



Windows Server[™] Update Services

Windows Server Update Services 3.0 SP2 Operations Guide

Microsoft Corporation

Author: Anita Taylor

Editor: Theresa Haynie

Abstract

This guide describes how to manage Windows Server Update Services 3.0 SP2 (WSUS 3.0 SP2). You will find best practices and instructions for managing updates, maintaining client computers and groups, and running reports. This guide also offers server and client troubleshooting information.

Copyright Notice

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. 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.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveX, Authenticode, Excel, InfoPath, Internet Explorer, MSDN, Outlook, Visual Studio, Win32, Windows, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

Windows Server Update Services 3.0 SP2 Operations Guide	11
In this guide	11
Administering Windows Server Update Services 3.0 SP2	11
Overview of Windows Server Update Services 3.0 SP2	12
How WSUS Works	12
Software Updates	12
Managing Windows Server Update Services 3.0 SP2	13
Setting Up Synchronizations	13
Synchronizing Updates by Product and Classification	13
Synchronizing Updates by Language	14
Configuring Proxy Server Settings	14
Configuring the Update Source	15
Configuring Update Storage	16
Synchronizing Manually or Automatically	16
Managing the Client Computers and Computer Groups	17
Managing the Client Computers	17
Managing the Computer Groups	17
Managing the Updates	18
Overview of Updates	19
How WSUS Stores Updates	19
Managing Updates with WSUS	19
Update Products and Classifications	20
Products Updated by WSUS	20
Update Classifications	20
Viewing the Updates	21
WSUS 3.0 SP2 and the Catalog Site	24
Importing hotfixes from the Microsoft Update catalog site	24
Restricting access to hotfixes	24
Importing updates in different languages	25
Approving the Updates	25
Approving Updates	25

Declining Updates	27
Change an Approved Update to Not Approved	28
Approving Updates for Removal	28
Approving Updates Automatically	29
Automatically Approving Revisions to Updates and Declining Expired Updates	30
Approving Superseding or Superseded Updates	30
Best Practices for Approving a Superseding Update	31
Office Update Approval	32
SQL Server and Exchange Server Updates Approval	32
Updating Microsoft SQL Server instances	32
Updating Microsoft SQL Server and Microsoft Exchange Servers that are part of a cluster	33
Testing the Updates	33
Storing the Updates.....	34
Specifying Where to Store the Updates	34
Local Storage Considerations.....	34
About Express Installation Files.....	34
Updates, Update Files, and Languages.....	35
Changing the Location Where You Store Update Files Locally	35
Managing the Database	36
Additional resources.....	37
Migrating from Windows Internal Database to SQL Server.....	37
Why Migrate the WSUS Database to SQL Server.....	37
SQL Server Database Requirements.....	37
Scenarios.....	37
Migrating the WSUS Database.....	38
Migrating the WSUS Database and Moving to a Remote SQL Server.....	39
Remote SQL Scenario Limitations	39
Prerequisites	40
To migrate the WSUS database from a Windows Internal Database instance to an instance of SQL Server 2008 or SQL Server 2005 SP2 on a remote server	40
Using the Server Cleanup Wizard.....	42
Running the Server Cleanup Wizard	42
Running WSUS 3.0 SP2 in Replica Mode.....	43
Replica server synchronization	43
Backing Up Windows Server Update Services 3.0 SP2.....	44
Best Practices with Windows Server Update Services 3.0 SP2.....	46

Best practices for security	46
Best practices for resource usage	47
Disk space	47
Network bandwidth.....	48
Best practices for setting up WSUS networks	49
Best practices for maintaining WSUS databases	49
Other best practices.....	49
Manage restarts	49
Ensure WSUS availability	50
Test service packs carefully.....	50
Check overall system health.....	50
Managing WSUS 3.0 SP2 from the Command Line	51
Using the wsusutil utility	51
configuresl	52
Syntax.....	53
Output.....	53
healthmonitoring	53
Syntax.....	53
Output.....	56
export	56
Syntax.....	56
Import.....	57
Syntax.....	57
Movecontent.....	57
If the drive is full	58
If the hard disk fails.....	58
Syntax.....	58
listfrontendservers	58
deletefrontendserver	59
Syntax.....	59
checkhealth	59
Syntax.....	59
reset	59
Syntax.....	59
listinactiveapprovals.....	59
Syntax.....	60
removeinactiveapprovals	60
Syntax.....	60
usecustomwebsite	60
Syntax.....	60
Reports in Windows Server Update Services 3.0 SP2	61
In this section.....	61

Terminology for Update Status	61
Creating Reports	63
Using the Reports Page	63
Update Reports	64
Update Status Summary View	64
Computer Reports	65
Synchronization Results Report	66
Printing a Report.....	67
Exporting a Report.....	67
Extending Reports.....	67
Use WSUS APIs to Create Custom Reports	68
Use WSUS Public Views to Create Custom Reports	68
Securing Windows Server Update Services 3.0 SP2.....	68
Troubleshooting Windows Server Update Services 3.0 SP2	68
Health Monitoring in WSUS 3.0 SP2.....	69
Health checks	69
Polling WSUS components	69
Viewing event logs.....	69
Resolving problems	70
WSUS 3.0 SP2 Server Administration Issues	70
Issues with Setup	70
Troubleshooting WSUS setup	71
Check for required software and hardware.....	71
Check setup logs.....	71
Check the .NET framework installation.....	71
The WSUSService service is marked for deletion.....	71
On a domain controller, the NetBiosDomainName is different from the DNS domain name	72
Duplicate ASP.Net entries in the IIS Web services list.....	72
There is a SUSDB database from an earlier installation	72
UseCustomWebsite fails when the default Web site does not have a site ID of 1	72
API compression may not be used after installing WSUS 3.0 SP2 on Windows Server 2008	73
WSUS 3.0 SP2 setup fails to install to Windows Server 2008 when installing to a case-sensitive SQL and the computer name is in lowercase letters	73
Issues with Upgrades	73
Troubleshooting WSUS Upgrades.....	73
If a WSUS Upgrade Fails, WSUS May Be Uninstalled.....	73

Upgrading to WSUS 3.0 from WSUS 2.0	73
Certificate Not Configured after WSUS 2.0 SP2 is Upgraded to WSUS 3.0 with Custom Web site.....	73
Issues with the WSUS 3.0 SP2 Administration Console	74
Troubleshooting the WSUS administration console	74
Cannot access the WSUS administration console and a timeout error message appears .	74
Get an error looking at a network load balanced cluster if the "master" is unavailable.....	74
Cannot see client computers in the WSUS administration console	75
Cannot see computers having 100 percent installed state on the Computers page when the "Installed/NotApplicable or No Status" filter is applied	75
Cannot connect to remote WSUS 3.0 server in a saved MMC console	75
Get error accessing WSUS 3.0 servers from the WSUS administration console because the WWW Publishing service is configured to allow interaction with the desktop	75
Get other errors accessing WSUS 3.0 servers from the WSUS administration console.....	76
Issues with Update Storage.....	76
Troubleshooting update storage	76
The updates listed in the WSUS administrative console do not match the updates listed in your local folder.....	76
Downloads from a WSUS server are failing.....	76
The local content directory is running out of disk space.....	77
Issues with Synchronization	78
Troubleshooting synchronization	78
Check the error in the synchronization's Details pane	78
Synchronization retries by downstream servers	79
Check proxy server settings by using the WSUS console.....	79
Check the firewall settings	79
Check the name of the upstream WSUS server	79
Verify that users and the network service have Read permissions to the local update storage directory	80
On a downstream WSUS server, check that the updates are available on the upstream WSUS server	80
Restart the BITS service	80
The number of updates that are approved on a parent upstream server does not match the number of approved updates on a replica server	81
The last catalog synchronization failed.....	81
A WSUS 2.0 replica times out when synchronizing	81
Issues with Update Approvals.....	81
Troubleshooting update approvals.....	81
New approvals can take up to one minute to take effect	81

Remote computers accessed by using Terminal Services cannot be restarted by non-administrators.....	82
The number of updates that are approved on a parent upstream server does not match the number of approved updates on a replica server	82
Issues with Backup and Restore.....	82
Troubleshooting backup and restore issues.....	82
Cannot access WSUS data after restoring the database	82
Clients have download failures after restoring the database	82
Issues with E-Mail Notifications	83
Troubleshooting the WSUS e-mail setup	83
Troubleshooting the SMTP server	83
Issues with the Database.....	83
Troubleshooting Database Issues	83
Issues with WSUS 3.0 Services	84
Troubleshooting services	84
General service troubleshooting.....	84
Reset IIS	84
SQL service.....	84
Access rights on Web service directories	85
IIS settings for Web services.....	85
WSUS 3.0 SP2 Client Computer Administration Issues.....	85
In This Section	85
Issues with Client Computer Groups.....	85
Client computers appear in the wrong groups.....	86
Verify that the WSUS console is set to use client-side targeting	86
Verify that target computer group names match groups on the WSUS server	86
Reset the Automatic Update client.....	86
Issues with Update Installation on Clients	86
Troubleshooting Update Installation Issues	87
Checking DCOM Configuration.....	87
Default DCOM Permissions	87
Issues with Clients Not Reporting	87
Troubleshooting client not reporting issues.....	87
Check the HTTP hotfix.....	87
Troubleshoot client connectivity	88
Troubleshoot the Automatic Update client	88
Reset the Automatic Update client	89

Issues with Client Self-Update	89
Troubleshooting client self-update issues	90
How to differentiate between the SUS client and WSUS client	90
Verify that the client software in your organization can self-update	92
Verify that SUS clients are pointed to the WSUS server	92
Check for the self-update tree on the WSUS server	93
Check IIS logs on the WSUS Server	93
If you have installed Windows SharePoint Services on the default Web site in IIS, configure it to coexist with Self-update	94
Check if the Content and Selfupdate Web sites have different authentication levels	94
Check network connectivity on the WSUS client computer	95
Check logs on the WSUS client computer	95
Manipulate registry settings on the WSUS client computer	95
Issues with BITS	97
Finding BITS	98
Stopping and Restarting BITS	98
Troubleshooting BITS Download Issues	99
The BITS service must run under the Local System user account	99
Proxy Servers Must Support HTTP 1.1 RANGE Requests	99
There is a mismatch between the BITS per-user job limit and the per-computer job limit ..	99
BITS Jobs are Failing	100
BITS Fails to Start	102
Repairing a Corrupted BITS Configuration	103
Issues with High CPU Utilization	104
Additional Resources for Windows Server Update Services 3.0 SP2	104
Windows Server Update Services communities	104
Additional references	104
Appendix A: Uninstalling Windows Internal Database	105
Appendix B: Uninstalling WSUS 3.0 SP2 from SQL Server	106
Uninstalling WSUS might leave some WSUS accounts on computers running SQL Server ...	106
Appendix C: IIS Settings for Web Services	106
IIS vroots	107
Using the adsutil IIS utility	108
Finding Web service paths with adsutil	108
Checking the properties of a Web service.....	109
Global properties.....	109
Global Properties of the WWW Web site	114
Properties of the API Remoting Web service	114
Properties of the Client Web service.....	115

Properties of the Downstream Server Authentication Web service	117
Properties of the Inventory Collection Web service	118
Checking the properties of the Reporting Web service	119
Properties of the Selfupdate Web service	120
Properties of the Server Synchronization Web service	120
Properties of the Simple Authorization Web service	122
Appendix D: Permissions on WSUS Directories and Registry Keys	123
The cacls system command	123
Permissions on WSUS registry keys	124
Appendix E: Configuring BITS 2.0 and 3.0 for Download Performance	124
Throttling	124
Peer caching	125
Appendix F: Configuring IIS for Download Performance	126
Limiting bandwidth on all Web sites	126
Limiting bandwidth on a specific Web site	127
Appendix G: Windows Update Agent Result Codes	127
Windows Update Agent result codes	127
Appendix H: The wuauctl Utility	149
Command line switches for wuauctl	149
Appendix I: Database Maintenance	149
Appendix J: Setup Return Codes	150
Windows Server Update Services 3.0 Setup Return Codes	150

Windows Server Update Services 3.0 SP2 Operations Guide

This guide describes the major tasks involved in administering and troubleshooting Windows Server Update Services 3.0 SP2.

In this guide

[Administering Windows Server Update Services 3.0 SP2](#)

[Troubleshooting Windows Server Update Services 3.0 SP2](#)

[Additional Resources for Windows Server Update Services 3.0 SP2](#)

[Appendix A: Uninstalling Windows Internal Database](#)

[Appendix B: Uninstalling WSUS 3.0 SP2 from SQL Server](#)

[Appendix C: IIS Settings for Web Services](#)

[Appendix D: Permissions on WSUS Directories and Registry Keys](#)

[Appendix E: Configuring BITS 2.0 and 3.0 for Download Performance](#)

[Appendix F: Configuring IIS for Download Performance](#)

[Appendix G: Windows Update Agent Result Codes](#)

[Appendix H: The wuauclt Utility](#)

[Appendix I: Database Maintenance](#)

[Appendix J: Setup Return Codes](#)

Administering Windows Server Update Services 3.0 SP2

This section contains background information and procedures for performing the major tasks involved in administering Windows Server Update Services 3.0 SP2.

In this guide

- [Overview of Windows Server Update Services 3.0 SP2](#)
- [Managing Windows Server Update Services 3.0 SP2](#)
- [Reports in Windows Server Update Services 3.0 SP2](#)
- [Securing Windows Server Update Services 3.0 SP2](#)

Overview of Windows Server Update Services 3.0 SP2

You can use Windows Server Update Services (WSUS) 3.0 SP2 to manage downloading software updates from Microsoft Update and distributing them to computers in your network.

How WSUS Works

WSUS provides a management infrastructure consisting of the following:

- Microsoft Update: the Microsoft Web site that distributes updates to Microsoft products.
- Windows Server Update Services server: the server component that is installed on a computer running a supported operating system inside the corporate firewall. WSUS server software enables administrators to manage and distribute updates through an administrative console, which can be used to manage any WSUS server in any domain with which it has a trust relationship. A WSUS server can obtain updates either from Microsoft Update or from another WSUS server, but at least one WSUS server in the network must connect to Microsoft Update to get available updates. The administrator can decide how many WSUS servers should connect directly to Microsoft Update, based on network configuration, bandwidth, and security considerations. These servers can then distribute updates to other downstream WSUS servers.
- Automatic Updates: the client computer component built into Windows operating systems. Automatic Updates enables both server and client computers to receive updates either from Microsoft Update or from a WSUS server.

Software Updates

Software updates consist of two parts:

- Update files: the actual files that are installed on client computers.
- Update metadata: the information needed to perform the installation, which includes:
 - Update properties: title, description, Knowledge Base article, Microsoft Security Response Center number.
 - Applicability rules: used by Automatic Updates to determine whether or not the update is needed on a particular computer.
 - Installation information: command-line options to apply when installing the updates.

The two parts of the update can be downloaded independently of each other. For example, if you choose not to store updates locally, only update metadata (and any applicable Microsoft Software License Terms) will be downloaded to the WSUS server; clients will get their update files directly from Microsoft Update. On the other hand, if you are storing updates locally on the WSUS server, you can either download everything at the time of synchronization, or download only the metadata during the synchronization, leaving the actual update files to be downloaded after you have approved the update.

Managing Windows Server Update Services 3.0 SP2

In this section

- [Setting Up Synchronizations](#)
- [Managing the Client Computers and Computer Groups](#)
- [Managing the Updates](#)
- [Running WSUS 3.0 SP2 in Replica Mode](#)
- [Backing Up Windows Server Update Services 3.0 SP2](#)
- [Managing WSUS 3.0 SP2 from the Command Line](#)

Setting Up Synchronizations

During synchronization, your WSUS server downloads updates (update metadata and files) from an update source. It also downloads new product classifications and categories, if any. When your WSUS server synchronizes for the first time, it will download all of the updates you specified when you configured synchronization options. After the first synchronization, your WSUS server downloads only updates from the update source, as well as revisions in metadata for existing updates and expirations to updates.



Note

The first time a WSUS server downloads updates may take a long time. If you are setting up multiple WSUS servers, you can speed up the process to a certain extent by downloading all the updates on one WSUS server and then copying the updates to the content directories of the other WSUS servers. Update metadata must be downloaded separately to each server during synchronization.

The **Options** page is the central access point in the WSUS Administration Console for customizing how your WSUS server synchronizes updates. You can specify which updates are synchronized automatically, where your server gets updates, connection settings, and the synchronization schedule. You can also use the Configuration Wizard from the **Options** page to configure or reconfigure your WSUS server at any time.

Synchronizing Updates by Product and Classification

Your WSUS server downloads updates based on the products or product families (for example, Windows, or Windows Server 2003, Datacenter Edition) and classifications (for example, critical updates or security updates) that you specify. At the first synchronization, your WSUS server downloads all of the updates available in the categories you have specified. In later

synchronizations your WSUS server downloads only the newest updates (or changes to the updates already available on your WSUS server) for the categories you specified.

You specify update products and classifications on the **Options** page under **Products and Classifications**. Products are listed in a hierarchy, grouped by product family. If you select Windows, you automatically select every product that falls under that product hierarchy. By selecting the parent check box you select all items under it, as well as all future versions. Selecting the child check boxes will not select the parent check boxes. The default setting for products is all Windows products, and the default setting for classifications is critical and security updates.

If your WSUS server is running in replica mode, you will not be able to perform this task. For more information about replica mode, see [Running WSUS 3.0 SP2 in Replica Mode](#).

To specify update products and classifications for synchronization

1. In the WSUS Administration Console, click the **Options** node.
2. Click **Products and Classifications**, and then click the **Products** tab.
3. Select the check boxes of the products or product families you want to update with WSUS, and then click **OK**.
4. In the **Classifications** tab, select the check boxes of the update classifications you want your WSUS server to synchronize, and then click **OK**.

Note

You can remove products or classifications in the same way. Your WSUS server will stop synchronizing new updates for the products you have cleared. However, updates that were synchronized for those products before you cleared them will remain on your WSUS server and will be listed as available. For more information about removing unused updates, see [Issues with Update Storage](#).

Synchronizing Updates by Language

Your WSUS server downloads updates based on the languages that you specify. You can synchronize updates in all of the languages in which they are available, or you can specify a subset of languages. If you have a hierarchy of WSUS servers, and you need to download updates in different languages, make sure that you have specified all the necessary languages on the upstream server. On a downstream server you can specify a subset of the languages you specified on the upstream server.

Configuring Proxy Server Settings

You can configure your WSUS server to use a proxy server during synchronization with an upstream server or Microsoft Update. This setting will apply only when your WSUS server runs synchronizations. By default your WSUS server will try to connect directly to the upstream server or Microsoft Update.

▶ To specify a proxy server for synchronization

1. In the WSUS Administration Console, click **Options**, and then click **Update Source and Proxy Server**.
2. On the **Proxy Server** tab, select the **Use a proxy server when synchronizing** check box, and then type the server name and port number (port 80 is the default) of the proxy server.
 - If you want to connect to the proxy server with specific user credentials, select the **Use user credentials to connect to the proxy server** check box, and then enter 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. Click **OK**.



Note

Because WSUS initiates all of its network traffic, there is no need to configure Windows Firewall on a WSUS server connected directly to Microsoft update.

Configuring the Update Source

The update source is the location from which your WSUS server gets its updates and update metadata. You can specify that the update source should be either Microsoft Update or another WSUS server (the WSUS server that acts as the update source is the upstream server, and your server is the downstream server).

Options for customizing how your WSUS server synchronizes with the update source include the following:

- You can specify a custom port for synchronization. For information about configuring ports, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).
- You can use Secure Socket Layers (SSL) to secure synchronization of update information between WSUS servers. For more information about using SSL, see [Securing Windows Server Update Services 3.0 SP2](#).

▶ To specify the update source for your WSUS server

1. In the WSUS Administration Console, click **Options**, and then click **Update Source and Proxy Server**.
2. On the **Update Source** tab, do one of the following:
 - If you want your WSUS server to synchronize directly from Microsoft Update, click **Synchronize from Microsoft Update**. If your server is running in replica mode, this option is disabled. For more information, see [Running WSUS 3.0 SP2 in Replica Mode](#).

- If you want to synchronize from another WSUS server in your network, click **Synchronize from an upstream Windows Server Update Services server**, and then type the server name and port number in the corresponding boxes.
 - If you want to use SSL when synchronizing, type the port number that the upstream server uses for SSL connections, and then select the **Use SSL when synchronizing update information** check box. For more information about using SSL during synchronization, see [Securing Windows Server Update Services 3.0 SP2](#).
 - If your WSUS server is running in replica mode, type the server name and port number in the **Server name** box. The upstream server does not have to be the administration server (for example, it can be another replica mode server). For more information about replica mode, see [Running WSUS 3.0 SP2 in Replica Mode](#).
3. Click **OK**.

Configuring Update Storage

For more information, see [Specifying Where to Store the Updates](#).

Synchronizing Manually or Automatically

You can either synchronize your WSUS server manually or specify a time for it to synchronize automatically.

▶ To synchronize your server manually

1. In the WSUS Administration Console, click **Options**, and then click **Synchronization Schedule**.
2. Click **Synchronize manually**, and then click **OK**.

▶ To set up an automatic synchronization schedule

1. In the WSUS Administration Console, click **Options**, then **Synchronization Schedule**.
2. Click **Synchronize automatically**.
3. For **First synchronization**, select the time you want synchronization to start each day.
4. For **Synchronizations per day**, select the number of synchronizations you want to do each day. For example, if you want four synchronizations a day starting at 3:00 A.M., then synchronizations will occur at 3:00 A.M., 9:00 A.M., 3:00 P.M., and 9:00 P.M. each day. (A random time offset will be added to the scheduled synchronization time in order to space out the server connections to Microsoft Update.)
5. Click **OK**.

▶ To synchronize your WSUS server immediately

1. On the WSUS Administration Console, select the top server node.

2. In the **Overview** pane, under **Synchronization Status**, click **Synchronize now**.

Managing the Client Computers and Computer Groups

In this section

- [Managing the Client Computers](#)
- [Managing the Computer Groups](#)

Managing the Client Computers

The central access point in the WSUS administrative console for managing computers is the **Computers** node. Under this node you can find the different groups you have set up (plus the default group, Unassigned Computers). Selecting one of the computer groups causes the computers in that group to be displayed in the **Details** pane. (If a computer is assigned to multiple groups, it will appear in the listings of both groups.) If you select a computer in the list, you can see its properties, which include general details about the computer and the status of updates for it, such as the installation or detection status of an update for a particular computer. You can filter the list of computers under a given computer group by status. The default shows only computers for which updates are needed or which have had installation failures; however, you can filter the display by any status. Click **Refresh** after changing the status filter.

You can also manage computer groups on the **Computers** page, which includes creating the groups and assigning computers to them. For more information about managing computer groups, see [Managing the Computer Groups](#).



Important

You must first configure client computers to contact the WSUS server before you can manage them from that server. Until you perform this task, your WSUS server will not recognize your client computers and they will not be displayed in the list on the **Computers** page. For more information about setting up client computers, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkID=139832) (<http://go.microsoft.com/fwlink/?LinkID=139832>).

Managing the Computer Groups

WSUS allows you to target updates to groups of client computers, so you can ensure that specific computers always get the right updates at the most convenient times. For example, if all the computers in one department (such as the Accounting team) have a specific configuration, you

can set up a group for that team, decide which updates their computers need and what time they should be installed, and then use WSUS reports to evaluate the updates for the team.

Computers are always assigned to the **All Computers** group, and remain assigned to the **Unassigned Computers** group until you assign them to another group. Computers can belong to more than one group.

Computer groups can be set up in hierarchies (for example, the Payroll group and the Accounts Payable group below the Accounting group). Updates that are approved for a higher group will automatically be deployed to lower groups, as well as to the higher group itself. Thus, if you approve Update1 for the Accounting group, the update will be deployed to all the computers in the Accounting group, all the computers in the Payroll group, and all the computers in the Accounts Payable group.

Because computers can be assigned to multiple groups, it is possible for a single update to be approved more than once for the same computer. However, the update will be deployed only once, and any conflicts will be resolved by the WSUS server. To continue with the example above, if ComputerA is assigned to both the Payroll and the Accounts Payable groups, and Update1 is approved for both groups, it will be deployed only once.

You can assign computers to computer groups by using one of two methods, server-side targeting or client-side targeting. With server-side targeting, you manually move one or more client computers to one computer group at a time. With client-side targeting, you use Group Policy or edit the registry settings on client computers to enable those computers to automatically add themselves into the previously created computer groups. This process can be scripted and deployed to many computers at once. You must specify the targeting method you will use on the WSUS server by selecting one of the two options on the **Computers** section of the **Options** page.



Note

If a WSUS server is running in replica mode, computer groups cannot be created on that server. All the computer groups needed for clients of the replica server must be created on the WSUS server that is the root of the WSUS server hierarchy. For more information about replica mode, see [Running WSUS 3.0 SP2 in Replica Mode](#).

For more information about server-side and client-side targeting, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Managing the Updates

In this section

- [Overview of Updates](#)
- [Viewing the Updates](#)
- [WSUS 3.0 SP2 and the Catalog Site](#)
- [Approving the Updates](#)

- [Testing the Updates](#)
- [Storing the Updates](#)

Overview of Updates

Updates are used for updating or providing a full file replacement for software that is installed on a computer. Every update that is available on Microsoft Update is made up of two components:

- **Metadata:** Provides information about the update. For example, metadata supplies information for the properties of an update, thus enabling you to find out for what the update is useful. Metadata also includes Microsoft Software License Terms. The metadata package downloaded for an update is typically much smaller than the actual update file package.
- **Update files:** The actual files required to install an update on a computer.

How WSUS Stores Updates

When updates are synchronized to your WSUS server, the metadata and update files are stored in two separate locations. Metadata is stored in the WSUS database. Update files can be stored either on your WSUS server or on Microsoft Update servers, depending on how you have configured your synchronization options. If you choose to store update files on Microsoft Update servers, only metadata is downloaded at the time of synchronization; you approve the updates through the WSUS console, and then client computers get the update files directly from Microsoft Update at the time of installation. For more information about your options for storing updates, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Managing Updates with WSUS

You will be setting up and running synchronizations, adding computers and computer groups, and deploying updates on a regular basis. The following list gives examples of general tasks you might undertake in updating computers with WSUS.

1. Determine an overall update management plan based on your network topology and bandwidth, company needs, and organizational structure. Considerations might include the following:
 - Whether to set up a hierarchy of WSUS servers, and how the hierarchy should be structured.
 - Which database to use for update metadata (for example, Windows® Internal Database, SQL Server 2005).
 - What computer groups to create, and how to assign computers to them (server-side or client-side targeting).
 - Whether updates should be synchronized automatically, and at what time.

2. Set synchronization options, such as update source, product and update classification, language, connection settings, storage location, and synchronization schedule.
3. Get the updates and associated metadata on your WSUS server through synchronization from either Microsoft Update or an upstream WSUS server.
4. Approve or decline updates. You have the option of allowing users to install the updates themselves (if they are local administrators on their client computers).
5. Configure automatic approvals. You can also configure whether you want to enable automatic approval of revisions to existing updates or approve revisions manually. If you choose to approve revisions manually, then your WSUS server will continue using the older version until you manually approve the new revision.
6. Check the status of updates. You can view update status, print a status report, or configure e-mail for regular status reports.

Update Products and Classifications

Updates available on Microsoft Update are differentiated by product (or product family) and classification.

Products Updated by WSUS

A product is a specific edition of an operating system or application, for example Windows Server 2003. A product family is the base operating system or application from which the individual products are derived. An example of a product family is Microsoft Windows, of which Windows Server 2003 is a member. You can select the products or product families for which you want your server to synchronize updates. You can specify a product family or individual products within the family. Selecting any product or product family will get updates for current and future versions of the product.

Update Classifications

Update classifications represent the type of update. For any given product or product family, updates could be available among multiple update classifications (for example, Windows XP family Critical Updates and Security Updates). The following table lists update classifications.

Update Classification	Description
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

Update Classification	Description
	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 set 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.

Viewing the Updates

On the **Updates** page, you can do the following:

- View updates. The update overview displays updates that have been synchronized from the update source to your WSUS server and are available for approval.
- Filter updates. In the default view you can filter updates by approval status and installation status. The default setting is for unapproved updates that are needed by some clients or that have had installation failures on some clients. You can change this view by changing the approval status and installation status filters, and then clicking **Refresh**.
- Create new update views. In the Actions pane, click **New Update View**. You can filter updates by classification, product, the group for which they have been approved, and synchronization date. You can sort the list by clicking the appropriate column heading in the title bar.

- Search for updates. You can search for an individual update or set of updates by title, description, Knowledge Base article, or the Microsoft Security Response Center number for the update.
- View details, status, and revision history for each update.
- Approve updates.
- Decline updates.

▶ To view updates

1. In the WSUS administration console, expand the **Updates** node, and then click **All Updates**.
2. By default, updates are displayed with their title, classification, installed/not applicable percentage, and approval status. If you wish to display more or different update properties, right-click the column heading bar and select the appropriate columns.
3. To sort by different criteria, such as download status, title, classification, release date, or approval status, click the appropriate column heading.

▶ To filter the list of updates displayed on the Updates page

1. In the WSUS administration console, expand the **Updates** node, and then click **All Updates**.
2. In the center pane next to **Approval**, select the desired approval status, and next to **Status** select the desired installation status. Click **Refresh**.

▶ To create a new update view

1. In the WSUS administration console, expand the **Updates** node, and then click **All Updates**.
2. In the Actions pane, click **New Update View**.
3. In the **Add Update View** window, under **Step 1: Select properties**, select the properties you need to filter the update view:
 - Select **Updates are in a specific classification** to filter on updates belonging to one or more update classifications.
 - Select **Updates are for a specific product** to filter on updates for one or more products or product families.
 - Select **Updates are approved for a specific group** to filter on updates approved for one or more computer groups.
 - Select **Updates were synchronized within a specific time period** to filter on updates synchronized at a specific time.
 - Select **Updates are WSUS updates** to filter on WSUS updates.
4. Under **Step 2: Edit the properties**, click the underlined words to pick the values you want.

5. Under **Step 3: Specify a name**, give your new view a name.
6. Click **OK**.
7. Your new view will appear in the tree view pane under **Updates**. It will be displayed, like the standard views, in the center pane when you select it.

▶ **To search for an update**

1. Select the **Updates** node (or any node under it).
2. In the Actions pane, click **Search**.
3. In the Search window, on the **Updates** tab, enter your search criteria. You can use text from the **Title**, **Description**, and **Microsoft Knowledge Base (KB) article number** fields. Each of these items is a property listed on the **Details** tab in the update properties.

▶ **To view the properties for an update**

1. In the WSUS administration console, expand the **Updates** node, and then click **All Updates**.
2. In the list of updates, click the update you want to view.
3. In the lower pane, you will see the different property sections:
 - The title bar displays the title of the update; for example, **Security Update for Windows Media Player 9 (KB911565)**.
 - The **Status** section displays the installation status of the update (the computers on which it needs to be installed, computers on which it was installed with errors, computers on which it has been installed or is not applicable, and computers that have not reported status for the update), as well as general information (KB and MSRC numbers release date, etc.).
 - The **Description** section displays a brief description of the update.
 - The **Additional Details** section displays the following information:
 - a. The installation behavior of the update (whether or not it is removable, requests a restart, requires user input, or must be installed exclusively)
 - b. Whether or not the update has Microsoft Software License Terms
 - c. The products to which the update applies
 - d. The updates that supersede this update
 - e. The updates that are superseded by this update
 - f. The languages supported by the update
 - g. The update ID



Note

You can perform this procedure on only one update at a time. If you select multiple updates, the first update in the list will be displayed in the **Properties** pane.

WSUS 3.0 SP2 and the Catalog Site

The catalog site is the Microsoft location from which you can import hotfixes and hardware drivers.

Importing hotfixes from the Microsoft Update catalog site

In order to import hotfixes into WSUS, you must access the Microsoft Update catalog site from a WSUS computer.



Note

Any computer that has the WSUS administrative console installed, whether or not it is a WSUS server, can be used to import hotfixes from the catalog site. You must be logged on to the computer as an administrator to import the hotfixes.

▶ To access the Microsoft Update catalog site

1. In the WSUS administrative console, select either the top server node or the **Updates** node, and in the **Actions** pane click **Import Updates**.
2. A browser window will open at the Microsoft Update Catalog Web site.
3. In order to access the updates at this site, you must install the Microsoft Update Catalog ActiveX control.
4. You can browse this site for Windows hotfixes and hardware drivers. When you have found the ones you want, add them to your basket.
5. When you have finished browsing, go to the basket and click **Import** to import your updates. To download the updates without importing them, clear the **Import directly into Windows Server Update Services** checkbox.

Restricting access to hotfixes

WSUS administrators should use the following steps to restrict access to the hotfixes they have downloaded from the Microsoft Update catalog site.

▶ To restrict access to hotfixes

1. Enable Windows authentication on the IIS Content vroot.
 - Start **IIS Manager** (click **Start**, then **Administrative Tools**, and then **Internet Information Services (IIS) Manager**).
 - Navigate to the Content node of the WSUS Web site.
 - Click **Properties** and open the **Directory Security** tab.

- Under **Authentication and access control**, click **Edit**.
 - In the **Authentication Methods** screen, clear the **Enable anonymous access** checkbox and select the **Integrated Windows authentication** check box.
2. Create a WSUS target group for the computers that need the hotfix, and add them to the group. For more information about computers and groups, see [Managing the Client Computers and Computer Groups](#).
 3. Download the files for the hotfix.
 4. Set the permissions of these files so that only machine accounts of those machines can read them. You will also need to allow the Network Service account full access to the files
 5. Approve the hotfix for the WSUS target group created in Step 2.

Importing updates in different languages

The Microsoft Update Catalog Web site includes updates that support multiple languages. It is very important to match the languages supported by the WSUS server with the languages supported by these updates. If the WSUS server does not support all the languages included in the update, the update will not be deployed to client computers. Likewise, if an update supporting multiple languages has been downloaded to the WSUS server but not yet deployed to client computers, and an administrator deselects one of the languages included the update, the update will not be deployed to the clients.

Approving the Updates

After updates have been synchronized to your WSUS server, they will be scanned automatically for relevance to the server's client computers. However, you must approve the updates before they are deployed to the computers on your network. When you approve an update, you are essentially telling WSUS what to do with it (your choices are **Install** or **Decline** for a new update). You can approve updates for the **All Computers** group or for subgroups. If you do not approve an update, its approval status remains **Not approved**, and your WSUS server allows clients to evaluate whether or not they need the update.

If your WSUS server is running in replica mode, you will not be able to approve updates on your WSUS server. For more information about replica mode, see [Running WSUS 3.0 SP2 in Replica Mode](#).

Approving Updates

You can approve the installation of updates for all the computers in your WSUS network or for different computer groups. After approving an update, you can do one (or more) of the following:

- Apply this approval to child groups, if any.

- Set a deadline for automatic installation. When you select this option, you set specific times and dates to install updates, overriding any settings on the client computers. In addition, you can specify a past date for the deadline if you want to approve an update immediately (to be installed the next time client computers contact the WSUS server).
- Remove an installed update if that update supports removal.

Important

You cannot set a deadline for automatic installation for an update if user input is required (for example, specifying a setting relevant to the update). To determine whether an update will require user input, look at the **May request user input** field in the update properties for an update displayed on the **Updates** page. Also check for a message in the **Approve Updates** box that says, "**The selected update requires user input and does not support an installation deadline.**"

Important

If there are updates to the WSUS server component, you cannot approve other updates to client systems until the WSUS update is approved. You will see this warning message in the Approve Updates dialog box: "There are WSUS updates that have not been approved. You should approve the WSUS updates before approving this update." In this case, you should click the WSUS Updates node and make sure that all of the updates in that view have been approved before returning to the general updates.

To approve updates

1. In the WSUS administrative console, click **Updates**.
2. In the list of updates, select the update that you want to approve and right-click (or go to the **Actions** pane).
3. In the **Approve Updates** dialog box, select the computer group for which you want to approve the update, and click the arrow next to it.
4. Select **Approved for Install**, and then click **Approve**.
5. The **Approval Progress** window will display the progress toward completing the approval. When the process is complete, the **Close** button will be available. Click **Close**.
6. You may select a deadline by right-clicking the update, selecting the appropriate computer group, clicking the arrow next to it, and then clicking **Deadline**.
 - You may select one of the standard deadlines (one week, two weeks, one month), or you may click **Custom** to specify a date and time.
 - If you want an update to be installed as soon as the client computers contact the server, click **Custom**, and set a date and time to the current date and time or to one in the past.

To approve multiple updates

1. In the WSUS administrative console, click **Updates**.

2. To select multiple contiguous updates, press **SHIFT** while clicking updates. To select multiple noncontiguous updates, press and hold down **CTRL** while clicking updates.
3. Right-click the selection and click **Approve**. The **Approve Updates** dialog box opens with the Approval status set to **Keep existing approvals** and the **OK** button disabled .
4. You can change the approvals for the individual groups, but doing so will not affect child approvals. Select the group for which you want to change the approval, and click the arrow to its left. In the shortcut menu, click **Approved for Install**.
5. The approval for the selected group changes to **Install**. If there are any child groups, their approval remains **Keep existing approval**. To change the approval for the child groups, click the group and click the arrow to its left. In the shortcut menu, click **Apply to Children**
6. To set a specific child to inherit all its approval from the parent, click the child and click the arrow to its left. In the shortcut menu, click **Same as Parent**. If you set a child to inherit approvals, but are not changing the parent approvals, the child will inherit the existing approvals of the parent.
7. If you want the approval behavior to change for all children, approve **All Computers**, and then choose **Apply to Children**.
8. Click **OK** after setting all your approvals. The **Approval Progress** window will display the progress toward completing the approval. When the process is complete, the **Close** button will be available. Click **Close**.



Note

For more information about downloading and installing updates, see [Best Practices with Windows Server Update Services 3.0 SP2](#).

Declining Updates

If you select this option, the update is removed from the default list of available updates and the WSUS server will not offer the update to clients, either for evaluation or installation. You can reach this option by selecting an update or group of updates and right-clicking or going to the Actions pane. Declined updates will appear in the updates list only if you select **Declined** in the Approval list when specifying the filter for the update list under **View**.

► To decline updates

1. In the WSUS administrative console, click **Updates**.
2. In the list of updates, select one or more updates that you want to decline.
3. Select **Decline**.
4. Click **Yes** on the confirmation message.

Change an Approved Update to Not Approved

If an update has been approved and you decide not to install it at this time, and instead want to save it for a future time, you can change the update to a status of Not Approved. This means that the update will remain in the default list of available updates and will report client compliance, but will not be installed on clients.

► To change an approved update to Not Approved

1. In the WSUS administrative console, click **Updates**.
2. In the list of updates, select one or more approved updates that you want to change to Not Approved.
3. In the shortcut menu or the **Actions** pane, select **Not Approved**.
4. Click **Yes** on the confirmation message.

Approving Updates for Removal

You can approve an update for removal (that is, to uninstall an already-installed update). This option is available only if the update is already installed and supports removal. You can specify a deadline for the update to be uninstalled, or specify a past date for the deadline if you want to remove the update immediately (the next time client computers contact the WSUS server).



Note

Not all updates support removal. You can see whether an update supports removal by selecting an individual update and looking at the **Details** pane. Under **Additional Details**, you will see the **Removable** category. If the update cannot be removed through WSUS, in many cases it can be removed with **Add or Remove Programs** from **Control Panel**.

► To approve updates for removal

1. In the WSUS administrative console, click **Updates**.
2. In the list of updates, select one or more updates that you want to approve for removal and right-click them (or go to the **Actions** pane).
3. In the **Approve Updates** dialog box, select the computer group from which you want to remove the update, and click the arrow next to it.
4. Select **Approved for Removal**, and then click the **Remove** button.
5. After the remove approval has completed, you may select a deadline by right-clicking the update once more, selecting the appropriate computer group, and clicking the arrow next to it. Then select **Deadline**.
 - You may select one of the standard deadlines (one week, two weeks, one month), or you may click **Custom** to select a specific date and time.
6. If you want an update to be removed as soon as the client computers contact the server,

click **Custom**, and set a date in the past.

Approving Updates Automatically

You can configure your WSUS server for automatic approval of certain updates. You can also specify automatic approval of revisions to existing updates as they become available. This option is selected by default. A revision is a version of an update that has had changes made to it (for example, it might have expired, or its applicability rules might have changed). If you do not choose to approve the revised version of an update automatically, WSUS will use the older version, and you must manually approve the update revision.

You can create rules that your WSUS server will automatically apply during synchronization. You specify what updates you want to automatically approve for installation, by update classification, by product, and by computer group. This applies only to new updates, as opposed to revised updates. You can also specify an update approval deadline, which sets a number of days and a specific time of offering before the approved update is deadline-installed. These settings are available in the **Options** pane, under **Automatic Approvals**.

► To automatically approve updates

1. In the WSUS administration console, click **Options**, and then click **Automatic Approvals**.
2. In **Update Rules**, click **New Rule**.
3. In the **Add Rule** dialog box, under **Step 1: Select properties**, select whether to use **When an update is in a specific classification** or **When an update is in a specific product** (or both) as criteria. Optionally, select whether to **Set a deadline for the approval**.
4. In **Step 2: Edit the properties** click the underlined properties to select the **Classifications**, **Products**, and **Computer groups** for which you want automatic approvals, as applicable. Optionally, choose the update approval deadline **Day** and **Time**.
5. In **Step 3: Specify a name** box, type a unique name for the rule.
6. Click **OK**.



Note

Automatic approval rules will not apply to updates requiring an End User License Agreement (EULA) that has not yet been accepted on the server. If you find that applying an automatic approval rule does not cause all the relevant updates to be approved, you should approve these updates manually.

Automatically Approving Revisions to Updates and Declining Expired Updates

The **Automatic Approvals** section of the **Options** pane contains a default option to automatically approve revisions to approved updates. You can also set your WSUS server to automatically decline expired updates. If you choose not to approve the revised version of an update automatically, your WSUS server will use the older revision, and you must manually approve the update revision.



Note

A revision is a version of an update that has changed (for example, it might have expired or have updated applicability rules).

► To automatically approve revisions to updates and decline expired updates

1. In the WSUS administration console, click **Options**, and then click **Automatic Approvals**.
2. On the **Advanced** tab, make sure that both **Automatically approve new revisions of approved updates** and **Automatically decline updates when a new revision causes them to expire** check boxes are selected.
3. Click **OK**.



Important

Keeping the default values for these options allows you maintain good performance on your WSUS network. If you do not want expired updates to be declined automatically, you should make sure to decline them manually on a periodic basis.

Approving Superseding or Superseded Updates

Typically, an update that supersedes other updates does one or more of the following:

- Enhances, improves, or adds to the fix provided by one or more previously released updates.
- Improves the efficiency of its update file package, which is installed on client computers if the update is approved for installation. For example, the superseded update might contain files that are no longer relevant to the fix or to the operating systems now supported by the new update, so those files are not included in the superseding update's file package.
- Updates newer versions of operating systems. It is also important to note that the superseding update might not support earlier versions of operating systems.

Conversely, an update that is *superseded* by another update does the following:

- Fixes a problem similar to that of the update that supersedes it. However, the update that supersedes it might enhance the fix that the superseded update provides.
- Updates earlier versions of operating systems. In some cases, these versions of operating systems are no longer updated by the superseding update.

In an individual update's detail pane, an informational icon and a message at the top indicates that it either supersedes or is superseded by another update. In addition, you can determine which updates supersede or are superseded by the update by looking at the **Updates superseding this update** and **Updates superseded by this update** entries in the Additional Details section of the Properties. An update's detail pane is displayed below the list of updates. WSUS does not automatically decline superseded updates, and it is recommended that you do not assume that superseded updates should be declined in favor of the new, superseding update. Before declining a superseded update, make sure that it is no longer needed by any of your client computers. The following are examples of scenarios in which you might need to install a superseded update:

- If a superseding update supports only newer versions of an operating system, and some of your client computers run earlier versions of the operating system.
- If a superseding update has more restricted applicability than the update it supersedes, which would make it inappropriate for some client computers.
- If an update no longer supersedes a previously released update because of new changes. It is possible that through changes at each release, an update no longer supersedes an update it previously superseded in an earlier version. In this scenario, you will still see a message about the superseded update, even though the update that supersedes it has been replaced by an update that does not.

Best Practices for Approving a Superseding Update

Because a superseding update typically enhances a fix provided by a previously released update, it is recommended that you first see how many client computers will be compliant with the new update and work backward from there. Use the following process.

▶ To approve a superseding update

1. Check the status of the update on client computers. Note which computers show status as **Not applicable** for the update, and then compare the properties of those computers with the properties of the update.
2. Use the information available in the update properties to help you determine which previously released versions are available. You can look under **Updates superseded by this update** in the update's properties, and check the **Description** and **KB article number** entries if appropriate.
3. Look at the properties of the superseded versions of the updates.
4. When you find a superseded update that seems appropriate for the remaining client computers, approve the update for installation.

Office Update Approval

If you use WSUS to update Microsoft Office on your network computers, consider the following:

- You must use an original baseline source for Microsoft Office Administrative Install Points (AIP) to use WSUS to update Office XP and Office 2003 on client computers. If you are applying updates to the AIP, you cannot use WSUS. The two methods of applying updates are mutually exclusive. If you have applied an update to an AIP and want to roll back the AIP to an original baseline source, use the instructions found at the [Microsoft Support Web site](http://go.microsoft.com/fwlink/?LinkId=63962) (<http://go.microsoft.com/fwlink/?LinkId=63962>).



Important

Administrative Install Points are relevant only to Office XP and Office 2003. They are not used with Office 2007.

- If you have purchased a "per user" license agreement for Office or have installed Office per user, WSUS will not update Office.
- Users can access the public Microsoft Office Online Web site to look for updates to their Office installation through the Microsoft Office Update wizard. Using Group Policy, you might want to create policies that prevent users from getting their own Office updates from Microsoft Office Online.

For more information and troubleshooting advice, see the following Knowledge Base articles.

- [Office 2003 updates are offered to a user even if that user has installed those updates when you use WSUS to deploy software updates and hotfixes to computers that are in your organization](http://go.microsoft.com/fwlink/?LinkId=78874) (<http://go.microsoft.com/fwlink/?LinkId=78874>)
- [No appropriate Microsoft Office updates are displayed when you use Microsoft Update or Windows Server Update Services](http://go.microsoft.com/fwlink/?LinkId=78871) (<http://go.microsoft.com/fwlink/?LinkId=78871>)
- [How to change the source for a client computer from an updated administrative installation point to an Office 2003 original baseline source or Service Pack 2](http://go.microsoft.com/fwlink/?LinkId=78872) (<http://go.microsoft.com/fwlink/?LinkId=78872>)

SQL Server and Exchange Server Updates Approval

Updating Microsoft SQL Server instances

SQL Server installations can become quite complex, with multiple instances or even versions of SQL Server on a single computer. You will need to make sure that when you specify your synchronization options, you account for all the versions of the SQL Server you have on the computer. For more information about configuring synchronization options, see [Setting Up Synchronizations](#).

Updating Microsoft SQL Server and Microsoft Exchange Servers that are part of a cluster

Both Microsoft SQL Server and Microsoft Exchange Server can be installed in a *clustered environment*. If there is an update available for clustered servers, each server in the cluster must be updated individually. Microsoft recommends that you update passive cluster nodes individually. You will need to stop the cluster service for each server while you update it, and then restart the service.

Note

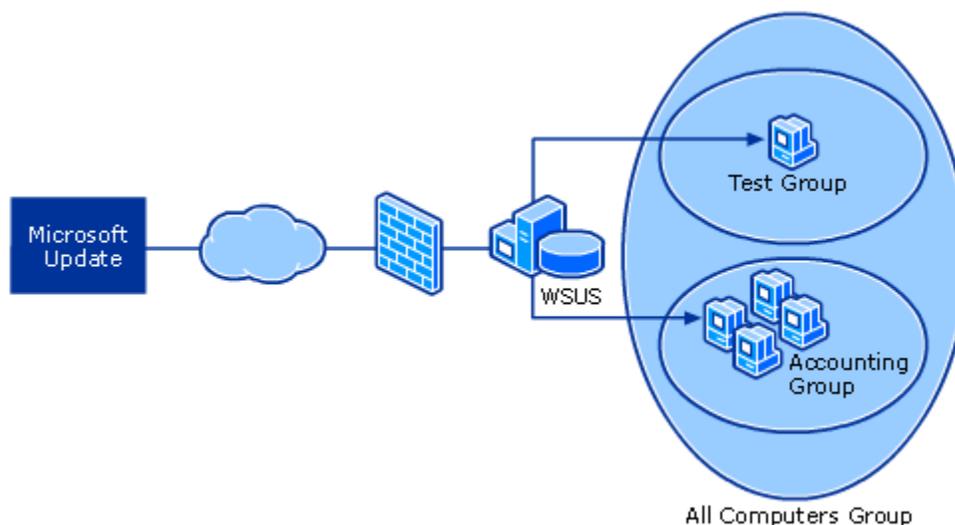
You can have both a stand-alone instance and a clustered instance of SQL Server on the same server. If you are updating a server that is running both a stand-alone instance and a clustered instance of SQL server, both SQL Server instances will be updated if you have specified the correct synchronization options.

Testing the Updates

Until you install an update, you cannot be certain about the impact it will have on other programs running on your systems. By installing an update in a test environment, you can assess its impact before you decide whether or not to deploy it to your production systems. This approach can prevent unplanned downtime and lost productivity.

WSUS enables you to create custom computer groups that you can use to test updates. For example, the following figure depicts three computer groups: two custom groups created by the administrator (Test and Accounting), as well as the built-in All Computers group.

In this example, the Test group contains a small number of computers representative of the computers in the Accounting group. The administrator can first approve updates for the Test group. If the testing goes well, the administrator can roll out the updates to the Accounting group.



You can create multiple test computer groups with different configurations that resemble the computers in different departments in your organization.

Storing the Updates

In this section

- [Specifying Where to Store the Updates](#)
- [Managing the Database](#)

Specifying Where to Store the Updates

You can specify whether to store update files on your local WSUS server or on Microsoft Update. If you store updates locally, you can limit the updates downloaded by language. If you store the update files on Microsoft Update, then your WSUS server will download only update metadata. Update files are downloaded to the client computers at the time of installation. If you choose this option, you will need to make sure all your client computers have direct access to Microsoft Update.

Local Storage Considerations

If you decide to store update files on your server, the recommended minimum disk size is 30 GB. However, depending on your synchronization options (in particular, multiple update languages or express installation files), you might need more disk space. If you download updates in five languages, you will need approximately double the size of the content directory you would need for just one language.

If your disk gets full, you can move the update files to a different location. To do this you will need to run the WSUSutil.exe tool. For this procedure, see [Managing WSUS 3.0 SP2 from the Command Line](#).

About Express Installation Files

Express installation files are usually many times larger than a regular update package. An express installation file package containing all the versions of the update for different computer configurations is downloaded to your WSUS server. However, when your client computers connect to the server, they will download only the changes in the update files that the update needs. You should select the express installation file option only in situations where you are less concerned with external bandwidth than internal bandwidth usage.

Besides bandwidth, another consideration when choosing to download express installation files, as mentioned earlier, is disk space. If you choose to download express installation files, they will take more disk space. Therefore, use a larger disk (more than 30 GB) if you select this option.

► To specify where to store downloaded update files

1. In the WSUS administrative console, click **Options**, and then click **Update Files and Languages**.
2. Click the **Update Files** tab.
3. Select whether to store update files locally or on Microsoft Update. If you decide to store update files on your server, you can also choose to download update files only when they are approved, or to download express installation files.
4. If you decide to store the files on the WSUS server, click the **Update Languages** tab, and then select whether to limit the updates downloaded to your WSUS server by language. You should limit the languages you download if you are going to store update files on your WSUS server.
5. Click **OK**.



Note

If your WSUS server is running in replica mode, you will not be able to perform this task. For more information about replica mode, see [Running WSUS 3.0 SP2 in Replica Mode](#).

Updates, Update Files, and Languages

If you are storing updates locally, and you have set up a WSUS server to download updates in a limited number of languages, you may notice that there are updates in languages other than the ones you specified. This is because many updates are in fact bundles of update files for different languages, and the update in question includes at least one of the language settings on the server.

Changing the Location Where You Store Update Files Locally

You might need to change your local update storage location if the disk becomes full or fails and the replacement disk uses a new drive letter.

You accomplish this move with the **movecontent** command of `WSUSutil.exe`, a command-line tool that can be found in the `WSUSInstallationDirectory\Tools\` directory (where `WSUSInstallationDirectory` is the directory to which you installed WSUS).

`WSUSutil.exe` can be run only on the WSUS server itself. Only members of the local Administrators group on the WSUS server can run `WSUSutil.exe`.

You create the new path for local WSUS update storage before moving the content. The **movecontent** command takes an optional **-skipcopy** parameter, which enables you to change the storage location without copying any files. For more information about `WSUSutil.exe`, see [Managing WSUS 3.0 SP2 from the Command Line](#).

► To change the location of local WSUS update storage

1. Open a command shell.
2. Navigate to the directory that contains WSUSutil.exe:
`cd WSUSInstallationDirectory\Tools.`
3. Type the following command:

```
wsusutil.exe movecontent contentpath logfile [-skipcopy]
```

For example, type:

```
wsusutil.exe movecontent D:\WSUS1\ D:\move.log
```

where D:\WSUS1 is the new path for local WSUS update storage, and D:\move.log is the path to the log file.



Note

If you do not want to use WSUSutil.exe to change the location of local WSUS update storage, you can also use NTFS functionality to add a partition to the current location of local WSUS update storage. For more information about NTFS, see [NTFS technical documentation](http://go.microsoft.com/fwlink/?LinkId=79488) (<http://go.microsoft.com/fwlink/?LinkId=79488>).

Managing the Database

The WSUS database is configured during setup to store the following types of information:

- WSUS server configuration information
- Information about client computers, updates, and client interaction with updates
- Update metadata

Update metadata (the information about the update) is part of every update available on Microsoft Update. The update files are stored separately from the metadata, either on Microsoft Update or on your WSUS server. For more information, see [Specifying Where to Store the Updates](#).

Depending on your server and network configurations, you use a Windows® Internal Database or SQL Server database for your WSUS installation. For more information about your database options when installing WSUS, see the [WSUS Deployment Guide](#) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

You may have to perform one or two special database tasks as part of regular operations. You should regularly back up the WSUS database. For more information, see [Backing Up Windows Server Update Services 3.0 SP2](#). You should also re-index the database to improve its performance. For more information, see [Appendix I: Database Maintenance](#). In addition, you may want to move WSUS data from a Windows Internal Database installation to a SQL Server installation.

Additional resources

- [Migrating from Windows Internal Database to SQL Server](#)

Migrating from Windows Internal Database to SQL Server

This topic explains how to migrate the Windows Server Update Services (WSUS) database from a Windows Internal Database instance (installed by default during WSUS setup) to a full version of Microsoft SQL Server 2008 or SQL Server 2005 SP2.

Why Migrate the WSUS Database to SQL Server

If you chose to use Windows Internal Database as the WSUS database when you set up your WSUS server, you may want to upgrade the database engine to a full installation of SQL Server 2008 or SQL Server 2005 SP2. SQL Server lets you administer the WSUS database through the SQL Server Management Studio.

SQL Server Database Requirements

- WSUS requires SQL Server 2008 or SQL Server 2005 SP2. If you use the full version of SQL Server, the database administrator should first verify that the nested triggers option is turned on before setting up the WSUS database.
- You cannot use SQL authentication. WSUS supports Windows authentication only.

Scenarios

The topic presents the following scenarios:

- Migrating the Windows Internal Database database to an instance of SQL Server 2008 or SQL Server 2005 SP2 that is running on the WSUS server
- Migrating the Windows Internal Database database to an instance of SQL Server 2008 or SQL Server 2005 SP2 that is running on another server (remote SQL)

Warning

The procedures in this document use Registry Editor. Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require you to reinstall the operating system. Microsoft cannot guarantee that these problems can be resolved. Modify the registry at your own risk. Before you edit the registry, export the keys in the registry that you plan to edit, or back up the whole registry. If a problem occurs, you can then restore the registry to its previous state.

Migrating the WSUS Database

Use the following steps to migrate the WSUS database from a Windows Internal Database instance to an instance of SQL Server 2008 or SQL Server 2005 SP2.

► To migrate the WSUS database

1. Install SQL Server 2008 or SQL Server 2005 SP2 with the **Server and Client Tools** option on your WSUS server.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.
3. Right-click **IIS Admin Service**, and then click **Stop**.
4. Right-click **Update Services**, and then click **Stop**.
5. Run the following SQL command to detach the WSUS database (SUSDB) from the Windows Internal Database instance, by using the **sqlcmd** utility. For more information about the **sqlcmd** utility, see [sqlcmd Utility](http://go.microsoft.com/fwlink/?LinkId=81183) (<http://go.microsoft.com/fwlink/?LinkId=81183>).

```
sqlcmd -S np:\\.\pipe\MSSQL$MICROSOFT##SSEE\sql\query
use master
alter database SUSDB set single_user with rollback immediate
go
sp_detach_db SUSDB
go
```

6. In SQL Server Management Studio, under the instance node, right-click **Databases**, select **Properties**, and then click **Attach**.
7. In this step, you will verify that NT AUTHORITY\NETWORK SERVICE has login permissions to the instance of SQL Server and to the WSUS database. If it does not, you will have to add it to both locations. This account should also be a member of the webService role on the WSUS database.
 - To verify permissions on the instance of SQL Server, in SQL Server Management Studio, open the instance and select **Security**, and then **Logins**. The NT AUTHORITY\NETWORK SERVICE account should be listed as a login. If it is not, it should be added.
 - To verify permissions on the database, right-click the database, select **Properties** and then click **Permissions**. The NT AUTHORITY\NETWORK SERVICE account should be listed as a login. If it is not, it should be added.
 - To verify members of the webService role, under the WSUS database, select **Roles**, right-click **webService**, and then select **Properties**. The NT AUTHORITY\NETWORK SERVICE account should be listed as a member of this role. If it is not, it should be added.
8. In the **Attach Databases** box, under **Databases to attach**, locate the susdb.mdf file (by default, this is **C:\WSUS\UpdateServicesDbFiles** if you installed Windows Internal

- Database), and then click **OK**.
9. In this step, you will edit the registry to both point WSUS to the instance of SQL server that now holds the WSUS database and recognize the new database for future WSUS updates. If you have not already done this, export the keys in the registry that you plan to edit, or back up the whole registry.
 - a. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
 - b. Find the following key:
HKLM\SOFTWARE\Microsoft\UpdateServices\Server\Setup\SqSqlServerName, and in the **Value** box, type **[ServerName]\[InstanceName]**, and then click **OK**. If the instance name is the default instance, type **[ServerName]**.
 - c. Find the following key: **HKLM\Software\Microsoft\Update Services\Server\Setup\wYukonInstalled**. In the **Value** box, type **0**, and then click **OK**.
 10. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.
 11. Right-click **IIS Admin Service**, and then click **Start**.
 12. Right-click **Update Services**, and then click **Start**.
 13. Verify that the database migration was successful by opening the WSUS administrative console. (Click **Start**, click **Administrative Tools**, and then click **Microsoft Windows Server Update Services 3.0**.)

 **Note**

You might have to restart the server for these settings to take effect.

Migrating the WSUS Database and Moving to a Remote SQL Server

The goal of this scenario is to take the WSUS database running in a Windows Internal Database instance on the WSUS server and move and upgrade it to an instance of SQL Server 2008 or SQL Server 2005 SP2 that is running on a remote server. Only a full SQL Server 2008 or SQL Server 2005 SP2 database may be used in a remote SQL installation. Each step, where appropriate, indicates the server on which you perform the procedure.

Remote SQL Scenario Limitations

- You cannot use a server configured as a domain controller for either the front end or the back end of the remote SQL server pair.
- You cannot use a server that is running as a Terminal Services server for the front end of the remote SQL server pair.
- You cannot use Windows Internal Database for database software on the back-end server.
- Both the front-end and the back-end servers must be joined to an Active Directory directory service domain.

Prerequisites

Front end server starting configuration:

- Windows Server 2003 Service Pack 1 or Windows Server 2008 operating system
- WSUS with Windows Internal Database

Back end server starting configuration:

- Windows Server 2003 Service Pack 1 or Windows Server 2008 operating system
- SQL Server 2008 or SQL Server 2005 SP2

To migrate the WSUS database from a Windows Internal Database instance to an instance of SQL Server 2008 or SQL Server 2005 SP2 on a remote server

1. On the front end server: Install Microsoft SQL Server 2008 or SQL Server 2005 SP2 with the **Server and Client Tools** option. This step will enable you to use the SQL Server Enterprise Manager on the front end server.
2. On the front end server:
 - a. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.
 - b. Right-click **IIS Admin Service**, and then click **Stop**.
 - c. Right-click **Update Services**, and then click **Stop**.
3. On the front end server: Run the following SQL command to detach the WSUS database by using the **sqlcmd** utility. For more information about the **sqlcmd** utility, see [sqlcmd Utility](http://go.microsoft.com/fwlink/?LinkId=81183) (<http://go.microsoft.com/fwlink/?LinkId=81183>).

```
sqlcmd -S np:\\.\pipe\MSSQL$MICROSOFT##SSEE\sql\query
use master
alter database SUSDB set single_user with rollback immediate
go
sp_detach_db 'SUSDB'
go
```

4. On the front end server: copy the SUSDB.mdf and SUSDB_log.ldf files from the front end server to the back end server.
5. On the back end server:
 - a. To attach **SUSDB** to the destination instance of SQL server, under the instance node, right-click **Databases**, select **Properties**, and then click **Attach**.
 - b. In the **Attach Databases** box, under **Databases to attach**, locate the susdb.mdf file (by default this is **C:\WSUS\UpdateServicesDbFiles** if you installed Windows Internal Database), and then click **OK**.
6. On the back end server:
 - To verify permissions on the instance of SQL Server, in SQL Server Management Studio, open the instance, select **Security**, and then **Logins**. The front end server machine account should be listed as a login. If it is not, it should be added.

- To verify permissions on the database, right-click the database, select **Properties**, and then click **Permissions**. The front end server machine account should be listed as a login. If the server account is not listed, it should be added.
 - To verify members of the webService role, under the WSUS database, select **Roles**, right-click **webService**, and then select **Properties**. The front end server machine account should be listed as a member of this role. If the server account is not listed, it should be added.
7. On the front end server: In this step, you will edit the registry to point WSUS to the destination instance of SQL and to recognize the new database for future WSUS updates. If you have not already done so, export the keys in the registry that you plan to edit, or back up the whole registry.
- a. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
 - b. Find the following key:
HKLM\SOFTWARE\Microsoft\UpdateServices\Server\Setup\Sq|ServerName. In the **Value** data box, type **[BEName]\[InstanceName]**, and then click **OK**. If the instance name is the default instance, type **[BEName]**.

 **Note**

When typing **[BEName]**, do not add the domain name before the name.

- c. Find the following key: **HKLM\Software\Microsoft\Update Services\Server\Setup\wYukonInstalled**. In the **Value** box, type **0**, and then click **OK**. This indicates that Windows Internal Database is not used.
 - d. Find the following key:
HKLM\SOFTWARE\Microsoft\UpdateServices\Server\Setup\Sq|InstancesRemote. In the **Value** box, change the value to **1**, and then click **OK**.
8. On the front end server:
- a. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.
 - b. Right-click **IIS Admin Service**, and then click **Start**.
 - c. Right-click **Update Services**, and then click **Start**.
9. On the front end server: Verify that the database migration was successful by opening the WSUS administrative console. (Click **Start**, click **Administrative Tools**, and then click **Microsoft Windows Server Update Services 3.0**).

 **Note**

You might have to restart the front end server in order for these settings to take effect.

For more information about the databases that you can use with WSUS, see the following:

- In this guide, see **Managing the Databases**.
- In [Deploying Microsoft Windows Server Update Services](#), see "Choose the Database Used for WSUS 3.0."

- In [Deploying Microsoft Windows Server Update Services](#), see "Appendix B: Configure Remote SQL" for general information about how to set up WSUS by using a remote SQL server to host the WSUS database.

Using the Server Cleanup Wizard

The Server Cleanup Wizard is integrated into the user interface of WSUS 3.0, WSUS 3.0 with SP1, and WSUS with SP2e, and can be used to help you manage your disk space. This wizard can do the following things:

1. Remove unused updates and update revisions
The wizard will remove all older updates and update revisions that have not been approved.
2. Delete computers not contacting the server
The wizard will delete all client computers that have not contacted the server in thirty days or more.
3. Delete unneeded update files
The wizard will delete all update files that are not needed by updates or by downstream servers.
4. Decline expired updates
The wizard will decline all updates that have been expired by Microsoft.
5. Decline superseded updates
The wizard will decline all updates that meet all the following criteria:
 - The superseded update is not mandatory
 - The superseded update has been on the server for thirty days or more
 - The superseded update is not currently reported as needed by any client
 - The superseded update has not been explicitly deployed to a computer group for ninety days or more
 - The superseding update must be approved for install to a computer group

Important

If you choose to remove unneeded content with the Server Cleanup Wizard, all the private update files that you have downloaded from the Catalog Site will be removed as well. You will need to re-import these files after running the Server Cleanup Wizard.

Running the Server Cleanup Wizard

To run the Server Cleanup Wizard

1. In the WSUS administration console, select **Options**, and then **Server Cleanup Wizard**.
2. By default this wizard will remove unneeded content and computers that have not

- contacted the server for 30 days or more. Select all possible options, and then click **Next**.
3. The wizard will begin the cleanup process, and will present a summary of its work when it is finished. Click **Finish** to complete the process.

In some cases, particularly if you run the Server Cleanup Wizard on a WSUS 3.0, WSUS 3.0 with SP1, or WSUS 3.0 with SP2 server that has WSUS 2.0 downstream servers, you may see discrepancies in update metadata on upstream and downstream servers. If this is the case, you may solve your problem by running **iisreset** on the upstream server to refresh the Web cache.

Running WSUS 3.0 SP2 in Replica Mode

A WSUS server running in replica mode inherits the update approvals and computer groups created on its parent WSUS administration server. You will typically have a single parent server with one or more downstream replica WSUS servers. You approve updates and create computer groups on the parent server, which the replica servers will then mirror.

► To designate any WSUS server as a downstream replica

1. In the WSUS administration console, select **Options**, then select **Update Source and Proxy Server**.
2. On the **Update Source** tab, select the **Synchronize from another Windows Server Update Services server** and **This server is a replica of the upstream server** check boxes.

You will be able to perform only limited administration capabilities on a WSUS replica server, which will primarily consist of:

- Adding and removing computers from computer groups
A replica server inherits the computer groups that were created on the administration server. You must assign the replica server's client computers to the computer groups.
- Viewing available updates
- Monitoring update, synchronization, and computer status, and monitoring WSUS settings on the server

All standard WSUS reports are available on replica mode servers.

For more information about setting up and running in replica mode, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Replica server synchronization

If you are setting up many replica servers to connect to a single upstream WSUS server, you should not schedule synchronization to run at the same time on each replica server. This practice will avoid sudden surges in bandwidth utilization.

If a replica server tries and fails to synchronize with the upstream server, it will retry the synchronization twice at approximately fifteen-minute intervals. If both retries fail, the replica server will run synchronization at the next scheduled time.

Backing Up Windows Server Update Services 3.0 SP2

As a best practice, back up WSUS data and update content in order not to lose information about the state of your WSUS network. Update content can always be synchronized from Microsoft Update, but all WSUS information (administrative settings, computer groups and group membership, and the installation status of updates) is kept in the WSUS database. Moreover, re-synchronization can take a considerable amount of time.

Backing up WSUS involves backing up the following:

- The WSUS database, which contains:
 - Update metadata.
 - WSUS server configuration information.
 - Information about client computers, updates, and client interaction with updates.
- The folder where the update files are stored, if you are storing updates locally and not on Microsoft Update. By default, update files are stored in the \WSUS\WSUSContent folder on the largest partition of your WSUS server.
- The folder containing the WSUS repair path (by default, \WSUS\UpdateServicesPackage on the largest partition of your WSUS server). The repair path is the location of any .msi files used to repair locally published packages.

Although WSUS does not provide a built-in backup tool, you can use the Backup Utility that is available on all servers running Windows Server to back up and restore both the WSUS database and update file storage folder. The Backup Utility is also known as **Ntbackup.exe**. If you are using a full version of Microsoft SQL Server for your database, you should use SQL Server Enterprise Manager as an alternative to the Backup Utility. For more information about SQL Server Enterprise Manager, refer to your SQL Server documentation. For more information about database options and configurations for WSUS, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

▶ To back up content and data

1. On your WSUS server, click **Start**, and then click **Run**.
2. In the **Open** box, type `%windir%\system32\ntbackup.exe`, and then click **OK**.
3. In the **Backup or Restore** Wizard, click **Next**.
4. Verify that **Back up files and settings** is selected, and then click **Next**.
5. Click **Let me choose what to back up**, and then click **Next**.

6. Under Items to back up, select the WSUS folder (typically `%systemdrive%\WSUS\`), and then click **Next**.
7. Click the **Browse** button to choose a place to save your backup, type a name for the backup, and then click **Next**.
8. If you want to set additional specifications for your backup, including whether it will be an incremental backup, whether you want to verify the backup, set a recurring schedule for the backup, or other options, click **Advanced**, and then follow the instructions in the wizard.
9. When the wizard is finished, click **Finish**.
10. When the message appears that informs you that the backup is complete, click **Close**.

To restore content and data

1. On your WSUS server, click **Start**, and then click **Run**.
2. In the **Open** box, type `%windir%\system32\ntbackup.exe`, and then click **OK**.
3. In the **Backup or Restore Wizard**, click **Next**.
4. Click **Restore files and settings**, and then click **Next**.
5. In the **What to restore** dialog box, under Items to restore, expand the file that contains the WSUS folder (typically `%systemdrive%\WSUS\`), and then click **Next**.
6. If you want to set additional specifications for your restore, including whether you want to restore the files or folders to a different location, replace existing files, restore security settings, or specify other options, click **Advanced**, and then follow the instructions in the wizard.
7. When the wizard is finished, click **Finish**.
8. When the message appears that informs you that restoring is complete, click **Close**.

Important

You should restore the backup file to only one WSUS server. The backed-up information includes the Server ID, so if you restore the same backup file to two or more WSUS servers there will be two or more WSUS servers with the same ID. If you attempt to roll up information from downstream servers with duplicate IDs to an upstream server, you will get information from only one of these downstream servers.

After restoring the WSUS database you must recycle the WSUS Application Pool in IIS, as described in the next procedure. This will ensure that the restored database will sync up correctly with IIS, through which you manage the WSUS Web site and Web services. For more information about application pools, see IIS Help.

To recycle the WSUS Application Pool in IIS

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services**

(IIS) Manager.

2. In the tree view, expand the tree under the WSUS server name, and then expand Application Pools.
3. Right-click **WSUSPool**, and then click **Recycle**.
4. Close **IIS Manager**.

If you store updates locally on the WSUS server, after restoring the WSUS database *reset* it with the **wsusutil.exe** command-line utility, which ensures that every row of update metadata in the database is matched by the corresponding update files in the local storage location. If the utility does not find matching data, it will download the update files from Microsoft Update. For more information about the WSUS command-line utility, see [Managing WSUS 3.0 SP2 from the Command Line](#).

► To reset update content

1. Open a Command Prompt window.
2. Navigate to the WSUS tools directory at **WSUSInstallDir\Tools**.
3. Type the following command: **wsusutil reset**
4. Wait until the command completes and then close the Command Prompt window.

Best Practices with Windows Server Update Services 3.0 SP2

This section provides a list of best practices for managing updates with WSUS. There are four main sections: one on security practices, one on resource usage, one on setting up a WSUS network, and the last on miscellaneous best practices.

Best practices for security

The following practices can help you secure your WSUS network.

1. Use the Secure Sockets Layer (SSL) for WSUS connections (server to server, server to client) on all computers that download updates via the Internet. For information about configuring SSL, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).
2. If you do not want to use SSL, you can deploy Internet Protocol security (IPsec) on your network to secure network traffic. The [Overview of IPsec Deployment](http://go.microsoft.com/fwlink/?LinkId=45154) (<http://go.microsoft.com/fwlink/?LinkId=45154>) topic offers guidance about how to deploy IPsec in your environment.

3. Make sure that the WSUS server that downloads updates from Microsoft Update is secured behind a firewall, and allows access only to the domains needed by WSUS. For a description of these domains, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).
4. Make sure that WSUS servers have only the file and folder permissions that are needed by WSUS. For a description of the necessary file and folder permissions, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).
5. If a WSUS server is Internet-facing, its database should be located on a different computer that is not reachable from the Internet. For remote SQL Server installation information, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).
6. There are two security groups that are set up for WSUS: WSUS Administrators and WSUS Reporters. WSUS Administrators can perform any WSUS task, while WSUS Reporters have read-only access (view server settings, get reports, and so on). Make sure that the only people in the WSUS Administrators group are the ones who need to perform administrative tasks.

Best practices for resource usage

Disk space

The following practices can help you conserve resources on your WSUS server.

1. Make sure that your WSUS server is configured to download only approved updates. When the server synchronizes updates, it downloads only the update metadata and will download the update files only after the update has been approved.
2. Use the Cleanup Wizard on a regular basis. This will keep the number of unneeded updates and revisions to a minimum.
3. If a WSUS server has a small number of clients, or if most of the clients are "roaming" clients with Internet access, you may wish to host update content on Microsoft Update rather than on the local WSUS server. Clients will get update approvals from the server, but can pull the upload files directly from the Internet.
4. If you are storing update content locally on your WSUS server, make sure you have enough disk space on the storage partition. Monitor disk usage on this partition carefully. One way to do this is to configure the WSUS health monitoring thread to warn you with an event if disk usage exceeds a specified percentage. For more information about configuring the health monitoring thread, see the explanation of the **healthmonitoring** parameter of the **wsusutil** utility in [Managing WSUS 3.0 SP2 from the Command Line](#).
5. Approve only the updates that are really needed on your network. Limit the product updates to the products that are installed on the network. You can also set up separate WSUS servers for computers with different sets of Microsoft products.
6. Synchronize only the update languages needed on your network. If you need to synchronize more than one language and you are storing updates locally, you should estimate your needed disk space by multiplying the recommended space times the number of update

languages. For more information about recommended disk space, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

7. Make sure that your WSUS server is configured to synchronize all the needed languages, because you will not be notified of needed updates in the unsynchronized languages. These updates will appear as “Not Needed” on clients who require the language. To help avoid that problem, make sure to include all operating system languages in your WSUS server's synchronization options. You can see all the operating system languages by going to the Computers view of the WSUS administration console and sorting the computers by operating system language. However, you may need to include more languages if there are Microsoft applications in more than one language (for example, if Microsoft Word in French is installed on some computers with Windows XP in English).
8. You should allow WSUS to decline expired updates automatically (click **Options**, click **Automatic Approvals**, click the **Advanced** tab, and then click **Automatically decline updates when a new revision causes them to expire**). If you do not wish to decline expired updates automatically, you should decline them manually on a periodic basis.
9. You should not choose to synchronize express installation files unless you have a pressing need to minimize downloads between the WSUS server and its clients. Typically, using express installation files reduces downloads from WSUS servers to clients by a factor of two but increases downloads from Microsoft Update (or an upstream server) to the WSUS server by a factor of four. You should decide which criteria are more important to your network: local network bandwidth or server disk space and Internet bandwidth.

Network bandwidth

The following practices will help you improve the way WSUS uses network bandwidth.

1. When deploying large updates (such as service packs), you can avoid saturating the network by doing the following:
 - a. Use BITS throttling. BITS bandwidth limitations can be controlled by time of day, but apply to all applications using BITS. For more information about BITS throttling, see [Appendix E: Configuring BITS 2.0 and 3.0 for Download Performance](#).
 - b. Use IIS throttling, which limits throttling to one or more Web services. For more information about IIS throttling, see [Appendix F: Configuring IIS for Download Performance](#).
 - c. Use targeting to control the rollout. You can set up multiple computer groups, then approve large service pack downloads for a subset of these groups at one time.
2. Use peer caching (available only on Windows Vista and Windows Server 2008 operating systems) to minimize downloads from WSUS servers to clients and maximize the "sharing" of downloads among peer computers on a subnet of the network. This will reduce network load and in particular load on the WSUS server. For more information about peer caching, see [Appendix E: Configuring BITS 2.0 and 3.0 for Download Performance](#).
3. Consider configuring WSUS clients to synchronize more frequently from the WSUS server and configuring downstream WSUS servers to synchronize more frequently from their

upstream servers. This will allow updates to be deployed to clients faster, which could be important if you need to deploy an “emergency update” that must be installed as quickly as possible. This will result in smaller downloads from server to client, but will add additional load to the WSUS server. It will also add additional load to the network when updates are deployed, because clients start downloading updates as soon as they synchronize with the server.

Best practices for setting up WSUS networks

The following practices will help you configure WSUS networks.

1. If possible, set up WSUS networks with a hub-and-spoke topology rather than a hierarchical one. The greater the number of tiers in the network, the greater the latency in downloading updates.
2. Consider using DNS netmask ordering for roaming clients. For more information about setting up this configuration, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).
3. Configure roaming clients, so they get their updates from the Internet-facing WSUS server, if they do not usually connect to your local intranet.

Best practices for maintaining WSUS databases

The following practices will help you get the best performance from your WSUS network.

1. Have a maintenance plan for your WSUS database that includes regular backups and periodic re-indexing.
2. Make sure to re-index the WSUS database at least once a month. See [Appendix I: Database Maintenance](#) for more information.

Other best practices

Manage restarts

The following practices will help you manage computer restarts.

1. Client computers (and most servers) often need restarts after an update is installed. Deferring the restarts will put machines in an unsupported and unstable state, which may include mismatched client and server binaries. These computers should be set up to get automatic downloads and scheduled installs. You can pick a time for scheduled installations when there is little chance for lost productivity (for example, on Sunday at 3:00 A.M). For information about setting up client computers for a scheduled installation, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).
2. Critical servers cannot generally be restarted daily. If this is the case, you can either configure them for installations at longer intervals (weekly), or configure them to get

automatic downloads but manual installations at a time when the servers can be restarted if necessary.

3. Configure e-mail notification to tell you when updates become available, so you can plan the deployment of these updates in advance.
4. If you need to deploy an “emergency update” and can’t wait for the next scheduled installation, approve the update with a deadline in the past. This will cause the update to be installed the next time the clients synchronize from the server. If you can’t wait for the next synchronization, create a script to automate installing the updates and then restarting your server. For more information about creating scripts to automate Automatic Updates tasks, see the [Windows Update Agent Software Developer's Kit](http://go.microsoft.com/fwlink/?LinkID=43101) (<http://go.microsoft.com/fwlink/?LinkID=43101>).
5. Configure client computers or WSUS servers to immediately install updates that do not require a restart. For information about setting up client computers for a scheduled installation, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Ensure WSUS availability

The following practices will help you ensure that WSUS servers are always available to their clients.

1. There are typically two different backup strategies. The first is a standard backup and restore strategy. For information about backing up and restoring WSUS, see [Backing Up Windows Server Update Services 3.0 SP2](#). This strategy requires more work to maintain and requires extra storage for the backup files, but makes it possible to restore the system to a known state without needing to download the update files once more. The other strategy is to rebuild the server. This is a fairly fast operation and is preferred by many customers, because it requires less work and less disk space.
2. Consider using network load balancing if you have a requirement for high availability. Load balancing involves a more complex configuration and is not typically considered necessary, because new updates are not released very frequently. For more information about setting up network load balancing, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Test service packs carefully

You should thoroughly test large bundles of updates such as service packs to ensure that they do not break line-of-business applications. A typical test strategy is to set up test computer groups in which the test computers are configured with the same applications as the production groups, approve installation only to these groups, and then verify that the applications continue to function correctly.

Check overall system health

The following practices will help you monitor the general health of your WSUS network.

1. You should check the WSUS administration console home page at least once a day to view overall update compliance and network health.
2. Check application logs frequently, if you suspect problems such as download failures or clients that are failing to report to the WSUS server.
3. Install the WSUS MOM Pack to monitor overall service health.

Managing WSUS 3.0 SP2 from the Command Line

The **wsusutil** command-line utility is used in managing WSUS servers and is located in the *WSUSInstallDir\Tools* folder of WSUS servers. The table below summarizes the different parameters that can be used with this utility, and later sections explain the syntax and usage of each parameter.



Note

You can also use Windows® PowerShell® to access the WSUS 3.0 APIs from the command line.

Using the wsusutil utility

You must be an administrator to run the **wsusutil** utility. This utility is installed only on WSUS server machines, not on console-only installations.



Tip

To see all **wsusutil** parameters, type **wsusutil help** on the command line. To see usage for each of the parameters, type **wsusutil help parameterName**.

Summary of wsusutil Commands

Command	Description
configuressl	Updates the WSUS server registry key after the IIS configuration has changed.
healthmonitoring	Configures health monitoring values in the database. If new values are not specified, the current values are displayed.
export	Part of the export/import process used to synchronize a downstream WSUS without using a network connection. Exports update metadata to an export package file. You cannot use this parameter to export update files, update approvals, or server

Command	Description
	settings.
import	The second part of the export/import process. Imports update metadata to a server from an export package file created on another WSUS server. This synchronizes the destination WSUS server without using a network connection.
movecontent	Changes the file system location where the WSUS server stores update files, and optionally copies any update files from the old location to the new location
listfrontendservers	Lists the front-end servers related to this WSUS server.
deletefrontendserver	Deletes the specified front-end server from the WSUS database.
checkhealth	Checks the health of the WSUS serve. Results will appear in the Application Event log.
reset	Checks that every update metadata row in the database has corresponding update files stored in the file system. If update files are missing or have been corrupted, downloads the update files again.
listinactiveapprovals	Returns a list of update titles with approvals that are in a permanently inactive state because of a change in server language settings.
removeinactiveapprovals	Removes approvals for updates that are in a permanently inactive state because of a change in WSUS server language settings.
usecustomwebsite	Changes the port number used by the WSUS Web services from 80 to 8530 or vice versa.

configuressl

Updates the WSUS server registry key after the IIS configuration has changed. If this command is run with the optional parameter *ServerCertificateName*, it updates the certificate name. If it is run without the optional parameter, it updates the setting for host headers, if there are any. For more

information about configuring SSL for WSUS, see the **Securing WSUS with the Secure Sockets Layer Protocol** section in the Windows Server Update Services 3.0 SP2 Deployment Guide.

Syntax

The following command updates the host headers, if any:

wsusutil configuressl

The following command updates the server certificateName:

wsusutil configuressl *ServerCertificateName*//sets the server certificate name

Parameter	Description
<i>ServerCertificateName</i>	An optional parameter. When present, it provides the name in the Issued to field of the server certificate.

Output

The output from the **wsusutil configuressl** command is the address of the WSUS Web site (including the port number), for example **https://serverName:443**.

healthmonitoring

This command sets and gets the different parameters for WSUS health monitoring.

Syntax

Wsusutil healthmonitoring *parameterName*



Note

You may set or get only one parameter at a time.

Parameter	Description
IntervalsInMinutes [<i>DetectInterval</i>] [<i>RefreshInterval</i>]	Sets the values for detect and refresh intervals. If the detect interval is 0, the detect cycle will not run. If the refresh interval is 0, the refresh cycle will not run. For more information about the detect and refresh cycles, see Health Monitoring in WSUS 3.0 SP2 .
DiskSpaceInMegabytes [<i>ErrorLevel</i>] [<i>WarningLevel</i>]	Sets the amount of available disk

Parameter	Description
	space (in megabytes) at which a low disk space warning or error event should be logged.
CatalogSyncIntervallInDays <i>[Days]</i>	Sets the number of days that should have passed after synchronization before a warning event should be logged..
InstallUpdatesInPercent <i>[WarningPercent][ErrorPercent]</i>	Sets the percentage of update installation failures at which a warning or error event should be given.
InventoryInPerce <i>n[WarningPercent][ErrorPercent]</i>	Sets the percentage of inventory reporting failures at which a warning or error should be given.
SilentClientsInPercent <i>[WarningPercent][ErrorPercent]</i>	Sets the percentage of clients not reporting to the server at which a warning or error should be given.
SilentClientsInDays <i>[Days]</i>	Sets the number of days clients can fail to report before an error should be given.
TargetComputersInPercent <i>[WarningPercent][ErrorPercent]</i>	Sets the maximum percentage of target computers reporting to this server below which a warning or error event should be given. For example, if you set values of 80 and 60, a warning event will be logged if only 80 percent of computers have reported, and an error event will be logged if only 60 percent of computers have reported.
CheckAcls <i>on off</i>	If on, health monitoring should check ACLs on the relevant directories.
CheckForLowDiskSpace <i>on off</i>	If on, health monitoring should check for low disk space.

Parameter	Description
CheckForCatalogSyncFailures <i>on off</i>	If on, health monitoring should check for catalog synchronization failures.
CheckForContentSyncFailures <i>on off</i>	If on, health monitoring should check for content synchronization failures.
CheckForEmailNotificationFailures <i>on off</i>	If on, health monitoring should check for e-mail notification failures.
CheckSelfUpdate <i>on off</i>	If on, health monitoring should check for client self-update failures.
CheckClientsExist <i>on off</i>	If on, health monitoring should check whether this server has any clients.
CheckForUpdateInstallFailures <i>on off</i>	If on, health monitoring should check for update installation failures.
CheckForInventoryFailures <i>on off</i>	If on, health monitoring should check for clients failing to report inventory..
CheckForSilentClients <i>on off</i>	If on, health monitoring should check for clients that have failed to report to the server.
CheckForTooManyClients <i>on off</i>	If on, health monitoring should check whether the number of clients is approaching the maximum number allowed.
CheckReportingWebService <i>on off</i>	If on, health monitoring should check the Reporting Web service.
CheckApiRemotingWebService <i>on off</i>	If on, health monitoring should check the API Remoting Web service.
CheckServerSyncWebService <i>on off</i>	If on, health monitoring should check the Server Synchronization Web service.

Parameter	Description
CheckClientWebService <i>on off</i>	If on, health monitoring should check the client Web service.
CheckSimpleAuthWebService <i>on off</i>	If on, health monitoring should check the Simple Authentication Web service.
CheckDssAuthWebService <i>on off</i>	If on, health monitoring should check the Downstream Server Authentication Web service.

Output

The output from **wsusutil** *paramName* is usually the current state of the given parameter. Some examples are given below:

wsusutil healthmonitoring *IntervalsInMinutes*

Output:

Detect interval: 10 min, Refresh interval: 360 min

wsusutil healthmonitoring *DiskSpaceInMegabytes*

Output:

Error level: 200 MB, Warning level: 500 MB

However, with the parameters setting on or off the different health monitoring checks (for example, **wsusutil healthmonitoring** *CheckAcIs*), the output will simply be a warning that the WSUS Service must be stopped and restarted for the change to take effect.

export

For more information about exporting and importing updates, see the **Set Up a Disconnected Network (Import and Export the Updates)** section in the Windows Server Update Services 3.0 SP2 Deployment Guide.

Syntax

wsusutil export *package logfile*

Parameter	Description
<i>package</i>	The path and file name of the package .cab to create.
<i>logfile</i>	The path and file name of the log file to create.

 **Note**

Exporting from a WSUS 2.0 server to a WSUS 3.0, WSUS 3.0 SP1, or WSUS 3.0 SP2 server (or from a WSUS 3.0, WSUS 3.0 SP1, or WSUS 3.0 SP2 server to a WSUS 2.0 server) is not supported.

Import

For background and procedural information about exporting and importing updates, see the WSUS Deployment Guide at [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Syntax

wsusutil import *package logfile*

Parameter	Description
<i>package</i>	The path and file name of the package .cab to import.
<i>logfile</i>	The path and file name of the log file to import.

 **Note**

Importing from a WSUS 2.0 server to a WSUS 3.0, WSUS 3.0 SP1, or WSUS 3.0 SP2 server (or from a WSUS 3.0, WSUS 3.0 SP1, or WSUS 3.0 SP2 server to a WSUS 2.0 server) is not supported.

Movecontent

When you run this command, **wsusutil** does the following:

- Copies the update files from the old location to the new location. The old location is not deleted.
- Updates the WSUS database to refer to the new location of the update files.
- Ensures that the content and metadata are synchronized. This check is always run, even if the **-skipcopy** parameter is used.

The destination folder to which update files are moved must be on an NTFS partition. The utility will not try to copy update files if they already exist in the destination folder. The destination folder will have the same permissions that were set on the original folder.

 **Note**

You can use **xcopy**, the Backup utility, or other methods to copy update files from the old location to the new one. If you copy the files by using a method other than **wsusutil**, you still need to run **wsusutil** to perform the second part of the move, using the **-skipcopy** parameter. See the "Syntax" section for more information.

There are two scenarios in which you might move update files from one WSUS drive to another:

- If the drive is full
- If the hard disk fails

If the drive is full

If the drive where WSUS stores update files is full, you can do one of the following:

- Add more space to your current drive by using NTFS functionality. This operation can be done without using **wsusutil**, because it does not affect WSUS configuration or operation.
- Install a new drive, and then move the update files from the old drive to the new location by using **wsusutil**.

If the hard disk fails

If the hard disk fails, you must do the following:

1. Install the new disk on your computer, and then restore the update files from your backup files. Note: If you have not backed up your update files, WSUSutil.exe downloads the missing files at the end of the content move operation.
2. Run **wsusutil movecontent newLocation**, specifying the location for the new disk. In addition, you specify the **-skipcopy** parameter, because you are either putting the files in the new folder through the backup utility or the source folder does not exist; the update files will be downloaded at the end of this process.
3. When the move operation is complete, all the missing files are downloaded.

Syntax

wsusutil movecontent contentpath logfile -skipcopy

Parameter	Description
<i>contentpath</i>	The new root for content files. The path must exist.
<i>logfile</i>	The path and file name of the log file to create.
<i>-skipcopy</i>	Indicates that only the server configuration should be changed, and that the content files should not be copied.

listfrontendservers

This command lists the different front-end servers in a network load balancing configuration. It can be useful in troubleshooting a NLB (network load balancing) configuration and after setting up a new front-end server to make sure that it is configured properly.

deletefrontendserver

This command deletes the given front-end server.

Syntax

wsusutil deletefrontendserver *serverName*

Parameter	Description
<i>serverName</i>	The name of the front-end server to be deleted.



Important

This command removes the front-end server from the database only. You will need to run **wsussetup /u** on the front-end server to uninstall WSUS.

checkhealth

This command checks the health of the WSUS server. The health check is configured by **wsusutil healthmonitoring**). The results are written to the event logs.

Syntax

wsusutil checkhealth

reset

You use this command if you store updates locally on your WSUS server and want to ensure that the metadata information stored in your WSUS database is accurate. With this command, you verify that every update metadata row in the WSUS database corresponds to update files stored in the local update file storage location on your WSUS server. If update files are missing or have been corrupted, WSUS downloads the update files again. This command might be useful to run after you restore your database, or as a first step when troubleshooting update approvals.

Syntax

wsusutil reset

listinactiveapprovals

If you change language options on an upstream WSUS server, the number of approved updates on the upstream server may not match the number of approved updates on a replica server. For example, consider the following scenario. You configure your upstream server to synchronize all languages, then synchronize and approve 300 updates, of which 50 are non-English language updates. Afterward, you change the language setting on the server to English only. Later, a replica server synchronizes from the upstream server and downloads the "active" approvals,

which now are only the English language ones (replica servers synchronize only active approvals). At this point, you will see 300 updates approved on the upstream server, but only 250 approved on the replica server. You can use **listinactiveapprovals** to see a list of the updates on the parent upstream server that are permanently inactive—in this case, the 50 updates that are not English. You do not have to run this command before running the **removeinactiveapprovals** command.

Syntax

wsusutil listinactiveapprovals

removeinactiveapprovals

See the explanation above for a description of situations in which you might need to use **removeinactiveapprovals**. You do not have to run the **listinactiveapprovals** command before running this command.

Syntax

wsusutil removeinactiveapprovals

usecustomwebsite

If you set this value to **true**, WSUS Setup will use port 8530 for its Default Web site. If you set it to **false**, WSUS will use port 80.



Important

You must use this command before you configure SSL.



Important

If you are installing SharePoint on the same machine as WSUS, the value of **usecustomwebsite** should be set to **true** before the install.



Important

Using this command after running WSUS Setup will fail if the index of the default Web site is set to a value other than 1.

Syntax

wsusutil usecustomwebsite true

Reports in Windows Server Update Services 3.0 SP2

Reports are an important part of managing WSUS. You can keep track of nearly every aspect of the WSUS network by means of reports. The following types of reports are provided:

- Summary compliance reports (the number of computers that need to install updates and the number of updates missing from computers). You can generate these reports from the root node of the WSUS administration console.
- Individual computer reports. You can generate these reports by right-clicking the computer in the **Details** pane.
- Individual update reports. You can generate these reports by right-clicking the update in the **Details** pane.
- Downstream server summary compliance reports. You can generate these reports by right-clicking the server in the **Details** pane.
- Synchronization reports. You can generate these reports by right-clicking the synchronization in the **Details** pane.

In this section

[Terminology for Update Status](#)

[Creating Reports](#)

Terminology for Update Status

You can access update status from various locations in the WSUS console. The following table defines each possible status that can be reported by WSUS for an update. Typically, WSUS presents update status for a particular computer (for example, the status of an update on one computer) or computer group (for example, status for the five computers in Computer Group X on which the update has been installed). You can filter the default views of computers or updates by update status, and in some cases by combinations of statuses (Failed or Needed, Installed/Not Applicable or No Status, and so on).

Update Status Definitions

Status	Description
Installed	The update is installed on the computer.
Needed	When referring to the status of one computer, Needed means the update is compatible with (and should be installed on) the computer.

Status	Description
	<p>When referring to status for a computer group, the Needed column displays the number of computers in the group to which the update is applicable. A positive Needed result means that the update was determined to be applicable, but has not been installed the last time client computers contacted the WSUS server,. Any of the following could be true when the status for an update is Needed:</p> <ul style="list-style-type: none"> • You have approved the update for installation, but the client computers have not yet contacted the WSUS server since you made this change. • The update has already been downloaded and installed, but the client computer has not contacted the WSUS server since the update was installed. • The update has already been downloaded and installed, but the client computer must be restarted before changes go into effect, and the client computer has not yet been restarted. • The update has been downloaded to the computer but not installed. • The update has been neither downloaded nor installed on the computer.
Installed/Not Applicable	<p>When referring to the status of one computer, Installed/Not Applicable means the update is not applicable to or required by that computer. When referring to the status for a computer group, the Installed/Not Applicable column displays the number of computers in the group for which the update is not applicable or not required.</p>
No status	<p>This usually means that since the time that the update was synchronized to the WSUS server, the computer has not contacted the WSUS server.</p>
Failed	<p>An error occurred when either a detection or an</p>

Status	Description
	installation was attempted on the computer for the update.
Last contacted	This is the date on which the computer last contacted the WSUS server.

Creating Reports

Reports enable you to monitor different aspects of the WSUS network: updates, client computers, and downstream servers. If a WSUS server has replica servers, you can choose to roll up the replica servers' client status to the upstream server. For information about creating a replica server and status rollup, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

You can generate different kinds of update reports from different places in the WSUS administration console.

1. General reports on the Reports page.
2. Reports on specific updates: right-click the update (or go to the **Actions** pane) and choose **Status Report**.
3. Reports on specific computers: right-click the computer (or go to the **Actions** pane) and choose **Status Report**.



Note

Generating detailed reports for large numbers of computers and/or updates can be very memory-intensive. Detailed reports are most effective for smaller subsets of your computers or updates. If you need to create a very large report and are concerned about using CPU and memory resources on the WSUS server, you may generate the report from a remote WSUS Administration console.

Using the Reports Page

You can generate three kinds of reports as described in the following table.

Report name	Function
Update Reports	View update status.
Computer Reports	View computer status.
Synchronization Reports	View the results of the last synchronization.

Update Reports

Update reports show you the status of your updates. You can run update reports in four ways: summary, detailed, tabular, and tabular for approved updates. You can also filter an update report by update classification, product, target computer group, and update installation status.

The report displays information from the most recent contact between client computers and the WSUS server. The frequency with which client computers contact the WSUS server is configured through Group Policy. By default, this is every 22 hours. Unless you want to change the contact frequency for your client computers, generate this report the day after you approve updates, so that it reflects your latest approvals.



Note

You can run **wuauclt /detectnow** from the command prompt on computers that are running WSUS client software (Automatic Updates) in order to start contact between the client computer and WSUS server. This is used primarily to update status for a particular computer. There will be a few minutes delay between running the command and seeing the results on the WSUS server. After forcing the client to contact the server, you can get its status with an update status report. For more information about wuauclt, see [Appendix H: The wuauclt Utility](#).

► To run an update report

1. In the WSUS Administration console, select the **Reports** node
2. In the **Reports** pane, click one of the options in the **Update Reports** section: **Update Status Summary**, **Update Detailed Status**, **Update Tabular Status**, or **Update Tabular Status for Approved Updates**.
3. In the **Updates Report** window you can select the updates you want to see by classification, product, computer group, and update installation status.
4. Click **Run Report**. See the [Terminology for Update Status](#) section for information about the Status values shown on the report.
5. You can change the view of an Update report to a detail, summary, or tabular view by clicking **Report View** in the **Updates Report** toolbar.

Update Status Summary View

The Update Status Summary view contains the elements listed in the following table.

Description of elements displayed in the Update Status Summary view

Column name	Description
Updates Report tree view	The tree listing all the updates in the report.
Title	The title of the update.
Description	The description of the update.

Column name	Description
Classification	The classification of the update.
Products	The products to which the update applies.
MSRC Severity Rating	Microsoft Security Response Center rating.
MSRC Number	Microsoft Security Response Center identification number.
More information	Redirection to the relevant Web site.
Approval Summary for Computer Group	The listing of groups and approvals.
Group	The computer group.
Approval	Approval status (Approved, Not approved, Declined).
Deadline	The date by which the update must be installed.
Administrator	The administrative action.

Computer Reports

Computer reports show you the status of computers. You can run computer reports in four ways: summary, detailed, tabular, and tabular for approved updates. You can also filter a computer report by update classification, product, target computer group, and update installation status.

► To run a status report for computers

1. In the WSUS administrative console, select the **Reports** node.
2. In the **Reports** pane, click one of the options in the **Computer Reports** section: **Computer Status Summary**, **Computer Detailed Status**, **Computer Tabular Status**, or **Computer Tabular Status for Approved Updates**.
3. In the **Computers Report** window, you can select the updates you want to see by classification, product, computer group, and update installation status.

Note that for the **Computer Tabular Status for Approved Updates** report both the update approvals and the set of computers considered by the report are scoped based on the selected target group.

- The updates considered by the report are those for which the selected target group has a direct or inherited approval for install.
 - The computers considered by the report are those that are direct members of the selected target group, and optionally its child target groups.
4. Click **Run Report**.

5. You can change the view of a Computer report to a detail, summary, or tabular view by clicking **Report View** in the **Updates Report** toolbar.

Synchronization Results Report

The Synchronization Results report enables you to see synchronization information for the WSUS server for a given time period, including errors that occurred during synchronization and a list of new updates. In addition, you can get general, status, and revision information for each new update.

► To run a Synchronization Results report

1. In the WSUS administrative console, click **Reports**.
2. On the **Reports** pane, click **Synchronization Results**. By default, the report shows any synchronization done today.
3. To change the synchronization period for the report, in the **Synchronization Report** window, click **Between these dates** and specify the dates you want included in the report.
4. Click **Run Report**.

The report has four components, which are described in the following table.

Components of the Synchronization Results Report

Component name	Purpose
Report Options	Shows the start and end dates of the period shown in the report, as well as the date of the report and the server for which the report was made.
Synchronization Summary	Displays summary information of the numbers of new, revised, and expired updates in each synchronization.
New Updates	Displays the new updates that have been synchronized to the WSUS server during the report's time period. You can view the properties for each update by clicking the update. An update status report will be generated for that individual report.
Revised Updates	Displays the revised updates that have been synchronized to the WSUS server during the report's time period. You can view the properties for each update by

Component name	Purpose
	clicking the update. An update status report will be generated for that individual report.
Expired Updates	Displays the updates that have been expired during the report's time period.

Printing a Report

You can print the report in update summary, detailed, or tabular views, depending on how you have formatted the update status report.

To print a report

1. On the report toolbar, click the printer icon.
2. In the **Print** dialog, select your options and click **Print**.

Exporting a Report

You can print a report in its original format, or you can export it to Microsoft Excel or PDF formats.

Important

Exporting a large report can be extremely time-consuming and may exceed your computer's memory resources. If you are planning to export a report, consider limiting the size of the report to 200 pages or fewer. You can use different filters to reduce the size of the report, or you can choose the tabular format rather than the detailed format to reduce the number of pages to export.

To export a report to Excel or PDF format

1. Run the report you want to export.
2. On the report toolbar, click the down arrow associated with the **Save** icon.
3. You will see two options: **Excel** and **Acrobat (PDF) file**. Click one of the options.

Extending Reports

You can customize WSUS reports in different ways:

1. Use the WSUS APIs to create a custom report
2. Use WSUS public views to create and extend custom reports

Use WSUS APIs to Create Custom Reports

For more information on WSUS APIs, see the [Windows Server Update Services SDK](http://go.microsoft.com/fwlink/?LinkId=85713) documentation on MSDN (<http://go.microsoft.com/fwlink/?LinkId=85713>). You can use these APIs to create reports on updates, approvals, installation information, and the like.

Use WSUS Public Views to Create Custom Reports

For more information on public views, as well as sample queries, see the [WSUS SDK conceptual documentation](http://go.microsoft.com/fwlink/?LinkId=85715) on MSDN (<http://go.microsoft.com/fwlink/?LinkId=85715>.) If you are using SQL Server as the WSUS database, you can use the SQL Server Report Builder to generate custom reports using these views, or you can access the views from the command line. If you are using Windows Internal Database as the WSUS database, you can access it via the command line if you download the Microsoft SQL Server Command Line Query Utility and the SQL Native Client. You can download the install packages from the [Microsoft Download Center](http://go.microsoft.com/fwlink/?LinkId=70728) (<http://go.microsoft.com/fwlink/?LinkId=70728>).

Securing Windows Server Update Services 3.0 SP2

For synchronization with upstream WSUS servers, you can use Secure Sockets Layer (SSL) protocol to secure the update metadata portion of the synchronization. WSUS can use SSL to:

- Enable client computers and downstream WSUS servers to authenticate an upstream WSUS server.
- Encrypt metadata passed on to client computers and downstream WSUS servers.

For more information about configuring your WSUS server to use SSL, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Troubleshooting Windows Server Update Services 3.0 SP2

This guide provides troubleshooting information for Windows Server Update Services. For additional information about troubleshooting, see [How to troubleshoot Windows Update, Microsoft Update, and Windows Server Update Services installation issues](http://go.microsoft.com/fwlink/?LinkId=80711) (<http://go.microsoft.com/fwlink/?LinkId=80711>).

In this guide

- [Health Monitoring in WSUS 3.0 SP2](#)
- [WSUS 3.0 SP2 Server Administration Issues](#)
- [WSUS 3.0 SP2 Client Computer Administration Issues](#)

Health Monitoring in WSUS 3.0 SP2

WSUS monitors the health of the WSUS server and its components by means of a service that runs at frequent intervals and logs the results as events in the event log. You can look at the events with the Event Viewer, and you can get more information by downloading the WSUS 3.0 MOM Pack.

Health checks

The WSUS health monitoring service automatically checks the health of WSUS components as long as WSUS server components are installed on the computer. (The service does not run on computers where only the console or only the database is installed.) The health check service has two cycles: detect and refresh. In the detect cycle, only changes are logged (for example, a service was running but has stopped). In the refresh cycle, all errors and warnings are logged. By default the detect cycle polls WSUS components every ten minutes and the refresh cycle polls every six hours, but if you wish to run the health check at other times (for example, to verify a configuration change to WSUS or to configure the service to run more or less often), you can use the **wsusutil** utility. For instructions on running the utility, see [Managing WSUS 3.0 SP2 from the Command Line](#) under the "healthmonitoring" section.

Polling WSUS components

The following WSUS components are checked for potential problems:

- Core: issues with disk space, permissions, e-mail notifications, and catalog and content synchronization
- Database: issues with connectivity and availability
- Web Services: issues with permissions and Web service health
- Clients: issues with clients not reporting, client self-update, the update agent, client inventory, and clients' ability to install updates

Viewing event logs

The events generated by the health monitoring service are logged in the Application event log.

To view WSUS events

1. Start the Event Viewer (click **Start**, click **Run**, and then type **eventvwr**).
2. In the left pane, click **Application**.
3. Find the events whose source is Windows Server Update Services.

WSUS logs error, warning, and informational events. Errors are problems that should be fixed immediately (for example, that available local storage has dropped below a certain level), warnings are notifications of situations that are tending to become problems (for example, that

WSUSService has stopped, or that synchronization has not taken place in the last 24 hours), and informational events are notifications of situations that are probably not problems (for example, that a service has stopped or started).

Resolving problems

In many cases the solution to an error or warning event will be obvious. For example, if disk space is low, you would remove unneeded files. In other cases, you might need to do more investigation before deciding on the right solution. You could read the troubleshooting sections of this document, or search online for similar issues. If you are using the Microsoft Operations Manager, you can also download the WSUS 3.0 (MOM) Pack.

[WSUS 3.0 SP2 Server Administration Issues](#)

[WSUS 3.0 SP2 Client Computer Administration Issues](#)

WSUS 3.0 SP2 Server Administration Issues

In this section

- [Issues with Setup](#)
- [Issues with Upgrades](#)
- [Issues with the WSUS 3.0 SP2 Administration Console](#)
- [Issues with Update Storage](#)
- [Issues with Synchronization](#)
- [Issues with Update Approvals](#)
- [Issues with Backup and Restore](#)
- [Issues with E-Mail Notifications](#)
- [Issues with the Database](#)
- [Issues with WSUS 3.0 Services](#)

Issues with Setup

If you are having trouble installing WSUS, use the following information to troubleshoot the problem.

Troubleshooting WSUS setup

Check for required software and hardware

WSUS has a number of requirements that need to be met before installation. For more information, see [Deploying Microsoft Windows Server Update Services](http://go.microsoft.com/fwlink/?linkid=79983) (<http://go.microsoft.com/fwlink/?linkid=79983>).

Check setup logs

WSUS setup creates the following four log files that can help you diagnose problems with setup. These log files are located in the %temp% directory of the user who ran the installation process.

- **WSUSSetup.log:** The status of each of the component installations performed during WSUS setup is logged to this file. You can check this log to see whether any of the component installations failed. If you see a failure, you can check the corresponding log to see what went wrong during the installation of that component.
- **WSUSSetupMsi_timestamp.log:** This log file is generated by MSI for WSUS component setup. Windows installer, before invoking any of the custom actions and standard actions, logs that information to this file. The return values from the custom actions are logged to this file as well. This log file is useful if there are errors invoking any of the custom actions.
- **WSUSCa_timestamp.log:** This log file is used by custom actions. Errors that occurred while executing any of the custom actions in WSUS component or BITS setup are logged to this file.
- **WSUSWyukonSetup_timestamp.log:** This is the log file for Windows Internal Database setup. All Windows Internal Database installation/uninstallation information is logged to this file.

Check the .NET framework installation

If the .NET framework has not been installed correctly, WSUS setup may fail.

- One symptom of this is the failure to run HideConsoleApp.exe. Search WSUSSetupMsi_timestamp.log file for "HideConsoleApp.exe" and look at the return value of the corresponding custom action. If the return value is non-zero, the executable failed to run. Note that HideConsoleApp.exe may fail because of several other reasons. The WSUSCa_timestamp.log file will give the specific reason it failed.
- Reinstalling .NET framework may solve this problem.

The WSUSService service is marked for deletion

WSUS installs the WSUSService service during setup and deletes it during uninstallation. During uninstallation, if some other process is using the service, the service is not deleted completely but is marked for deletion. It is deleted only after all processes have stopped using the service. If the service is not deleted properly after uninstallation, then the next installation may fail, because WSUSService cannot be installed while it is marked for deletion.

- Look at the `WSUSSetupMsi_timestamp.log` file for the return value of `HideConsoleApp.exe`. If the return value is not zero, that means that the custom action running `HideConsoleApp.exe` failed.
- Look at the `WSUSCa_timestamp.log` file to see whether the failure is due to the service being marked for deletion.
- Reboot the machine and rerun setup. All the open handles to the service are closed when the machine shuts down, and this should resolve the problem.

On a domain controller, the NetBiosDomainName is different from the DNS domain name

Setup can fail because it uses the DNS domain name instead of the `NetBiosDomainName` when setting database permissions to the `IWAM` account.

- Check the `NetBiosDomainName` and the DNS domain name on the machine. These names must be identical for WSUS setup to succeed.

Duplicate ASP.Net entries in the IIS Web services list

The ASP.Net Web service extension may occasionally be listed twice in the IIS configuration. If this is the case, WSUS setup will fail when it tries to install and configure its v-roots.

- Check `WSUSSetup.log` for the following entry:

```
Error IISCustomAction Command /Install FailedSystem.ArgumentException: Item has already
been added. Key in dictionary: "enableasp.net" Key being added: "enableasp.net"
```

- Disable and then reenable the ASP.NET V2.0.50727 Web service extension through the IIS UI. Make sure that the final status of this Web service extension is “allowed.”

There is a SUSDB database from an earlier installation

Reinstallation of WSUS can fail if there is a `SUSDB` database from a previous WSUS installation. You will need to remove this database before restarting WSUS setup.

UseCustomWebsite fails when the default Web site does not have a site ID of 1

If the default Web site has been deleted and recreated, the default Web site will get assigned a Web site ID other than 1 by IIS. Consequently, WSUS Setup at the default Web site will fail.

There are two ways you can work around this issue:

- Reinstall IIS in order to ensure the default Web site is created with a Web site index.
- WSUS Setup will still work if installed to port 8530. Check if the value of `usecustomwebsite` value is set to **on**.

API compression may not be used after installing WSUS 3.0 SP2 on Windows Server 2008

If you want to use API compression on Windows 2008 ensure that dynamic compression IIS role service is installed. This feature is not installed in the default IIS installation on Windows Server 2008.

WSUS 3.0 SP2 setup fails to install to Windows Server 2008 when installing to a case-sensitive SQL and the computer name is in lowercase letters

SQL requires the computer name to be in uppercase letters. Rename the computer using all uppercase letters.

Issues with Upgrades

Use the information below to troubleshoot WSUS upgrade issues.

Troubleshooting WSUS Upgrades

If a WSUS Upgrade Fails, WSUS May Be Uninstalled

You may lose your previous WSUS settings and data if an upgrade fails. Therefore, before attempting an upgrade, back up the following:

- WSUS database
- Update file storage folder

For information about backing up and restoring your existing WSUS installation, see [Backing Up Windows Server Update Services 3.0 SP2](#).

Upgrading to WSUS 3.0 from WSUS 2 0

When upgrading to WSUS 3.0 from WSUS 2.0, the configuration points to the port 8530. This causes a mismatch in the WSUS environment because other machines are configured to point to the original port (80) of this WSUS server. In this case, the WSUS 3.0 port should be switched back to 80 by using the following syntax.

WSUSUtil.exe useCustomWebsite false

Certificate Not Configured after WSUS 2.0 SP2 is Upgraded to WSUS 3.0 with Custom Web site

If WSUS 2.0 SP2 was configured to use SSL, you will need to reinstall the certificate after the upgrade is complete by using the following syntax:

wsusutil configuressl *ServerCertificateName*

Issues with the WSUS 3.0 SP2 Administration Console

If you get an error when using or trying to access the WSUS console, use the following information to troubleshoot the problem.

Troubleshooting the WSUS administration console

Cannot access the WSUS administration console and a timeout error message appears

If you cannot access the WSUS console and a timeout error message appears, the CPU of the WSUS server may be at, or very close to, maximum utilization, causing the database to time out. If the database software times out, the WSUS console cannot be displayed.

One way of inadvertently overtaxing your WSUS server is to have antivirus software monitor the WSUS content directory. During synchronization, the antivirus software can overload the CPU. You can work around this situation by setting the antivirus software to ignore the directory where WSUS content is stored.

Get an error looking at a network load balanced cluster if the "master" is unavailable

If you are looking at a WSUS server on a network load balanced cluster from a remote administration console, and the server that is currently the "master" server becomes unavailable, you may see the following error:

```
System.Net.Sockets.SocketException Message:
```

```
No connection could be made because the target machine actively refused it
```

```
Source: System
```

```
Stack Trace:
```

```
    at System.Net.Sockets.Socket.DoConnect(EndPoint endPointSnapshot, SocketAddress socketAddress)
    at System.Net.Sockets.Socket.InternalConnect(EndPoint remoteEP)
    at System.Net.ServicePoint.ConnectSocketInternal(Boolean connectFailure, Socket s4, Socket s6, Socket& socket, IPAddress& address, ConnectSocketState state, IAsyncResult asyncResult, Int32 timeout, Exception& exception)
```

You should wait at least 30 seconds before clicking **Reset** on the error message.

Cannot see client computers in the WSUS administration console

If client computers do not appear on the **Computers** page in the WSUS administration console, there is probably a problem with client self-update, which is the mechanism that WSUS uses to update Automatic Update software. For more information about client self-update, see [Issues with Client Self-Update](#).

Cannot see computers having 100 percent installed state on the Computers page when the "Installed/NotApplicable or No Status" filter is applied

If there are locally published updates on the server, you may not see accurate status or counts for your computer because locally published updates interfere with the filtering mechanisms.

Cannot connect to remote WSUS 3.0 server in a saved MMC console

If you want to distribute an .msc file that connects to a server, you cannot create the .msc file on that server. Instead use a console on another machine to connect to this server and then save and distribute that .msc.

Get error accessing WSUS 3.0 servers from the WSUS administration console because the WWW Publishing service is configured to allow interaction with the desktop

If you attempt to access the WSUS administration console and fail to connect to the server, you may have gotten the following error:

```
The WSUS administration console was unable to connect to the WSUS Server via the remote API.
```

```
Verify that the Update Services service, IIS, and SQL are running on the server. If the problem persists, try restarting IIS, SQL, and the Update Services Service.
```

```
The WSUS administration console has encountered an unexpected error. This may be a transient error; try restarting the administration console. If this error persists, try removing the persisted preferences for the console by deleting the wsus file under %appdata%\Microsoft\MMC\.
```

```
System.IO.IOException -- The handshake failed due to an unexpected packet format.
```

...

This error is probably due to the WWW Publishing service being configured to allow interaction with the desktop. To solve this problem, take the following steps:

1. Open the Services snap-in (click **Start**, click **Run**, and then type **services.msc**).
2. Right-click the World Wide Web Publishing service and select **Properties**.
3. On the **LogOn** tab, clear the **Allow service to interact with desktop** check box.
4. Click **OK**, and then dismiss the Services snap-in.
5. From a command shell, type **iisreset**.

6. At this point you should be able to access the WSUS server from the console again.

This error is caused by the issue described in [KB919085](http://go.microsoft.com/fwlink/?LinkId=86366) (<http://go.microsoft.com/fwlink/?LinkId=86366>).

Get other errors accessing WSUS 3.0 servers from the WSUS administration console

In many cases, when you have gotten a connection error, it may be helpful to run the **iisreset** command.

Issues with Update Storage

Updates can be stored on the local WSUS server or on Microsoft Update. Use this section to troubleshoot problems with update storage.

Troubleshooting update storage

The updates listed in the WSUS administrative console do not match the updates listed in your local folder

This can happen under different circumstances. For example, if updates are stored on a disk separate from the one on which WSUS is installed, and that disk fails, when you replace the failed disk with a new (empty) disk, the WSUS application will still show all of the updates as downloaded.

To have WSUS resynchronize the updates in local storage with the updates in the database, you must run the WSUSUtil utility **reset** command. For more information about WSUSUtil, see [Managing WSUS 3.0 SP2 from the Command Line](#).



Note

Performing a reset causes the WSUS server to be unresponsive for up to five minutes.

▶ To have WSUS verify locally stored updates

1. Open a command window.
2. Navigate to the directory that contains WSUSutil.exe. (It can be found in the Tools subdirectory of the WSUS installation directory.)
3. Type **wsusutil reset**

Downloads from a WSUS server are failing

There may be problems with the permissions on the WSUS server's local content directory. Permissions are set correctly by WSUS setup when the directory is created, but subsequent

changes may have reset these permissions. One indication of this problem may be event ID 10012 in the Application log file.

The following permissions are necessary:

- The root folder of the local content directory must have at least Read permissions for the Users security group and the NT Authority\Network Service account. In other words, if the WSUS content directory is C:\Updates\WSUSContent, the Updates directory must have the correct permissions. The BITS service will fail if these permissions are not set.
- The content directory itself (in the above example, the WSUSContent directory) must have Full Control permissions for the NT Authority\Network Service account.
- The temporary ASP.NET directory (%windir%\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files) must have Full Control permissions for the NT Authority\Network Service account.
- The %TEMP% directory (usually %windir%\TEMP) must have Full Control permissions for the NT Authority\Network Service account.

The local content directory is running out of disk space

Synchronization may fail if the local WSUS content directory does not have sufficient disk space. It is recommended that you monitor disk space carefully to keep this problem from arising. Low disk space is indicated by event ID 10041 and event ID 10042.

The following procedures will help you overcome low disk space problems:

- Using Disk Cleanup to remove unneeded files on the drive.
- Using the Server Cleanup Wizard to remove unneeded content. For more information about this wizard, see [Using the Server Cleanup Wizard](#).
- Moving the content directory to another drive.
- Moving the SQL Server database to another drive.

▶ To use Disk Cleanup to remove unneeded files on the drive

1. Click **Start**, click **All Programs**, click **Accessories**, click **System Tools**, and then click **Disk Cleanup**.
2. Select the Windows components, applications, and files that can be removed, and then click **OK**.

▶ To move the content directory to another drive

1. Create a new content directory on another drive.
2. Locate the WSUSUtil.exe utility in the Tools directory of your WSUS installation (typically C:\Program Files\Update Services\Tools).
3. Open a command window, navigate to the Tools directory, and type the following:

```
wsusutil movecontent NewContentPath MoveLog
```

where *NewContentPath* is the new content directory, and *MoveLog* is the path and filename

of the log for this operation.

 **Note**

For more information about using the WSUSUtil utility, see [Managing WSUS 3.0 SP2 from the Command Line](#).

Before you move the SQL Server installation to another drive, you should make sure that the WSUS administration console is not open. If you have problems with the move, make sure that the WSUS Web services have been stopped. Occasionally, a move will fail if the clients are communicating with the server.

▶ **To move the SQL Server installation to another drive**

1. Open a command window.
2. Type **net stop wsusservice**
3. Detach the SUSDB database.
4. Copy SUSDB.mdf and SUSDB_log.ldf to the new location.
5. Attach the SUSDB database from the new location.
6. Type **net start wsusservice**
7. When the system is working properly, delete SUSDB.mdf and SUSDB_log.ldf from the old location.

 **Note**

Consult your SQL Server documentation to find out how to detach and reattach databases.

Issues with Synchronization

Synchronization is the process in which the WSUS server connects to Microsoft Update or another WSUS server and downloads updates. 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 approval. If synchronizations are failing, you can use the information below to troubleshoot the problem.

Troubleshooting synchronization

Check the error in the synchronization's Details pane

If a synchronization has failed, in the WSUS administration console, go to the **Synchronizations** node, and in the middle pane select the failed synchronization. In the **Synchronization Details** pane you will see **Details**, which links to the full error description.

Synchronization retries by downstream servers

If the upstream WSUS server is not available for synchronization from a downstream server at the scheduled time, the downstream server will try to synchronize twice more, at approximately 15 minute intervals. If neither of the retries succeeds, the downstream server will try again the next day at the scheduled synchronization time.

Check proxy server settings by using the WSUS console

If your WSUS server is connected to Microsoft Update via a proxy server, you must use the WSUS console to configure WSUS so that it can access the Internet. For basic instructions about setting up a proxy server, see [Deploying Microsoft Windows Server Update Services](http://go.microsoft.com/fwlink/?linkid=79983) (<http://go.microsoft.com/fwlink/?linkid=79983>). If your proxy server supports authentication, make sure you have the correct user name, password, and domain. Note that if you use the WSUS console option for **Allow basic authentication (password in cleartext)**, the password for the account is sent over the network in unencrypted text.

One major cause of synchronization failure is an expired password on the proxy server. Make sure the user name and password for the proxy server are always up to date.

Check the firewall settings

If your network has a firewall between the WSUS server and the Internet, make sure that all the necessary ports are open and the necessary domains are allowed. For more information, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Check the name of the upstream WSUS server

If your WSUS uses another WSUS server as its update source, make sure you are using the correct name for the upstream WSUS server and that you have spelled it correctly. For basic instruction about synchronizing two WSUS servers, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>). The name that you enter in the WSUS console on the downstream WSUS server must match the name of the upstream WSUS server.

To determine if there is a problem with network name resolution services, use the **ping** command from the downstream WSUS server that cannot synchronize. You should use the same naming convention that is used in the WSUS console. For example, if you used a NetBIOS name in WSUS console, use the NetBIOS name of the upstream server with the **ping** command. If you cannot ping the upstream server, you might have a problem with network name resolution services. To work around this type of issue, you could use a different name resolution service or the IP address of the upstream server.

► To contact an upstream WSUS server by using the ping command

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **cmd**, and then click **OK**.
3. Type the following, and then press ENTER:

ping *WSUSServerName*

where *WSUSServerName* is the name of the upstream WSUS server with which you are trying to synchronize.

Verify that users and the network service have Read permissions to the local update storage directory

If you store update files on your WSUS server, you need to ensure that the folder to which you download update files (by default C:\WSUS) has at least Read permissions for the network service and for users. This is true for both upstream and downstream WSUS servers.

On a downstream WSUS server, check that the updates are available on the upstream WSUS server

There are a number of situations where the updates on the upstream server no longer match the updates being requested at synchronization by the downstream server. Some of the following are examples of when this might occur:

- An upstream WSUS server is reinstalled and the set of classifications and products the administrator selects is smaller than the set previously selected for the earlier installation. The downstream servers might then attempt to synchronize updates that the newly rebuilt upstream server has not downloaded. Synchronization will fail for updates that do not exist on the upstream server.
- A downstream server is reconfigured to get updates from a different upstream server with different products and classifications selected.

To troubleshoot this issue, make a note of the updates for which download failed on the downstream server. These will be visible on the Updates page, and marked with a red "X." Check if these updates exist on the upstream server (look at the Updates page). If they do not match, do one of the following, depending on which updates you need:

- Specify the missing updates on the upstream server, and then synchronize from the update source.
- If the failed updates are not needed, cancel and then decline the updates that are not on the upstream server
- If the missing updates are actually available on the upstream server, then the error is transient, meaning the update might have been downloaded to the upstream server after it was requested by the downstream server. This issue will resolve itself the next time the downstream server synchronizes to the upstream server.

Restart the BITS service

If the BITS service was disabled during synchronization, synchronization will fail. To ensure that the BITS services is properly enabled, restart both the BITS service and the WSUS service.

► **To restart the BITS service and the WSUS service**

1. On the WSUS server, click **Start**, point to **Administrative Tools**, and then click **Services**.
2. Right-click **Background Intelligent Transfer Service**, click **Properties**, and make sure that **Startup Type** is **Manual**. After that click **Start**.
3. Right-click **Windows Update Service**, and then click **Restart**.
4. Retry synchronization: In the WSUS console, click **Options**, click **Synchronization Options**, and then under **Tasks**, click **Synchronize now**.

You should also ensure that both the BITS and the WSUS service are set to start automatically on reboot.

The number of updates that are approved on a parent upstream server does not match the number of approved updates on a replica server

This might occur if you have changed language settings on the parent upstream server after first synchronizing with the old language settings. For more information see "Listinactiveapprovals" in [Managing WSUS 3.0 SP2 from the Command Line](#).

The last catalog synchronization failed

If your last catalog synchronization failed and you see event ID 10021 or 10022, check your upstream server and proxy settings in the WSUS administration console (**Options**, then **Update Source and Proxy Server**).

A WSUS 2.0 replica times out when synchronizing

In some cases WSUS 2.0 replica servers time out during synchronization. This issue has been fixed in WSUS 2.0 Service Pack 1 and in WSUS 3.0. See [KB 910847](#), "Time-out error when approving multiple updates on Microsoft WSUS Server" (<http://go.microsoft.com/fwlink/?LinkId=86496>) for more information.

Issues with Update Approvals

If you are having problems with approvals, use the following sections to troubleshoot the problem.

Troubleshooting update approvals

New approvals can take up to one minute to take effect

If you approve an update on the WSUS console and there are client computers running detection at that exact moment, those computers might not get the approved update until they go through another detection cycle. The WSUS server requires approximately one minute to begin offering newly approved updates to client computers.

Remote computers accessed by using Terminal Services cannot be restarted by non-administrators

Non-administrators using terminal services computers will not be able to restart their computers remotely. Therefore, if a remote computer on which an update is installed needs to be restarted for the update to take effect, users without administrative permissions will be unable to complete the updating of their remote computer.

The number of updates that are approved on a parent upstream server does not match the number of approved updates on a replica server

This might occur if you have changed language settings on the parent upstream server after first synchronizing with the old language settings. For more information see "listinactiveapprovals" in [Managing WSUS 3.0 SP2 from the Command Line](#).

Issues with Backup and Restore

Use the information in this section to troubleshoot issues around backing up and restoring WSUS.

Troubleshooting backup and restore issues

Cannot access WSUS data after restoring the database

If you restore a WSUS database but cannot access it from the WSUS administration console, check for the following:

- If you have changed the WSUS server name since the backup, you must add the server to the WSUS administration console.
- If you restore the backup to a WSUS server other than the one from which you backed up the database, you must add the server to the WSUS administration console.
- Verify that your user permissions are still valid for the database.

Clients have download failures after restoring the database

If you are storing content locally, and the metadata in the database does not match the update files in the content directory, clients could suffer download failures when attempting to install an update listed in the database but not found in the content directory. You can resolve this problem, or prevent it from occurring, by making sure to run **wsusutil reset** after every restore procedure. For details, see the "wsusutil reset" section in [Managing WSUS 3.0 SP2 from the Command Line](#).

Issues with E-Mail Notifications

If you are not receiving e-mail notifications after having set up your WSUS server to send them, you should check both the WSUS server's e-mail setup and the SMTP configuration on the e-mail server.

Troubleshooting the WSUS e-mail setup

In the WSUS administration console, click **Options**, and then click **E-Mail Notifications**. On the **E-Mail Server** tab, check the SMTP server name and port, the sender name and address, and the SMTP server authentication, if necessary. You can use the **Test** button to verify your settings.

Troubleshooting the SMTP server

You can refer to articles such as [SMTP: Troubleshooting the TCP/IP Layer of the Mail Gateway](http://go.microsoft.com/fwlink/?LinkId=81082) (<http://go.microsoft.com/fwlink/?LinkId=81082>) for more information about troubleshooting issues with the SMTP server.

Issues with the Database

If you have problems with the SQL Server database or Windows Internal Database, make sure that the WSUS database in question is in the correct SQL instance before starting to troubleshoot SQL issues.



Note

You will need to use the **sqlcmd** utility. For more information about the **sqlcmd** utility, see [sqlcmd Utility](http://go.microsoft.com/fwlink/?LinkId=81183) (<http://go.microsoft.com/fwlink/?LinkId=81183>).

Troubleshooting Database Issues

► To ensure that the WSUS database is in the correct SQL instance

1. Verify the SQL server name by opening a Command Prompt window and typing the following:

```
Reg query "HKLM\SOFTWARE\Microsoft\Update  
Services\Server\Setup" /v SqlServerName
```

The output contains the SQL server name to be used in the next step.

2. Type the following:

```
sqlcmd -S Sql/ServerName -E -d SUSDB
```

Review any error messages and correct the problems.

If you are using Windows Internal Database as the WSUS database, use the following string in place of *SqlServerName* in the command:

```
np:\\.\pipe\MSSQL$MICROSOFT##SSEE\sql\query
```

Issues with WSUS 3.0 Services

WSUS uses seven services. They are the Update Service (wsusservice.exe), the Reporting Web Service, the API Remoting Web Service, the Client Web Service, the Simple Web Authentication Web Service, the Server Synchronization Service, and the DSS Authentication Web Service. This section explains how to troubleshoot these services in general.

Troubleshooting services

General service troubleshooting

You can use the following steps to restart services that are not functioning properly:

1. Locate the service (click **Start**, point to **Administrative Tools**, click **Services**, and then look for the service).
2. Verify that the service is running. Click **Start** if it is stopped or **Restart** to refresh the service.

You can also use the Event Viewer to check the Application, Security, and System event logs to see if there are any events that indicate a problem. You should also check the SoftwareDistribution.log to see if there are events that indicate a problem.

Reset IIS

You should reset IIS if you suspect that there are problems with Web services.

1. Open a command window.
2. Type **iisreset**

SQL service

The SQL service must be running for all the services except the self-update service. If any of the log files indicate SQL connection problems, check the SQL service first. To access the SQL service, click the **Start** button, point to **Administrative Tools**, click **Services**, and then look for one of the following:

- **MSSQLSERVER** (if you are using Windows Internal Database, or if you are using SQL Server and are using the default instance name for the instance name).
- **MSSQL\$WSUS** (if you are using a SQL Server database and have named your database instance "WSUS").

Right-click the service, and then click **Start** if the service is not running or **Restart** to refresh the service if it is running.

Access rights on Web service directories

Incorrectly set permissions on Web service directories can cause problems for WSUS Web services. WSUS setup will create these directories and set the access rights correctly, but subsequent developments, such as the installation of different applications or the operation of security software, may have reduced the permissions. See [Appendix D: Permissions on WSUS Directories and Registry Keys](#) for more information about the different Web service directories and the correct access rights for them.

IIS settings for Web services

IIS must be configured correctly for WSUS Web services. WSUS setup will configure its Web services correctly, but the subsequent addition of new Web services or reconfiguration of the default Web site (if the default site is used by WSUS) may cause the configuration to change. See [Appendix C: IIS Settings for Web Services](#) for an explanation of how to check IIS configuration, as well as the correct settings on each of the Web services and for the WWW web service.

WSUS 3.0 SP2 Client Computer Administration Issues

In This Section

- [Issues with Client Computer Groups](#)
- [Issues with Update Installation on Clients](#)
- [Issues with Clients Not Reporting](#)
- [Issues with Client Self-Update](#)
- [Issues with BITS](#)
- [Issues with High CPU Utilization](#)

Issues with Client Computer Groups

Use the information in this section to troubleshoot issues with client computer groups.

Client computers appear in the wrong groups

Using Group Policy or registry settings to move computers into target groups is called *client-side targeting*. For information about how to set up client-side targeting, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>). There are a number of reasons why computers might not appear in groups when you are using client-side targeting. Use the following information to try to resolve this problem.

Verify that the WSUS console is set to use client-side targeting

By default the WSUS server is set to use server-side targeting. If you are using client-side targeting, you need to set an option on the WSUS server. For information about how to set up client-side targeting, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

Verify that target computer group names match groups on the WSUS server

Make sure the name of the target computer group matches the name of the computer group on the WSUS server. Check the Group Policy object (GPO) or the registry setting where you enabled client-side targeting. Make sure that there are no discrepancies between the name of the computer group used in Group Policy and the name of the group used on the server. If WSUS cannot find a computer group on the server reported by a client computer, the computer will appear in the Unassigned Computers group.

Reset the Automatic Update client

If you make a change to group membership by using client-side targeting, you can reset the Automatic update client with the `wuauclt` utility. For more information about **wuauclt**, see [Appendix H: The wuauclt Utility](#).

▶ To reset the Automatic Update client

1. Open a command window.
2. Type **wuauclt.exe /resetauthorization /detectnow**
3. Wait 10 minutes for the detection cycle to finish.

Issues with Update Installation on Clients

If WSUS clients are not installing updates, there may be issues with DCOM configuration. You will see event ID 10311 or 10312 in the application log if this is the case.

Troubleshooting Update Installation Issues

Checking DCOM Configuration

The process of checking DCOM configuration is slightly different on different operating systems.

▶ To check DCOM configuration on Windows Vista and Windows XP

1. Open a Command Prompt window.
2. Type the following command: **dcomcnfg**
(The **Component Services** window will appear.)
3. Right-click **My Computer**, click **Properties**.
4. Click the **Default Properties** tab.
5. Make sure that **Enable Distributed COM on this computer** is selected.
6. Make sure that **Default Impersonation Level** is set to **Identify**.
7. Click **OK**, and then close the **Component Services** window.

Default DCOM Permissions

Default DCOM permissions can also be a source of problems.

▶ To remove default DCOM permissions

1. Open the **Registry Editor**.
2. Navigate to HKLM/SOFTWARE/Microsoft/Ole.
3. If there is a **DefaultAccessPermission** key, delete it.

Issues with Clients Not Reporting

If you have configured clients for a particular WSUS server, but they have not reported over a period of days, use the following procedures to isolate and repair the problem.

Troubleshooting client not reporting issues

Check the HTTP hotfix

Some clients have been affected by a known issue with Windows Server 2003 http.sys and IIS. In some cases this transient issue will prevent clients from checking in, because they receive incorrect responses from the server after a number of attempts. Further information about the issue can be found at [FIX: IIS 6.0 may send an "HTTP 100 Continue" response in the middle of](#)

[the response stream when you send a POST request](#)

(<http://go.microsoft.com/fwlink/?LinkId=80715>).



Note

Failure of clients to contact the server is not related to compression. Administrators should not disable IIS compression, because allowing noncompressed data can increase network traffic and server load, while reducing the number of clients that can be served effectively.

Troubleshoot client connectivity

Ensure that the client connection to the WSUS server is working properly.

► To troubleshoot client connectivity

1. Open a command window.
2. Contact the WSUS server: **ping** *WSUSServerName*
3. Contact the WSUS HTTP server. Open Internet Explorer and in the Address bar type: **http://WSUSServerName:portNumber** where *WSUSServerName* is the name of the WSUS server, and *portNumber* is the port that has been configured for it (for example, 80 for HTTP, 443 for SSL, and 8530 for a custom port).
4. Verify the existence of the self-update tree. In an Internet Explorer Address bar type **http://WSUSServerName/selfupdate/wuident.cab**
5. If the WSUS server is functioning properly, you should see a **File Download** window asking you whether to open or save the file. Close the window.



Note

If you do not see the **File Download** window, make sure that the client self-update tree has been configured properly. For more information, see [Issues with Client Self-Update](#).

Troubleshoot the Automatic Update client

Ensure that the Automatic Update client has been configured correctly.

► To troubleshoot the Automatic Update client

1. Open a command window.
2. Type:
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
You should see output like the following if the client has been configured to get its updates from a WSUS server:

```
HKKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
WUServer    REG_SZ    http://WSUSServerName
```

```
WUStatusServer      REG_SZ  http://WSUSServerName
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
```

You should see output similar to the following if Automatic Update is functioning, but the client has not been configured to get its updates from a WSUS server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
```

If the query returns the error, "The system was unable to find the specified registry key or value," Automatic Update has not been configured on this computer.

If the output from step 2 above contains values for *WU*Server and *WU*StatusServer, try to contact the WSUS server listed in these values.

3. Open Internet Explorer and in the Address bar type **http://WU**Server where *WU*Server stands for the value in the output from step 2.

You should see an "Under Construction" page if the *WU*Server value is valid. If it is not, you will get an HTTP error of some kind.

Reset the Automatic Update client

It can be a good idea to reset the Automatic Update client if you are experiencing difficulty with contacting the WSUS server with the *wuauctl* utility. For more information about *wuauctl*, see [Appendix H: The *wuauctl* Utility](#).

▶ To reset the Automatic Update client

1. Open a command window.
2. Type **wuauctl.exe /resetauthorization /detectnow**
3. Wait 10 minutes for the detection cycle to finish.

Issues with Client Self-Update

WSUS uses IIS to update most computers to the WSUS-compatible Automatic Update. This process is called *client self-update*. To accomplish client self-update, WSUS Setup creates a virtual directory under the WSUS Web site named *Selfupdate*. This virtual directory holds the WSUS-compatible Automatic Updates. This is called the *self-update tree*.

Using Group Policy to point client computers to your WSUS server should eventually cause an Automatic Updates detection and client self-update. For more information about this process, see the [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>).

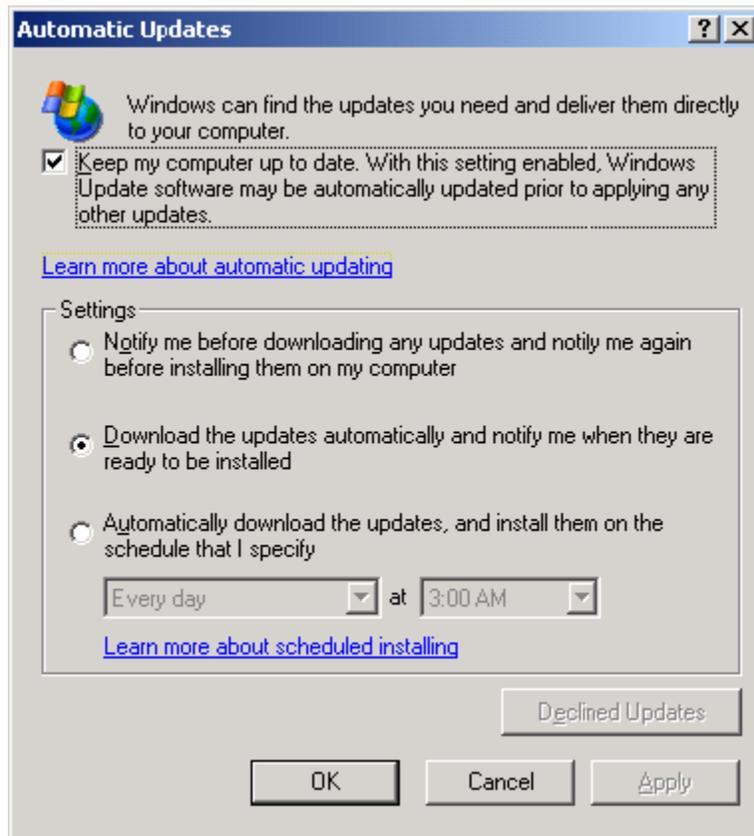
Troubleshooting client self-update issues

If the client self-update does not work automatically, use the following suggestions to troubleshoot the problem.

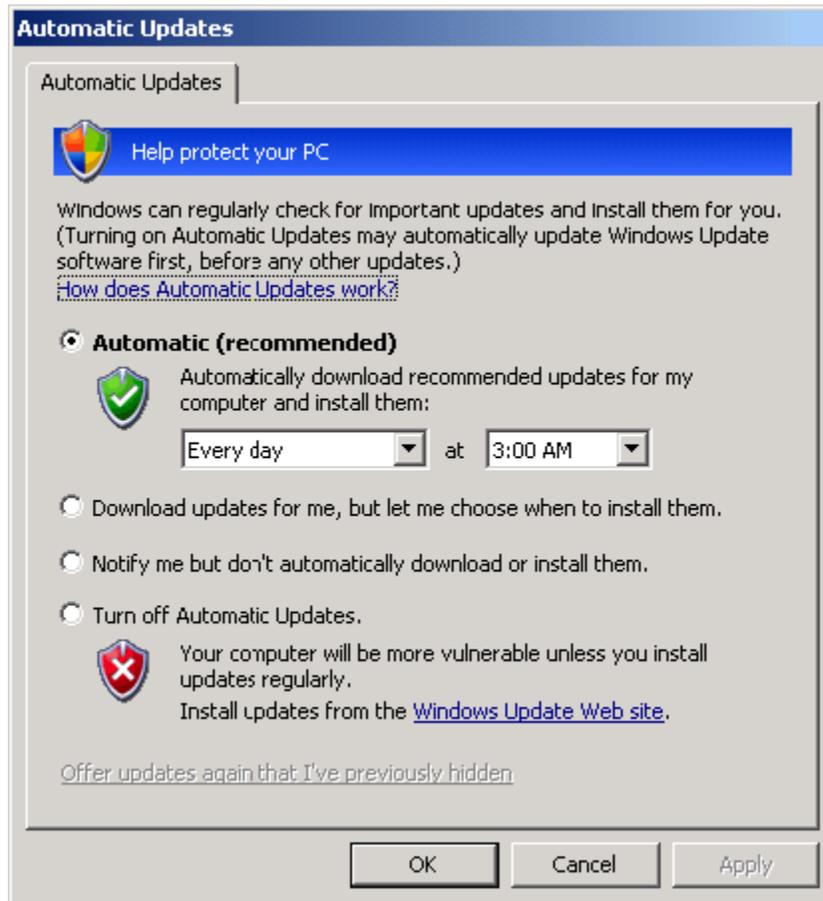
How to differentiate between the SUS client and WSUS client

Use the Automatic Updates user interface to differentiate between the SUS and WSUS clients. The following illustrations show the user interface of the SUS and WSUS clients.

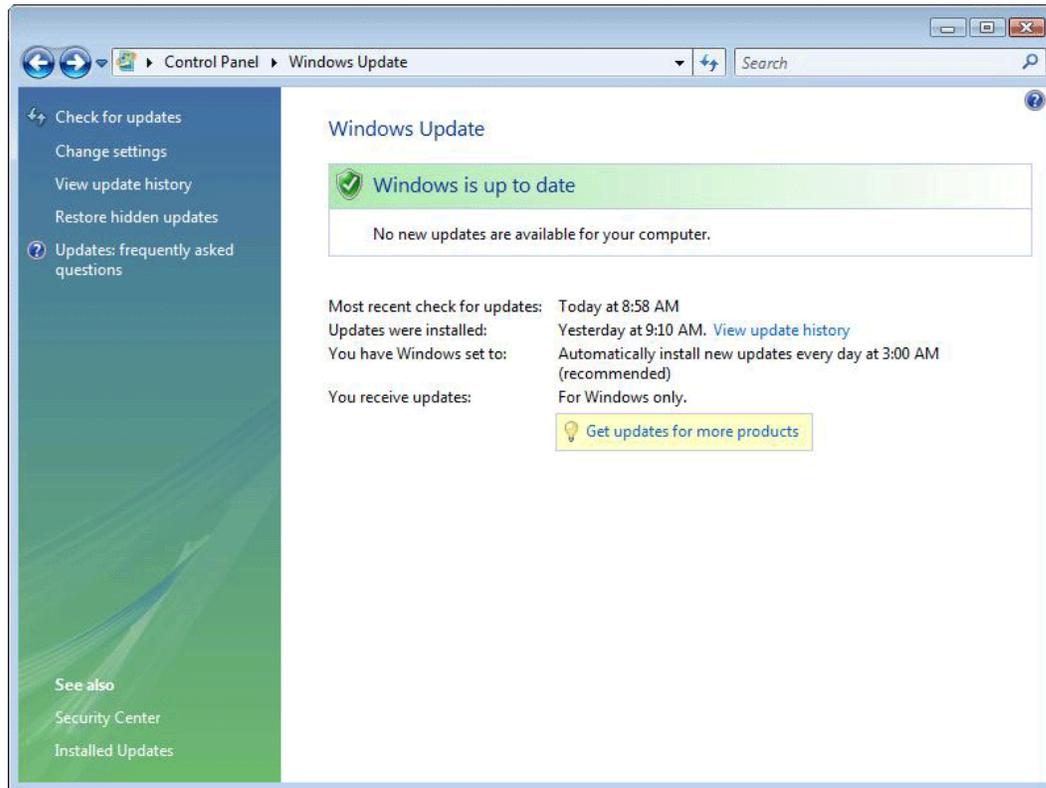
SUS Client



WSUS Client (Windows XP)



WSUS Client (Windows Vista)



Verify that the client software in your organization can self-update

Some computers might already have the WSUS client installed. Other computers might have a version of Automatic Updates that is incapable of performing self-update. For more information see [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (<http://go.microsoft.com/fwlink/?LinkId=139832>). If the clients in your organization are capable of and require self-update but are still not self-updating, see the next section.

Verify that SUS clients are pointed to the WSUS server

If you have the WSUS client installed but the client computer is pointed to a SUS server, Automatic Updates falls into legacy mode and the client computer uses the SUS client user interface. In this case you need to redirect the computer away from the SUS server to get the WSUS client to function. When you point Automatic Updates to a WSUS server, the WSUS client user interface appears.

If your client computers are pointed to the WSUS server and you do not see the WSUS client user interface shown above, see the next section.

Check for the self-update tree on the WSUS server

WSUS Setup creates a virtual directory named Selfupdate under the Web site running on port 80 of the computer where you install WSUS. This virtual directory, called the *self-update tree*, holds the latest WSUS client. For this reason, you must have a Web site running on port 80, even if you put the WSUS Web site on a custom port. The Web site on port 80 does not have to be dedicated to WSUS. WSUS uses the site on port 80 only to host the self-update tree.

To ensure that the self-update tree is working properly, first make sure there is a Web site set up on port 80 of the WSUS server. After that you should run the WSUS script that ensures a proper configuration of self-update on port 80. Open a command window on the WSUS server and type the following:

```
cscript WSUSInstallDirectory\setup\installselfupdateonport80.vbs
```

where *WSUSInstallDirectory* is the directory in which WSUS is installed. If the script is successful, you should see the following output:

```
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

SetupSelfupdateTree: Finding the index of the Web site on which WUS is installed...
SetupSelfupdateTree: Leaving GetWUSWebSiteIndex.
SetupSelfupdateTree: Finding the index of the web site bound to port 80...
SetupSelfupdateTree: iWebSiteIndex: 1 ServerBindings: :80:index: 0
SetupSelfupdateTree: Found the index of site on Port 80: 1
SetupSelfupdateTree: rootMetabasePath: IIS://LocalHost/W3SVC/1/ROOT
SetupSelfupdateTree: szPort80RootPath=c:\inetpub\wwwroot
SetupSelfupdateTree: iWusWebSiteIndex=1 iPort80WebSiteIndex=1
SetupSelfupdateTree: Warning: This is standalone WUS install. No need to do configuration
for SxS install.
Success: InstallSelfupdateOnPort80 succeeded.
```

If you have WSUS client self-update running on port 80 of the WSUS server, see the next section.

Check IIS logs on the WSUS Server

Check the IIS logs on the WSUS server. IIS logs are typically located in *%windir%\system32\LogFiles\W3SVC1* for the default Web site. Typical errors might be 404 (file not found) 401/403 (authentication/access), and 500 (Internal server error). Use IIS Help to troubleshoot any problems found in the IIS logs.

If you have installed Windows SharePoint Services on the default Web site in IIS, configure it to coexist with Self-update

If you install Windows SharePoint Services on the same server that is running WSUS, you might see the following issues:

- An "Access denied" message appears when Automatic Updates tries to update itself, and the latest Automatic Updates will not be running.
- A message appears warning you that the SelfUpdate service is not available.

If client computers are not running the WSUS-compatible version of Automatic Updates, they will not be able to receive updates through WSUS.

► To resolve this issue

1. Grant Anonymous access (Anonymous Auth) to the Default Web site, ClientWebService and Selfupdate v-roots in IIS.
2. Exclude specific requests from being intercepted by the Windows SharePoint Services ISAPI DLL by doing the following:
 - a. Open the Windows SharePoint Services Central Administration Site (click **Start**, point to **Administrative Tools**, and then click **Sharepoint Central Administration**).
 - b. Click **Virtual Server Configuration**, and then click **Configure Virtual Server Settings**.
 - c. Click **Default Web Site**.
 - d. Click **Virtual Server Management**, and then click **Define managed paths**.
 - e. In the **Add a new path** box, set the type to **Excluded Path**. Under **Path**, type the following:
 - **/iident.cab**
 - **/clientwebservice**
 - **/Selfupdate**

For more information, see [KB 828810](http://go.microsoft.com/fwlink/?LinkId=81417) (http://go.microsoft.com/fwlink/?LinkId=81417), "How to enable an ASP Net application to run on a SharePoint virtual server."

Check if the Content and Selfupdate Web sites have different authentication levels

If the Content site is configured for **Enable anonymous access** and Selfupdate site is configured for **Authenticated access - Integrated Windows Authentication**, then client will fail to Selfupdate

► To resolve this issue

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 **Selfupdate**, and then click **Properties**.
5. On the **Directory Security** tab, under **Authentication and access control**, click **Edit**.
6. In the **Authentication Methods** dialog box, check the **Enable anonymous access** check box, and then clear all the buttons below if checked. The **user name** and **password** box should be pre populated.
7. Click **OK** twice.

Check network connectivity on the WSUS client computer

Check network connectivity on the WSUS client computer. Use Internet Explorer to determine whether self-update files on the WSUS server are accessible to the client computer. If you perform the following procedure and are prompted to download or open the files, you have verified network connectivity. If you do not have access to these files, there are problems with network connectivity between the WSUS server and the client computer.

► To check network connectivity on the WSUS client computer

1. Open Internet Explorer.
2. In the **Address** bar, type:

http://WSUSServerName/selfupdate/wuident.cab

where *WSUSServerName* is the name of the WSUS server. You should be prompted to download or open *wuident.cab*. This verifies network connectivity from the WSUS client and the availability of the *wuident.cab* file on the WSUS server. If you do not have connectivity or the Web site is not configured correctly, you will get an HTTP error. Check the network settings of the WSUS server and any proxy servers.

3. If there are any boxes prompting you to download or save, click **Cancel**.

If you are prompted to save or download both of these files, see the next section.

Check logs on the WSUS client computer

Check the *%windir%\WindowsUpdate.log* on the client computer to see if there has been any activity or any attempts to contact the server, such as cached server pingbacks. If you can find no problem with the logs on the WSUS client, see the next section.

Manipulate registry settings on the WSUS client computer

If all else has failed, you can attempt to manually manipulate registry settings to get the client computer to self-update to the WSUS client.

► To manually manipulate registry settings on the SUS client computer

1. Click **Start**, then **Run**, and type **regedit**, and then click **OK**.
2. In Registry Editor, navigate to the **WindowsUpdate** key by expanding the following:
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows
If the **WindowsUpdate** key does not exist, you need to add it.
3. On the menu, click **Edit**, point to **New**, and then click **Key**.
4. Type **WindowsUpdate** as the name for the new key.
5. Double-click the **WUserver** setting, type the URL to your WSUS server, and then press ENTER.
If the **WUserver** setting does not exist, you need to add it.
On the menu, click **Edit**, point to **New**, and then click **String Value**.
6. Type **WUserver** as the setting name.
7. Double-click the **WUstatusServer** setting, type the URL to your WSUS server, and then press ENTER.
If the **WUstatusServer** setting does not exist, do the following:
On the menu, click **Edit**, point to **New**, and then click **String Value**.
8. Type **WUstatusServer** as the setting name.
9. Navigate to the following:
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
If the **AU** key does not exist, do the following:
On the menu, click **Edit**, point to **New**, and then click **Key**.
10. Type **AU** as the name for the new key.
11. Verify that the **UseWUserver** setting has a value of 1 (0x1). If it does not, modify it by double-clicking the setting and then changing the value.
If the **UseWUserver** setting does not exist, do the following:
On the menu, click **Edit**, point to **New**, and then click **DWORD Value**.
12. Type **UseWUserver** for the setting name.
13. Navigate to the following:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update
14. Enable and configure Automatic Updates through Control Panel:
Click **Start**, click **Control Panel**, and then double-click **Automatic Updates**.
15. In the **Automatic Updates** dialog box, specify download and installation options, and then click **OK**. Make sure that **Turn off Automatic Updates** is not selected.
16. Ensure that the **AUState** setting has a value of 2 (0x2). If it does not, modify it by double-clicking and changing the value.
17. If the **LastWaitTimeout** setting exists, delete it.

18. If the **DetectionStartTime** setting exists, delete it.
19. Close the Registry Editor.

▶ **To force the WSUS client computer to check with the WSUS server**

1. At the command prompt, stop the Automatic Updates service by typing the following, and then pressing ENTER:
net stop wuauerv
2. At the command prompt, restart the Automatic Updates service by typing the following, and then pressing ENTER:
net start wuauerv
3. The self-update should occur in six to ten minutes.
4. Wait approximately one minute, and then refresh the registry. You should now see the following settings and values:
 - **DetectionStartTime (REG_SZ) YYYY.MM.DD HH.MM.SS.** The **DetectionStartTime** value is written in local time, but the detection actually occurs 5 minutes after the time noted.
 - **LastWaitTimeout (REG_SZ) YYYY.MM.DD HH.MM.SS.** The **LastWaitTimeout** value is written in GMT or Universal Time, and represents the actual time that detection occurs.

Although these values refer to the time that detection is going to start, the first phase of detection is the process of checking whether a self-update is necessary. Therefore, these values actually refer to the time that the self-update from SUS client to the WSUS client should occur.

If the client software has not self-updated after ten minutes, refresh the **Auto Update** registry key. If the **LastWaitTimeout** value has changed and is now 24 hours later than its previous value, that indicates that Automatic Updates was not able to contact the server URL that you specified in the **WUServer** value.

You should also check the functioning of the Client Web Service. See [Issues with WSUS 3.0 Services](#) for more information.

Issues with BITS

Background Intelligent Transfer Service (BITS) is the service used by WSUS to download updates from Microsoft Update to the main WSUS server, as well as from WSUS servers to their clients. BITS also supports the transfer of files between peer computers in a domain.

Some download issues may be caused by problems with running BITS on the server or client computers. When you are troubleshooting download problems, after you have verified that all WSUS settings are correct on both the server and its clients, you should ensure that BITS is running properly on all affected computers.

BITS provides a downloadable tool called bitsadmin that allows you to verify and change BITS settings. For more information about the bitsadmin utility, see [BITSAdmin Tool](http://go.microsoft.com/fwlink/?LinkId=80934) (<http://go.microsoft.com/fwlink/?LinkId=80934>). This tool is available as part of the Windows Vista operating system, and also as part of the Windows XP Service Pack 2 Support Tools.

Finding BITS

To find the BITS service, open a Command Prompt and type:

```
sc query bits
```

If BITS is running, you should see output like the following:

```
SERVICE_NAME: bits

TYPE                : 20  WIN32_SHARE_PROCESS
STATE                : 4  RUNNING
                    (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE      : 0  (0x0)
SERVICE_EXIT_CODE  : 0  (0x0)
CHECKPOINT           : 0x0
WAIT_HINT            : 0x0
```

If BITS is not running, you should see output like the following:

```
SERVICE_NAME: bits

TYPE                : 20  WIN32_SHARE_PROCESS
STATE                : 1  STOPPED
                    (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
WIN32_EXIT_CODE      : 0  (0x0)
SERVICE_EXIT_CODE  : 0  (0x0)
CHECKPOINT           : 0x0
WAIT_HINT            : 0x0
```

Stopping and Restarting BITS

Often it is possible to resolve BITS issues simply by stopping the service and restarting it. The following procedure shows how to stop and restart the service from a Command Prompt.



Note

To modify, stop, or restart BITS, log on as a local administrator.



To stop and restart BITS

1. Open a Command Prompt window.

2. Type **sc stop bits**
3. Type **sc start bits**

Troubleshooting BITS Download Issues

The following sections are an incomplete list of possible problems with BITS configuration. For more information about BITS, refer to [Background Intelligent Transfer Service](http://go.microsoft.com/fwlink/?LinkId=81083) (<http://go.microsoft.com/fwlink/?LinkId=81083>).

The BITS service must run under the Local System user account

By default BITS runs under the LocalSystem account.

▶ To configure the service to run under the correct account

1. Open a Command Prompt window.

Type:

```
sc config bits obj= LocalSystem
```

Note that a space must occur between `obj=` and `LocalSystem`.

2. Verify that output from the command is:
[SC] ChangeServiceConfig SUCCESS
3. Stop and restart BITS.

Proxy Servers Must Support HTTP 1.1 RANGE Requests

- BITS supports HTTP and HTTPS downloads and uploads and requires that the server support the HTTP 1.1 protocol. For downloads, the HTTP server's HEAD method must return the file size, and its GET method must support the Content-Range and Content-Length headers. BITS can use an HTTP/1.0 server as long as it meets the HEAD and GET method requirements (MIME headers must include the standard Content-Range and Content-Type headers plus a maximum of 180 bytes of other headers, and a maximum of two CR/LF characters may occur between the HTTP headers and the first boundary string).

There is a mismatch between the BITS per-user job limit and the per-computer job limit

▶ To detect or correct a mismatch between the per-user job limit and the per-computer job limit specified through Group Policy

1. Run `gpedit.msc`, if the policy is specified locally; if the policy is a domain policy edit the Group Policy object with GPMC.
2. In the Group Policy Object Editor, navigate to Computer Configuration\Administrative Templates\Network\Background Intelligent Transfer Service (BITS).

3. Ensure that the setting "Maximum number of BITS jobs for each user" is set to a lower value than the setting "Maximum number of BITS jobs for this computer"
4. Type **gpupdate /force**
5. Stop and restart BITS.
6. Verify that there are no errors in the event logs.

BITS Jobs are Failing

If BITS jobs fail, look in the event log to find errors. You can use the following table to diagnose the cause of the errors.

Error name	Error code	Description
E_INVALIDARG	0x80070057	An incorrect proxy server name was specified in the user's Internet Explorer proxy settings. This error is also seen when credentials are supplied for authentication schemes that are not NTLM/Negotiate, but the user name or password is null. Change the user's IE settings to be a valid proxy server or Change the credentials not to be NULL user name/password for schemes other than NTLM/Negotiate.
ERROR_WINHTTP_NAME_NOT_RESOLVED	0x80072ee7	The server/proxy could not be resolved by BITS. Internet Explorer on the same machine in the context of the job owner would see the same problem. Try downloading the same file via the web browser

Error name	Error code	Description
		using the context of the job owner.
ERROR_HTTP_INVALID_SERVER_RESPONSE	0x80072f78	This is a transient error and the job will continue downloading.
BG_E_INSUFFICIENT_RANGE_SUPPORT	0x80200013	BITS uses range headers in HTTP requests to request parts of a file. If the server or proxy server doesn't understand Range requests and returns the full file instead of the requested range, BITS puts the job into the ERROR state with this error. Capture the network traffic during the error and examine if HTTP GET requests with "Range" header are getting valid responses. Check proxy servers to ensure that they are configured correctly to support Range requests.
BG_E_MISSING_FILE_SIZE	0x80200011	When BITS sends a HEAD request and the server/proxy does not return Content-Length header in the response, BITS puts the job in ERROR state with this error. Check the proxy server and WSUS server to ensure that they are configured correctly. Some

Error name	Error code	Description
		versions of the Apache 2.0 proxy server are known to exhibit this behavior.
BG_E_HTTP_ERROR_403	0x80190193	When the server returns HTTP 403 response in any of the requests, BITS puts the job in ERROR state with this error code. HTTP 403 corresponds to "Forbidden: Access is denied." Check access permissions for the account running the job.
ERROR_NOT_LOGGED_ON	0x800704dd	The SENS service is not receiving user logon notifications. BITS (version 2.0 and up) depends on logon notifications from Service Control Manager, which in turn depends on the SENS service. Ensure that the SENS service is started and running correctly.

BITS Fails to Start

If the BITS service fails to start, use the following table to diagnose the cause of the error.

ERROR_SERVICE_DOES_NOT_EXIST	0x80070424	See the section on repairing the BITS configuration below.
ERROR_SERVICE_NOT_IN_EXE	0x8007043B	BITS is not listed as one of the services in the netsvcs svchost group.
ERROR_SERVICE_DISABLED	0x80070422	BITS has been disabled. Enable the BITS service.

ERROR_SERVICE_DEPENDEN CY_DELETED ERROR_SERVICE_DEPENDEN CY_FAIL	0x80070 433, 0x80070 42c	A service appearing in the BITS service dependency list cannot be started. Make sure the dependency list for the BITS service is correct: <ul style="list-style-type: none"> • Windows Vista: RpcSs, EventSystem (also http.sys and LanManWorkstation when peercaching is enabled) • Windows Server 2003: Rpcss, EventSystem • Windows XP: Rpcss
ERROR_PATH_NOT_FOUND	0x80070 003	Pre-Windows Vista: %ALLUSERSPROFILE%\Microsoft\Network doesn't exist
ERROR_FILE_NOT_FOUND	0x80070 002	The "Parameters" key is missing. Ensure that the following keys and values exist: HKLM\SYSTEM\CurrentControlSet\Services\BITS\ Parameters\ServiceDll= %SystemRoot%\System32\qmgr.dll

Repairing a Corrupted BITS Configuration

To repair corrupted BITS service configuration, you can enter the BITS service configuration manually.

Important

This action should only be taken in circumstances where all other troubleshooting attempts have failed. You must be an administrator to modify the BITS configuration.

To repair a corrupted BITS configuration

1. Open a Command Prompt window.
2. Type:

```
Sc config bits binpath="%systemroot%\system32\svchost.exe -k netsvcs" Sc config bits
depend = RpcSs EventSystem
Sc config bits start=delayed-auto
Sc config bits type=interact
Sc config bits error=normal
Sc config bits obj=LocalSystem
Sc privs bits
privileges=SeCreateGlobalPrivilege/SelmpersonatePrivilege/SeTcbPrivilege/SeAssignPri
maryTokenPrivilege/SelcreateQuotaPrivilege
Sc sidtype bits type= unrestricted
```

Sc failure bits reset= 86400 actions=restart/60000/restart/120000

3. Stop and restart BITS.

Issues with High CPU Utilization

Clients may notice very high (approaching 100 percent) CPU utilization under the following circumstances.

▶ **An access violation error message appears and the system may appear to become unresponsive when you try to install an update from Windows Update or from Microsoft Update**

- There is an update for this issue described by [Microsoft KB Article number 927891](http://go.microsoft.com/fwlink/?LinkId=85649) (<http://go.microsoft.com/fwlink/?LinkId=85649>).

▶ **There are a large number of superseded updates approved on the WSUS server**

- This problem occurs if you do not decline expired definition updates or expired malicious software (also known as malware) updates on the WSUS server. There is an update for this issue described by [Microsoft KB article number 938947](http://go.microsoft.com/fwlink/?LinkId=148750) (<http://go.microsoft.com/fwlink/?LinkId=148750>).

Additional Resources for Windows Server Update Services 3.0 SP2

For more information and support, see the following resources.

Windows Server Update Services communities

Microsoft communities are great places to exchange ideas with other users and discuss common issues. You can read and write messages by using an NNTP-based newsreader such as Microsoft Outlook Express. You can also use the Web-based newsreader provided by Microsoft to access all of the newsgroups. To access the WSUS Communities, see the [Windows Server Update Services Communities Homepage](http://go.microsoft.com/fwlink/?LinkId=45215) (<http://go.microsoft.com/fwlink/?LinkId=45215>).

Additional references

For complete information about installing and using WSUS, see the following:

- [WSUS Step by Step Installation Guide](http://go.microsoft.com/fwlink/?LinkId=139836) (http://go.microsoft.com/fwlink/?LinkId=139836)
- [WSUS Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=139832) (http://go.microsoft.com/fwlink/?LinkId=139832)
- [WSUS Release Notes](http://go.microsoft.com/fwlink/?LinkId=139840) (http://go.microsoft.com/fwlink/?LinkId=139840)
- WSUS Administration Console online Help
- For information that helps you automate tasks or customize WSUS, see the [Microsoft Windows Server Update Services Software Developer's Kit](http://go.microsoft.com/fwlink/?LinkId=43099) (http://go.microsoft.com/fwlink/?LinkId=43099) and [Windows Update Agent Software Developer's Kit](http://go.microsoft.com/fwlink/?LinkId=43101) (http://go.microsoft.com/fwlink/?LinkId=43101). Note that the Windows Update Agent is the Automatic Updates service. Both SDKs contain information about the application programming interface (API), as well as sample scripts and ready-to-use tools for your WSUS deployment and implementation.

Appendix A: Uninstalling Windows Internal Database

It is not usually necessary to uninstall Windows Internal Database, which WSUS installs as the default SQL Server version. It is not possible to remove this application with **Add or Remove Programs**, and it will not be uninstalled automatically when WSUS is uninstalled. If you wish to do so, you will need to call the **msiexec** executable with the correct key for the operating system platform.



Important

Uninstalling Windows Internal Database is not recommended, because it may affect other applications that may be using the same database instance (such as Windows SharePoint Services).



To uninstall Windows Internal Database

1. Open a command shell.
2. Call **msiexec** with the correct key for the operating system platform.
 - On 32-bit platforms: **msiexec /x {CEB5780F-1A70-44A9-850F-DE6C4F6AA8FB} callerid=ocsetup.exe**
 - On 64-bit platforms: **msiexec /x {BDD79957-5801-4A2D-B09E-852E7FA64D01} callerid=ocsetup.exe**



Important

The removal of the application may not remove the default .mdb and .ldb files, which will cause a subsequent WSUS 3.0 installation to fail. These files can be deleted from the %windir%\SYSMS\SSEE directory.

Appendix B: Uninstalling WSUS 3.0 SP2 from SQL Server

Read the following information before uninstalling WSUS.

Uninstalling WSUS might leave some WSUS accounts on computers running SQL Server

Local SQL Server accounts that are created by WSUS Setup are not removed by the WSUS uninstall component. The WSUS uninstall component does not remove the Network Service and ASP.NET accounts from the local computer running SQL Server. If some other application or database is using these accounts, this ensures that these applications or databases do not fail. If you are sure that no other application or database requires the Network Service or ASP.NET accounts, you can manually remove them from the computer running SQL Server.

For information about how to manually remove Network Service or ASP.NET accounts from a computer running SQL Server 2005 or Windows Internal Database, see SQL Server product documentation. You can download product documentation for SQL Server at [SQL Server Books Online](http://go.microsoft.com/fwlink/?LinkId=81092) (<http://go.microsoft.com/fwlink/?LinkId=81092>).

Appendix C: IIS Settings for Web Services

Troubleshooting WSUS Web services may be simplified if you compare your current IIS settings for the different WSUS Web services with the ones given below, which are the ones set by WSUS setup. A service may have stopped working correctly because one of these settings was changed by another installation or application.

The values of these IIS settings are sometimes represented with variable names instead of actual values. This is because the actual value may vary from one installation to another.

The variable names used in the settings, and in the instructions below, are:

- *windir*:- The standard environment variable for the Windows directory (on Windows Server 2003, usually C:\WINDOWS).
- *InetpubDir*:- The IIS inetpub directory on Windows Server 2003 (usually C:\inetpub).
- *WSUSInstallDir*:- The directory where WSUS is installed (usually C:\Program Files\Update Services).
- *WebSiteID*:- The number IIS uses to identify Web sites (1 is the ID of the default Web site, but other Web sites are assigned random numbers).

IIS vroots

The following virtual directories (vroots) are created in IIS (in the Default Web Site by default) for client-to-server synchronization, server to server synchronization, reporting, and client self-update.

Root in IIS	Properties
ClientWebService	Directory: %ProgramFiles%Update Services\WebServices\ClientWebService Application Pool: WsusPool Security: Anonymous Access Enabled Execute Permissions: Scripts Only
Content	Directory[the location of the WSUS content directory] Security: Anonymous Access Enabled Execute Permissions: None
DssAuthWebService	Directory: %ProgramFiles%Update Services\WebServices\DssAuthWebService Application Pool: WsusPool Security: Anonymous Access Enabled Execute Permissions: Scripts Only
Inventory	Directory: %ProgramFiles%Update Services\Inventory Application Pool: WsusPool Security: Anonymous Access Enabled Execute Permissions: Scripts Only
ReportingWebService	Directory: %ProgramFiles%Update Services\WebServices\ReportingWebService Application Pool: WsusPool Security: Anonymous Access Enabled Execute Permissions: Scripts Only
ServerSyncWebService	Directory: %ProgramFiles%Update Services\WebServices\ServerSyncWebService Application Pool: WsusPool Security: Anonymous Access Enabled Execute Permissions: Scripts Only

Root in IIS	Properties
SimpleAuthWebService	Directory: %ProgramFiles%\Update Services\WebServices\SimpleAuthWebService Application Pool: WsusPool Security: Anonymous Access Enabled Execute Permissions: Scripts Only
ApiRemoting30	Directory: %ProgramFiles%\Update Services\Administration Application Pool: WsusPool Security: Integrated Windows Authentication, Digest Authentication Execute Permissions: Scripts Only
SelfUpdate	Directory: %ProgramFiles%\Update Services\SelfUpdate Security: Anonymous Access Enabled Execute Permissions: Scripts Only

Using the adsutil IIS utility

The adsutil IIS utility can be found on your server in the Inetpub\AdminScripts directory. For more information about using adsutil.vbs, see [Using the Adsutil.vbs Administration Script](http://go.microsoft.com/fwlink/?LinkId=162432) (<http://go.microsoft.com/fwlink/?LinkId=162432>).

Finding Web service paths with adsutil

You can use adsutil to find the paths for different Web services on your computer with the following procedure.

► To find the paths of Web services

1. Open a command window.
2. Navigate to the directory where adsutil is located: **cd %Inetpubdir%\AdminScripts**
3. Type the following command: **adsutil.vbs find path**
4. If you have WSUS installed, you should see output like the following:

Property path found at:

```

W3SVC/WebSiteID/ROOT
W3SVC/WebSiteID/ROOT/ApiRemoting30
W3SVC/WebSiteID/D/ROOT/ClientWebService

```

W3SVC/WebSiteID/ROOT/Content
W3SVC/WebSiteID/ROOT/DssAuthWebService
W3SVC/WebSiteID/ROOT/Inventory
W3SVC/WebSiteID/ROOT/ReportingWebService
W3SVC/WebSiteID/ROOT/Selfupdate
W3SVC/WebSiteID/ROOT/ServerSyncWebService
W3SVC/WebSiteID/ROOT/SimpleAuthWebService



Note

If you have installed WSUS on the default Web site, *WebSiteID* will be 1, but if you have installed it on another Web site, *WebSiteID* will be a random number.

Checking the properties of a Web service

You can also use `adsutil` to find the properties of a given Web service. You will use one of the Web service paths listed above to specify the Web service you want to check. For example, if you want to check the properties of the Reporting Web service, you use the path **W3SVC/WebSiteID/ROOT/ReportingWebService**, where *WebSiteID* stands for the number of the WSUS Web site.

▶ **To check the properties of a Web service**

1. Open a command window.
2. Navigate to the directory where `adsutil` is located: **cd Inetpub\id\AdminScripts**
3. Type the following command: **adsutil.vbs enum WebServicePath** where *WebServicePath* stands for the path of the Web service you want to check.
4. Compare the output to the standard values given in the sections below.

Global properties

These global properties can be retrieved with the following `adsutil` command:

adsutil.vbs enum W3SVC

The properties listed below are a partial list.

Property	Value
KeyType	(STRING) "IlsWebService"
MaxConnections	(INTEGER) 4294967295
AnonymousUserName	(STRING) "IUSR_<machinename>"
ConnectionTimeout	(INTEGER) 120

Property	Value
AllowKeepAlive	(BOOLEAN) True
DefaultDoc	(STRING) "Default.htm,Default.asp,index.htm"
CacheSAPI	(BOOLEAN) True
CGITimeout	(INTEGER) 300
ContentIndexed	(BOOLEAN) True
DownlevelAdminInstance	(INTEGER) 1
AspBufferingOn	(BOOLEAN) True
AspLogErrorRequests	(BOOLEAN) True
AspScriptErrorSentToBrowser	(BOOLEAN) True
AspScriptErrorMessage	(STRING) "An error occurred on the server when processing the URL. Please contact the system administrator"
AspAllowOutOfProcComponents	(BOOLEAN) True >
AspScriptFileCacheSize	(INTEGER) 500
AspDiskTemplateCacheDirectory	(EXPANDSZ) "%windir%\system32\inetrv\ASP Compiled Templates"
AspMaxDiskTemplateCacheFiles	(INTEGER) 2000
AspScriptEngineCacheMax	(INTEGER) 250
AspScriptTimeout	(INTEGER) 90
AspSessionTimeout	(INTEGER) 20
AspEnableParentPaths	(BOOLEAN) False
AspAllowSessionState	(BOOLEAN) True
AspScriptLanguage	(STRING) "VBScript"
AspExceptionCatchEnable	(BOOLEAN) True
AspCodepage	(INTEGER) 0
AspLCID	(INTEGER) 2048
AspQueueTimeout	(INTEGER) 4294967295

Property	Value
AspEnableAspHtmlFallback	(BOOLEAN) False
AspEnableChunkedEncoding	(BOOLEAN) True
AspEnableTypelibCache	(BOOLEAN) True
AspErrorsToNTLog	(BOOLEAN) False
AspProcessorThreadMax	(INTEGER) 25
AspTrackThreadingModel	(BOOLEAN) False
AspRequestQueueMax	(INTEGER) 3000
AspEnableApplicationRestart	(BOOLEAN) True
AspQueueConnectionTestTime	(INTEGER) 3
AspSessionMax	(INTEGER) 4294967295
AppAllowDebugging	(BOOLEAN) False
AppAllowClientDebug	(BOOLEAN) False
PasswordChangeFlags	(INTEGER) 6
AuthChangeUnsecure	(BOOLEAN) False
AuthChangeDisable	(BOOLEAN) True
AuthAdvNotifyDisable	(BOOLEAN) True
DirBrowseFlags	(INTEGER) 1073741886
EnableDirBrowsing	(BOOLEAN) False
DirBrowseShowDate	(BOOLEAN) True
DirBrowseShowTime	(BOOLEAN) True
DirBrowseShowSize	(BOOLEAN) True
DirBrowseShowExtension	(BOOLEAN) True
DirBrowseShowLongDate	(BOOLEAN) True
EnableDefaultDoc	(BOOLEAN) True
AuthFlags	(INTEGER) 1
AuthBasic	(BOOLEAN) False

Property	Value
AuthAnonymous	(BOOLEAN) True
AuthNTLM	(BOOLEAN) False
AuthMD5	(BOOLEAN) False
AuthPassport	(BOOLEAN) False
InProcessIsapiApps	(LIST) (6 Items) "%windir%\system32\inetsrv\httpext.dll" "%windir%\system32\inetsrv\httpodbc.dll" "%windir%\system32\inetsrv\ssinc.dll" "%windir%\system32\msw3prt.dll" "%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll"
LogOdbcDataSource	(STRING) "HTTPLOG">
LogOdbcTableName	(STRING) "InternetLog"
LogOdbcUserName	(STRING) "InternetAdmin"
WAMUserName	(STRING) "IWAM_<machinename>">
AuthChangeURL	(STRING) "/iisadmpwd/achg.asp"
AuthExpiredURL	(STRING) "/iisadmpwd/aexp.asp"
AuthNotifyPwdExpURL	(STRING) "/iisadmpwd/annot.asp"
AuthExpiredUnsecureURL	(STRING) "/iisadmpwd/aexp3.asp"
AuthNotifyPwdExpUnsecureURL	(STRING) "/iisadmpwd/annot3.asp"
AppPoolId	(STRING) "DefaultAppPool"
IIs5IsolationModeEnabled	(BOOLEAN) False
MaxGlobalBandwidth	(INTEGER) 4294967295
MinFileBytesPerSec	(INTEGER) 240
LogInUTF8	(BOOLEAN) False
AspAppServiceFlags	(INTEGER) 0
AspEnableTracker	(BOOLEAN) False
AspEnableSxs	(BOOLEAN) False
AspUsePartition	(BOOLEAN) False

Property	Value
AspKeepSessionIDSecure	(INTEGER) 0
AspExecuteInMTA	(INTEGER) 0
CentralBinaryLoggingEnabled	(BOOLEAN) False
AspRunOnEndAnonymously	(BOOLEAN) True
AspBufferingLimit	(INTEGER) 4194304
AspCalcLineNumber	(BOOLEAN) True
ApplicationDependencies	(LIST) (6 Items) "Active Server Pages;ASP" "Internet Data Connector;HTTPODBC" "Server Side Includes;SSINC" "WebDAV;WEBDAV" "ASP.NET v1.1.4322;ASP.NET v1.1.4322"
WebSvcExtRestrictionList	(LIST) (8 Items) "0,*.*.dll" "0,*.*.exe"> "0,<windir>\system32\inetsrv\asp.dll,0,ASP,Active Server Pages"> "0,<windir>\system32\inetsrv\httpodbc.dll,0,HTTPODBC,Internet Data Connector" "0,<windir>\system32\inetsrv\ssinc.dll,0,SSINC,Server Side Includes" "0,<windir>\system32\inetsrv\httpext.dll,0,WEBDAV,WebDAV"> "1,<windir>\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll,0,ASP.NET v2.0.50727,ASP.NET v2.0.50727"
AspMaxRequestEntityAllowed	(INTEGER) 204800
[/w3svc/1]	n/a
[/w3svc/AppPools]	n/a
[/w3svc/Filters]	n/a

Property	Value
[/w3svc/Info]	n/a

Global Properties of the WWW Web site

These properties can be retrieved with the following adsutil command:

adsutil.vbs enum W3SVC/WebSiteID

The properties listed below comprise a partial list.

Property	Value
KeyType	(STRING) "IIsWebServer"
ServerState	(INTEGER) 2
ServerComment	(STRING) "Default Web site"
ServerSize	(INTEGER) 1
ServerBindings	(LIST) (1 Items) ":80:" (or 8530)
SecureBindings	(LIST) (1 Items) ":443:" (or 8531)
ConnectionTimeout	(INTEGER) 180
DefaultDoc	(STRING) "Default.htm,Default.asp,index.htm,iisstart.htm"
AspBufferingOn	(BOOLEAN) False
LogPluginClsid	(STRING) "{FF160663-DE82-11CF-BC0A-00AA006111E0}"
Win32Error	(INTEGER) 0
AppPoolId	(STRING) "DefaultAppPool"

Properties of the API Remoting Web service

Property	Value
KeyType	(STRING) "IIsWebVirtualDir"
AppRoot	(STRING) "/LM/W3SVC/WebSiteID/ROOT/ApiRemoting30"

Property	Value
AppFriendlyName	(STRING) "ApiRemoting30"
AppIsolated	(INTEGER) 2
Path	(STRING) "<WSUSInstallDir>\WebServices\ApiRemoting30"
AccessFlags	(INTEGER) 513
AccessExecute	(BOOLEAN) False
AccessSource	(BOOLEAN) False
AccessRead	(BOOLEAN) True
AccessWrite	(BOOLEAN) False
AccessScript	(BOOLEAN) True
AccessNoRemoteExecute	(BOOLEAN) False
AccessNoRemoteRead	(BOOLEAN) False
AccessNoRemoteWrite	(BOOLEAN) False
AccessNoRemoteScript	(BOOLEAN) False
AccessNoPhysicalDir	(BOOLEAN) False
AspScriptErrorSentToBrowser	(BOOLEAN) False
AspEnableParentPaths	(BOOLEAN) False
AuthFlags	(INTEGER) 21
AuthBasic	(BOOLEAN) False
AuthAnonymous	(BOOLEAN) True
AuthNTLM	(BOOLEAN) True
AuthMD5	(BOOLEAN) True
AuthPassport	(BOOLEAN) False
AppPoolId	(STRING) "WsusPool"

Properties of the Client Web service

Property	Value
KeyType	(STRING) "IIsWebVirtualDir"
AppRoot	(STRING) "/LM/W3SVC/WebsiteID/ROOT/ClientWebService"
AppFriendlyName	(STRING) "ClientWebService"
AppIsolated	(INTEGER) 2
Path	(STRING) "<WSUSInstallDir>\WebServices\ClientWebService"
AccessFlags	(INTEGER) 513
AccessExecute	(BOOLEAN) False
AccessSource	(BOOLEAN) False
AccessRead	(BOOLEAN) True
AccessWrite	(BOOLEAN) False
AccessScript	(BOOLEAN) True
AccessNoRemoteExecute	(BOOLEAN) False
AccessNoRemoteRead	(BOOLEAN) False
AccessNoRemoteWrite	(BOOLEAN) False
AccessNoRemoteScript	(BOOLEAN) False
AccessNoPhysicalDir	(BOOLEAN) False
AspScriptErrorSentToBrowser	(BOOLEAN) False
AspEnableParentPaths	(BOOLEAN) False
AuthFlags	(INTEGER) 1
AuthBasic	(BOOLEAN) False
AuthAnonymous	(BOOLEAN) True
AuthNTLM	(BOOLEAN) False
AuthMD5	(BOOLEAN) False
AuthPassport	(BOOLEAN) False
AppPoolId	(STRING) "WsusPool"

Properties of the Downstream Server Authentication Web service

Property	Value
KeyType	(STRING) "IlsWebVirtualDir"
AppRoot	(STRING) "/LMW3SVC/WebSiteID/ROOT/DssAuthWebService"
AppFriendlyName	(STRING) " DssAuthWebService "
AppIsolated	(INTEGER) 2
Path	(STRING) "<WSUSInstallDir>\WebServices\DssAuthWebService"
AccessFlags	(INTEGER) 513
AccessExecute	(BOOLEAN) False
AccessSource	(BOOLEAN) False
AccessRead	(BOOLEAN) True
AccessWrite	(BOOLEAN) False
AccessScript	(BOOLEAN) True
AccessNoRemoteExecute	(BOOLEAN) False
AccessNoRemoteRead	(BOOLEAN) False
AccessNoRemoteWrite	(BOOLEAN) False
AccessNoRemoteScript	(BOOLEAN) False
AccessNoPhysicalDir	(BOOLEAN) False
AspScriptErrorSentToBrowser	(BOOLEAN) False
AspEnableParentPaths	(BOOLEAN) False
AuthFlags	(INTEGER) 1
AuthBasic	(BOOLEAN) False
AuthAnonymous	(BOOLEAN) True
AuthNTLM	(BOOLEAN) False
AuthMD5	(BOOLEAN) False
AuthPassport	(BOOLEAN) False

Property	Value
AppPoolId	(STRING) "WsusPool"

Properties of the Inventory Collection Web service

Property	Value
KeyType	(STRING) "IlsWebVirtualDir"
AppRoot	(STRING) "/LM/W3SVC/WebsiteID/ROOT/Inventory"
AppFriendlyName	(STRING) "Inventory"
AppIsolated	(INTEGER) 2
Path	(STRING) "<WSUSInstallDir>WebServices\Inventory"
AccessFlags	(INTEGER) 513
AccessExecute	(BOOLEAN) False
AccessSource	(BOOLEAN) False
AccessRead	(BOOLEAN) True
AccessWrite	(BOOLEAN) False
AccessScript	(BOOLEAN) True
AccessNoRemoteExecute	(BOOLEAN) False
AccessNoRemoteRead	(BOOLEAN) False
AccessNoRemoteWrite	(BOOLEAN) False
AccessNoRemoteScript	(BOOLEAN) False
AccessNoPhysicalDir	(BOOLEAN) False
AspScriptErrorSentToBrowser	(BOOLEAN) False
AspEnableParentPaths	(BOOLEAN) False
AuthFlags	(INTEGER) 1
AuthBasic	(BOOLEAN) False
AuthAnonymous	(BOOLEAN) True
AuthNTLM	(BOOLEAN) False

Property	Value
AuthMD5	(BOOLEAN) False
AuthPassport	(BOOLEAN) False
AppPoolId	(STRING) "WsusPool"

Checking the properties of the Reporting Web service

Property	Value
KeyType	(STRING) "IlsWebVirtualDir"
AppRoot	(STRING) "/LM/W3SVC/ <i>WebSiteID</i> /ROOT/ReportingWebService"
AppFriendlyName	(STRING) " ReportingWebService "
AppIsolated	(INTEGER) 2
Path	(STRING) "<WSUSInstallDir>\WebServices\ReportingWebService"
AccessFlags	(INTEGER) 513
AccessExecute	(BOOLEAN) False
AccessSource	(BOOLEAN) False
AccessRead	(BOOLEAN) True
AccessWrite	(BOOLEAN) False
AccessScript	(BOOLEAN) True
AccessNoRemoteExecute	(BOOLEAN) False
AccessNoRemoteRead	(BOOLEAN) False
AccessNoRemoteWrite	(BOOLEAN) False
AccessNoRemoteScript	(BOOLEAN) False
AccessNoPhysicalDir	(BOOLEAN) False
AspScriptErrorSentToBrowser	(BOOLEAN) False
AspEnableParentPaths	(BOOLEAN) False
AuthFlags	(INTEGER) 1

Property	Value
AuthBasic	(BOOLEAN) False
AuthAnonymous	(BOOLEAN) True
AuthNTLM	(BOOLEAN) False
AuthMD5	(BOOLEAN) False
AuthPassport	(BOOLEAN) False
AppPoolId	(STRING) "WsusPool"

Properties of the Selfupdate Web service

Property	Value
KeyType	(STRING) "IIsWebVirtualDir"
Path	(STRING) "<WSUSInstallDir>\WebServices\ServerSyncWebService"
AccessFlags	(INTEGER) 513
AccessExecute	(BOOLEAN) False
AccessSource	(BOOLEAN) False
AccessRead	(BOOLEAN) True
AccessWrite	(BOOLEAN) False
AccessScript	(BOOLEAN) True
AccessNoRemoteExecute	(BOOLEAN) False
AccessNoRemoteRead	(BOOLEAN) False
AccessNoRemoteWrite	(BOOLEAN) False
AccessNoRemoteScript	(BOOLEAN) False
AccessNoPhysicalDir	(BOOLEAN) False

Properties of the Server Synchronization Web service

Property	Value
KeyType	(STRING) "IIsWebVirtualDir"
AppRoot	(STRING) "/LM/W3SVC/WebSiteID/ROOT/ServerSyncWebService"
AppFriendlyName	(STRING) " ServerSyncWebService "
AppIsolated	(INTEGER) 2
Path	(STRING) "<WSUSInstallDir>\WebServices\ServerSyncWebService"
AccessFlags	(INTEGER) 513
AccessExecute	(BOOLEAN) False
AccessSource	(BOOLEAN) False
AccessRead	(BOOLEAN) True
AccessWrite	(BOOLEAN) False
AccessScript	(BOOLEAN) True
AccessNoRemoteExecute	(BOOLEAN) False
AccessNoRemoteRead	(BOOLEAN) False
AccessNoRemoteWrite	(BOOLEAN) False
AccessNoRemoteScript	(BOOLEAN) False
AccessNoPhysicalDir	(BOOLEAN) False
AspScriptErrorSentToBrowser	(BOOLEAN) False
AspEnableParentPaths	(BOOLEAN) False
AuthFlags	(INTEGER) 1
AuthBasic	(BOOLEAN) False
AuthAnonymous	(BOOLEAN) True
AuthNTLM	(BOOLEAN) False
AuthMD5	(BOOLEAN) False
AuthPassport	(BOOLEAN) False
AppPoolId	(STRING) "WsusPool"

Properties of the Simple Authorization Web service

Property	Value
KeyType	(STRING) "IIsWebVirtualDir"
AppRoot	(STRING) "/LM/W3SVC/WebSiteID/ROOT/SimpleAuthWebService"
AppFriendlyName	(STRING) "SimpleAuthWebService"
AppIsolated	(INTEGER) 2
Path	(STRING) "<WSUSInstallDir>\WebServices\SimpleAuthWebService"
AccessFlags	(INTEGER) 513
AccessExecute	(BOOLEAN) False
AccessSource	(BOOLEAN) False
AccessRead	(BOOLEAN) True
AccessWrite	(BOOLEAN) False
AccessScript	(BOOLEAN) True
AccessNoRemoteExecute	(BOOLEAN) False
AccessNoRemoteRead	(BOOLEAN) False
AccessNoRemoteWrite	(BOOLEAN) False
AccessNoRemoteScript	(BOOLEAN) False
AccessNoPhysicalDir	(BOOLEAN) False
AspScriptErrorSentToBrowser	(BOOLEAN) False
AspEnableParentPaths	(BOOLEAN) False
AuthFlags	(INTEGER) 1
AuthBasic	(BOOLEAN) False
AuthAnonymous	(BOOLEAN) True
AuthNTLM	(BOOLEAN) False
AuthMD5	(BOOLEAN) False
AuthPassport	(BOOLEAN) False

Property	Value
AppPoolId	(STRING) "WsusPool"

Appendix D: Permissions on WSUS Directories and Registry Keys

Troubleshooting Web services often involves checking permissions on related directories and registry keys. The following sections will explain in detail how to check permissions on WSUS Web services directories and registry keys.

The `cacls` system command

The `cacls` system command displays or modifies file or directory access control lists (ACLs). The output of this command specifies the level of access (f=full control, w=write, r=read, n=none) and whether or not the access is inherited by subdirectories (OI=this folder and files, CI=this folder and subfolders, IO=does not apply). See the [cacls command reference](http://go.microsoft.com/fwlink/?LinkId=81084) (<http://go.microsoft.com/fwlink/?LinkId=81084>) for more information.

The WSUS installation creates several Web service directories.

- `WSUSInstallDir\WebServices\apiremoting30` (where `WSUSInstallDir` is the directory where WSUS has been installed)
- `WSUSInstallDir\WebServices\clientwebservice`
- `WSUSInstallDir\WebServices\dssauthwebservice`
- `WSUSInstallDir\WebServices\reportingwebservice`
- `WSUSInstallDir\WebServices\serversyncwebservice`
- `WSUSInstallDir\WebServices\simpleauthwebservice`
- `WSUSInstallDir\Inventory`
- `WSUSInstallDir\Selfupdate`

All of the directories above (except for the self-update directory) should have the following ACLs:

- NT AUTHORITY\NETWORK SERVICE:(OI)(CI)R
- BUILTIN\Users:(OI)(CI)R
- NT AUTHORITY\Authenticated Users:(OI)(CI)R
- BUILTIN\Administrators:(OI)(CI)F
- NT AUTHORITY\SYSTEM:(OI)(CI)F
- The self-update directory should have the following ACLs:
- BUILTIN\Users:(OI)(CI)R
- BUILTIN\Administrators:(OI)(CI)F

- NT AUTHORITY\SYSTEM:(OI)(CI)F

Permissions on WSUS registry keys

The following permissions are set for the registry during WSUS setup.

- The **Users** and **WSUS Reporters** group must have Read access to the **\HKLM\Software\Microsoft\Update Services\Server** registry key.
- The following accounts must have Full Control permissions to the **\HKLM\Software\Microsoft\Update Services\Server\Setup** registry key:
 - **Network Service**
 - **WSUS Administrators**
 - **Administrators**
 - **System**

Appendix E: Configuring BITS 2.0 and 3.0 for Download Performance

BITS (Background Intelligent Transfer Service) is the service that Windows Update and Microsoft Update use for downloads. BITS 2.0 is available for download on Windows XP and Windows Server 2003 operating systems, and BITS 3.0 is part of the Windows Vista and Windows 2008 operating systems. You can optimize the performance of downloads by configuring BITS through Group Policy. BITS 3.0 offers a number of configurable features that do not exist in earlier versions of BITS.

For more information about BITS, see [Background Intelligent Transfer Service](http://go.microsoft.com/fwlink/?LinkId=79389) (<http://go.microsoft.com/fwlink/?LinkId=79389>).

Throttling

Versions of BITS use the computer's network card to measure network traffic. BITS 3.0 can also use the Internet gateway device to monitor traffic if the computer is correctly configured; see [Background Intelligent Transfer Service](http://go.microsoft.com/fwlink/?LinkId=79389) (<http://go.microsoft.com/fwlink/?LinkId=79389>) for details. However, in some situations the network card in itself does not give an accurate measurement of the actual state of network traffic. For example, if a computer has a fast network card but a slow network connection (such as a dial-up connection), BITS will give an overly optimistic measurement. It is possible to use Group Policy (in both BITS 2.0 and 3.0) to throttle or limit the network bandwidth that BITS uses for downloads or uploads.



Note

BITS bandwidth limitations are system wide, not application specific. You cannot use this setting to limit only WSUS download bandwidth, because the BITS settings will affect BITS in any application.

► To set BITS bandwidth limitations

1. Start the Group Policy Object Editor (click **Start**, click **Run**, and then type **gpedit.msc**).
2. Expand **Computer Configuration**, then **Administrative Templates**, then **Network**, then **Background Intelligent Transfer Service**.
3. Open the **Maximum network bandwidth that BITS uses** (BITS 2.0) or **Maximum network bandwidth for BITS background transfers** (BITS 3.0) setting.
4. Set the transfer rate in kilobits per second that you want BITS to use (the default is 10).
5. Set the times at which you want to limit the bandwidth (the default is 8:00 A.M. to 5:00 P.M.).
6. Set the limitations to be used outside of the designated time (the default is **Use all available unused bandwidth**, but you may select another limitation).
7. Click **OK**.



Note

You must be an administrator to perform this procedure.

Peer caching

Peer caching is a new feature of BITS 3.0 that allows *peers* (computers within the same subnet of a network that have the peer caching feature enabled) to share files. If peer caching is enabled on a computer, the Automatic Update agent instructs BITS to make downloaded files available to that computer's peers as well.

When the files have been downloaded, BITS caches them. When another (peer caching-enabled) computer tries to download the same update, BITS on that computer sends a multicast request to all of that computer's peers. If one or more of the peers responds to the request, BITS will download the file from the first computer to respond. If the download from the peer fails or take too long, BITS continues the download from the WSUS server or Microsoft Update.

This feature of BITS can optimize the bandwidth used by WSUS in several ways.

1. Peer caching decreases the amount of data transferred from the WSUS server to its clients, because computers in the same subnet will usually download the updates from each other.
2. Peer caching decreases the amount of data transferred across the WAN when some or all of the clients of a WSUS server are located in different locations.
3. Peer caching decreases the amount of data transferred across the Internet if WSUS clients in the same subnet are configured to download updates from Microsoft Update.



Note

BITS peer caching requires computers to be running Windows Vista or Windows Server 2008, and to be part of an Active Directory Domain.

For more information about peer caching and peer servers, see [Peer Caching](http://go.microsoft.com/fwlink/?LinkId=79432) (<http://go.microsoft.com/fwlink/?LinkId=79432>).

▶ **To enable peer caching (on Windows Vista)**

1. Start the Group Policy Object Editor (click **Start**, click **Run**, and then type **gpedit.msc**).
2. Expand **Computer Configuration**, then **Administrative Templates**, then **Network**, then **Background Intelligent Transfer Service**.
3. Enable the **Allow BITS Peercaching** setting.
4. Enable the **Maximum network bandwidth used for Peercaching** setting, and set the maximum bandwidth in bits per second (the default is 104857), then click **OK**.
5. Enable the **Limit the BITS Peercache size** setting, and set the percentage of disk space to be used for the peer cache (the default is 5 percent), and then click **OK**.
6. Enable the **Limit age of items in the BITS Peercache** setting, and set the number of days (the default is 90), and then click **OK**.



Note

You must be an administrator to perform this procedure.

Appendix F: Configuring IIS for Download Performance

You can limit the bandwidth for all Web sites or a specific Web site, such as the WSUS Web site, using IIS Manager.

Limiting bandwidth on all Web sites

▶ **To limit bandwidth on all Web sites (on Windows Server 2003)**

1. Open IIS Manager (click **Start**, click **Administrative Tools**, and then click **Internet Information (IIS) Manager**).
2. Navigate to the **Web Sites** node under the local computer, right-click the node, and then click **Properties**.
3. Select the **Performance** tab.
4. Under **Bandwidth throttling**, select **Limit the total network bandwidth available for all Web sites on this server**, and then specify the maximum bandwidth in kilobytes per second (the default is 1024). You cannot specify a bandwidth lower than 1024 kilobytes per second.
5. Click **OK**.

 **Note**

You must be logged on as an administrator or have run IIS as an administrator to perform this procedure.

Limiting bandwidth on a specific Web site

▶ **To limit bandwidth on a specific Web site (on Windows Server 2003)**

1. Open IIS Manager (click **Start**, click **Administrative Tools**, and then click **Internet Information (IIS) Manager**).
2. Navigate to the **Web Sites** node under the local computer, select the specific Web site, right-click the node, and then click **Properties**.
3. Select the **Performance** tab.
4. Under **Bandwidth throttling**, select **Limit the total network bandwidth available for all Web sites on this server**, and then specify the maximum bandwidth in kilobytes per second (the default is 1024). You cannot specify a bandwidth lower than 1024 kilobytes per second.
5. Click **OK**.

 **Note**

You must be logged on as an administrator or have run IIS as an administrator to perform this procedure.

Appendix G: Windows Update Agent Result Codes

The Windows Update Agent uses the following set of result codes.

Windows Update Agent result codes

The tables in this section show the result code (hexadecimal value), the corresponding string, and the description.

The following table shows WUA success codes.

Result Code	Result String	Description
0x240001	WU_S_SERVICE_STOP	Windows Update Agent was stopped successfully.
0x240002	WU_S_SELFUPDATE	Windows Update Agent

Result Code	Result String	Description
		updated itself.
0x240003	WU_S_UPDATE_ERROR	Operation completed successfully but there were errors applying the updates..
0x240004	WU_S_MARKED_FOR_DISCONNECT	A callback was marked to be disconnected later because the request to disconnect the operation came while a callback was executing.
0x240005	WU_S_REBOOT_REQUIRED	The system must be restarted to complete installation of the update.
0x240006	WU_S_ALREADY_INSTALLED	The update to be installed is already installed on the system.
0x240007	WU_S_ALREADY_UNINSTALLED	The update to be removed is not installed on the system.
0x240008	WU_S_ALREADY_DOWNLOADED	The update to be downloaded has already been downloaded.

The following table shows WUA error codes.

Result Code	Result String	Description
0x80240001	WU_E_NO_SERVICE	Windows Update Agent was unable to provide the service.
0x80240002	WU_E_MAX_CAPACITY_REACHED	The maximum capacity of the service was exceeded.
0x80240003	WU_E_UNKNOWN_ID	An ID cannot be found.
0x80240004	WU_E_NOT_INITIALIZED	The object could not be initialized.

Result Code	Result String	Description
0x80240005	WU_E_RANGEOVERLAP	The update handler requested a byte range overlapping a previously requested range.
0x80240006	WU_E_TOOMANYRANGES	The requested number of byte ranges exceeds the maximum number ($2^{31} - 1$).
0x80240007	WU_E_INVALIDINDEX	The index to a collection was invalid.
0x80240008	WU_E_ITEMNOTFOUND	The key for the item queried could not be found.
0x80240009	WU_E_OPERATIONINPROGRESS	Another conflicting operation was in progress. Some operations such as installation cannot be performed twice simultaneously.
0x8024000A	WU_E_COULDNOTCANCEL	Cancellation of the operation was not allowed.
0x8024000B	WU_E_CALL_CANCELLED	Operation was cancelled.
0x8024000C	WU_E_NOOP	No operation was required.
0x8024000D	WU_E_XML_MISSINGDATA	Windows Update Agent could not find required information in the update's XML data.
0x8024000E	WU_E_XML_INVALID	Windows Update Agent found invalid information in the update's XML data.
0x8024000F	WU_E_CYCLE_DETECTED	Circular update relationships were detected in the metadata.
0x80240010	WU_E_TOO_DEEP_RELATION	Update relationships too deep to evaluate were evaluated.
0x80240011	WU_E_INVALID_RELATIONSHIP	An invalid update relationship was detected.
0x80240012	WU_E_REG_VALUE_INVALID	An invalid registry value was read.

Result Code	Result String	Description
0x80240013	WU_E_DUPLICATE_ITEM	Operation tried to add a duplicate item to a list.
0x80240016	WU_E_INSTALL_NOT_ALLOWED	Operation tried to install while another installation was in progress or the system was pending a mandatory restart.
0x80240017	WU_E_NOT_APPLICABLE	Operation was not performed because there are no applicable updates.
0x80240018	WU_E_NO_USERTOKEN	Operation failed because a required user token is missing.
0x80240019	WU_E_EXCLUSIVE_INSTALL_CONFLICT	An exclusive update cannot be installed with other updates at the same time.
0x8024001A	WU_E_POLICY_NOT_SET	A policy value was not set.
0x8024001B	WU_E_SELFUPDATE_IN_PROGRESS	The operation could not be performed because the Windows Update Agent is self-updating.
0x8024001D	WU_E_INVALID_UPDATE	An update contains invalid metadata.
0x8024001E	WU_E_SERVICE_STOP	Operation did not complete because the service or system was being shut down.
0x8024001F	WU_E_NO_CONNECTION	Operation did not complete because the network connection was unavailable.
0x80240020	WU_E_NO_INTERACTIVE_USER	Operation did not complete because there is no logged-on interactive user.
0x80240021	WU_E_TIME_OUT	Operation did not complete because it timed out.
0x80240022	WU_E_ALL_UPDATES_FAILED	Operation failed for all the updates.

Result Code	Result String	Description
0x80240023	WU_E_EULAS_DECLINED	The license terms for all updates were declined.
0x80240024	WU_E_NO_UPDATE	There are no updates.
0x80240025	WU_E_USER_ACCESS_DISABLED	Group Policy settings prevented access to Windows Update.
0x80240026	WU_E_INVALID_UPDATE_TYPE	The type of update is invalid.
0x80240027	WU_E_URL_TOO_LONG	The URL exceeded the maximum length.
0x80240028	WU_E_UNINSTALL_NOT_ALLOWED	The update could not be uninstalled because the request did not originate from a WSUS server.
0x80240029	WU_E_INVALID_PRODUCT_LICENSE	Search may have missed some updates before there is an unlicensed application on the system.
0x8024002A	WU_E_MISSING_HANDLER	A component required to detect applicable updates was missing.
0x8024002B	WU_E_LEGACYSERVER	An operation did not complete because it requires a newer version of server.
0x8024002C	WU_E_BIN_SOURCE_ABSENT	A delta-compressed update could not be installed because it required the source.
0x8024002D	WU_E_SOURCE_ABSENT	A full-file update could not be installed because it required the source.
0x8024002E	WU_E_WU_DISABLED	Access to an unmanaged server is not allowed.
0x8024002F	WU_E_CALL_CANCELLED_BY_POLICY	Operation did not complete because the DisableWindowsUpdateAccess policy was set.
0x802400	WU_E_INVALID_PROXY_SERVER	The format of the proxy list was

Result Code	Result String	Description
30		invalid.
0x80240031	WU_E_INVALID_FILE	The file is in the wrong format.
0x80240032	WU_E_INVALID_CRITERIA	The search criteria string was invalid.
0x80240033	WU_E_EULA_UNAVAILABLE	License terms could not be downloaded.
0x80240034	WU_E_DOWNLOAD_FAILED	Update failed to download.
0x80240035	WU_E_UPDATE_NOT_PROCESSED	The update was not processed.
0x80240036	WU_E_INVALID_OPERATION	The object's current state did not allow the operation.
0x80240037	WU_E_NOT_SUPPORTED	The functionality for the operation is not supported.
0x80240038	WU_E_WINHTTP_INVALID_FILE	The downloaded file has an unexpected content type.
0x80240039	WU_E_TOO_MANY_RESYNC	Agent is asked by server to resync too many times.
0x80240040	WU_E_NO_SERVER_CORE_SUPPORT	WUA API method does not run on Server Core installation.
0x80240041	WU_E_SYSPREP_IN_PROGRESS	Service is not available while sysprep is running.
0x80240042	WU_E_UNKNOWN_SERVICE	The update service is no longer registered with AU.
0x80240FFF	WU_E_UNEXPECTED	An operation failed due to reasons not covered by another error code.
0x80241001	WU_E_MSI_WRONG_VERSION	Search may have missed some updates because the Windows Installer is less than version 3.1.
0x80241002	WU_E_MSI_NOT_CONFIGURED	Search may have missed some updates because the Windows Installer is not configured.

Result Code	Result String	Description
0x80241003	WU_E_MSP_DISABLED	Search may have missed some updates because policy has disabled Windows Installer patching.
0x80241004	WU_E_MSI_WRONG_APP_CONTEXT	An update could not be applied because the application is installed per-user.
0x80241FFF	WU_E_MSP_UNEXPECTED	Search may have missed some updates because there was a failure of the Windows Installer.
0x80242000	WU_E_UH_REMOTEUNAVAILABLE	A request for a remote update handler could not be completed because no remote process is available.
0x80242001	WU_E_UH_LOCALONLY	A request for a remote update handler could not be completed because the handler is local only.
0x80242002	WU_E_UH_UNKNOWNHANDLER	A request for an update handler could not be completed because the handler could not be recognized.
0x80242003	WU_E_UH_REMOTEALREADYACTIVE	A remote update handler could not be created because one already exists.
0x80242004	WU_E_UH_DOESNOTSUPPORTACTION	A request for the handler to install (uninstall) an update could not be completed because the update does not support install (uninstall).
0x80242005	WU_E_UH_WRONGHANDLER	An operation did not complete because the wrong handler was specified.
0x80242006	WU_E_UH_INVALIDMETADATA	A handler operation could not be completed because the update contains invalid metadata.
0x80242007	WU_E_UH_INSTALLERHUNG	An operation could not be completed because the installer

Result Code	Result String	Description
		exceeded the time limit.
0x80242008	WU_E_UH_OPERATIONCANCELLED	An operation being done by the update handler was cancelled.
0x80242009	WU_E_UH_BADHANDLERXML	An operation could not be completed because the handler-specific metadata is invalid.
0x8024200A	WU_E_UH_CANREQUIREINPUT	A request to the handler to install an update could not be completed because the update requires user input.
0x8024200B	WU_E_UH_INSTALLERFAILURE	The installer failed to install (uninstall) one or more updates.
0x8024200C	WU_E_UH_FALLBACKTOSELFCONTAINED	The update handler should download self-contained content rather than delta-compressed content for the update.
0x8024200D	WU_E_UH_NEEDANOTHERDOWNLOAD	The update handler did not install the update because it needs to be downloaded again.
0x8024200E	WU_E_UH_NOTIFYFAILURE	The update handler failed to send notification of the status of the install (uninstall) operation.
0x8024200F	WU_E_UH_INCONSISTENT_FILE_NAMES	The file names contained in the update metadata and in the update package are inconsistent.
0x80242010	WU_E_UH_FALLBACKERROR	The update handler failed to fall back to the self-contained content.
0x80242011	WU_E_UH_TOOMANYDOWNLOADREQUESTS	The update handler has exceeded the maximum number of download requests.
0x80242012	WU_E_UH_UNEXPECTEDCBSRESPONSE	The update handler has received an unexpected response from CBS.
0x80242013	WU_E_UH_BADCBSPACKAGEID	The update metadata contains an invalid CBS package identifier.

Result Code	Result String	Description
0x80242014	WU_E_UH_POSTREBOOTSTILLPENDING	The post-reboot operation for the update is still in progress.
0x80242015	WU_E_UH_POSTREBOOTRESULTUNKNOWN	The result of the post-reboot operation for the update could not be determined.
0x80242016	WU_E_UH_POSTREBOOTUNEXPECTEDSTATE	The state of the update after its post-reboot operation has completed is unexpected.
0x80242017	WU_E_UH_NEW_SERVICING_STACK_REQUIRED	The operating system servicing stack must be updated before this update is downloaded or installed.
0x80242FFF	WU_E_UH_UNEXPECTED	An update handler error not covered by another WU_E_UH_* code.
0x80243001	WU_E_INSTALLATION_RESULTS_UNKNOWN_VERSION	The results of download and installation could not be read from the registry due to an unrecognized data format version.
0x80243002	WU_E_INSTALLATION_RESULTS_INVALID_DATA	The results of download and installation could not be read from the registry due to an invalid data format.
0x80243003	WU_E_INSTALLATION_RESULTS_NOT_FOUND	The results of download and installation are not available; the operation may have failed to start.
0x80243004	WU_E_TRAYICON_FAILURE	A failure occurred when trying to create an icon in the taskbar notification area.
0x80243FFD	WU_E_NON_UI_MODE	Unable to show UI when in non-UI mode; WU client UI modules may not be installed.
0x80243F FE	WU_E_WUCLTUI_UNSUPPORTED_VERSION	Unsupported version of WU client UI exported functions.
0x80243FFF	WU_E_AUCLIENT_UNEXPECTED	There was a user interface error not covered by another WU_E_AUCLIENT_* error code.

Result Code	Result String	Description
0x80244000	WU_E_PT_SOAPCLIENT_BASE	WU_E_PT_SOAPCLIENT_* error codes map to the SOAPCLIENT_ERROR enum of the ATL Server Library.
0x80244001	WU_E_PT_SOAPCLIENT_INITIALIZE	SOAPCLIENT_INITIALIZE_ERROR - initialization of the SOAP client failed, possibly because of an MSXML installation failure.
0x80244002	WU_E_PT_SOAPCLIENT_OUTOFMEMORY	SOAPCLIENT_OUTOFMEMORY - SOAP client failed because it ran out of memory.
0x80244003	WU_E_PT_SOAPCLIENT_GENERATE	SOAPCLIENT_GENERATE_ERROR - SOAP client failed to generate the request.
0x80244004	WU_E_PT_SOAPCLIENT_CONNECT	SOAPCLIENT_CONNECT_ERROR - SOAP client failed to connect to the server.
0x80244005	WU_E_PT_SOAPCLIENT_SEND	SOAPCLIENT_SEND_ERROR - SOAP client failed to send a message for reasons of WU_E_WINHTTP_* error codes.
0x80244006	WU_E_PT_SOAPCLIENT_SERVER	SOAPCLIENT_SERVER_ERROR - SOAP client failed because there was a server error.
0x80244007	WU_E_PT_SOAPCLIENT_SOAPFAULT	SOAPCLIENT_SOAPFAULT - SOAP client failed because there was a SOAP fault for reasons of WU_E_PT_SOAP_* error codes.
0x80244008	WU_E_PT_SOAPCLIENT_PARSEFAULT	SOAPCLIENT_PARSEFAULT_ERROR - SOAP client failed to parse a SOAP fault.
0x80244009	WU_E_PT_SOAPCLIENT_READ	SOAPCLIENT_READ_ERROR - SOAP client failed while reading the response from the server.
0x802440	WU_E_PT_SOAPCLIENT_PARSE	SOAPCLIENT_PARSE_ERROR - SOAP client failed to parse the

Result Code	Result String	Description
0A		response from the server.
0x802440 0B	WU_E_PT_SOAP_VERSION	SOAP_E_VERSION_MISMATCH - SOAP client found an unrecognizable namespace for the SOAP envelope.
0x802440 0C	WU_E_PT_SOAP_MUST_UNDERSTAND	SOAP_E_MUST_UNDERSTAND - SOAP client was unable to understand a header.
0x802440 0D	WU_E_PT_SOAP_CLIENT	SOAP_E_CLIENT - SOAP client found the message was malformed; fix before resending.
0x802440 0E	WU_E_PT_SOAP_SERVER	SOAP_E_SERVER - The SOAP message could not be processed due to a server error; resend later.
0x802440 0F	WU_E_PT_WMI_ERROR	There was an unspecified Windows Management Instrumentation (WMI) error.
0x802440 10	WU_E_PT_EXCEEDED_MAX_SERVER_TRIPS	The number of round trips to the server exceeded the maximum limit.
0x802440 11	WU_E_PT_SUS_SERVER_NOT_SET	WU Server policy value is missing in the registry.
0x802440 12	WU_E_PT_DOUBLE_INITIALIZATION	Initialization failed because the object was already initialized.
0x802440 13	WU_E_PT_INVALID_COMPUTER_NAME	The computer name could not be determined.
0x802440 15	WU_E_PT_REFRESH_CACHE_REQUIRED	The reply from the server indicates that the server was changed or the cookie was invalid; refresh the state of the internal cache and retry.
0x802440 16	WU_E_PT_HTTP_STATUS_BAD_REQUEST	HTTP 400 - the server could not process the request due to invalid syntax.
0x802440 17	WU_E_PT_HTTP_STATUS_DENIED	HTTP 401 - the requested resource requires user authentication.

Result Code	Result String	Description
0x802440 18	WU_E_PT_HTTP_STATUS_FORBIDDEN	HTTP 403 - server understood the request, but declined to fulfill it.
0x802440 19	WU_E_PT_HTTP_STATUS_NOT_FOUND	HTTP 404 - the server cannot find the requested URI (Uniform Resource Identifier).
0x802440 1A	WU_E_PT_HTTP_STATUS_BAD_METHOD	HTTP 405 - the HTTP method is not allowed.
0x802440 1B	WU_E_PT_HTTP_STATUS_PROXY_AUTH_REQ	HTTP 407 - proxy authentication is required.
0x802440 1C	WU_E_PT_HTTP_STATUS_REQUEST_TIMEOUT	HTTP 408 - the server timed out waiting for the request.
0x802440 1D	WU_E_PT_HTTP_STATUS_CONFLICT	HTTP 409 - the request was not completed due to a conflict with the current state of the resource.
0x802440 1E	WU_E_PT_HTTP_STATUS_GONE	HTTP 410 - requested resource is no longer available at the server.
0x802440 1F	WU_E_PT_HTTP_STATUS_SERVER_ERROR	HTTP 500 - an error internal to the server prevented fulfilling the request.
0x802440 20	WU_E_PT_HTTP_STATUS_NOT_SUPPORTED	HTTP 501 - server does not support the functionality required to fulfill the request.
0x802440 21	WU_E_PT_HTTP_STATUS_BAD_GATEWAY	HTTP 502 - the server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
0x802440 22	WU_E_PT_HTTP_STATUS_SERVICE_UNAVAILABLE	HTTP 503 - the service is temporarily overloaded.
0x802440 23	WU_E_PT_HTTP_STATUS_GATEWAY_TIMEOUT	HTTP 504 - the request was timed out waiting for a gateway.
0x802440 24	WU_E_PT_HTTP_STATUS_VERSION_NOT_SUPPORTED	HTTP 505 - the server does not support the HTTP protocol version used for the request.

Result Code	Result String	Description
0x80244025	WU_E_PT_FILE_LOCATIONS_CHANGED	Operation failed due to a changed file location; refresh internal state and resend.
0x80244026	WU_E_PT_REGISTRATION_NOT_SUPPORTED	Operation failed because Windows Update Agent does not support registration with a non-WSUS server.
0x80244027	WU_E_PT_NO_AUTH_PLUGINS_REQUESTED	The server returned an empty authentication information list.
0x80244028	WU_E_PT_NO_AUTH_COOKIES_CREATED	Windows Update Agent was unable to create any valid authentication cookies.
0x80244029	WU_E_PT_INVALID_CONFIG_PROP	A configuration property value was wrong.
0x8024402A	WU_E_PT_CONFIG_PROP_MISSING	A configuration property value was missing.
0x8024402B	WU_E_PT_HTTP_STATUS_NOT_MAPPED	The HTTP request could not be completed and the reason did not correspond to any of the WU_E_PT_HTTP_* error codes.
0x8024402C	WU_E_PT_WINHTTP_NAME_NOT_RESOLVED	ERROR_WINHTTP_NAME_NOT_RESOLVED - the proxy server or target server name cannot be resolved.
0x8024402F	WU_E_PT_ECP_SUCCEEDED_WITH_ERRORS	External cab file processing completed with some errors.
0x80244030	WU_E_PT_ECP_INIT_FAILED	The external cab processor initialization did not complete.
0x80244031	WU_E_PT_ECP_INVALID_FILE_FORMAT	The format of a metadata file was invalid.
0x80244032	WU_E_PT_ECP_INVALID_METADATA	External cab processor found invalid metadata.
0x80244033	WU_E_PT_ECP_FAILURE_TO_EXTRACT_DIGEST	The file digest could not be extracted from an external cab file.

Result Code	Result String	Description
0x80244034	WU_E_PT_ECP_FAILURE_TO_DECOMPRESS_CAB_FILE	An external cab file could not be decompressed.
0x80244035	WU_E_PT_ECP_FILE_LOCATION_ERROR	External cab processor was unable to get file locations.
0x80244FFF	WU_E_PT_UNEXPECTED	A communication error not covered by another WU_E_PT_* error code
0x80245001	WU_E_REDIRECTOR_LOAD_XML	The redirector XML document could not be loaded into the DOM class.
0x80245002	WU_E_REDIRECTOR_S_FALSE	The redirector XML document is missing some required information.
0x80245003	WU_E_REDIRECTOR_ID_SMALLER	The redirector ID in the downloaded redirector cab is less than in the cached cab.
0x8024502D	WU_E_PT_SAME_REDIR_ID	Windows Update Agent failed to download a redirector cabinet file with a new redirector ID value from the server during the recovery.
0x8024502E	WU_E_PT_NO_MANAGED_RECOVER	A redirector recovery action did not complete because the server is managed.
0x80245FFF	WU_E_REDIRECTOR_UNEXPECTED	The redirector failed for reasons not covered by another WU_E_REDIRECTOR_* error code.
0x80246001	WU_E_DM_URLNOTAVAILABLE	A download manager operation could not be completed because the requested file does not have a URL.
0x80246002	WU_E_DM_INCORRECTFILEHASH	A download manager operation could not be completed because the file digest was not recognized.
0x80246003	WU_E_DM_UNKNOWNALGORITHM	A download manager operation could not be completed because the file metadata requested an unrecognized hash algorithm.

Result Code	Result String	Description
0x80246004	WU_E_DM_NEEDDOWNLOADREQUEST	An operation could not be completed because a download request is required from the download handler.
0x80246005	WU_E_DM_NONETWORK	A download manager operation could not be completed because the network connection was unavailable.
0x80246006	WU_E_DM_WRONGBITSVERSION	A download manager operation could not be completed because the version of Background Intelligent Transfer Service (BITS) is incompatible.
0x80246007	WU_E_DM_NOTDOWNLOADED	The update has not been downloaded.
0x80246008	WU_E_DM_FAILTOCONNECTTOBITS	A download manager operation failed because the download manager was unable to connect the Background Intelligent Transfer Service (BITS).
0x80246009	WU_E_DM_BITSTRANSFERERROR	A download manager operation failed because there was an unspecified Background Intelligent Transfer Service (BITS) transfer error.
0x8024600a	WU_E_DM_DOWNLOADLOCATIONCHANGED	A download must be restarted because the location of the source of the download has changed.
0x8024600B	WU_E_DM_CONTENTCHANGED	A download must be restarted because the update content changed in a new revision.
0x80246FFF	WU_E_DM_UNEXPECTED	There was a download manager error not covered by another WU_E_DM_* error code.
0x80247001	WU_E_OL_INVALID_SCANFILE	An operation could not be completed because the scan

Result Code	Result String	Description
		package was invalid.
0x80247002	WU_E_OL_NEWCLIENT_REQUIRED	An operation could not be completed because the scan package requires a greater version of the Windows Update Agent.
0x80247FFF	WU_E_OL_UNEXPECTED	Search using the scan package failed.
0x80248000	WU_E_DS_SHUTDOWN	An operation failed because Windows Update Agent is shutting down.
0x80248001	WU_E_DS_INUSE	An operation failed because the data store was in use.
0x80248002	WU_E_DS_INVALID	The current and expected states of the data store do not match.
0x80248003	WU_E_DS_TABLEMISSING	The data store is missing a table.
0x80248004	WU_E_DS_TABLEINCORRECT	The data store contains a table with unexpected columns.
0x80248005	WU_E_DS_INVALIDTABLENAME	A table could not be opened because the table is not in the data store.
0x80248006	WU_E_DS_BADVERSION	The current and expected versions of the data store do not match.
0x80248007	WU_E_DS_NODATA	The information requested is not in the data store.
0x80248008	WU_E_DS_MISSINGDATA	The data store is missing required information or has a NULL in a table column that requires a non-null value.
0x80248009	WU_E_DS_MISSINGREF	The data store is missing required information or has a reference to missing license terms, file, localized property or linked row.
0x802480	WU_E_DS_UNKNOWNHANDLER	The update was not processed

Result Code	Result String	Description
0A		because its update handler could not be recognized.
0x802480 0B	WU_E_DS_CANTDELETE	The update was not deleted because it is still referenced by one or more services.
0x802480 0C	WU_E_DS_LOCKTIMEOUTEXPIRED	The data store section could not be locked within the allotted time.
0x802480 0D	WU_E_DS_NOCATEGORIES	The category was not added because it contains no parent categories and is not a top-level category itself.
0x802480 0E	WU_E_DS_ROWEXISTS	The row was not added because an existing row has the same primary key.
0x802480 0F	WU_E_DS_STOREFILELOCKED	The data store could not be initialized because it was locked by another process.
0x802480 10	WU_E_DS_CANNOTREGISTER	The data store is not allowed to be registered with COM in the current process.
0x802480 11	WU_E_DS_UNABLETOSTART	Could not create a data store object in another process.
0x802480 13	WU_E_DS_DUPLICATEUPDATEID	The server sent the same update to the client with two different revision IDs.
0x802480 14	WU_E_DS_UNKNOWNSERVICE	An operation did not complete because the service is not in the data store.
0x802480 15	WU_E_DS_SERVICEEXPIRED	An operation did not complete because the registration of the service has expired.
0x802480 16	WU_E_DS_DECLINENOTALLOWED	A request to hide an update was declined because it is a mandatory update or because it was deployed with a deadline.

Result Code	Result String	Description
0x80248017	WU_E_DS_TABLESESSIONMISMATCH	A table was not closed because it is not associated with the session.
0x80248018	WU_E_DS_SESSIONLOCKMISMATCH	A table was not closed because it is not associated with the session.
0x80248019	WU_E_DS_NEEDWINDOWSSERVICE	A request to remove the Windows Update service or to unregister it with Automatic Updates was declined because it is a built-in service and/or Automatic Updates cannot fall back to another service.
0x8024801A	WU_E_DS_INVALIDOPERATION	A request was declined because the operation is not allowed.
0x8024801B	WU_E_DS_SCHEMAMISMATCH	The schema of the current data store and the schema of a table in a backup XML document do not match.
0x8024801C	WU_E_DS_RESETPREQUIRED	The data store requires a session reset; release the session and retry with a new session.
0x8024801D	WU_E_DS_IMPERSONATED	A data store operation did not complete because it was requested with an impersonated identity.
0x80248FFF	WU_E_DS_UNEXPECTED	A data store error not covered by another WU_E_DS_* code.
0x80249001	WU_E_INVENTORY_PARSEFAILED	Parsing of the rule file failed.
0x80249002	WU_E_INVENTORY_GET_INVENTORY_TYPE_FAILED	Failed to get the requested inventory type from the server.
0x80249003	WU_E_INVENTORY_RESULT_UPLOAD_FAILED	Failed to upload inventory result to the server.
0x80249004	WU_E_INVENTORY_UNEXPECTED	There was an inventory error not covered by another error code.
0x80249005	WU_E_INVENTORY_WMI_ERROR	A WMI error occurred when enumerating the instances for a

Result Code	Result String	Description
		particular class.
0x8024A000	WU_E_AU_NOSERVICE	Automatic Updates was unable to service incoming requests.
0x8024A002	WU_E_AU_NONLEGACYSERVER	The old version of the Automatic Updates client has stopped because the WSUS server has been upgraded.
0x8024A003	WU_E_AU_LEGACYCLIENTDISABLED	The old version of the Automatic Updates client was disabled.
0x8024A004	WU_E_AU_PAUSED	Automatic Updates was unable to process incoming requests because it was paused.
0x8024A005	WU_E_AU_NO_REGISTERED_SERVICE	No unmanaged service is registered with AU.
0x8024AFF	WU_E_AU_UNEXPECTED	An Automatic Updates error not covered by another WU_E_AU * code.
0x8024C001	WU_E_DRV_PRUNED	A driver was skipped.
0x8024C002	WU_E_DRV_NOPROP_OR_LEGACY	A property for the driver could not be found. It may not conform with required specifications.
0x8024C003	WU_E_DRV_REG_MISMATCH	The registry type read for the driver does not match the expected type.
0x8024C004	WU_E_DRV_NO_METADATA	The driver update is missing metadata.
0x8024C005	WU_E_DRV_MISSING_ATTRIBUTE	The driver update is missing a required attribute.
0x8024C006	WU_E_DRV_SYNC_FAILED	Driver synchronization failed.
0x8024C007	WU_E_DRV_NO_PRINTER_CONTENT	Information required for the synchronization of applicable printers is missing.
0x8024C	WU_E_DRV_UNEXPECTED	A driver error not covered by

Result Code	Result String	Description
FFF		another WU_E_DRV_* code.
0x8024D001	WU_E_SETUP_INVALID_INFDATA	Windows Update Agent could not be updated because an INF file contains invalid information.
0x8024D002	WU_E_SETUP_INVALID_IDENTDATA	Windows Update Agent could not be updated because the wuident.cab file contains invalid information.
0x8024D003	WU_E_SETUP_ALREADY_INITIALIZED	Windows Update Agent could not be updated because of an internal error that caused setup initialization to be performed twice.
0x8024D004	WU_E_SETUP_NOT_INITIALIZED	Windows Update Agent could not be updated because setup initialization never completed successfully.
0x8024D005	WU_E_SETUP_SOURCE_VERSION_MISMATCH	Windows Update Agent could not be updated because the versions specified in the INF do not match the actual source file versions.
0x8024D006	WU_E_SETUP_TARGET_VERSION_GREATER	Windows Update Agent could not be updated because a WUA file on the target system is newer than the corresponding source file.
0x8024D007	WU_E_SETUP_REGISTRATION_FAILED	Windows Update Agent could not be updated because regsvr32.exe returned an error.
0x8024D008	WU_E_SELFUPDATE_SKIP_ON_FAILURE	An update to the Windows Update Agent was skipped because previous attempts to update have failed.
0x8024D009	WU_E_SETUP_SKIP_UPDATE	An update to the Windows Update Agent was skipped due to a directive in the wuident.cab file.
0x8024D00A	WU_E_SETUP_UNSUPPORTED_CONFIGURATION	Windows Update Agent could not be updated because the current

Result Code	Result String	Description
		system configuration is not supported.
0x8024D00B	WU_E_SETUP_BLOCKED_CONFIGURATION	Windows Update Agent could not be updated because the system is configured to block the update.
0x8024D00C	WU_E_SETUP_REBOOT_TO_FIX	Windows Update Agent could not be updated because a restart of the system is required.
0x8024D00D	WU_E_SETUP_ALREADYRUNNING	Windows Update Agent setup is already running.
0x8024D00E	WU_E_SETUP_REBOOTREQUIRED	Windows Update Agent setup package requires a reboot to complete installation.
0x8024D00F	WU_E_SETUP_HANDLER_EXEC_FAILURE	Windows Update Agent could not be updated because the setup handler failed during execution.
0x8024D010	WU_E_SETUP_INVALID_REGISTRY_DATA	Windows Update Agent could not be updated because the registry contains invalid information.
0x8024D011	WU_E_SELFUPDATE_REQUIRED	Windows Update Agent must be updated before search can continue.
0x8024D012	WU_E_SELFUPDATE_REQUIRED_ADMIN	Windows Update Agent must be updated before search can continue. An administrator is required to perform the operation.
0x8024D013	WU_E_SETUP_WRONG_SERVER_VERSION	Windows Update Agent could not be updated because the server does not contain update information for this version.
0x8024DFFF	WU_E_SETUP_UNEXPECTED	Windows Update Agent could not be updated because of an error not covered by another WU_E_SETUP_* error code.
0x8024E0	WU_E_EE_UNKNOWN_EXPRESSION	An expression evaluator operation

Result Code	Result String	Description
01		could not be completed because an expression was unrecognized.
0x8024E002	WU_E_EE_INVALID_EXPRESSION	An expression evaluator operation could not be completed because an expression was invalid.
0x8024E003	WU_E_EE_MISSING_METADATA	An expression evaluator operation could not be completed because an expression contains an incorrect number of metadata nodes.
0x8024E004	WU_E_EE_INVALID_VERSION	An expression evaluator operation could not be completed because the version of the serialized expression data is invalid.
0x8024E005	WU_E_EE_NOT_INITIALIZED	The expression evaluator could not be initialized.
0x8024E006	WU_E_EE_INVALID_ATTRIBUTEDATA	An expression evaluator operation could not be completed because there was an invalid attribute.
0x8024E007	WU_E_EE_CLUSTER_ERROR	An expression evaluator operation could not be completed because the cluster state of the computer could not be determined.
0x8024EFF	WU_E_EE_UNEXPECTED	There was an expression evaluator error not covered by another WU_E_EE_* error code.
0x8024F001	WU_E_REPORTER_EVENTCACHECORRUPT	The event cache file was defective.
0x8024F002	WU_E_REPORTER_EVENTNAMESPACEPARSEFAILED	The XML in the event namespace descriptor could not be parsed.
0x8024F003	WU_E_INVALID_EVENT	The XML in the event namespace descriptor could not be parsed.
0x8024F004	WU_E_SERVER_BUSY	The server rejected an event because the server was too busy.
0x8024FF	WU_E_REPORTER_UNEXPECTED	There was a reporter error not

Result Code	Result String	Description
FF		covered by another error code.

Appendix H: The wuauctl Utility

The wuauctl utility allows you some control over the functioning of the Windows Update Agent. It is updated as part of Windows Update.

Command line switches for wuauctl

The following are the command line for wuauctl.

Option	Description
/a /ResetAuthorization	Initiates an asynchronous background search for applicable updates. If Automatic Updates is disabled, this option has no effect.
/r /ReportNow	Sends all queued reporting events to the server asynchronously.
/? /h /help	Shows this help information.

Appendix I: Database Maintenance

In order to keep your WSUS server functioning correctly, you should have a maintenance plan that includes re-indexing the database on a regular basis, preferably at least once a month.

The [WsusDBMaintenance](http://go.microsoft.com/fwlink/?LinkId=87027) script (<http://go.microsoft.com/fwlink/?LinkId=87027>) allows you to re-index any version of the WSUS database, either SQL Server or Windows Internal Database.

If you are using Windows Internal Database, you will need to use the **sqlcmd** utility. For more information about the **sqlcmd** utility, see [sqlcmd Utility](http://go.microsoft.com/fwlink/?LinkId=81183) (<http://go.microsoft.com/fwlink/?LinkId=81183>).

To use this script with Windows Internal Database, you should run the following command:

```
sqlcmd -S np:\\.\pipe\MSSQL$MICROSOFT##SSEE\sql\query -i
<scriptLocation>\WsusDBMaintenance.sql
```

where *<scriptLocation>* is the directory where you have copied the WsusDBMaintenance script.

Appendix J: Setup Return Codes

Windows Server Update Services 3.0 uses the following return codes to determine the success or the failure of its Setup.

Windows Server Update Services 3.0 Setup Return Codes

The table in this section shows the return codes (hexadecimal values) returned by **wsussetup.exe**, the return string, and the meaning. A return code of zero indicates success; anything else indicates a failure.

Return Code	Return String	Meaning
0x001450	SUS_LAUNCH_ERROR	Setup Launch Conditions not satisfied.
0x001451	SUS_UNKNOWN_ERROR	Unknown error.
0x001452	SUS_REBOOT_REQUIRED	Reboot required to complete the installation. This most commonly occurs when installing wmsde.
0x001453	SUS_INVALID_COMMANDLINE	Invalid CommandLine
0x001454	SUS_LOWSQLVERSION	Low SQL version. SQL 2005 or SQL 2008 is required.
0x001455	SUS_TRIGGERSNOTSET	SQL triggers are not set. When installing on an existing SQL instance, that instance must support nested triggers.
0x001456	SUS_INVALIDPATH	Invalid content path specified.
0x001457	SUS_NETWORKPATH	Specified content path is a network path.
0x001458	SUS_NONNTFS_PATH	Specified content path is not NTFS.
0x001459	SUS_NONFIXEDDRIVE	Specified content path is

Return Code	Return String	Meaning
		not on a fixed drive.
0x00145a	SUS_NONTFS_DRIVES_PRESENT	No NTFS drives present on the system.
0x00145b	SUS_INSUFFICIENT_SPACE	Not enough space is available at the given path. At least 6 GB of space is required.
0x00145c	SUS_NEED_SERVER_AND_PORT	Need both server name and port for replica mode.
0x00145d	SUS_MSCOM_SERVER	Specified server name ends in ".microsoft.com".
0x001460	SUS_ERROR_PREREQCHECK_FAIL	Prerequisite check failed.
0x001461	SUS_LOWDBSCHEMAUPGRADE_VERSION	This database schema is too old to be upgraded.
0x001462	SUS_UPGRADE_REQUIRED	Setup needs to upgrade from a previous version. Use the /G to avoid this error.