Step-by-Step Guide to Getting Started with Microsoft Windows Server Update Services 3.0

Microsoft Corporation

Author: Susan Norwood

Editor: Craig Liebendorfer

Abstract

This guide provides instructions for getting started with Microsoft® Windows Server® Update Services (WSUS) 3.0. You will find instructions for deploying WSUS 3.0 on your network, including installing WSUS; configuring WSUS 3.0 to obtain updates; configuring client computers to install updates from WSUS 3.0; and approving, managing, and distributing updates. Although WSUS 3.0 is a feature-rich update management solution, this guide offers only a single way to accomplish any of these tasks.

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

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

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

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

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

©2007 Microsoft Corporation. All rights reserved.

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

Contents

Step-by-Step Guide to Getting Started with Microsoft Windows Server Update Services 3.0..... 5

Step 1: Review WSUS 3.0 Installation Requirements..... 5
- Software Requirements for Installing WSUS 3.0 on Windows Server 2003 Service Pack 1..... 5
- Software Requirements for Installing WSUS 3.0 on Windows Server 2008..... 6
- Disk requirements and recommendations 6
- Console-only installation requirements 7
- Automatic Updates requirements..... 7
- Permissions..... 7

Step 2: Install WSUS 3.0 on Your Server..... 8

Step 3: Configure the Network Connection for WSUS 3.0..... 11

Step 4: Configure Updates and Set Up Synchronization 15

Step 5: Configure Automatic Updates 18

Step 6: Create a Computer Group for Updates..... 21

Step 7: Approve and Deploy Updates in WSUS 3.0 22

Step-by-Step Guide to Getting Started with Microsoft Windows Server Update Services 3.0

Microsoft Windows Server Update Services (WSUS) 3.0 provides a comprehensive solution for managing updates within your network. This document provides instructions for basic tasks for deploying WSUS 3.0 on your network. Use this guide to perform the following tasks:

- Install WSUS 3.0.
- Configure WSUS 3.0 to obtain updates from Microsoft.
- Configure client computers to install updates from WSUS 3.0.
- Approve, manage, and distribute updates.

Although WSUS 3.0 is a feature-rich update-management solution, this guide offers only a single way to accomplish any of these tasks. When there are options to perform a task in different ways, the alternative approaches are noted.

Note

To download a copy of this document, see http://go.microsoft.com/fwlink/?LinkId=71190.

Step 1: Review WSUS 3.0 Installation Requirements

This guide explains how to install WSUS 3.0. For software requirements and supported platforms for WSUS 3.0, see the Release Notes (http://go.microsoft.com/fwlink/?LinkId=71220). on Windows Server 2003 Service Pack 1 and Windows Server® 2008 operating systems.

Software Requirements for Installing WSUS 3.0 on Windows Server 2003 Service Pack 1

To install WSUS 3.0 on Windows Server 2003 Service Pack 1, you must have the following installed on your computer. If any of these updates require restarting the server when installation is completed, you should restart your server before installing WSUS 3.0.

- Microsoft Internet Information Services (IIS) 6.0.
- Update for Background Intelligent Transfer Service (BITS) 2.0 and WinHTTP 5.1 Windows Server 2003. To download this software, go to the Download Center (http://go.microsoft.com/fwlink/?LinkID=47251).

- Microsoft .NET Framework Version 2.0 Redistributable Package (x86). To download this software, go to the Download Center (http://go.microsoft.com/fwlink/?LinkID=68935). (For 64-bit platforms, also go to the Download Center [http://go.microsoft.com/fwlink/?LinkID=70637].)
- Microsoft Report Viewer Redistributable 2005. To obtain this software, go to the Download Center (http://go.microsoft.com/fwlink/?LinkID=70410).
- Microsoft Management Console 3.0 for Windows Server 2003 (KB907265). To download this software, go to the Download Center (http://go.microsoft.com/fwlink/?LinkID=70412). (For 64-bit platforms, also go to the Download Center [http://go.microsoft.com/fwlink/?LinkID=70638].)

Software Requirements for Installing WSUS 3.0 on Windows Server 2008

To install WSUS 3.0 on Windows Server 2008, you must have the following installed on your computer. If any of these updates require restarting the server when installation is completed, you should restart your server before installing WSUS 3.0.

- Microsoft Internet Information Services (IIS) 7.0. Ensure that the following components are enabled:
  - Windows Authentication
  - ASP.NET
  - 6.0 Management Compatibility
  - IIS Metabase Compatibility
- Microsoft Report Viewer Redistributable 2005. To download this software, go to the Download Center (http://go.microsoft.com/fwlink/?LinkID=70410).
- Microsoft SQL Server™ 2005 Service Pack 1. To download this software, go to the Download Center (http://go.microsoft.com/fwlink/?LinkID=66143).

The .NET Framework 2.0 and BITS 2.0 update are available on Windows Server 2008 as part of the operating system.

Disk requirements and recommendations

To install WSUS 3.0, the file system of the server must meet the following requirements:

- Both the system partition and the partition on which you install WSUS 3.0 must be formatted with the NTFS file system.
- A minimum of 1 GB of free space is recommended for the system partition.
- A minimum of 20 GB of free space is recommended for the volume where WSUS stores content; 30 GB of free space is recommended.
- A minimum of 2 GB of free space is recommended on the volume where WSUS Setup installs Windows® Internal Database.

Console-only installation requirements

WSUS 3.0 now allows you to install the WSUS Administration console on remote systems separate from the WSUS server. Console-only installations may be performed on the following operating systems:

- Windows Server® 2008
- Windows Vista®
- Windows Server 2003 Service Pack 1
- Windows XP Service Pack 2

The following are the software prerequisites for console-only installation

- Microsoft .NET Framework Version 2.0 Redistributable Package (x86), available on the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=68935). For 64-bit platforms, go to Microsoft .NET Framework Version 2.0 Redistributable Package (x64) (http://go.microsoft.com/fwlink/?LinkId=70637).
- Microsoft Management Console 3.0 for Windows Server 2003 (KB907265), available on the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=70412). For 64-bit platforms, go to Microsoft Management Console 3.0 for Windows Server 2003 x64 Edition (KB907265) (http://go.microsoft.com/fwlink/?LinkId=70638).
- Microsoft Report Viewer Redistributable 2005, available on the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=70410).

Automatic Updates requirements

Automatic Updates is the client component of WSUS 3.0. Automatic Updates has no hardware requirements other than being connected to the network. You can use Automatic Updates with WSUS 3.0 on computers running any of the following operating systems:

- Windows Vista.
- Windows Server® 2008.
- Microsoft Windows® Server 2003, all versions and service packs.
- Microsoft Windows XP Professional, Service Pack 1 or Service Pack 2.
- Microsoft Windows 2000 Professional Service Pack 4, Windows 2000 Server Service Pack 4, or Windows 2000 Advanced Server Service Pack 4.

Permissions

The following disk permissions must be granted to the specified users for the specified directories:

1. Either the built-in group Users or the NT Authority\Network Service account (on Windows Server 2003) should have read permission for the root folder on the drive where the WSUS content directory resides. If this permission is missing, BITS downloads will fail.

2. The NT Authority\Network Service account should have "Full Control" permission for the WSUS content directory, usually <SystemDriver>:WSUS\WsusContent. This permission is set by WSUS server setup when it creates the directory, but some security software may reset this permission. If this permission is missing, BITS downloads will fail.
3. The NT Authority\Network Service account should have “Full Control” permission for the following folders in order for the WSUS Administration snap-in to display correctly:
   - %windir%\Microsoft .NET\Framework\v2.0.50727\Temporary ASP.NET Files
   - %windir%\Temp

For more information about setting permissions, see DCPROMO Does Not Retain Permissions on Some IIS Folders at http://go.microsoft.com/fwlink/?LinkID=76332.

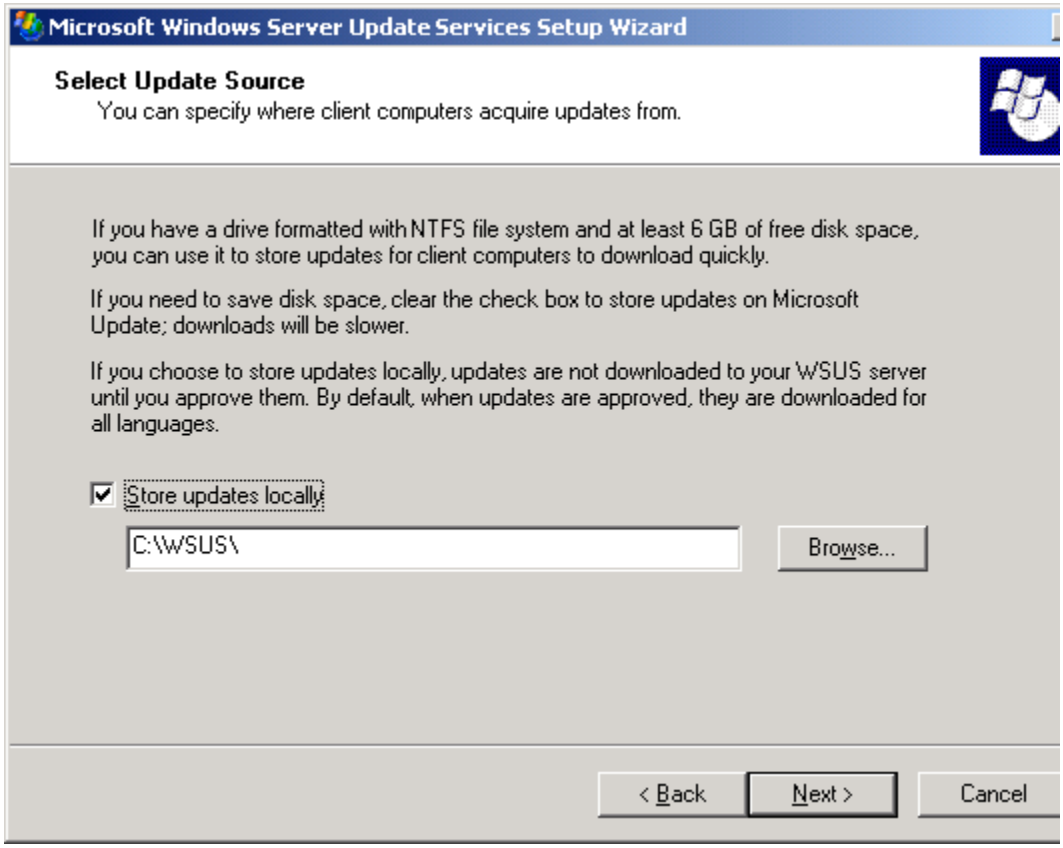
Step 2: Install WSUS 3.0 on Your Server

After ensuring that your server meets the installation requirements, you are ready to install WSUS 3.0. You must log on to the server on which you plan to install WSUS 3.0 by using an account that is a member of the local Administrators group. Only members of the local Administrators group can install WSUS 3.0.

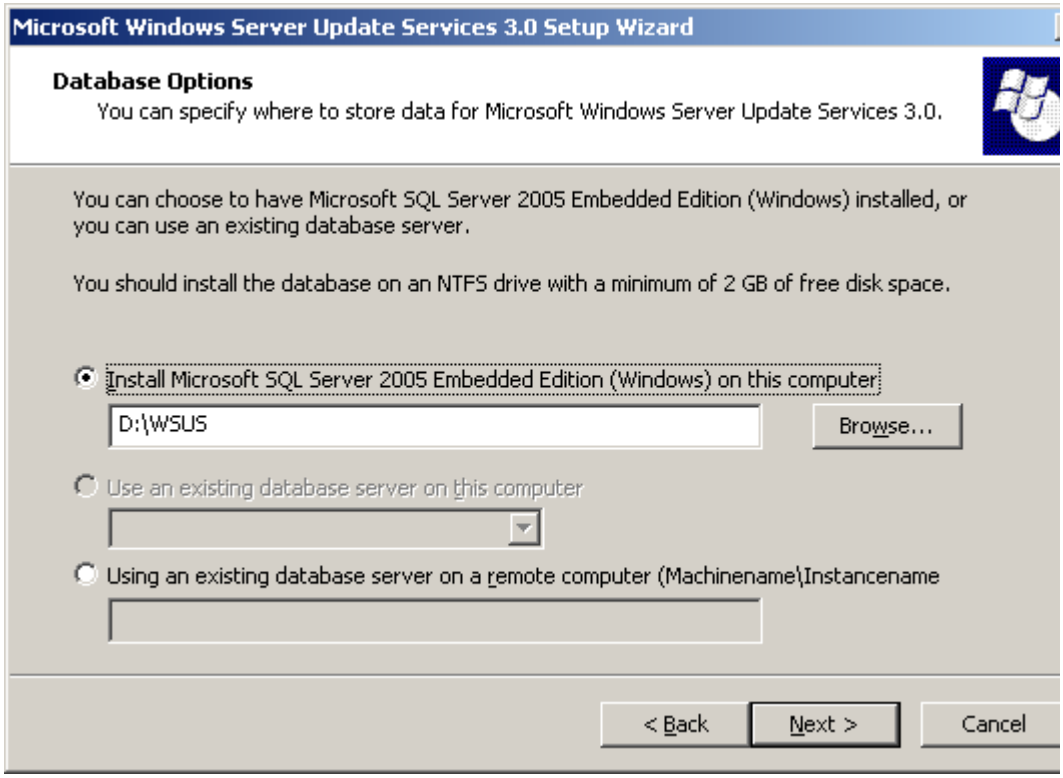
The following procedure uses the default WSUS installation options, which include installing Windows Internal Database for the WSUS 3.0 database software, storing updates locally, and using the IIS Default Web site on port 80.

To install WSUS 3.0

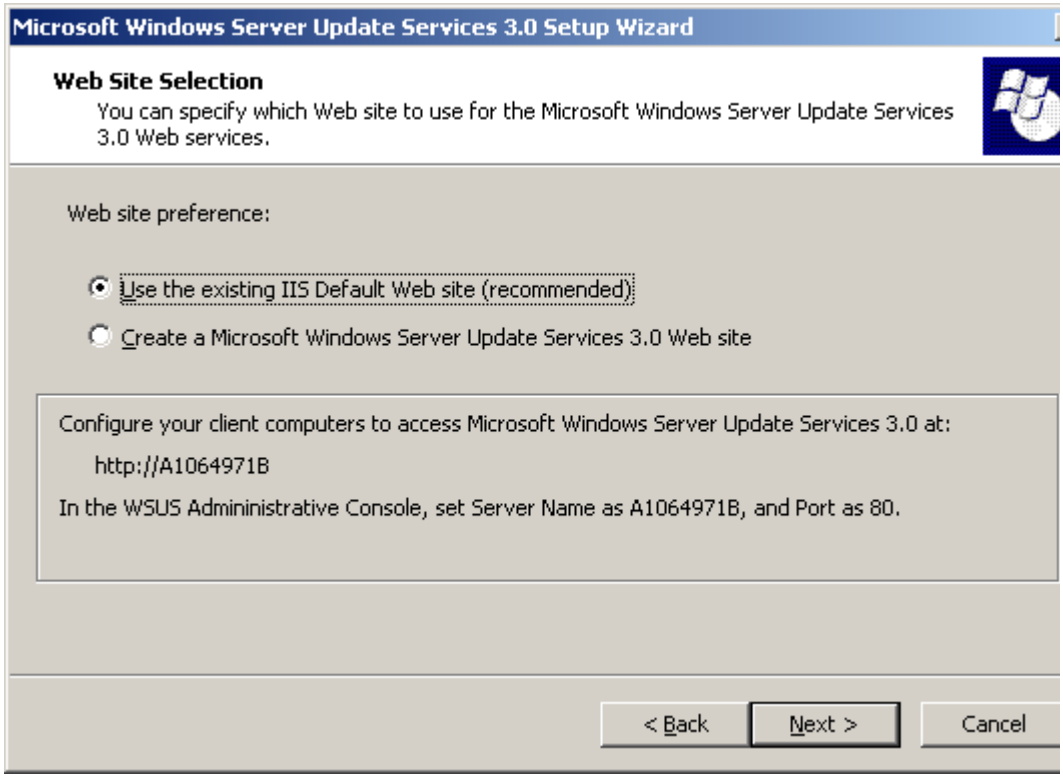
1. Double-click the installer file, **WSUSSetup.exe**.
2. On the **Welcome** page of the installation wizard, click **Next**.
3. On the **Installation Mode Selection** page, click **Full server installation including Administration Console** if you wish to install the server on this computer, or **Administration Console only** if you wish to install the administration console only.
4. On the **License Agreement** page, read the terms of the license agreement carefully, click **I accept the terms of the License agreement**, and then click **Next**.



5. On the **Select Update Source** page of the installation wizard, you can specify where clients get updates. If you select the **Store updates locally** check box, updates are stored on the WSUS 3.0 server, and you select a location in the file system to store updates. If you do not store updates locally, client computers connect to Microsoft Update to get approved updates. Keep the default options, and click **Next**.



6. On the **Database Options** page, select the software used to manage the WSUS 3.0 database. By default, WSUS Setup offers to install Windows Internal Database, if the computer on which you are installing runs Windows Server 2003.
7. If you do not wish to use Windows Internal Database, you must provide a SQL Server instance for WSUS to use, by clicking **Using an existing database server on this computer** and typing the instance name in the box. The instance name should appear as *<serverName>\<instanceName>*, where *serverName* is the name of the server and *instanceName* is the name of the SQL instance. Make your selection, and then click **Next**.
8. On the **Connecting to SQL Server Instance** page, WSUS will try to connect to the specified instance of SQL Server. When it has connected successfully, click **Next** to continue.



9. On the **Web Site Selection** page, specify the Web site that WSUS 3.0 will use. If you wish to use the default IIS Web site on port 80, select the first option. If you already have a Web site on port 80, you can create an alternate site on port 8530 by selecting the second option. Keep the default option and click **Next**.
10. On the **Ready to Install Windows Server Update Services** page, review the selections, and then click **Next**.
11. The final page of the installation wizard will tell you whether or not the WSUS 3.0 installation was completed successfully. After you click **Finish** the configuration wizard will be launched.

Step 3: Configure the Network Connection for WSUS 3.0

After installing WSUS 3.0, the configuration wizard will launch automatically. You can also run it later through the **Options** page of the WSUS 3.0 console.

Before beginning the configuration process, be sure you know the answers to the following questions:

1. Is the server's firewall configured to allow clients to access the server?

2. Can this computer connect to the upstream server (such as Microsoft Update)?

3. Do you have the name of the proxy server and the user credentials for the proxy server, if needed?

By default, WSUS is configured to use Microsoft Update as the location from which to obtain updates. If you have a proxy server on your network, you can configure WSUS to use the proxy server. If there is a corporate firewall between WSUS and the Internet, you might need to configure the firewall to ensure that WSUS can obtain updates.

Note

Although you must have Internet connectivity to download updates from Microsoft Update, WSUS offers you the ability to import updates onto networks not connected to the Internet.

Step 3 contains the following procedures:

- Configure your firewall.
- Specify the way this server will obtain updates (either from Microsoft Update or from another WSUS server).
- Configure proxy server settings, so WSUS can obtain updates.

To configure your firewall

- If there is a corporate firewall between WSUS and the Internet, you might need to configure that firewall to ensure WSUS can obtain updates. To obtain updates from Microsoft Update, the WSUS server uses port 80 for HTTP protocol and port 443 for HTTPS protocol. This is not configurable.
- If your organization does not allow port 80 or port 443 to be open to all addresses, you can restrict access to only the following domains, so WSUS and Automatic Updates can communicate with Microsoft Update:
  - http://windowsupdate.microsoft.com
  - http://*.windowsupdate.microsoft.com
  - https://*.windowsupdate.microsoft.com
  - http://*.update.microsoft.com
  - https://*.update.microsoft.com
  - http://*.windowsupdate.com
  - http://download.windowsupdate.com
  - http://download.microsoft.com
  - http://*.download.windowsupdate.com
  - http://wustat.windows.com
  - http://ntservicepack.microsoft.com

Note

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

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

The next two procedures assume that you are using the configuration wizard. In a later section in this step, you will learn how to start the WSUS Administration snap-in and configure the server through the **Options** page.

To specify the way this server will obtain updates

1. From the configuration wizard, after joining the Microsoft Improvement Program, click **Next** to choose the upstream server.
2. If you choose to synchronize from Microsoft Update, you are finished with this page. Click **Next**, or select **Specify Proxy Server** from the left pane.
3. If you choose to synchronize from another WSUS server, specify the server name and the port on which this server will communicate with the upstream server.
4. To use SSL, check the **Use SSL when synchronizing update information** check box. In that case the servers will use port 443 for synchronization. (You should make sure that both this server and the upstream server support SSL.)
5. If this is a replica server, check the **This is a replica of the upstream server** check box.
6. At this point you are finished with upstream server configuration. Click **Next**, or select **Specify proxy server** from the left panel.

To configure proxy server settings

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

The following two procedures assume that you are using the WSUS Administration snap-in for configuration. These two procedures show you how to start the WSUS Administration snap-in and configure the server from the **Options** page.

To start the WSUS Administration console

- To start the WSUS Administration console, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Microsoft Windows Server Update Services 3.0**.

Note

In order to use all the features of the WSUS console, you must be a member of either the WSUS Administrators or the local Administrators security groups on the server on which WSUS is installed. However, members of the WSUS Reporters security group have read-only access to the administration console.

To specify an update source and proxy server

1. On the WSUS console, click **Options** in the left panel under the name of this server and then click **Update Source and Proxy Server** in the middle panel.
2. A dialog box will be displayed with **Update Source** and **Proxy Server** tabs.
3. In the **Update Source** tab, select the location from which this server will obtain updates. If you choose to synchronize from Microsoft Update (the default), you are finished with this wizard page.
4. If you choose to synchronize from another WSUS server, you need to specify the port on which the servers will communicate (the default is port 80). If you choose a different port, you should ensure that both servers are able to use that port.
5. You may also specify whether to use SSL when synchronizing from the upstream WSUS server. In that case, the servers will use port 443 to synchronize from the upstream server.
6. If this server is a replica of the second WSUS server, select the **This is a replica of the upstream server** check box. In this case all updates must be approved on the upstream WSUS server only.
7. In the **Proxy server** tab, select the **Use a proxy server when synchronizing** check box, and then type the proxy server name and port number (port 80 by default) in the corresponding boxes.
8. If you want to connect to the proxy server by using specific user credentials, select the **Use user credentials to connect to the proxy server** check box, and then type the user name, domain, and password of the user in the corresponding boxes. If you want to enable basic authentication for the user connecting to the proxy server, select the **Allow basic authentication (password in cleartext)** check box.
9. Click **OK** to save these settings.

Step 4: Configure Updates and Set Up Synchronization

Before downloading updates, you will need to specify which updates you want to download. This section describes how to configure the set of updates you wish to download.

The procedures in this step describe how to:

- Save and download information about your upstream server and proxy server.
- Choose the language of the updates you want.
- Choose the products for which you want to get updates.
- Choose the classifications of updates you want.
- Specify the synchronization schedule for this server.

The next five procedures describe how to configure your updates using the configuration wizard. Later procedures describe how to perform this configuration from the WSUS Administration console by choosing specific options.

Save and download your upstream server and proxy information

1. You should have completed configuration of the upstream server and the proxy server in the configuration wizard, and you should see the **Connect to Upstream Server** page.
2. Click the **Start Connecting** button, which will save and upload your settings and get information about available updates.
3. While the connection is being made, the **Stop Connecting** button will be available. If there are problems with the connection, click **Stop Connecting**, fix the problems, and restart the connection.
4. After the download has completed successfully, click **Next** to go to the **Choose Languages** page, or select a different page from the left panel.

Choose update languages

1. The **Choose Languages** page allows you to get updates from all languages or from a subset of languages. Selecting a subset of languages will save disk space, but it is important to choose all of the languages that will be needed by all of the clients of this WSUS server.
2. If you choose to get updates for only a few languages, select **Download updates only in these languages**, and select the languages for which you want updates. Click **Next** to go to the **Choose Products** page, or select a different page from the left panel.

Choose update products

1. The **Choose Products** page allows you to specify the products for which you want updates.

2. You may check product categories, such as Windows, or specific products, such as Windows Server 2003. Selecting a product category will cause all of the products under it to be selected. Click **Next** to proceed to the **Choose Classifications** page, or select a different page from the left panel.

Choose the update classifications

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

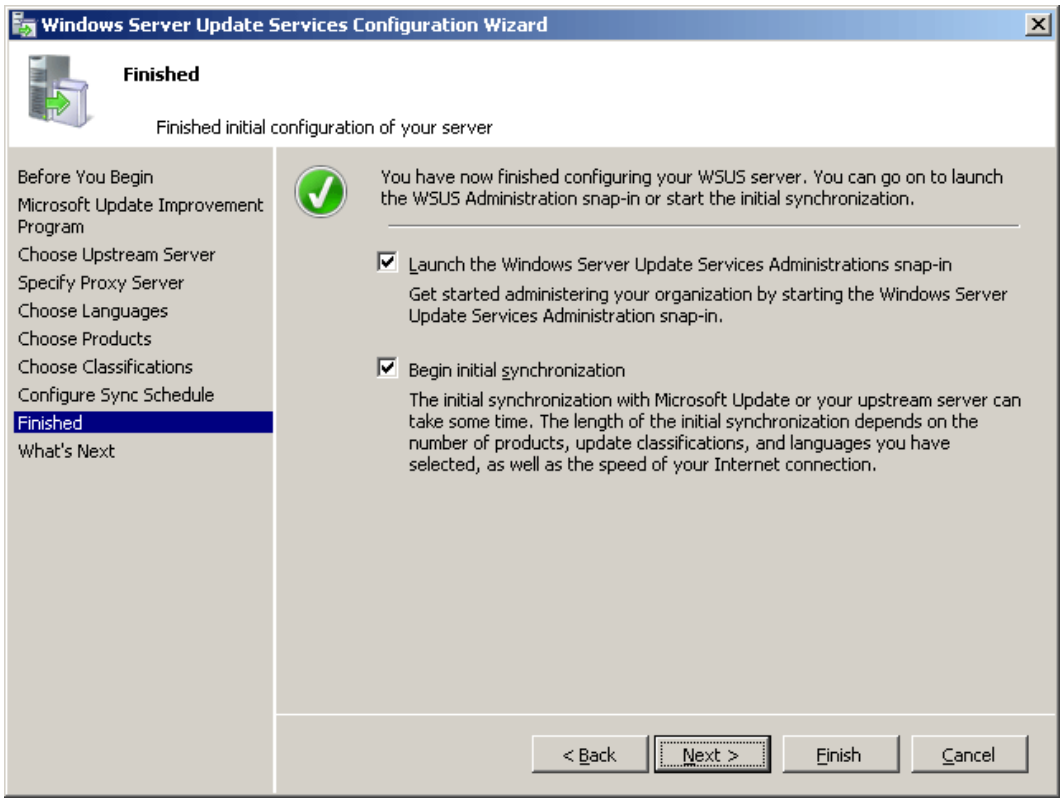
Configure the synchronization schedule

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

After you have completed all of the above configuration steps, select the **Finished** page in the configuration wizard. You can launch the WSUS Administration console by leaving the **Launch the Windows Server Update Services Administrations snap-in** check box selected, and you can start the first synchronization by leaving the **Begin initial synchronization** check box selected.

Note

You cannot save configuration changes that are made while the server is synchronizing. Wait until synchronization is finished to make your changes.



The following procedures explain how to perform the above configuration steps through the **Options** page of the WSUS Administration console:

- Choose products and classifications
- Update files and languages

Choose products and classifications

1. Launch the WSUS Administration console: Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Microsoft Windows Server Update Services**.
2. Select **Options** under your WSUS server in the left pane.
3. In the middle pane, select **Products and Classifications**.
4. You will see a dialog box with two tabs: **Products** and **Classifications**.
5. In the **Products** tab, select the product category or specific product for which you want this server to get updates, or else select **All Products**.
6. In the **Classifications** tab, select the update classifications you want, or else select **All Classifications**.
7. Click **OK** to save your selections.

Update files and languages

1. In the **Options** page, select **Update Files and Languages**.
2. You will see a dialog box with two tabs: **Update Files** and **Update Languages**.
3. In the **Update Files** tab, you can choose whether to store update files locally or to have all client computers install from Microsoft Update. If you choose to store update files on this server, you can choose whether to download only those updates that are approved or to download express installation files.
4. In the **Update Languages** tab, you can choose to get updates for all languages (the default) or to get updates for only the specified languages. If this WSUS server has downstream servers, they will get updates only in the languages specified by the upstream server.
5. Click **OK** to save these settings.

After you configure the network connection, you can download updates by synchronizing the WSUS server.

Synchronization involves the WSUS server contacting Microsoft Update. After making contact, WSUS determines whether any new updates have been made available since the last time you synchronized. Because this is the first time you are synchronizing the WSUS server, all of the updates are available and are ready for your approval for installation. The initial synchronization may take a fairly long time.

Note

This document describes synchronizing with the default settings, but WSUS includes options that enable you to minimize bandwidth use during synchronization.

To synchronize your WSUS server

1. In the WSUS Administration console, select **Synchronizations**.
2. Right-click or go to the **Actions** pane on the right, and then click **Synchronize now**.

Note

If you do not see the **Actions** pane on the right side of the console, on the console toolbar click **View**, click **Customize**, and ensure that the **Action pane** check box is selected.

After the synchronization finishes, click **Updates** in the left panel to view the list of updates.

Step 5: Configure Automatic Updates

WSUS client computers require a compatible version of Automatic Updates. WSUS Setup automatically configures IIS to distribute the latest version of Automatic Updates to each client computer that contacts the WSUS server.

The best way to configure Automatic Updates depends on your network environment. In an environment with Active Directory, you can use a domain–based Group Policy object (GPO). In an environment without Active Directory, use the Local Group Policy object. Whether you use the Local Group Policy object or a domain-based GPO, you must point your client computers to the WSUS server, and then configure Automatic Updates.

The following instructions assume that your network runs Active Directory. These procedures also assume that you are familiar with Group Policy and use it to manage your network. You need to create a new GPO for WSUS settings, and link the GPO to the domain.

For more information about Group Policy, see the Group Policy Tech Center Web site (http://go.microsoft.com/fwlink/?LinkID=47375).

Step 5 contains the following procedures:

- Add the WSUS Administrative Template.
- Configure Automatic Updates.
- Point your client computer to your WSUS server.
- Manually initiate detection by the WSUS server.

Perform the first three procedures on a domain–based Group Policy object. You will need to create a new GPO or use an existing GPO. If you are using Group Policy Management Console (GPMC) to manage your GPOs, navigate to the GPO you wish to modify, and then click **Edit**.

In order to view policy settings to manage WSUS, you will need to ensure that the WSUS administrative template file, wuau.adm, is added to Group Policy Object Editor. Because wuau.adm is released by default in the operating system, it should already be present in Group Policy Object Editor.

To add the WSUS Administrative Template

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

To configure Automatic Updates

1. In Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, double-click **Configure Automatic Updates**.
3. Click **Enabled**, and then click one of the following options:
   - **Notify for download and notify for install**: This option notifies a logged-on administrative user before the download and before the installation of the updates.
   - **Auto download and notify for install**: This option automatically begins downloading updates and then notifies a logged-on administrative user before installing the

updates.

- **Auto download and schedule the install**: If Automatic Updates is configured to perform a scheduled installation, you must also set the day and time for the recurring scheduled installation.
- **Allow local admin to choose setting**: With this option, local administrators are allowed to use Automatic Updates in Control Panel to select a configuration option of their choice. For example, they can choose their own scheduled installation time. Local administrators are not allowed to disable Automatic Updates.

4. Click **OK**.

Note

The setting **Allow local admin to choose setting** appears only if Automatic Updates has updated itself to the version compatible with WSUS.

To point your client computer to your WSUS server

1. In Group Policy Object Editor, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
2. In the details pane, double-click **Specify intranet Microsoft update service location**.
3. Click **Enabled**, and type the HTTP URL of the same WSUS server in the **Set the intranet update service for detecting updates** box and in the **Set the intranet statistics server** box. For example, type *http://servername* in both boxes, and then click **OK**.

Note

If you are using the Local Group Policy object to point this computer to WSUS, this setting takes effect immediately and this computer should appear in the WSUS administrative console after a short time. You can speed up this process by manually initiating a detection cycle.

After you set up a client computer, it will take a few minutes before it appears on the **Computers** page in the WSUS console. For client computers configured with a domain-based Group Policy, it will take about 20 minutes after Group Policy refreshes (that is, applies any new policy settings to the client computer). By default, Group Policy refreshes in the background every 90 minutes, with a random offset of 0–30 minutes. If you want to refresh Group Policy sooner, you can go to a command prompt on the client computer and type: **gpupdate /force**.

For client computers configured with the Local GPO, Group Policy is applied immediately, and the refresh will take about 20 minutes.

After Group Policy is applied, you can initiate detection manually. If you initiate detection manually, you do not have to wait 20 minutes for the client computer to contact WSUS.

To manually initiate detection by the WSUS server

1. On the client computer, click **Start**, and then click **Run**.
2. Type **cmd** in the **Open** box, and then click **OK**.
3. At the command prompt, type **wuauclt.exe /detectnow**. This command-line option instructs Automatic Updates to contact the WSUS server immediately.

Step 6: Create a Computer Group for Updates

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

You can create custom computer groups. One benefit of creating computer groups is that they enable you to test updates before deploying updates widely. If testing goes well, you can roll out the updates to the All Computers group. There is no limit to the number of custom groups you can create.

To set up computer groups

1. Specify how you are going to assign computers to the computer groups. There are two options: server-side targeting and client-side targeting. Server-side targeting involves manually adding each computer to its group by using WSUS. Client-side targeting involves automatically adding the clients by using either Group Policy or registry keys.
2. Create the computer group on WSUS.
3. Move the computers into groups by using the method you chose in step 1.

This section explains how to use server-side targeting and manually move computers to their groups by using the WSUS Administration console. If you have multiple client computers to assign to computer groups, you can use client-side targeting, which automates moving computers into computer groups.

You can use Step 6 to set up a test group that contains at least one test computer.

Step 6 contains the following procedures:

- Create a group.
- Add a computer to the group.

To create a group

1. In the WSUS Administration console, expand **Computers** and select **All Computers.**
2. Right-click **All Computers**, or go to the **Actions** pane and then click **Add Computer Group**.
3. You will see an **Add Computer Group** dialog box. Specify the name of the new group.

Use the next procedure to assign a client computer to the test group. A client computer appropriate for testing is any computer with software and hardware indicative of the majority of computers on your network, but not a computer assigned to a critical role. In this way, you can tell how well computers like the test computer will fare with the updates you approve.

To add a computer to the group

1. In the WSUS Administration console, click **Computers**.
2. Click the group of the computer you want to move.
3. In the list of computers, select the computer you want to move.
4. Right-click **Change Membership**.
5. You will see a dialog box, **Set Computer Group Membership**, with a list of groups.
6. Check the group to which you want to move the computer, and then click **OK**.

Step 7: Approve and Deploy Updates in WSUS 3.0

In this step, you approve an update for any test client computers in the test group. Computers in the group will contact the WSUS server over the next 24 hours. After this period, you can use the WSUS reporting feature to determine if those updates have been deployed to the computers. If testing goes well, you can then approve the same updates for the rest of the computers in your organization.

Step 7 contains the following procedures:

- Approve and deploy an update.
- Check the status of the update.

To approve and deploy an update

1. On the WSUS Administration console, click **Updates**. Doing so will display a summary of updates in the default views (**All Updates**, **Critical Updates**, **Security Updates**, and **WSUS Updates**). Use **All Updates** for this procedure.
2. On the list of updates, select the updates you want to approve for installation. Information about a selected update is available in the lowermost pane of the Updates panel. To

select multiple contiguous updates, press and hold down the **SHIFT** key while clicking updates; to select multiple noncontiguous updates, press and hold down the **CTRL** key while click updates.

3. Right-click the selection and click **Approve**. The **Approve Updates** dialog box appears.
4. Select one of the groups (for example, **Test**) and click the arrow to its left. You will see a context menu with the choices **Approved for Install**, **Approved for Removal**, **Not Approved**, **Deadline**, **Same as Parent**, and **Apply to Children**. Click **Approved for Install** and then click **OK**.
5. You will see a new window, **Approval Progress**, which shows progress of the different tasks affecting the approval of the updates. When approval is completed, click **Close** to close this window.

Note

Many options are associated with approving updates, such as setting deadlines and uninstalling updates.

After 24 hours, you can use the WSUS reporting feature to determine whether the updates have been deployed to the computers.

To check the status of an update

1. In the WSUS Administration console, click **Reports** in the left pane.
2. On the **Reports** page, you will see a number of standardized reports. Click the **Update Status Summary** report. You will see the **Updates Report** window.
3. If you want to filter the list of updates, select the criteria you want to use (for example, **Include updates in these classifications**), and then click **Run Report** on the window's toolbar.
4. You will see the **Updates Report** pane. You can check the status of individual updates by selecting the update in the left section of the pane. The last section of the report pane shows the status summary of the update.
5. You can save or print this report by clicking the appropriate icon on the toolbar.

If the updates were successfully deployed to the test group, you can approve the same updates for the rest of the computers in your organization.