIS) Manager** management console.
3. Click the server node, then the **Web Sites** node, then the node for the WSUS Web site (either **Default Web Site** or **WSUS Administration**).
4. Right-click the **Content** node and select **Properties**.
5. In the **Content Properties** dialog box, click the **Virtual Directory** tab. In the top frame you will see **The content for this resource should come from:**
6. Select **A share located on another computer** and fill in the UNC name of the share.
7. Click **Connect As**, and enter the user name and password that can be used to access that share.
8. Be sure to follow these steps for each of the front-end WSUS servers that are not on the same machine as the DFS share.

Step 6: Move the local content directory on the first front-end WSUS server to the DFS share

Now it is possible to move the content directories on the first front-end WSUS server to the DFS share. This is the first WSUS front-end server you set up in Step 1. You will not have to move the local content directory on the front-end servers you set up in Step 2.

▶ To move the content directories on the front-end WSUS servers

1. Open a command window.
2. Go to the WSUS tools directory on the WSUS server:

```
cd \Program Files\Update Services\Tools
```

3. Type the following command:

```
wsusutil movecontent DFSsharename logfile
```

where *DFSsharename* is the name of the DFS share to which the content should be moved, and *logfile* is the name of the log file.

Step 7: Configure the NLB

See [Network Load Balancing Clusters](http://go.microsoft.com/fwlink/?LinkId=76491) at <http://go.microsoft.com/fwlink/?LinkId=76491> for more information about this topic.

▶ To configure Network Load Balancing

1. Enable Network Load Balancing:
 - Click **Start**, then **Control Panel**, **Network Connections**, **Local Area Connection**, and click **Properties**.
 - Under **This connection uses the following items**, you may see an entry for Network Load Balancing. If you do not, click **Install**, then (on the **Select Network Component Type** screen) select **Service**, then click **Add**, then (on the **Select Network Service** screen) select **Network Load Balancing**, then **OK**.
 - On the **Local Area Connection Properties** screen, select **Network Load Balancing**, and then click **OK**.
2. On the **Local Area Connection Properties** screen, select **Network Load**

Balancing, and then click **Properties**.

3. On the **Cluster Parameters** tab, fill in the relevant information (the virtual IP address to be shared among the front end computers, and the subnet mask). Under **Cluster operation mode**, select **Unicast**.
4. On the **Host Parameters** tab, make sure that the unique host identifier is different for each member of the cluster.
5. On the **Port Rules** tab, make sure that there is a port rule specifying single affinity (the default). (Affinity is the term used to define how client requests are to be directed. Single affinity means that requests from the same client will always be directed to the same cluster host.)
6. Click **OK**, and return to the **Local Area Connection Properties** screen.
7. Select **Internet Protocol (TCP/IP)** and click **Properties**, and then click **Advanced**.
8. On the **IP Settings** tab, under **IP addresses**, add the virtual IP of the cluster (so that there will be two IP addresses). This should be done on each cluster member.
9. On the **DNS** tab, clear the **Register this connection's addresses in DNS** checkbox. Make sure that there is no DNS entry for the IP address.

Step 8: Test the WSUS NLB configuration

You should first make sure that at least one of the WSUS front-end servers can perform an initial synchronization. If the synchronization is successful, continue to the next step. Otherwise, review the WSUS setup and NLB cluster setup.

Step 9: Configure WSUS clients to sync from the DFS share

Instructions for configuring WSUS client machines are given in [Update and Configure the Automatic Updates Client](#). However, in the case of WSUS on NLB clusters, you should specify the virtual address of the NLB cluster rather than one of the individual servers. For example, if you are setting up your clients with a Group Policy object or Local Group Policy object, the setting for the **Specify intranet Microsoft update service location** setting should be the virtual Web address.

 **Important**

If you are using a DFS share, be careful when uninstalling WSUS from one but not all of the front-end servers. If you allow the WSUS content directory to be deleted, this will affect all the WSUS front-end servers.

Appendix D: Configure WSUS for Roaming Clients

If there are many roaming WSUS clients on your network, who often log on to your network from different locations, you may want to configure WSUS so that these computers always get their updates from the nearest WSUS server. This procedure presupposes that you have several different DNS subnets in your network, and that you want to install WSUS servers in the subnets.

Step 1: Identify the servers to use as WSUS servers

Identify one server in each of the subnets that you plan to use as a WSUS server. Keep a record of their IP addresses.

Step 2: Set up the host names on the DNS server

Set up as many DNS host (A) resource records as there are planned WSUS servers.

 **To set up the host names on the DNS server**

1. Launch the DNS console.
2. Click **Action**, and then click **New Host (A)**.
3. In the New Host dialog box, type the server name (for example, WSUSServer) in the **Name** box.
4. Type the appropriate IP address in the **IP address** box.
5. Click **Add Host**.
6. Repeat this procedure for the rest of the planned WSUS servers.

 **Important**

Make sure that each of the planned WSUS servers has the same host name.

Step 3: Set up the DNS server for netmask ordering and round robin

 **To set up netmask ordering and round robin on the DNS server**

1. In the DNS console, right-click the DNS server node, click **Properties**, and then click the **Advanced** tab.
2. In the **Server options** box, select the **Enable round robin** and **Enable netmask ordering** check boxes.
3. Click **OK**.

 **Note**

With netmask ordering, you restrict name resolution to computers in the same subnet, if there are any. With round robin, if there are multiple name resolutions, the result that is returned will rotate through the list of available hosts. Therefore, if there is a subnet without a WSUS server, host name resolution for clients in that subnet will rotate through the list of WSUS servers in the other subnets.

Step 4: Configure the WSUS servers

Set up and configure the WSUS servers in the different subnets. See [Install the WSUS 3.0 Server](#) for details.

Step 5: Configure WSUS clients to use the same host name

When you set up WSUS client computers (see [Update and Configure the Automatic Updates Client](#)), make sure to use the same host name you have set up as the WSUS server.

Appendix E: List of Security Settings

This appendix lists the recommended security settings for WSUS. The recommendations are categorized into settings for Windows Server 2003, IIS 6.0, and SQL Server 2005.

Windows Server 2003

The following are security recommendations for Windows Server 2003 with WSUS.

Audit policy

Enable audit events to ensure that adequate logs are collected for system activities.

Audit policy settings

Option	Security setting	Setting rationale
Audit account logon events	Success, Failure	Auditing for successful and failed logon events provides useful data regarding password brute-forcing attempts.
Audit account management	Success, Failure	Auditing for successful and failed account management events tracks management activities.
Audit directory service access	No Auditing	This is only important for domain controllers running the Active Directory Domain Services (AD DS).
Audit logon events	Success, Failure	Auditing for successful and failed logon events provides useful data regarding password brute-forcing attempts.

Option	Security setting	Setting rationale
Audit object access	No Auditing	Auditing object access is unnecessary and creates many unnecessary logs for WSUS activity.
Audit policy change	Success, Failure	Auditing for successful and failed policy changes tracks management activities.
Audit privilege use	Success, Failure	Auditing for successful and failed privilege use tracks administrator activities.
Audit process tracking	No Auditing	Process-tracking events are unnecessary for WSUS implementations.
Audit system events	Success, Failure	Auditing for successful and failed system events tracks system activities.

Security options

Configure Windows Server 2003 security settings to help ensure optional security and functionality.

Security options settings

Option	Security setting	Setting rationale
Accounts: Administrator account status	Enabled	Because it is necessary to have an administrator, the administrator account should be enabled for authorized users.
Accounts: Guest account Status	Disabled	Because it is risky to have guest accounts, the guest account should be disabled unless specifically required.

Option	Security setting	Setting rationale
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Accounts with blank passwords significantly increase the likelihood of network-based attacks.
Accounts: Rename administrator account	Not Defined	Renaming the administrator account forces a malicious individual to guess both the account name and password. Note that even though the account can be renamed, it still uses the same well known SID, and there are tools available to quickly identify this and provide the name.
Accounts: Rename Guest account	Not Defined	Because the Guest account is disabled by default, and should never be enabled, renaming the account is not important. However, if an organization decides to enable the Guest account and use it, it should be renamed beforehand.
Audit: Audit the access of global system objects	Enabled	This setting needs to be enabled for auditing to take place in the Event Viewer. The auditing setting can be set to Not Defined, Success or Failure in the Event View.
Audit: Audit the use of backup and restore privilege	Enabled	For security reasons, this option should be enabled so that auditors will be aware of users creating backups of potentially sensitive data.

Option	Security setting	Setting rationale
Audit: Shut down system immediately if unable to log security audits	Disabled	Enabling this option shuts down the system if it is unable to log audits. This can help prevent missed audit events. Enabling very large log files on a separate partition helps mitigate this.
Devices: Allow undock without having to log on	Disabled	Disabling this option ensures that only authenticated users can dock and undock computers.
Devices: Allow to format and eject removable media	Administrators	This option is not typically useful for desktop images.
Devices: Prevent users from installing printer drivers	Enabled	Because the Windows GDI system runs in kernel space, allowing a user to install a printer driver could lead to elevated privileges.
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled	Enabling this option prevents remote users from accessing the local CD-ROM, which may contain sensitive information.
Devices: Restrict floppy access to locally logged-on user only	Enabled	In situations in which the server is physically secured and password authentication is required by the Recover Console, this option can be enabled to facilitate system recovery.

Option	Security setting	Setting rationale
Devices: Unsigned driver installation behavior	Warn but allow installation	Most driver software is signed. Administrators should not install unsigned drivers unless the origin and authenticity can be verified and the software has been thoroughly tested in a lab environment first. Because only senior administrators will be working on these systems, it is safe to leave this to their discretion.
Domain controller: Allow server operators to schedule tasks	Disabled	The ability to schedule tasks should be limited to administrators only.
Domain controller: LDAP server signing requirements	Not Defined	This option applies only to domain controllers.
Domain controller: Refuse machine account password changes	Disabled	Enabling this option allows machine accounts to automatically change their passwords.
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled	If the domain controller is known to support encryption of the secure channel, this option can be enabled to protect against local network attacks.
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Enabling this option provides the most flexibility while enabling the highest security when the server supports it.
Domain member: Digitally sign secure channel data (when possible)	Enabled	Enabling this option provides the most flexibility while enabling the highest security when the server supports it.

Option	Security setting	Setting rationale
Domain member: Disable machine account password changes	Disabled	Disabling this option allows machine accounts to automatically change their passwords.
Domain member: Maximum machine account password age	30 days	Less frequently changed passwords are easier to break than passwords that are changed more frequently.
Domain member: Require strong (Windows 2000 or later) session key	Enabled	Enabling this option sets strong session keys for all computers running Windows 2000 or later.
Interactive logon: Do not display last user name	Enabled	Hiding the last user name should be enabled, especially when the administrator user account is renamed. This helps prevent a passerby from determining account names.
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	The CTRL+ALT+DEL sequence is intercepted at a level lower than user mode programs are allowed to hook. Requiring this sequence at logon is a security feature designed to prevent a Trojan Horse program masquerading as the Windows logon from capturing users' passwords.
Interactive logon: Message text for users attempting to log on	[provide legal text]	An appropriate legal and warning message should be displayed according to the Corporate Security Policy.

Option	Security setting	Setting rationale
Interactive logon: Message title for users attempting to log on	[provide legal title text]	An appropriate legal and warning message should be displayed according to the Corporate Security Policy.
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	This option is usually appropriate only for laptops that might be disconnected from their domain. It also presents a security risk for some types of servers, such as application servers. If a server is compromised and domain logons are cached, the attacker may be able to use this locally stored information to gain domain-level credentials.
Interactive logon: Prompt user to change password before expiration	14 days	Password prompts should be aligned according to the Corporate Security Policy.
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled	Enabling this option allows a domain controller account to unlock any workstation. This should only be allowed for the local Administrator account on the computer.
Interactive logon: Require smart card	Not Defined	If this system will not be using smart cards, this option is not necessary.
Interactive logon: Smart card removal behavior	Not Defined	If this system will not be using smart cards, this option is not necessary.

Option	Security setting	Setting rationale
Microsoft network client: Digitally sign communications (always)	Disabled	For systems communicating to servers that do not support SMB signing, this option should be disabled. However, if packet authenticity is required, this can be enabled.
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	For systems communicating to servers that do support SMB signing, this option should be enabled.
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	If this option is enabled, then a third-party SMB server could negotiate a dialect that does not support cryptographic functions. Authentication would be performed using plain-text passwords.
Microsoft network server: Amount of idle time required before suspending session	15 minutes	This should be set appropriately for the end-user system such that idle connections do not linger or consume resources.
Microsoft network server: Digitally sign communications (always)	Disabled	For systems communicating to servers that do not support SMB signing, this option should be disabled. However, if packet authenticity is required, this can be enabled.

Option	Security setting	Setting rationale
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	For systems communicating to servers that do not support SMB signing, this option should be disabled. However, if packet authenticity is required, this can be enabled.
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Enabling this option prevents users from logging on after authorized hours.
Network access: Allow anonymous SID/Name translation	Disabled	This option is highly important for securing Windows networking. Disabling it severely restricts the abilities granted to a user connecting with a Null session.
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	This option is highly important for securing Windows networking. Enabling this option severely restricts the abilities granted to a user connecting with a Null session. Because "Everyone" is no longer in the anonymous user's token, access to IPC\$ is disallowed. Pipes that are explicitly set to allow anonymous are inaccessible because the SMB tree connection to this share fails.

Option	Security setting	Setting rationale
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	This option is highly important for securing Windows networking. Enabling this option severely restricts the abilities granted to a user connecting with a Null session. Because "Everyone" is no longer in the anonymous user's token, access to IPC\$ is disallowed. Pipes that are explicitly set to allow anonymous are inaccessible because the SMB tree connection to this share fails.
Network access: Do not allow storage of credentials or .NET passports for network authentication	Enabled	Enabling this option prevents the storage of sensitive passwords in the computers' cache.
Network access: Let Everyone permissions apply to anonymous users	Disabled	Anonymous users should have no access to computers.
Network access: Named Pipes that can be accessed anonymously	Not Defined	Named pipes should be restricted anonymously. Restricting named pipes breaks some intersystem processes, such as network printing.
Network access: Remotely accessible registry paths	Not Defined	Registry paths should be restricted from remote access unless for monitoring circumstances.
Network access: Shares that can be accessed anonymously	None	No shares should be accessed anonymously.

Option	Security setting	Setting rationale
Network access: Sharing and security model for local accounts	Guest only—local users authenticate as Guest	Limit all local accounts to Guest privileges.
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabling this feature deletes the weaker LAN Manager hashes, reducing the likelihood of password attacks from sniffing the weak hash over the name or from the local SAM database file.
Network security: Force logoff when logon hours expire	Enabled	This option should be enabled as part of the acceptable policy.
Network security: LAN Manager authentication level	Send NTLMv2 response only	Sending LM is less secure than NTLM, and should only be enabled if the system will communicate with computers running Windows 98 or Windows 95. Additionally, use NTLMv2 only; however, computers running Windows 98, Windows 95, or unpatched Windows NT4.0 will not be able to communicate with servers running NTLMv2.
Network security: LDAP client signing requirements	Negotiate signing	Require signing when authenticating to third party LDAP servers. This prevents attacks against rogue LDAP servers and clear-text submission of passwords over the network.

Option	Security setting	Setting rationale
Network security: Minimum session security for NTLM SSP-based (including secure RPC) clients	Require NTLMv2 session security	The NTLM hashes contain weaknesses that attacks may exploit. When enabled, these requirements strengthen the authentication algorithms for Windows.
Network security: Minimum session security for NTLM SSP-based (including secure RPC) servers	Require NTLMv2 session security	The NTLM hashes contain weaknesses that attacks may exploit. When enabled, these requirements will strengthen the authentication algorithms for Windows.
Recovery console: Allow automatic administrative logon	Disabled	If automatic administrative logon is enabled, then a malicious user that has console access could simply restart the computer and gain administrative privileges. However, an organization may enable this feature if the computer is a physically secure server, allowing access to the system if the administrator password is forgotten.
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	The recovery console can be used as an attack method to gain access to SAM database files offline; therefore, this option should be enabled to prevent those files from being copied to a floppy disk.

Option	Security setting	Setting rationale
Shutdown: Allow system to be shut down without having to log on	Disabled	This option is used to prevent users without valid accounts from shutting down the system, and is a good precautionary measure.
Shutdown: Clear virtual memory pagefile	Disabled	Clearing the memory pagefile at shutdown can help prevent offline analysis of the file, which might contain sensitive information from system memory, such as passwords. However, in situations in which the computer is physically secured, this can be enabled to reduce time required for system restarts.
System cryptography: Force strong key protection for user keys stored on the computer	User is prompted when the key is first used	Protecting local cryptographic secrets helps prevent privilege escalation across the network, once access to one system is obtained.
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined	Require stronger, standard, and compliant algorithms for encryption, hashing, and signing.
System Objects: Default owner for objects created by members of the Administrators group	Administrators group	Administrators should only have access to the created file.
System objects: Require case insensitivity for non-Windows subsystems	Disabled	Require case-sensitivity for non-Windows subsystems, such as UNIX passwords.

Option	Security setting	Setting rationale
System settings: Optional subsystems	Enter POSIX here only if expressly required	The POSIX execution layer has had multiple local exploits in the past, and should be disabled unless required by third-party software. It is extremely rare for POSIX to be required by commercial software packages.
System settings: Use Certificate Rules on Windows executables for Software Restriction policies	Not Defined	When certificate rules are created, enabling this option enforces software restriction policies that check a Certificate Revocation List (CRL) to make sure the software's certificate and signature are valid.

Important

The WSUS subdirectories UpdateServicesPackages, WsusContent, and WsusTemp created as shared directories (for WSUS Administrators and the Network Service account) as part of WSUS setup. These directories can be found by default under the WSUS directory at the root of the largest partition on the WSUS server. Sharing of these directories may be disabled if you are not using local publishing.

Event log settings

Configure Event Log settings to help ensure an adequate level of activity monitoring.

Event log settings

Option	Security setting	Setting rationale
Maximum application log size	100489 kilobytes	A large event log allows administrators to store and search for problematic and suspicious events.

Option	Security setting	Setting rationale
Maximum security log size	100489 kilobytes	A large event log allows administrators to store and search for problematic and suspicious events.
Maximum system log size	100489 kilobytes	A large event log allows administrators to store and search for problematic and suspicious events.
Prevent local guests group from accessing application log	Enabled	Guest accounts should not be able to access sensitive information in the event log.
Prevent local guests group from accessing security log	Enabled	Guest accounts should not be able to access sensitive information in the event log.
Prevent local guests group from accessing system log	Enabled	Guest accounts should not be able to access sensitive information in the event log.
Retain application log	7 Days	After a week, logs should be stored on a centralized log server.
Retain security log	7 Days	After a week, logs should be stored on a centralized log server.
Retain system log	7 Days	After a week, logs should be stored on a centralized log server.
Retention method for application log	As Needed	Overwrite audit logs as needed when log files have filled up.
Retention method for security log	As Needed	Overwrite audit logs as needed when log files have filled up.

Option	Security setting	Setting rationale
Retention method for system log	As Needed	Overwrite audit logs as needed when log files have filled up.

System services

Enable only services that are required for WSUS.

Enabled operating system services

Option	Security setting	Setting rationale
Alerter	Disabled	The alerter service is of most use when an administrator is logged into the network and wants to be notified of events. For computers running WSUS, the service is not necessary.
Application Management	Manual	This service is only necessary when installing new applications to the environment with Active Directory.
Automatic Updates	Automatic	This service is required in order to support a fully patched operating environment.
Clipboard	Disabled	This service is unnecessary to the WSUS environment.
COM+ Event System	Manual	The COM+ event system might be used in the Web-based application.
Computer Browser	Automatic	The computer browser service is required on interactive workstations.

Option	Security setting	Setting rationale
DHCP Client	Automatic	DHCP is necessary to have an IP address on the WSUS server.
Distributed File System	Disabled	DFS is used for file sharing across multiple servers, which is not needed for WSUS.
Distributed Link Tracking Client	Disabled	This service is appropriate only if a domain has distributed link tracking configured.
Distributed Link Tracking Server	Disabled	This service is appropriate only if a domain has distributed link tracking configured.
Distributed Transaction Coordinator	Disabled	This service is appropriate only if a domain uses distributed transactions, which are not needed for WSUS.
DNS Client	Automatic	DNS is necessary for IP-address-to-name resolution.
Event Log	Automatic	The Event Log service is important for logging events on the system and provides critical auditing information.
File Replication	Disabled	This service is used for file replication and synchronization, which is not necessary for WSUS.
IIS ADMIN Service	Automatic	This service is required for WSUS administration.
Indexing Service	Manual	This service is used by IIS.

Option	Security setting	Setting rationale
Intersite Messaging	Disabled	This service needs to be enabled only on domain controllers.
Internet Connection Firewall/Internet Connection Sharing	Manual	This service is required if the local ICF firewall is being used.
IPsec Services	Automatic	This service is required if IPsec has been utilized.
Kerberos Key Distribution Center	Disabled unless functioning as a domain controller	This service is enabled by default in order to join and authenticate to Windows Server 2003 domain controllers.
License Logging Service	Disabled	This service is used on systems on which application licensing must be tracked.
Logical Disk Manager	Automatic	This service is used in logical disk management.
Logical Disk Manager Administrative Service	Manual	This service is used in logical disk management.
Messenger	Disabled	This service is only necessary if NetBIOS messaging is being used.
Net Logon	Automatic	This service is necessary to belong to a domain.
NetMeeting Remote Desktop Sharing	Disabled	NetMeeting is an application that allows collaboration over a network. It is used on interactive workstations, and should be disabled for servers as it presents a security risk.

Option	Security setting	Setting rationale
Network Connections	Manual	This service allows network connections to be managed centrally.
Network DDE	Disabled	Network DDE is a form of interprocess communication (IPC) across networks. Because it opens network shares and allows remote access to local resources, it should be disabled unless explicitly needed.
Network DDE DSDM	Disabled	Network DDE is a form of interprocess communication (IPC) across networks. Because it opens network shares and allows remote access to local resources, it should be disabled unless explicitly needed.
NTLM Security Support Provider	Manual	The NTLM Security Support Provider is necessary to authenticate users of remote procedure call (RPC) services that use transports such as TCP and UDP.
Performance Logs and Alerts	Manual	This service is only necessary when logs and alerts are used.
Plug and Play	Automatic	Plug and Play is needed if the system uses Plug and Play hardware devices.
Print Spooler	Disabled	This service is necessary if the system is used for printing.

Option	Security setting	Setting rationale
Protected Storage	Automatic	This service must be enabled because the IIS Admin service depends on it.
Remote Access Auto Connection Manager	Disabled	Enable this service only for RAS servers.
Remote Access Connection Manager	Disabled	Enable this service only for RAS servers.
Remote Procedure Call (RPC)	Automatic	This service is required for RPC communications.
Remote Procedure Call (RPC) Locator	Manual	This service is required for RPC communications.
Remote Registry	Manual	Remote Registry is a key target for attackers, viruses, and worms, and should be set to manual unless otherwise needed, where the server can enable it.
Removable Storage	Manual	For a dynamic server, this service is necessary.
Routing and Remote Access	Disabled	Enable this service only for RAS servers.
Security Accounts Manager	Automatic	This service should be enabled, as it manages local accounts.
Server	Automatic	This service should be enabled or disabled as necessary. The service supports file, print, and named-pipe sharing over the network for this computer.

Option	Security setting	Setting rationale
Smart Card	Manual	Because users will not be using smart cards for two-factor logon authentication, this service is unnecessary and should be disabled or set to manual.
System Event Notification	Automatic	This service is needed for COM+ events.
Task Scheduler	Manual	This service should be enabled or disabled as necessary. The service enables a user to configure and schedule automated tasks on this computer.
TCP/IP NetBIOS Helper	Automatic	This service is used in Windows networking for computers running an operating system earlier than Windows Server 2003.
Telephony	Disabled	This service is not necessary in this environment because telephony devices are not used.
Telnet	Disabled	The telnet service should be disabled and its use strongly discouraged.
Terminal Services	Manual	Terminal services should be enabled or disabled as necessary.
Uninterruptible Power Supply	Manual	This service is necessary if a Uninterruptible Power Supply is used.

Option	Security setting	Setting rationale
Windows Installer	Manual	Users may choose to use Windows Installer to install .msi packages on the system; therefore, this service should be set to manual.
Windows Management Instrumentation	Manual	WMI provides extended management capabilities.
Windows Management Instrumentation Driver Extensions	Manual	WMI Driver Extensions allow monitoring of network card connection state in the taskbar.
Windows Time	Automatic	External time synchronization is required for Kerberos key exchange in Active Directory environments.
Workstation	Automatic	The workstation service is necessary for Windows networking.

TCP/IP hardening

Microsoft recommends that you harden the TCP/IP interface for WSUS servers.

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\SynAttackProtect

Security setting	Setting rationale
REG_DWORD = 2	Causes TCP to adjust retransmission of SYN-ACKS.

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\tcpmaxportsexhausted

Security setting	Setting rationale
REG_DWORD = 1	Helps protect against SYN attacks.

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\TCPMAxHALFOPEN

Security setting	Setting rationale
REG_DWORD = 500	Helps protect against SYN attacks.

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\TCPmaxhalfopenretired

Security setting	Setting rationale
REG_DWORD = 400	Helps protect against SYN attacks.

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\AFd\parameters\enabledICMPRedirect

Security setting	Setting rationale
REG_DWORD = 0	Prevents the creation of expensive host routes when an ICMP redirect packet is received.

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\tcpip\parameters\enableddeadgwdetect

Security setting	Setting rationale
REG_DWORD = 0	Prevents the forcing of switching to a secondary gateway.

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\tcpip\parameters\disableipsourceouting

Security setting	Setting rationale
REG_DWORD = 1	Disables IP source routing.

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\tcpip\parameters\ipenabledrouter

Security setting	Setting rationale
REG_DWORD = 0	Disables forwarding of packets between network interfaces.

IIS security configuration

Consider enabling the following three security settings on the IIS Web server to help ensure secure WSUS administration.

Enable general IIS error messages

By default, IIS gives detailed error messages to remote Web clients. We recommend enabling IIS general, less-detailed error messages. This prevents an unauthorized user from probing the IIS environment with IIS error messages.

To enable general IIS error messages

1. On the **Start** menu, point to **Programs**, point to **Administrator Tools**, and then click **Internet Information Services Manager**.
2. Expand the local computer node.
3. Right-click **Web Sites**, and then click **Properties**.
4. On the **Home Directory** tab, click **Configuration**.
5. On the **Debugging** tab, under **Error messages for script errors**, click **Send the following text error message to client**, where the error message reads "An error occurred on the server when processing the URL. Please contact the system administrator."

Enable additional IIS logging options

By default, IIS enables logging for a number of options. However, we recommend logging several additional key options.

To enable additional IIS logging options

1. On the **Start** menu, point to **Programs**, point to **Administrator Tools**, and then click **Internet Information Services Manager**.
2. Expand the local computer node.

3. Right-click **Web Sites**, and then click **Properties**.
4. On the **Web Site** tab, under the **Active log format** box, click **Properties**.
5. In **Logging Properties** go to the **Advanced** tab, and select the check boxes for the following logging options:
 - **Server Name**
 - **Time taken**
 - **Host**
 - **Cookie**
 - **Referer**

Remove header extensions

By default, IIS enables header extensions for HTTP requests. We recommend removing any header extensions for IIS.

To remove header extensions for HTTP requests

1. On the **Start** menu, point to **Programs**, point to **Administrator Tools**, and then click **Internet Information Services Manager**.
2. Expand the local computer node.
3. Right-click **Web Sites**, and then click **Properties**.
4. On the **HTTP Headers** tab, select the **X-Powered-By: ASP.NET** check box, and then click **Remove**.

SQL Server 2005

The following are security recommendations for SQL Server 2005 with WSUS.

SQL registry permissions

Use access control permissions to secure the SQL Server 2005 registry keys.

HKLM\SOFTWARE\MICROSOFT\MSSQLSERVER

ISEC setting	Rationale
Administrators: Full Control SQL Service Account: Full Control System: Full Control	These settings help ensure limited access to the application's registry key to authorized administrators or system accounts.

Stored procedures

Remove all stored procedures that are unnecessary and that have the ability to control the database server remotely.

Unnecessary SQL Server 2005 stored procedures

Description	Stored procedures	Rationale
<p>Delete stored procedures by using the following command:</p> <p>use master exec sp_dropextendedproc stored procedure</p> <p>where <i>stored procedure</i> is the name of the stored procedure to be deleted.</p>	<ul style="list-style-type: none"> • Sp_OACreate • Sp_OADestroy • Sp_OAGetErrorInfo • Sp_OAGetProperty • Sp_OAMethod • Sp_OASetProperty • SP_OAStop • Xp_regaddmultistring • Xp_regdeletekey • Xp_regdeletevalue • Xp_regenumvalues • Xp_regread • Xp_regremovemultistring • Xp_regwrite • sp_sdidebug • xp_availablemedia • xp_cmdshell • xp_deletemail • xp_dirtree • xp_dropwebtask • xp_dsninfo • xp_enumdsn 	<p>Remove all stored procedures that are not necessary for WSUS and could possibly give unauthorized users the ability to perform command-line actions on the database.</p>

Description	Stored procedures	Rationale
	<ul style="list-style-type: none"> • xp_enumerrorlogs • xp_enumgroups • xp_eventlog • xp_findnextmsg • xp_fixeddrives • xp_getfiledetails • xp_getnetname • xp_logevent • xp_loginconfig • xp_makewebtask • xp_msver • xp_readerrorlog • xp_readmail • xp_runwebtask • xp_sendmail • xp_sprintf • xp_sscanf • xp_startmail • xp_stopmail • xp_subdirs • xp_unc_to_drive 	

Appendix F: Prerequisites Schema

The prerequisites.xml file is used to define the prerequisites for an installation. The schema is described in the following section

Prerequisites Schema

The elements of the prerequisites schema are listed in the following table.

Schema Element	Description
PrereqResults	Root element.
Result	The result of a single prerequisite check. There may be 0... <i>n</i> Result elements, one for each prerequisite.
Status	The localized description of the status code.
Check	The product or component to be checked.
Components	The component(s) for which this is a prerequisite. There may be 0... <i>n</i> Component elements in a Components element.
Component	One of the component(s) for which this is a prerequisite.
Description	The description of the problem.
Resolution	The way the customer may resolve the problem.

In addition, the **Result** element has an attribute **StatusCode**. The possible values of **StatusCode** are 0 (success), 1 (error), 2 (warning).

Example

The following is an example of a prerequisites.xml file.

```
<?xml version="1.0" encoding="utf-8"?>
<PrereqResults>
  <Result StatusCode="0">
    <Status>Passed</Status>
    <Check> Microsoft Windows Server 2003 Server </Check>
    <Components>
      <Component>Windows Server Update Services</Component>
    </Components>
  </Result>
  <Result StatusCode="1">
```

```

<Status>Failed</Status>
<Check>SQL Server 2005</Check>
<Components>
  <Component>Windows Server Update Services</Component>
</Components>
<Description>SQL Server 2005 or later not detected</Description>
<Resolution>Download the required version from
http://www.microsoft.com/downloads/</Resolution>
</Result>
<Result StatusCode="1">
  <Status>Warning</Status>
  <Check>SQLINSTANCE_NAME</Check>
  <Components>
    <Component>Windows Server Update Services</Component>
  </Components>
  <Description>This database version can not be upgraded.  Version is too
old.</Description>
  <Resolution>Choose another location for the database to keep this one
otherwise this database will be overridden.</Resolution>
</Result>
...
</PrereqResults>

```

Appendix G: Detect the Version of WSUS

The way you detect the version of a WSUS installation has changed in WSUS 3.0. In previous versions, WSUS used MSI product keys. In WSUS 3.0, versioning is persisted in the registry to support new installer technologies such as CBS for Windows Vista™ and Windows Server® Code Name "Longhorn".

Versioning in SUS 1.0

Check for the install state of the following MSI product key:

```
{AFF0D9D3-6F0D-437E-9327-98108B4A8644}
```



Note

SUS 1.0 must be removed before installing WSUS 3.0. Upgrade between these two versions is not supported.

Versioning in WSUS 2.0

Check for the install state of the following MSI product key:

```
{A0D46DC6-8950-451A-8990-53C86E17666E}
```

In WSUS 2.0, the WSUS registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Update Services\Server\Setup

has an **InstallType** subkey with the following possible values:

Frontend = 32

Backend = 64

FullInstall = 128



Note

You can upgrade from WSUS 2.0 to WSUS 3.0 for installations with the **Frontend** and **FullInstall** values. For the **Backend** value, you would uninstall WSUS, leaving the database behind. This database will be upgraded when the front-end WSUS server that points to the database is upgraded.

WSUS 3.0 pre-release candidate versions

Versions of WSUS 3.0 that precede the first release candidate version also have MSI product keys. There is one product key for 32-bit architectures and another for 64-bit architectures.

```
{BCE8923B-20C9-4EBD-AB18-31CDC13B92E6} (x86)
```

```
{2E3FC5F0-0415-4e75-A3D3-74077F809FDD} (x64)
```

WSUS 3.0 Release Candidate 1 and later versions

For WSUS 3.0, there is no MSI product key, but there are two registry values:

InstallType supports only two installation types: 1 = install or 2 = console-only install.

VersionString is a string of the form **Major.Minor.Build.Revision**.



To detect WSUS versions

1. Check that SUS 1.0 and WSUS 2.0 are not installed (by looking for the product

keys).

2. Find the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Update Services\Server\Setup.
3. Check the **InstallType** values (32/64/128 if WSUS 2.0, 1/2 if WSUS 3.0).
4. Check for **VersionString** values.