



Windows Server[™] Update Services

Microsoft Windows Server Update Services 3.0 Overview

Microsoft Corporation

Published: February 2007

Author: Susan Norwood

Editor: Craig Liebendorfer

Abstract

This paper introduces Microsoft® Windows Server® Update Services (WSUS) 3.0 and provides information about features, and server and client computer requirements. In addition, you will find examples of WSUS deployment scenarios and information about the role of WSUS in the update management process.

Microsoft[®]

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

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

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

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

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

© 2007 Microsoft Corporation. All rights reserved.

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

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

Contents

Microsoft Windows Server Update Services 3.0 Overview	7
How WSUS works	7
Microsoft Update	7
Windows Server Update Services server	7
Automatic Updates	8
New in Windows Server Update Services 3.0	8
Ease of use	8
Improved deployment options	10
Better support for complex server hierarchies	10
Better performance and bandwidth optimization	11
Extend WSUS 3.0 using improved APIs	11
Server and Client Requirements.....	12
WSUS requirements	12
Features of Windows Server Update Services 3.0	13
Server-side features.....	13
Client-side features.....	18
WSUS 3.0 Deployment Scenarios	19
Single WSUS server (small-sized or simple network)	19
Multiple WSUS servers (medium-sized or more complex network)	20
Multiple independent WSUS servers.....	20
Multiple internally synchronized WSUS servers.....	21
Disconnected WSUS servers (limited or restricted Internet connectivity).....	22
WSUS and the Update Management Process	23
1. Assess.....	24
2. Identify.....	24
3. Evaluate and Plan.....	25
4. Deploy	25
WSUS Next Steps.....	26

Microsoft Windows Server Update Services 3.0 Overview

Microsoft® Windows Server® Update Services 3.0 (WSUS 3.0) enables information technology administrators to deploy the latest Microsoft product updates to computers running Microsoft Windows Server 2003, Microsoft Windows® XP with Service Pack 2, and Windows 2000 with Service Pack 4 operating systems. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.



Note

A downloadable copy of this document is available at <http://go.microsoft.com/fwlink/?LinkId=71191>.

How WSUS works

WSUS provides a management infrastructure consisting of the following:

Microsoft Update

The Microsoft Web site that WSUS components connect to for updates of Microsoft products.

Windows Server Update Services server

The server component that is installed on a computer running a Windows Server 2003 operating system inside the corporate firewall. The WSUS server provides the features that administrators need to manage and distribute updates through the WSUS 3.0 Administration Console, which can be installed and accessed on any Windows computer in the corporate network. In addition, a WSUS server can be the update source for other WSUS servers within the organization. The WSUS server that acts as an update source is called an "upstream server." In a WSUS implementation, at least one WSUS server in the network must connect to Microsoft Update to get available update information. The administrator can determine, based on network security and configuration, how many other servers connect directly to Microsoft Update.

Automatic Updates

The client computer component built into Windows Server "Longhorn", Windows Server 2003, Windows XP, and Windows 2000 with Service Pack 4 operating systems. Automatic Updates enables both server and client computers to receive updates from Microsoft Update or from a server running WSUS.

New in Windows Server Update Services 3.0

Windows Server Update Services (WSUS) 3.0 provides a number of new features, making WSUS easier to use, deploy, and support. Specifically, WSUS 3.0 provides improvements in the following areas:

- [Ease of use](#)
- [Improved deployment options](#)
- [Better support for complex server hierarchies](#)
- [Better performance and bandwidth optimization](#)
- [Extend WSUS 3.0 using improved APIs](#)

Ease of use

Manage WSUS from the Administration Console

The WSUS 3.0 administration console has moved from a Web-based console to a plug-in to the Microsoft Management Console version 3.0. The new user interface provides the following features:

- Home pages at each node containing an overview of the tasks associated with the node
- Advanced filtering
- New columns allowing you to sort updates according to MSRC number, MSRC severity, KB article, and installation status
- Column selection, sorting, and reordering
- Shortcut menus, allowing you to right-click and choose an action

- Reporting integrated with update views
- Custom views

Manage WSUS remotely

The WSUS 3.0 administration console can be installed on other computers in the network to manage the WSUS 3.0 server remotely.

Configure post-setup tasks using a wizard

A configuration wizard guides new users through the process of post-setup server configuration.

Generate multiple reports with improved precision

Reports can now be generated directly from the update view. You can report on a subset of updates, such as security updates that are needed by computers but not yet approved for installation. You can create reports on all computers managed by a replica hierarchy, and you can save these reports in Excel or PDF format.

Maintain server health more easily

WSUS 3.0 now logs detailed server health information in the event log. A Microsoft Operations Manager (MOM) pack is now available to monitor events generated by the WSUS server.

Get e-mail messages about new updates

The server has built-in support for e-mail notification for new updates and for update compliance summaries.

Remove old information easily

The cleanup wizard allows you to remove old computers, updates, and update files from your server.

Upgrade seamlessly from WSUS 2.0 to WSUS 3.0

WSUS 3.0 can be installed on a server that already has WSUS 2.0 installed. The installation process will perform an in-place upgrade that preserves all the previous settings and approvals. The process of upgrading a server hierarchy should start from the central server and continue down the hierarchy. A WSUS 2.0 server can synchronize from a WSUS 3.0 server, but a WSUS 3.0 server cannot synchronize from a WSUS 2.0 server. Upgrading from WSUS 2.0 to WSUS 3.0 is a one-way process; going back to WSUS 2.0 requires that you first remove WSUS 3.0, then reinstall WSUS 2.0.

Improved deployment options

Obtain updates faster

With WSUS 3.0 you can configure a server to synchronize updates automatically as often as once per hour (compared to once a day with WSUS 2.0). This improvement allows new updates to replicate through your corporation more quickly.

Set more automatic approvals

WSUS 3.0 auto-approval rules allow you to specify different products and update classifications, such as automatic approval for definition updates for Microsoft Word. In addition, WSUS 3.0 supports the creation of multiple auto-approval rules, rather than a single rule. Auto-approval rules will now be applied to all updates that are currently on the WSUS server.

Limit access to read-only reporting

Members of the “WSUS Reporters” security group will have read-only access to the server. Members can generate reports but not approve updates or configure the server.

Better support for complex server hierarchies

Manage multiple servers from a single console

The WSUS 3.0 administration console will allow you to inspect and manage all the WSUS servers in your hierarchy.

Create reports for all computers

You can now create update reports for all the computers managed by a replica hierarchy.

Configure servers in a cluster

WSUS 3.0 servers can now be configured in a cluster for fault tolerance. Such servers must all point to the same SQL Server database instance, which can also be clustered.

Toggle replica mode

You can now move a child server between replica mode and autonomous mode without needing to reinstall WSUS 3.0.

Assign clients to multiple target groups

In WSUS 3.0 a computer can belong to multiple target groups (for example, both a “Desktops” group and a “Test” group). In addition, you can create hierarchical groups (for example, a “Servers” target group with the child groups “Critical Servers” and “Non-Critical Servers”). You can specify approvals for the parent target group that will automatically be inherited by computers in the child groups.

Better performance and bandwidth optimization

Utilize faster performance

WSUS 3.0 registers an approximately 50 percent scalability improvement over WSUS 2.0. In addition, WSUS 3.0 comes with native x64 support to further improve performance and scalability on 64-bit hardware.

Specify languages in branch offices

To save disk space and network load, you can now configure a branch office to download updates in fewer languages than the central server. For example, you can configure the central server to download updates in all languages and a branch office to download updates in English only.

Configure separate content and metadata channels

Branch offices with narrowband connections to the central server but broadband connections to the Internet can now be configured to get metadata from the central server and update content from Microsoft Update.

Extend WSUS 3.0 using improved APIs

Move up to .NET Framework 2.0 Support

The new API is based on .NET Framework 2.0.

Go beyond the WSUS console with APIs for advanced management tools

New APIs have been created for use by advanced management tools (such as System Center Essentials). These features are not exposed in the WSUS administration console.

Add optional installation approvals to administrator options

The new API supports creating approvals for “optional installation,” which tells the Windows Update Agent to make the update available for installation in the **Add or Remove Programs** dialog box, but not via Automatic Updates.

Collect hardware and software inventories

The new API supports collecting hardware and software inventories from managed devices.

Expand the set of updates with local publishing

The new API supports publishing applications and third-party updates, allowing the WSUS infrastructure to also distribute updates by other companies.



Note

For more information about WSUS features, see **Features of Windows Server Update Services**, later in this document.

Server and Client Requirements

WSUS requirements

The following software requirements are for WSUS servers and client computers.

WSUS servers

- Windows Server 2003 Service Pack 1 or Windows Server® Code Name "Longhorn"
- Microsoft Internet Information Services (IIS) 6.0 or later
- Background Intelligent Transfer service (BITS) 2.0 or later
- Windows Installer 3.1 or later
- Microsoft .NET Framework 2.0

Optional Prerequisites

- Microsoft Management Console 3.0
- SQL Server 2005 Service Pack 1 (on Windows Server 2003) or Service Pack 2 (on Windows Server "Longhorn")

- Microsoft Report Viewer Redistributable 2005

WSUS client computers

Windows Vista™, Windows Server 2003 (any edition), Windows XP, or Windows 2000 with Service Pack 4.



Note

WSUS 3.0 now allows you to install the WSUS Administration console on remote systems separate from the WSUS server. You may perform console-only installations on Windows XP Service Pack 2, Windows Vista™, Windows Server 2003, or Windows Server "Longhorn".

Features of Windows Server Update Services 3.0

Server-side features

The server-side component of the WSUS solution includes the following features.

More updates

Microsoft Update publishes updates for the following products:

- Windows 2000
- Windows XP (32-bit, IA-64 and x64 Editions)
- Windows Vista
- Windows Server 2003
- Windows Small Business Server 2003
- Exchange Server 2000
- Exchange Server 2003
- SQL Server
- SQL Server 2005
- Office XP
- Office 2003

- Microsoft ISA Server 2004
- Microsoft Data Protection Manager
- Microsoft ForeFront
- Windows Live
- Windows Defender

At least one upstream WSUS server connects to Microsoft Update to get available updates and update information, while other downstream servers get their updates from the upstream server.

Specific updates can be set to download automatically

When a WSUS server downloads available updates, either from Microsoft Update or an upstream WSUS server, synchronization occurs.

Administrators can choose which updates are downloaded to a WSUS server during synchronization, based on the following criteria:

- Product or product family (for example, Microsoft Windows Server 2003 or Microsoft Office)
- Update classification (for example, critical updates, and drivers)
- Language (for example, English and Japanese only)

In addition, administrators can specify a schedule for synchronization to initiate automatically.

Automated actions for updates determined by administrator approval

An administrator must approve every automated action to be carried out for the update.

Approval actions include the following:

- Approve
- Remove (this action is possible only if the update supports uninstall)
- Decline

In addition, the administrator can enforce a deadline, a specific date and time to install or remove (uninstall) updates. The administrator can force an immediate download by setting a deadline for a time in the past.

E-mail notification of new updates and status reports

WSUS 3.0 can be configured to send e-mail notification of new updates and status reports. Specified recipients can receive update notifications as they arrive on the WSUS server. Status reports can be sent at specified times and intervals.

Ability to determine the applicability of updates before installing them

WSUS 3.0 now automatically scans updates to determine the computers on which they should be installed. Before actually planning and deploying the update for installation, the administrator can analyze the update's impact by means of a status report that can be generated directly from the update view for a single update, a subset of updates, or all updates.

Targeting

Targeting enables administrators to deploy updates to specific computers and groups of computers. Targeting can be configured either on the WSUS server directly, on the WSUS server by using Group Policy in an Active Directory network environment, or on the client computer by editing registry settings.

The following are examples of targeting tasks that administrators can perform:

- Deploying new updates to a test computer group and then evaluating the updates before distributing them to the production environment.
- Protecting computers that run specific applications. For example, if a critical update is incompatible with an application used by only certain computers, an administrator can make sure that the update is not distributed to those computers.
- Specifying a deadline by which an update must be installed, and then setting different deadlines for different computers or computer groups.
- Making the same computer a member of more than one group. For example, a computer could be a member of the "Test" group and also a member of the "Special Applications" group.

Database options

The WSUS database stores update information, event information about update actions on client computers, and WSUS server settings.

Administrators have the following options for the WSUS 3.0 database:

- The Windows® Internal Database database that WSUS can install during setup on Windows Server 2003.
- An existing Microsoft SQL Server™ 2005 Service Pack 1 database.

Replica synchronization and reporting

WSUS enables administrators to create an update management infrastructure consisting of a hierarchy of WSUS servers. WSUS servers can be scaled out to handle any number of clients.

With replica synchronization, the administrator of the central WSUS server can create updates, target groups, and approvals that are automatically propagated to WSUS servers designated as replica servers. This means that branch office clients can get centrally approved updates from a local server without the need for a local WSUS administrator. Also, offices with a low-bandwidth link to the central server pose less of a problem, because the branch WSUS server connects only to the central WSUS server. Update status reports can be generated for all the clients of a replica server.

Management of multiple WSUS servers from a single console

WSUS 3.0 now allows administrators to manage a WSUS server hierarchy from a single WSUS console. The WSUS administration snap-in to the Microsoft Management Console can be installed on any computer in the network.

Reporting

Using WSUS reports, administrators can monitor the following activity (all reports are in a printable format and can be exported to Excel spreadsheets or Adobe .pdf files):

- **Update status:** Administrators can monitor the level of update compliance for their client computers on an ongoing basis using Update Status reports, which can provide status for update approval and deployment per update, per computer, and per computer group, based on all events that are sent from the client computer.
- **Computer status:** Administrators can assess the status of updates on client computers. For example, they can request a summary of updates that have been installed or are needed for a particular computer.
- **Computer compliance status:** Administrators can view or print a summary of compliance information for a specific computer, including basic software and hardware information, WSUS activity, and update status.
- **Update compliance status:** Administrators can view or print a summary of compliance information for a specific update, including the update properties and cumulative status for each computer group.
- **Synchronization (or download) status:** Administrators can monitor synchronization activity and status for a given time period, and view the latest updates that have been downloaded.

- **WSUS configuration settings:** Administrators can see a summary of options they have specified for their WSUS implementation.

Troubleshooting

The WSUS Management Pack allows administrators to troubleshoot WSUS infrastructure, including network connectivity, permissions, SQL connectivity, and WSUS-related services. The WSUS Management Pack exposes this information in the State view of the Microsoft Operations Manager. Administrators can get detailed information about the cause of the problem and related solutions.

Extensibility

A software development kit (SDK) is available to enable administrators and developers to work with the .NET-based API.

Administrators can create custom code to manage both Automatic Updates and WSUS servers. New APIs allow administrators to collect hardware and software inventories from managed devices, create approvals for installation via the **Add or Remove Programs** dialog box, and integrate WSUS management with that of other management tools, such as System Center Essentials.

Developers can create management applications to integrate with WSUS or to publish third-party updates using WSUS infrastructure.

Configurable communication options

Administrators have the flexibility of configuring computers to get updates directly from Microsoft Update, from an intranet WSUS server that distributes updates internally, or from a combination of both, depending on the network configuration.

Administrators can configure a WSUS server to use a custom port for connecting to the intranet or Internet, if appropriate. (The default port used by a WSUS server is port 80.) It is also possible to connect via SSL, in which case the default port is 443.

Administrators can configure proxy server settings if the WSUS server connects to the Internet through a proxy server.

Import and export and data migration from the command line

Administrators can import and export update metadata and content between WSUS servers. This is a necessary task in a network with limited or restricted Internet connectivity.

Administrators can seamlessly migrate their previous administrative settings, content approvals, and content from a WSUS 2.0 server to a WSUS 3.0 server. Migration can

also be useful for consolidation of WSUS servers. For example, administrators can migrate approvals for specific target groups from one WSUS server to another.

Backup and restore

WSUS supports ntbackup for update content files and SQL Server metadata.

Client-side features

The following features comprise the client-side component of the WSUS solution.

Powerful and extensible management of the Automatic Updates service

In an Active Directory service environment, administrators can configure the behavior of Automatic Updates by using Group Policy. In other cases, administrators can remotely configure Automatic Updates using registry keys through the use of a logon script or similar mechanism.

Administrator capabilities for configuring client computers include the following:

- Configuring notification and scheduling options for users through Group Policy.
- Configuring how often the client computer checks the update source (either Microsoft Update or another WSUS server) for new updates.
- Configuring Automatic Updates to install updates that do not require reboots or service interruptions as soon as it finds them and not to wait until the scheduled automatic installation time.
- Managing client computers through the Component Object Model (COM)–based API. An SDK is available.

Self-updating for client computers

WSUS client computers can detect from the WSUS server if a newer version of Automatic Updates is available, and then upgrade their Automatic Updates service automatically.

Automatic detection of applicable updates

Automatic Updates can download and install specific updates that are truly applicable to the computer. Automatic Updates works with the WSUS server to evaluate which updates should be applied to a specific client computer.

Under-the-hood efficiency

The Automatic Updates service works in the background so that the perceptible impact on employee productivity and network functionality is minimal.

Automatic Updates consolidates updates that require computer restarts into a single restart.

Automatic Updates eliminates the need for users in a managed environment to interact with Microsoft Software License Terms. License terms are accepted on the WSUS server by administrators on behalf of client computers.

BITS 2.0 employs delta compression to facilitate downloads that are invisible to the user. For example, after Automatic Updates downloads an update to a client computer, it will continue to monitor either the upstream WSUS server or Microsoft Update, and then download only changes in an update file to the client computer. This technology also enables efficient distribution of service packs through Automatic Updates.

WSUS 3.0 Deployment Scenarios

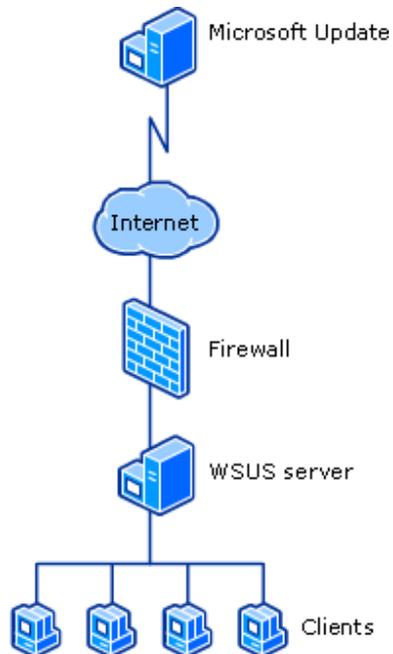
WSUS is flexible enough to meet the update management needs of a wide range of organizations—from small businesses with dial-up connectivity to the largest businesses with thousands of users distributed across multiple sites. Depending on the size of the organization, its location, and its connectivity infrastructure, administrators can determine the most efficient way to scale out their WSUS servers—a decision that might involve one or many WSUS servers.

In this section, you can learn more about the common scenarios for deploying WSUS components in small, medium, and restricted networks.

Single WSUS server (small-sized or simple network)

In a single WSUS server scenario, administrators can set up a server running WSUS inside their corporate firewall, which synchronizes content directly with Microsoft Update and distributes updates to client computers, as shown in the following figure.

Single WSUS Server



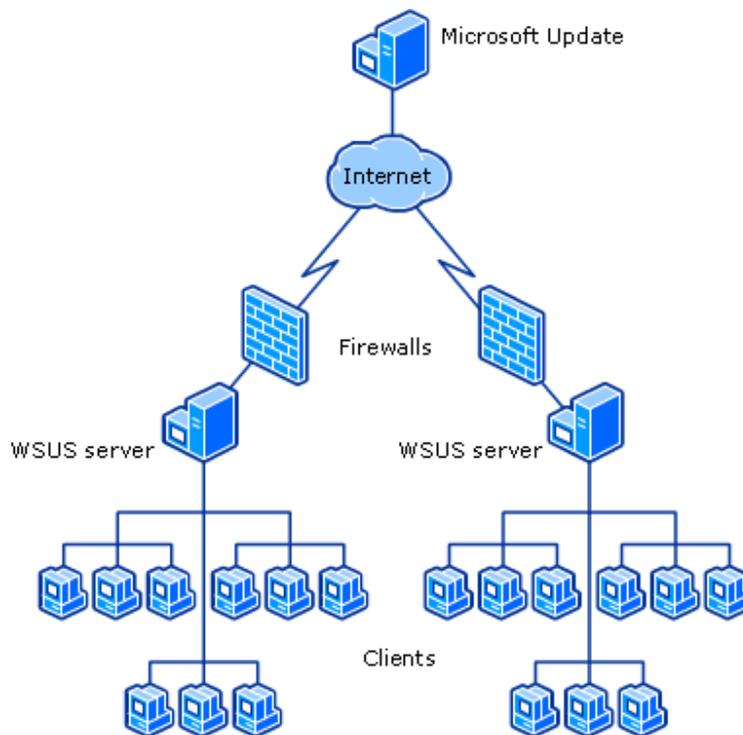
Multiple WSUS servers (medium-sized or more complex network)

The following are common scenarios for deploying WSUS components in a medium-sized or more complex network.

Multiple independent WSUS servers

Administrators can deploy multiple servers that are configured so that each server is managed independently and each server synchronizes its content from Microsoft Update, as shown in the following figure.

Multiple Independent WSUS Servers

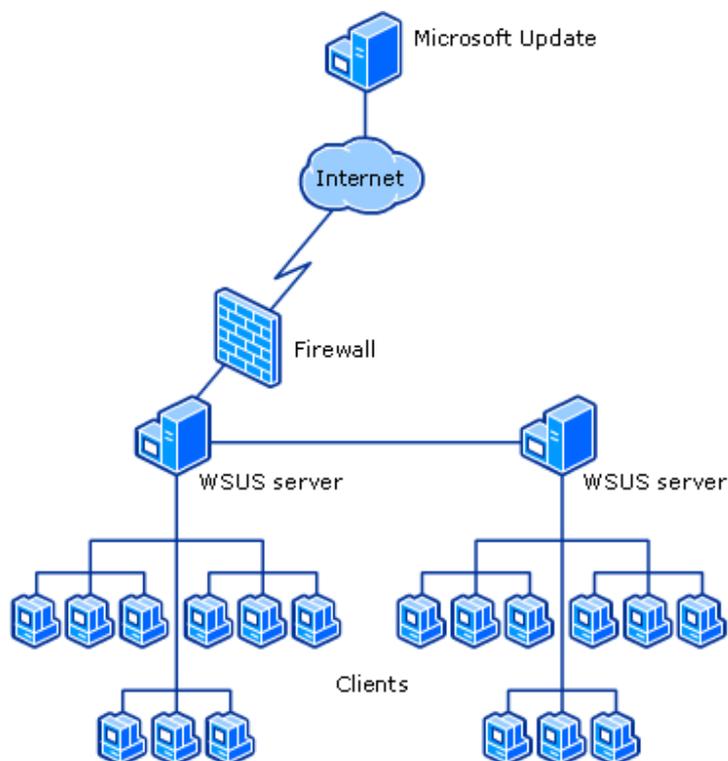


The deployment method in this scenario would be appropriate for situations in which different local area network (LAN) or wide area network (WAN) segments are managed as separate entities (for example, a branch office). It would also be appropriate when one server running WSUS is configured to deploy updates only to client computers running a certain operating system (such as Windows 2000), while another server is configured to deploy updates only to client computers running another operating system (such as Windows XP).

Multiple internally synchronized WSUS servers

Administrators can deploy multiple servers running WSUS that synchronize all content within their organization's intranet. In the following figure, only one server is exposed to the Internet. In this configuration, this is the only server that downloads updates from Microsoft Update. This server is set up as the upstream server—the source to which the downstream server synchronizes. When applicable, servers can be located throughout a geographically dispersed network to provide the best connectivity to all client computers.

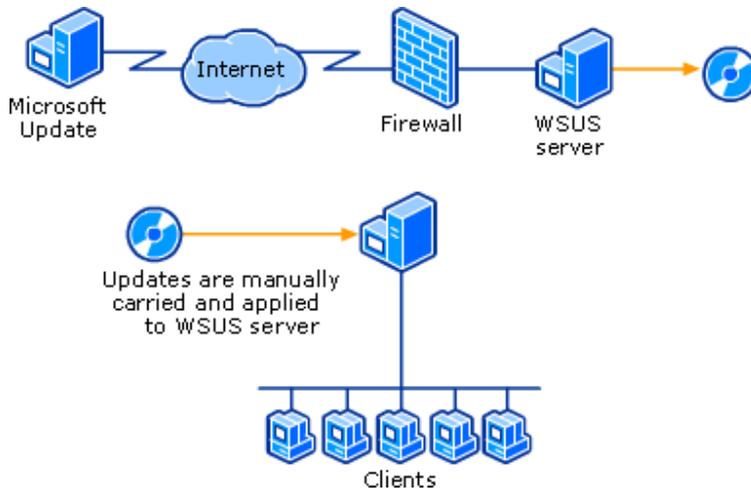
Multiple Internally Synchronized WSUS Servers



Disconnected WSUS servers (limited or restricted Internet connectivity)

If corporate policy or other conditions limit computer access to the Internet, administrators can set up an internal server running WSUS, as illustrated in the following figure. In this example, a server is created that is connected to the Internet but is isolated from the intranet. After downloading, testing, and approving the updates on this server, an administrator would then export the update metadata and content to the appropriate media; then, from the media, the administrator would import the update metadata and content to servers running WSUS within the intranet. Although the following figure illustrates this model in its simplest form, it could be scaled to a deployment of any size.

Disconnected WSUS Servers with No Intranet Connectivity to the Internet

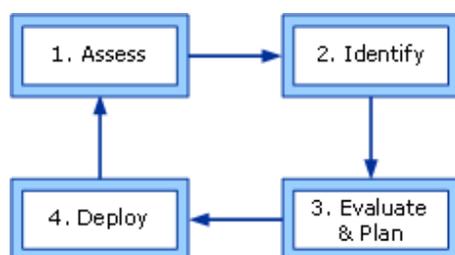


WSUS and the Update Management Process

This Microsoft recommended approach to the update management process consists of an ongoing set of four phases, as illustrated in the following figure. It is essential to repeat the update management process on an ongoing basis, as new updates become available that can enhance and protect the production environment.

Following the figure are the goals of each phase and examples of how administrators can use WSUS features to ensure success during each of the four phases of the process. It is important to note that many of the features can be employed in more than one phase.

The four phases of the update management process



1. Assess

The administrator's goals for the Assess phase are:

- To set up a production environment that will support update management for both routine and emergency scenarios.

Although it is the first step, the Assess phase is essentially an ongoing process. For example, administrators have to assess how many servers and client computers they need to update, what their storage and network bandwidth requirements are, and what time frame is acceptable to deploy an average update. Administrators also have to determine what platforms, products, and languages they want to update. Based on these factors, administrators can determine the most efficient topology for scaling out their WSUS components.

WSUS provides numerous options for setting up WSUS components, including the ability to store update content locally on WSUS servers or download content on demand from Microsoft Update. Administrators can also configure Automatic Updates to download and install missing updates on a computer automatically. WSUS provides options for managing client computers in both Active Directory and non-Active Directory environments.

WSUS provides standardized aggregate reports that administrators can run on an ongoing basis. These reports provide comprehensive information about all activity in the WSUS implementation, including information about updates that have been synchronized to a WSUS server, and which updates are installed or are missing from each computer.

2. Identify

The administrator's goals for the Identify phase are:

- To discover new updates in a convenient manner.
- To determine whether updates are relevant to the production environment.

WSUS enables administrators to determine which types of updates to synchronize from Microsoft Update and when to synchronize them. Because WSUS automatically gathers data about all the computers known to the WSUS server in order to determine whether an update is relevant, administrators can see immediately how many computers need the update and how the deployment of the update would impact the network before installing the update in the production environment.

3. Evaluate and Plan

The administrator's goals for the Evaluate and Plan phase are:

- To test updates in an environment that is separate from but resembles the production environment.
- To determine the tasks necessary to deploy updates into production, plan the update releases, build the releases, and then conduct acceptance testing of the releases.

When evaluating updates in a test environment, administrators can run many of the WSUS features they would be using in the actual deployment. They can set the criteria and schedule for automatically synchronizing their WSUS servers, create computer groups, and then target updates for those groups by approving updates for install. During and after testing, administrators can use the standardized reports that WSUS provides to monitor the success of their test update installations.

WSUS enables administrators to evaluate the result of installing updates before deploying them to a production environment. By creating a group of test computers and autoapproving different sets of updates by product, language, and other classifications, administrators can test various types of updates using automation. During and after testing, administrators can correlate WSUS update reports with their test results to validate installed updates and decide how and when to schedule download and installation approvals for the production environment.

4. Deploy

The administrator's goals for the Deploy phase are:

- To approve and schedule update installations.
- To review the process after the deployment is complete.

WSUS allows administrators to specify target groups of computers and approve the deployment of updates to those groups. To establish the order in which updates are deployed, administrators can use WSUS to create the most efficient upstream and downstream WSUS server configuration for their network and staffing resources. In addition, administrators can configure how client computers communicate with WSUS servers or Microsoft Update by using Group Policy or by scripting with the WSUS API. The administrator can then use reporting to determine the success of the update deployment by computer or target group.

WSUS Next Steps

Go to the Windows Server Update Services site (<http://go.microsoft.com/fwlink/?LinkId=71198>) to:

- Download WSUS.
- Download this WSUS documentation:
 - Step-by-Step Guide to Getting Started with Microsoft Windows Server Update Services (<http://go.microsoft.com/fwlink/?LinkID=71190>)
 - Readme for Windows Server Update Services 3.0 (<http://go.microsoft.com/fwlink/?LinkId=71220>)