

9 Maintaining the Operating System



Exam Objectives in this Chapter:

- Manage software update infrastructure
- Manage software site licensing

Why This Chapter Matters

On June 14, 2005, Microsoft released 10 security bulletins as part of its monthly update release. Three of these were rated “Critical,” and analysts expected that code exploiting the vulnerabilities would hit the streets within one week. In late 2005 a vulnerability in the Windows Metafile Format (WMF) was announced and exploits were released before Microsoft was able to fully regression test an update against the wide variety of operating systems and applications affected by the problem. No longer is it acceptable to wait for Service Pack 3 before deploying Service Pack 2, as was the practice in many organizations until recently. It is now understood that an enterprise network that is not updated with code fixes is simply not secure. Software updates now became part and parcel of the security strategies of an organization.

In this chapter, you will learn how to apply Microsoft Windows Server Update Services (WSUS) to keep servers and desktops up to date. WSUS allows an enterprise to centralize the downloading, testing, approval, and distribution of Windows-critical updates and Microsoft Windows security rollups. This service will play a significant role in maintaining the integrity of your enterprise network. You will also learn how to deploy Service Packs to one or more machines. Finally, you will examine the components of site software licensing.

Lessons in this Chapter:

- Lesson 1: Windows Server Update Services9-3
- Lesson 2: Service Packs9-27
- Lesson 3: Administering Software Licenses9-30

Before You Begin

This chapter presents the skills and concepts related to administering Windows Server Update Services, service pack deployment, and licensing. Although it is advantageous to have two computers (a computer running Microsoft Windows Server 2003 and a client running Windows XP or Windows 2000 Professional), you can complete the exercises in this chapter with only one computer. Prepare the following:

- Windows Server 2003 (Standard Edition or Enterprise Edition) installed as Server01 and configured as a domain controller in the domain *contoso.com*
- 10 GB of free disk space to support the installation of WSUS
 - A first-level organizational unit (OU) named Desktops
 - Networking configured to provide Internet connectivity

Lesson 1: Windows Server Update Services

To maintain a secure computing environment, it is critical to keep systems up to date with security patches. Since 1998, Microsoft has provided Windows Update as a Web-based source of information and downloads. With Windows XP and Windows 2000 Service Pack 3, Microsoft added Automatic Updates, through which a system automatically connects to Windows Update and downloads any new, applicable patches or “hotfixes.” Although the Windows Update servers and Automatic Updates client achieve the goal of keeping systems current, many administrators are uncomfortable with either computers or users deciding which patches should be installed because a patch might interfere with the functioning of a business-critical application.

Microsoft’s first effort to create a centralized technology for managing software updates was Software Update Services (SUS). SUS addressed the demands of Microsoft customers for easier deployment of security updates but lacked key features, including the capability to update applications such as Microsoft Office and to easily report the status of patched systems on the network.

In mid-2005, Microsoft released Windows Server Update Services (WSUS), a significant enhancement of the technologies that had been introduced as SUS. Like SUS, WSUS is a client-server application that enables a server on your intranet to act as a point of management for the distribution of updates. You can approve updates for WSUS clients, which then download and install the approved updates automatically without requiring local administrator account credentials or user interaction.

In this lesson, you will learn to install and administer WSUS on a computer running Windows Server 2003. The following lesson will guide you through the steps required to configure systems on your network to receive updates from WSUS.



Exam Tip As of the date of writing, the 70-290 certification exam objectives relate only to SUS. Although it would be expected that Microsoft will update the exam, it is important that you study and thoroughly understand SUS prior to taking the 70-290 exam. We have included the previous version of this chapter on the CD-ROM accompanying this book.

After this lesson, you will be able to

- Install WSUS on a computer running Windows Server 2003
- Configure WSUS
- Deploy and configure Automatic Updates for WSUS clients

Estimated lesson time: 30 minutes

Understanding WSUS

Since 1998, Microsoft Windows operating systems have supported Windows Update, a globally distributed source of updates. Windows Update servers interact with client-side software to identify critical updates, security rollups, and enhancements that are appropriate to the client platform and then to download approved patches. Several years later, Microsoft introduced Automatic Updates, a client-side component that enabled users to schedule update detection, download, and installation and thereby removed most of the risk presented by users who never visited the Windows Update site.

But Automatic Updates and the server-side Windows Update still had two major faults. First, they provided updates to only the Windows operating system. Users had to visit the Office Updates site to receive patches for Microsoft Office applications, and those patches could not be scheduled or installed without user interaction. There was no mechanism for automatically detecting updates to any other major Microsoft platform, server, or application. The second weakness of Automatic Updates and Windows Updates was that there was not a way to control exactly which updates were applied, leading to a risk that an update would “break” another system component or application. Administrators wanted a more centralized solution that would assure more direct control over updates that are installed on their clients.

These two key customer demands were addressed during the first half of the decade, first by SUS, which enabled enterprises to centralize and manage the approval and distribution of updates; second, by the new Microsoft Update service (<http://update.microsoft.com/microsoftupdate>), a revision and superset of Windows Update that provides updates to a variety of platforms, servers, and applications; and third, by WSUS, which empowers you with greater levels of control and reporting and provides a foundation for an update framework on which Microsoft and its customers can build new functionality. For example, Microsoft’s new corporate antispyware platform will deliver updates to spyware definitions through WSUS.

It is easiest to understand WSUS by focusing on its components:

- **Updates** Updates are revisions to the code of a platform, server, or application. Microsoft categorizes updates as security updates, nonsecurity-related patches simply called “updates,” enhancements to functionality called “feature packs,” fixes to highly specific issues called “hotfixes,” and collections of updates called “cumulative updates,” “rollups,” or “service packs.” The lines between these categories are sometimes blurry; however, two points are important to highlight. First, security updates warrant your immediate and focused attention with the goal of evaluating updates for deployment to appropriate systems as quickly as reasonably possible. To facilitate your analysis, Microsoft rates security updates as “Crit-

ical,” “Important,” “Moderate,” and “Low.” Second, hotfixes, which are highly specific and have not been regression tested, should be applied only to systems that are encountering the issue addressed by the hotfix. Other categories of updates fall between these two extremes.

Updates consist of two elements: the update file itself, which is downloaded and installed by the client, and information about the update, such as its release date, the technologies to which the update applies, and whether the update supersedes a previous update. The information about the update is called metadata.

- **The Windows Update and Microsoft Update services** These globally distributed services provide updates to clients. Users visiting these sites download an ActiveX control that interacts with the local system to identify, download, and install required updates.
- **Automatic Updates** The Automatic Updates client is responsible for downloading updates from Windows Update, Microsoft Update, or a WSUS server and installing those updates based on a schedule or an administrator’s initiation.
- **WSUS, running on an Internet Information Services (IIS) server with connectivity to a local or remote database** WSUS is responsible for synchronizing information about available updates from Microsoft Update and, typically, downloading approved updates. WSUS thereby centralizes the distribution of updates, so Automatic Updates clients can be directed to use an intranet update infrastructure rather than Microsoft’s online update services. You can distribute WSUS servers throughout an enterprise to provide the most effective delivery of updates to systems in the enterprise, and you can configure each WSUS server to download from either Microsoft’s update services or another internal WSUS server. The WSUS database, in which information about updates and clients is stored, can be either Microsoft SQL Server 2000 or later or SQL Server 2000 Desktop Engine (Windows) (WMSDE). The choice of a database engine will be discussed later in the lesson.
- **The WSUS administration Web site** All WSUS administration is Web-based. After installing and configuring WSUS, regular administration consists of ensuring that the WSUS server is synchronizing successfully, approving updates for distribution to network clients, and reporting the status of the update infrastructure. The Uniform Resource Locator (URL) of a WSUS server’s administrative Web site is, by default, <http://servername/WSUSAdmin>.
- **Group Policy settings** Automatic Updates clients can be configured to synchronize from a WSUS server rather than the Windows Update servers by modifying the clients’ registries or, more efficiently, by configuring Windows Update policies in a Group Policy Object (GPO). The configuration of the Automatic Updates client will be addressed in the next lesson.

An update infrastructure based upon these components functions using the following important processes:

- **Subscription to updates** A WSUS administrator subscribes to updates based on category (for example, security updates and service packs), technology (for example, Windows Server 2003, Windows XP, and Microsoft Office 2003), and language. Subscriptions can be modified at any time.
- **Synchronization** The WSUS server downloads metadata about updates only for subscribed content, technologies, and languages during a process called *synchronization*. If the server is configured to download update files themselves, as well as their metadata, the files are also downloaded during synchronization. Synchronization can be scheduled or initiated manually.
- **Approval** Updates can be approved by a WSUS administrator or can be autoapproved based on rules configured on the server. An update can be approved for one of several actions: detection, installation, or removal. These actions will be addressed later in this lesson.
- **Targeting** It is common for administrators to apply certain updates to a subset of systems, based on the role, location, function, or priority of the system. WSUS, unlike SUS, provides for targeting updates to specified groups of computers.
- **Client redirection** Through registry entries or Group Policy settings, clients can be directed to receive updates from a WSUS server rather than from Microsoft Update or Windows Update. It's very important to remember that *all* systems should be considered update clients. Servers and domain controllers require constant updating as much as workstations.
- **Detection** The Automatic Updates client receives metadata about an update and uses that metadata to determine whether the update is applicable.
- **Download** If a system identifies an applicable update, the update is downloaded to the local hard drive. Updates are downloaded using Background Intelligent Transfer Service (BITS) 2.0, which makes effective use of network bandwidth by using only available bandwidth for file transfer.
- **Installation** The update file is applied using elevated credentials, so no user interaction is required and administrative credentials are not necessary. Because Microsoft's updates are digitally signed and verified by both the WSUS server and the client, security exposure to a malformed update is minuscule.
- **Reporting** Clients report the status of updates to the WSUS server. Administrators can produce reports based on the status of computers or updates using the WSUS administrative Web site.
- **Rebooting** Some updates require a system restart; however, Microsoft is improving the functionality of updates so that patches to drivers, dynamic-link libraries

(DLLs), application programming interfaces (APIs), or any nonkernel-level component will not require a reboot—a feature called “hot patching” that was introduced in Service Pack 1.

Now that you understand the components and processes involved with getting an update from Microsoft to the client, we will spend the rest of this lesson focused on the server-side installation and configuration of WSUS. Keep in mind that you will use Group Policy to “point” clients to your WSUS server for updates. We will discuss the details of that task later in this lesson. Each of the concepts and procedures outlined in this chapter is explored in depth in the WSUS documentation, which is available along with the WSUS installation files, from <http://www.microsoft.com/wsus>.

Designing a WSUS Infrastructure

The WSUS documentation details the considerations related to the design of an update infrastructure. Key concepts include the selection and placement of WSUS servers and the relationships between WSUS servers and the Microsoft Update service.

Because the goal of WSUS is to deliver updates to clients as efficiently as possible, you should place WSUS servers as close to systems as you can. Ideally, you do not want clients to have to pull updates from a WSUS server on the other side of a slow or expensive wide area network (WAN) link. WSUS is not a particularly performance-intensive service, and you can design your update infrastructure to synchronize updates from Microsoft and deliver updates to clients during nonbusiness hours. Therefore, WSUS can be co-located on servers that perform other duties during business hours. Consider that each WSUS requires IIS and a database instance: SQL Server 2000 or later or WMSDE.



Planning There is another design driver that is particularly salient in larger organizations: WSUS can be administered only by users who are local administrators on the WSUS server. There is no other way to delegate administration of WSUS. Therefore, you should co-locate WSUS only with other services and resources for which the same users are administrators. This security and delegation characteristic also suggests that, where possible, WSUS should be installed on a member server rather than on a domain controller. Otherwise, to administer WSUS, a user must be logged on with credentials that have administrative privileges for the entire domain.

Using SUS, a server could have only one list of approved updates. Therefore, if you wanted to deliver different sets of updates to different clients—for example, one collection of updates to servers and a different collection of updates to workstations—you needed to point each group of computers to a separately administered SUS server.

WSUS introduces the concept of client groups, which allows you to create virtual collections of systems, each of which can receive a unique set of updates on a unique release schedule. For example, you might create a group called “Test Systems” for which you approve updates for installation soon after Microsoft releases the updates. If these test systems prove that the updates are appropriate for your organization, you can then approve the updates for installation on other computers. Using client groups, you can support many update configurations using a single WSUS server. Therefore, with WSUS, you are no longer forced into a multiple-server model solely to support multiple combinations of updates. The purpose of using multiple WSUS servers is solely to deliver the updates with minimal network cost to update clients.

After selecting the servers on which WSUS will be hosted, you must determine how updates will flow from Microsoft Update to each server. One or more servers can synchronize their updates directly from Microsoft Update. Each such server can be independently administered, allowing you to have a completely unique collection of approved updates on each server. In a highly decentralized update infrastructure, this might be desirable.

A more typical configuration involves one “upstream” WSUS server that synchronizes from Microsoft Update, with other “downstream” servers synchronizing from that server. You can, in fact, have several levels of downstream servers, each pointing to an upstream server as its source for updates. However, update service models more than three levels deep are not recommended.

A hierarchical configuration can be structured in two ways: as a replica or as a decentralized model. In a replica model, the downstream WSUS server mirrors exactly the updates and approvals of its upstream server. This highly centralized administrative model ensures consistently applied updates. Clients pointed to either of the WSUS servers will receive the same updates. The only differences between two replicas are the set of computers that have been pointed to each server and, therefore, the specific computers that belong to client computer groups on each server.

In a decentralized model, each downstream server synchronizes updates from an upstream server, but update approvals are managed on each downstream server individually. Downstream servers will synchronize an update from its upstream server only if the update has been approved on the upstream server. Therefore, the upstream server, rather than Microsoft Update, acts as the authoritative source of available updates. Administrators of downstream servers can approve any subset of those updates. Such a structure allows administrators of upstream servers to prevent updates that might cause problems from propagating to downstream servers and clients.

Installing WSUS on a Windows Server 2003 Computer

An update infrastructure has both client and server components. The client component, Automatic Updates, will be discussed later in this lesson. The server component, WSUS, runs on Windows 2000 Server (Service Pack 4) or Windows Server 2003 on a 32-bit system. WSUS *cannot* be installed on 64-bit Windows Server 2003 platforms. This is an important exception. Windows Server 2003 64-bit systems can be *clients* of WSUS: they can receive updates from WSUS but cannot actually provide update services to other clients.

WSUS is not included with the Windows Server 2003 media, but it is a free download from the Microsoft WSUS Web site at <http://www.microsoft.com/wsus>. WSUS includes the SQL Server 2000 Desktop Engine (Windows) (WMSDE) database, which is required to support WSUS, unless you choose to use an instance of SQL Server 2000 or later. WSUS requires BITS 2.0 or later, which is integrated into SP1 and can be downloaded separately from the WSUS site for earlier versions of Windows Server 2003 or Windows 2000.



Note The WSUS download is not available in every localized language. However, this download determines the installation and administrative interface for the server component only. Patches for *all* locales can be made available through WSUS.

Prior to installing WSUS, you must install IIS, which, as you learned in Chapter 6, is not installed by default on Windows Server 2003. For information about how to install IIS, see Chapter 6. You must also install BITS 2.0 or later if the server is not running SP1. Then run the WSUS installation package.

After you agree to the license agreement, the Setup Wizard will prompt you for the following information:

- **Select Update Source** Each update consists of two components: the patch file itself and metadata that specifies the platforms and languages to which the patch applies. WSUS always downloads metadata, which you will use to approve updates and which clients on your intranet will retrieve from WSUS. You can choose whether to download the update installation files themselves and, if so, where to save the updates.



Tip If you elect to maintain the update files on Microsoft Windows Update servers, Automatic Updates clients will connect to your WSUS server to obtain the list of approved updates and will then connect to Microsoft Update servers to download the files. You can thereby maintain control of client updating and take advantage of the globally dispersed hosting provided by Microsoft.

If you select the Store Updates Locally check box, the Setup Wizard defaults to the drive with the most free space and will create a folder called WSUS on that drive. You can save the files to any NT file system (NTFS) partition; Microsoft suggests a minimum of 6 gigabytes (GB) of free space in the WSUS documentation—however, significantly more is recommended: at least 40 GB.

- **Database Options** WSUS requires an instance of a database within which update metadata and client reports will be stored. On Windows Server 2003, WSUS will default to an installation of WMSDE on the disk with the greatest amount of free space. However, you can also select a local installation of SQL Server as the database for WSUS.



Note You can install WSUS and SQL Server on separate servers. The WSUS deployment guide, which you can download from Microsoft's WSUS Web site, contains step-by-step instructions. However, more than one WSUS server cannot "share" a SQL server. You must have one SQL server or WMSDE server for each WSUS server.

- **Web Site Selection** WSUS installs to the default Web site, port 80, of an IIS server. If the server hosts an existing Web site on port 80, you may configure WSUS to install to an alternate site, which will be assigned to port 8530. You can change this port after setup has completed.
- **Mirror Update Settings** This page of the Microsoft Windows Server Update Services Setup Wizard, shown in Figure 9-1, allows you to create a replica WSUS server, which replicates updates, approvals, group definitions, and configuration settings from another WSUS server. It is possible to configure a replica only at this point in the setup process: select the This Server Should Inherit Settings From The Following Server check box and enter the Server Name and TCP Port. After installation is complete, you cannot configure an existing stand-alone server as a replica, nor can you configure a replica to act as a standalone server. This page of the Setup Wizard is misleading for many administrators who attempt to create a downstream server during setup. Downstream servers, which download update files from an upstream server but maintain independent approvals, group definitions, and many settings, are configured after setup.

When installation is complete, you are ready to configure and administer WSUS. In fact, the last page of the Microsoft Windows Server Update Services Setup Wizard, by default, launches the Web administration page for WSUS.

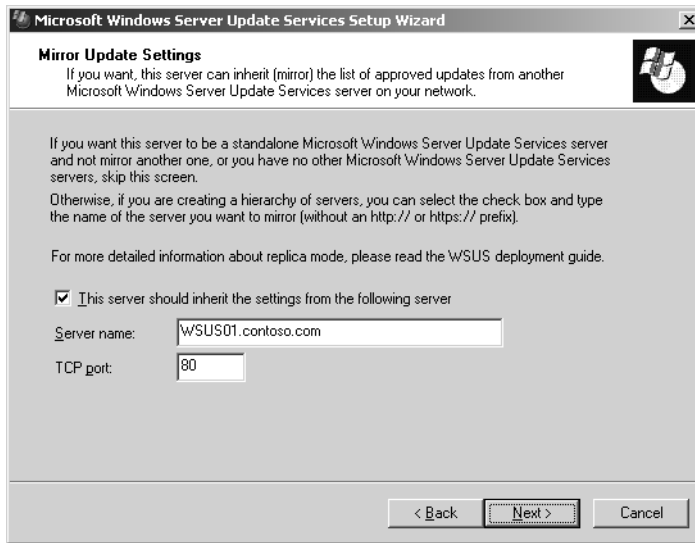


Figure 9-1 The Mirror Update Settings page of the WSUS Setup Wizard

Configuring and Administering WSUS

You will perform five categories of administrative tasks related to supporting WSUS servers: configuring settings, synchronizing content, approving updates, managing computer groups, and reporting update status. You perform these tasks using the WSUS Administration Web site, shown in Figure 9-2, which you can access by navigating to http://WSUS_servername/WSUSAdmin with Internet Explorer 5.5 or later. The administration of WSUS is entirely Web-based. The home page of the WSUS administration site contains a useful summary of server and update status, along with a To-Do list of issues requiring administrative attention.



Note You might need to add your WSUS server to the list of sites in the Trusted Sites zone. Open Internet Explorer and choose Internet Options from the Tools menu. Click the Security tab. Select Trusted Sites and click Sites. Clear the option to require Hypertext Transfer Protocol Secure (HTTPS), and then add your server. After adding the server, you may reselect the option to require HTTPS.

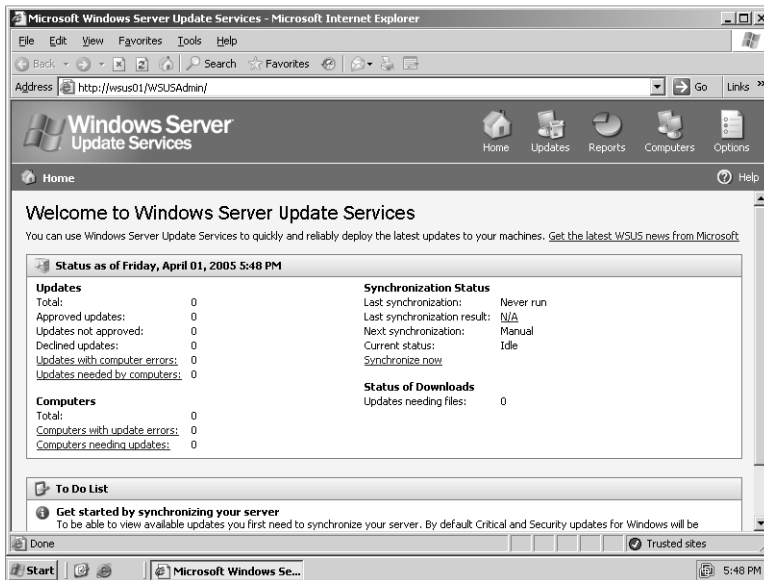


Figure 9-2 The WSUS Administration Web site

Configuring Windows Server Update Services Settings

Although you can specify some of the configuration of WSUS during a custom installation, all WSUS settings are accessible from the WSUS administration Web page. From the Windows Server Update Services administration page, click **Options** in the top navigation bar. Then click the **Synchronization Options** link.

The settings on the Synchronization Options page are easiest to understand if we categorize the issues you will be addressing through your choice of configuration.

- From where does this WSUS server synchronize?** You use the Update Source frame to configure the server as a true stand-alone server that synchronizes from Microsoft Update or to synchronize from an upstream server. If you select **Synchronize From An Upstream Windows Server Update Services Server**, you create a hierarchical model. The upstream server manages approvals at a “global” level. A downstream server will synchronize only those updates that have been approved upstream. An administrator of the downstream server can then approve one or more of those updates. Remember, this model differs from a replica model in that a replica synchronizes all approvals and settings from its source. Approvals and many settings on a downstream server are independently managed. A replica must be created during installation of WSUS.

- **What content do you wish to synchronize?** Use the Products, Classifications, and Languages buttons to select the types of content that will be synchronized to the WSUS server. As of the date of publication, WSUS can synchronize updates for Windows 2000 and later operating systems, Microsoft Office XP and later, Microsoft SQL Server, and Microsoft Exchange Server. There are a variety of classifications, including critical updates, security updates, service packs, drivers, and feature packs. Note that you will not see all available products or classifications until *after* the server synchronizes with Microsoft Updates for the first time. By default, WSUS downloads critical and security updates in every language. Use the language button to select the languages for which updates will be downloaded. In an environment in which localized versions of Windows have been installed, select all appropriate languages. If you use the Multilanguage User Interface, select English. If you use only one language, select that language or the option Download Only Those Updates That Match The Language Of This Server.
- **What will be downloaded during synchronization?** WSUS downloads update metadata for all updates available on its update source. The actual files with which the updates are installed may be downloaded to the server as well, or the WSUS server may be configured to act only as the list of approved updates, at which point clients download the update files from the Microsoft Web site. In most enterprises, updates are stored locally, as shown in Figure 9-3.

If updates will be stored locally, you may choose to defer downloading the update installation files until after the update has been approved. This conserves bandwidth by skipping the download of nonapproved updates. Additionally, you may select to download express installation files. Whereas a standard installation of an update completely replaces the file, express installation files apply the bit-level difference between the existing version of a file and its updated version. This type of updating is called “delta compression” because only the change, or delta, is applied. Therefore, the amount of data transferred from the WSUS server to the client is reduced significantly. However, to account for every possible variation between original versions of a file and the updated version, the WSUS server must download and store every possible delta. So a somewhat larger file is transferred from Microsoft to the WSUS server to preserve the bandwidth between the server and the end system.

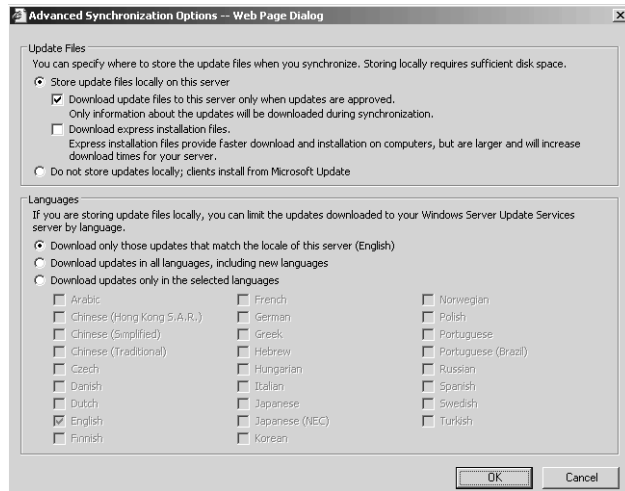


Figure 9-3 Update files storage options

- **Proxy server configuration** If the server running WSUS connects to Windows Update using a proxy server, you must configure proxy settings.



Tip Although you can configure the WSUS server to access Windows Update through a proxy server that requires authentication, the Automatic Updates client cannot access Windows Update if the proxy server requires authentication. If your proxy server requires authentication, you can configure WSUS to authenticate, and you must store all update content—files as well as metadata—locally.

Synchronizing Content

The Schedule frame of the Synchronization Options page exposes the settings to schedule synchronization. For the most hands-free operation of WSUS, schedule a daily synchronization during nonbusiness hours. You can also trigger synchronization manually by clicking the Synchronize Now link in the left navigation bar. During synchronization, you cannot change other server settings. The metadata for available updates is downloaded from the update source: either Microsoft Update or an upstream WSUS server. If specified in the Update Storage options, the update installation files or express installation files are downloaded as well. When deferred download is selected, those files are synchronized only after they are approved for installation on one or more clients. Synchronization progress is indicated in the left frame of the Synchronization Options page and on the WSUS home page.

Approving Updates

Update management includes identifying, evaluating, and approving updates. You perform each of these tasks using the Updates page of the WSUS administration site. From the WSUS home page, click the Updates link in the top navigation bar. The Updates page, shown in Figure 9-4, appears.

The screenshot displays the WSUS administration interface. At the top, there's a navigation bar with 'Home', 'Updates', 'Reports', 'Computers', and 'Options'. The main area is titled 'Updates' and shows a filtered view of 328 updates. The left-hand pane has 'Update Tasks' with 'Change approval' and 'Decline update' options, and a 'View' section for filtering updates by products, classification, approval, synchronization, and text. The main list shows updates like 'Windows Installer 3.1 Release Candidate' and 'Cumulative Security Update for Internet Explorer 6 Service Pack 1'. The details pane for a selected update shows its title, description, classification, release date, and installation information.

Title	Classification	Released	Approval
Windows Installer 3.1 Release Candidate	Critical Updates	4/4/2005	Install
Cumulative Security Update for Internet Explorer 6 Service Pack 1 (KB67801)	Security Updates	3/29/2005	Detect only
Critical Update for Windows XP (KB887822)	Critical Updates	3/25/2005	Detect only
Security Update for DirectX 8.2 (KB839643)	Security Updates	3/25/2005	Detect only
Cumulative Security Update for Outlook Express 6 Service Pack 1 (KB877000)	Security Updates	3/26/2005	Detect only

Details | Status | Revisions

Title: Critical Update for Windows XP (KB887822)
Description: This update corrects an issue that prevents some updates from properly installing on your system.
Classification: Critical Updates
Products: Windows XP Family
Release date: Friday, March 25, 2005
More information: <http://support.microsoft.com/kb/887822>
KB article number: 887822
MSRC number: None
MSRC severity rating: Unspecified
Update ID: a95d198-48f5-44f6-6d43-424fc8c272e7

Installation Information

Removable: No
May request user input: No
Restart behavior: Can request restart
Must be installed exclusively: No

Figure 9-4 Updates administration page

The list view in the top frame of the Updates page displays a subset of update metadata, including the update's title, classification, release date, and approval status. To locate a set of updates, use the view frame in the left task pane, with which you can filter updates by product type or name, classification, update type, approval status, synchronization date, or keywords, the last of which will allow you to search by knowledge base or security bulletin identifier or any word contained in the name or description of the update. When you select an update in the list, the details about the update appear in the details frame at the bottom of the page. Update metadata is displayed in three tabs: Details, Status, and Revisions.

To approve one or more updates for distribution to client computers, select the update(s) in the list, and then click the Change Approval link in the left navigation pane. The Approve Updates dialog box shown in Figure 9-5 appears. Using the drop-down list, you can configure one of four approval options:

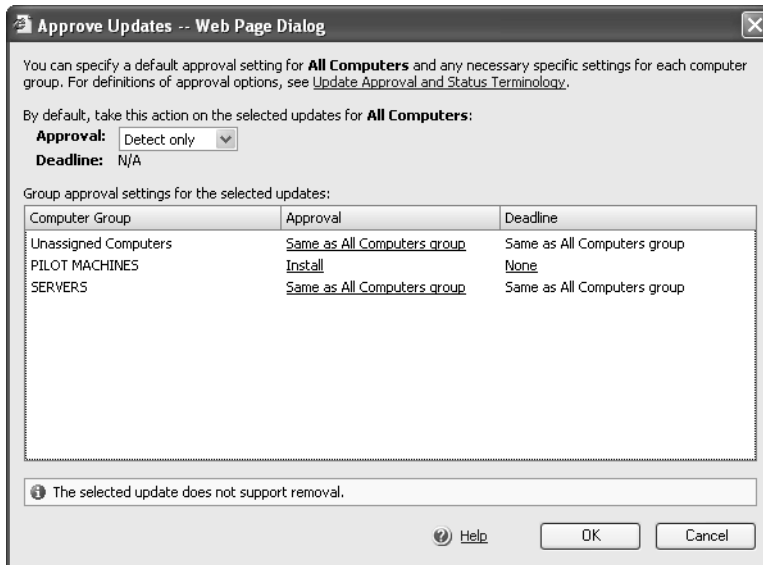


Figure 9-5 The Approve Updates page

- **Detect Only** Each client will discover the update on the WSUS server and, using update metadata, determine whether the update is needed. The client will then report whether the update is needed or not and you can view this feedback to determine whether to approve the update for installation. Detect Only approval does not result in the client installing the update; the client only detects and reports whether the update is needed.
- **Install** Each client will install the update if it is needed. Because updates contain detailed metadata that describes the update and its relationship to other updates, clients can evaluate the update to determine whether it is needed. If, for example, a client has already installed a service pack, any individual update that was included in that service pack would be unnecessary, so the client would skip the update even though it was approved for installation. This behavior ensures effective use of resources by preventing duplicate or superseded updates from being installed.
- **Not Approved** Clients will not download update metadata, so they will neither detect and report whether the update is needed nor install the update. If a client has already installed the update, it will not be removed, but no new clients will detect or install the update.
- **Remove** Some, but not all, updates support removal through WSUS and Automatic Updates. Approving an update for removal causes the client to uninstall the update. Most updates can be individually removed using Add or Remove Programs.

Note in Figure 9-5 that WSUS supports setting a deadline for installation of an update. This capability prevents even local administrators from delaying the update. If a client detects that an update has been approved for installation and the deadline has passed, the update will be installed. Although WSUS is inherently a “pull” technology—clients query the WSUS for updates and download the updates from the server—the deadline feature approaches the need to be able to “push” an urgent update to clients.

The option selected in the Approval drop-down list and the deadline configured in the top of the Approve Updates dialog box will apply, by default, to all computers directed to the WSUS server. WSUS introduces the ability to create computer groups, a feature discussed later in this lesson. Any computer that does not belong to a computer group is represented by the built-in group Unassigned Computers. After you create computer groups, you can configure approvals and deadlines differently for each computer group. For example, you might approve an update for installation on a group of pilot systems and for detection on other systems, as shown in Figure 9-5. If the update is successful on the pilot computers and is reported as needed by other computers, you can then approve the update for installation on remaining systems.

To decline an update, click the Decline Update link in the task pane of the Updates page. When you decline an update, it will not be installed by any clients; however, clients that have already installed the update will not remove it. The update installation files are not deleted from the WSUS server.

You can automate the approval workflow by configuring automatic approval. Click the Options link in the top navigation bar, and then click the Automatic Approval Options link. You can instruct WSUS to automatically approve updates based on classification for either detection or installation and for one or more computer groups. This version of WSUS does not support configuring automatic approvals based on product. By default, WSUS automatically approves critical updates and security updates for detection, so soon after Microsoft releases an update of those classifications, WSUS clients will begin to report whether those updates are required.

Occasionally, Microsoft will revise an update’s metadata or installation files. You can configure WSUS to automatically approve revisions to already-approved updates. Microsoft might also release updates to WSUS itself, and the Automatic Approval Options page exposes an option to approve such updates automatically.

Managing Computer Groups

Computer groups enable an enterprise to target updates to collections of systems based on their role, priority, location, function, or any other criteria. When designing your update infrastructure, consider how you might be able to leverage computer groups to attain the strategic objectives of your design. For example, by creating a computer group for pilot computers, you can approve new updates for installation

on those systems, monitor the results to ensure that the update does not cause problems, and then approve the update for installation on remaining systems. You might decide to have a group of computers that should be updated more quickly than others—for example, your servers exposed to the Internet. By placing those servers in a computer group, you can set a deadline for updates for those systems to ensure that those updates are installed quickly. WSUS always exposes two built-in groups: All Computers, representing every client that reports to the WSUS server; and Unassigned Computers, representing the subset of clients that do not belong to any custom computer group.

There are three steps to managing computer groups with WSUS. First, you select one of two ways to assign computers to groups: server-side targeting and client-side targeting. Server-side targeting, the default, requires you to add computers to groups using the WSUS administration site. Client-side targeting allows you to automatically assign clients to groups using either registry entries or Group Policy. Second, you create the computer groups on the WSUS server. Third, you move computers into groups using whichever method you selected in the first step.

To manage computer groups, click the Computers link in the top navigation bar. The Computers page lists all computers that have reported to the server. Remember that clients are directed to the WSUS server using registry entries or Group Policy settings that will be detailed later in this lesson. WSUS groups are not, interestingly, associated in any way with Active Directory directory service groups or with local security groups. WSUS groups are defined and maintained by the WSUS server itself. To create a new group, click the Create A Computer Group link and specify the group name. To delete a group, first select the group from the Groups list, and then click the Delete The Selected Group link in the Tasks frame.

To configure either client-side targeting or server-side targeting, click the Options link in the top navigation bar, and then click Computer Options. Select one of the following configurations:

- **Use The Move Computers Task In Windows Server Update Services** You will assign computers to groups using the WSUS administration page.
- **Use Group Policy Or Registry Settings On Client Computers** You will assign clients to groups using registry entries on the clients or using Group Policy.

With either server-side targeting or client-side targeting, you must create the groups on the WSUS server. Click the Computers link in the top navigation bar, and then click Create A Computer Group and enter the name for the group.

If you have configured server-side targeting, you must manage computer group membership on the WSUS server using the Computers page. Select a computer and, in the Tasks

pane, click Move The Selected Computer link. In an update infrastructure characterized by a small number of computer groups with limited membership, manual management of computer groups is possible.

In more complicated implementations, however, you will want to configure client-side targeting, also called computer-based targeting. In client-side targeting, clients register their group membership when they report to the WSUS server. Client computers are configured with their group membership using a registry entry or Group Policy. In a non-Active Directory environment, you configure the TargetGroup registry string entry with the name of the group, and you configure the TargetGroupEnabled registry dword entry with the value 1. Both these registry entries are found in the HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate key. In an Active Directory environment, you can automate the configuration of update group membership by enabling the Enable Client-Side Targeting Group Policy setting. In a GPO, open the Computer Configuration, Administrative Templates, Windows Components, Windows Update node. Open the Enable Client-Side Targeting setting and click Enabled. Type the name of the computer group in the box. Any computers within the scope of the GPO will report that group membership to the WSUS server.

With client-side targeting enabled, a client reports its group membership to WSUS, but the membership will not take effect unless the group exists on the WSUS server. So, as with server-based targeting, you must create all groups on the WSUS server that you have configured for client-side targeting. If a client reports membership in a group that does not exist on the WSUS server, a warning will register on the WSUS administration home page to help you identify the problem. Until you resolve the conflict, either by creating the computer group or by moving the computer into an existing group, the computer will be managed as an unassigned computer.

Reporting Update Status

The Reports page of the WSUS administration site enables you to view and print reports based on updates or computers. Click the Reports link in the top navigation bar, and then choose Status Of Computers or Status Of Updates. Reports can be filtered to show results from one computer group or for All Computers and to show results from one or more approval levels. Update reports summarize, for each update, the number of computers that report the update as installed, needed, not needed, uninstalled, or failed. You can expand an update to see detail for the update by computer group, and you can expand a computer group to see the detail for each computer in that group. An update report is displayed in Figure 9-6.

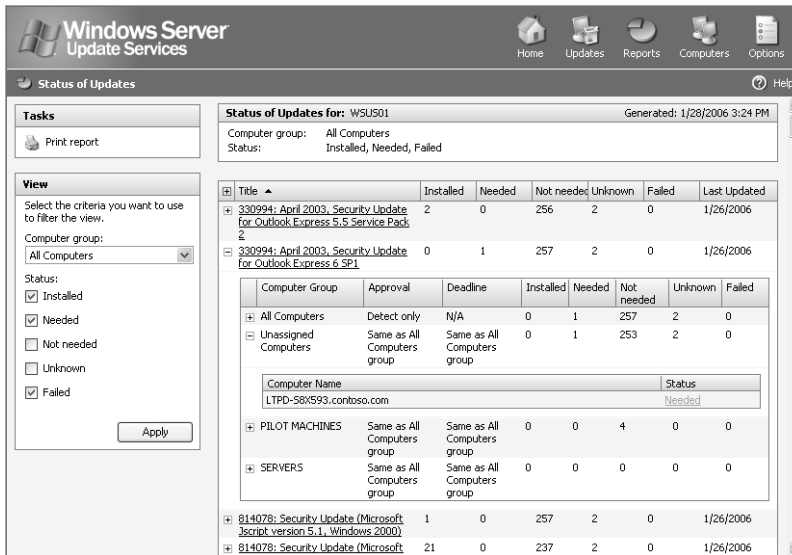


Figure 9-6 WSUS update report

A computer report displays, for each computer, the number of updates installed, needed, uninstalled, or failed. Expand a computer to see the detail for each update. A computer report is displayed in Figure 9-7.

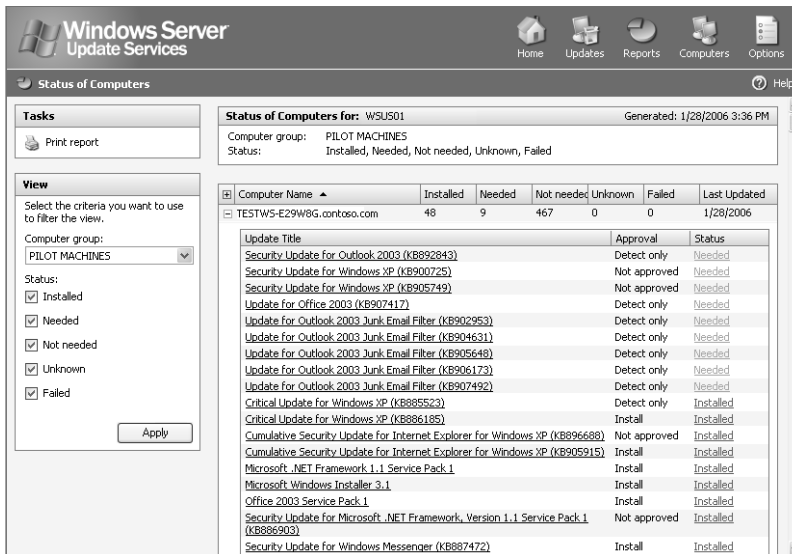


Figure 9-7 WSUS computer report

You can access two other reports through the Reports link in the top navigation bar: Synchronization reports, which detail synchronization activity, and Settings reports, which can be particularly useful when you are configuring additional WSUS servers and want to maintain consistency with existing servers. You can also access reports using the Status tab on either the Computers or Updates pages. All reports can be sorted by column and printed.



Note As you view reports, remember that you are seeing the activity of only one WSUS server. You must view the reports on each server separately. This version of WSUS does not natively support “rolling up” the status of multiple servers. However, Microsoft provides sample tools on the WSUS Web site, one of which provides rollup functionality. Another sample allows you to create and populate WSUS computer groups using Active Directory groups as a data source.

The Automatic Updates Client

The client component of WSUS is Windows Automatic Updates, which is supported on Windows 2000, Windows XP, and Windows Server 2003. The Automatic Updates client is included with Windows Server 2003, Windows 2000 Service Pack 3, and Windows XP Service Pack 1. When a client with the original version of Automatic Updates reports to WSUS, the client will upgrade itself automatically to the new version of Automatic Updates that is compatible with WSUS. This newer version is installed by default by Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1.

The Automatic Updates client is configured to connect automatically to the Microsoft Windows Update server and then download updates and prompt the user to install them. You can modify this behavior by accessing the Automatic Updates tab in the System Properties dialog box, accessible by clicking System in Control Panel in Windows XP and Windows Server 2003. In Windows 2000, click Automatic Updates in Control Panel. The Automatic Updates tab is shown in Figure 9-8. The options on the tab are limited and do not allow you to direct Automatic Updates to a WSUS server. You can use Group Policy settings or registry values to fully configure Automatic Updates for WSUS.

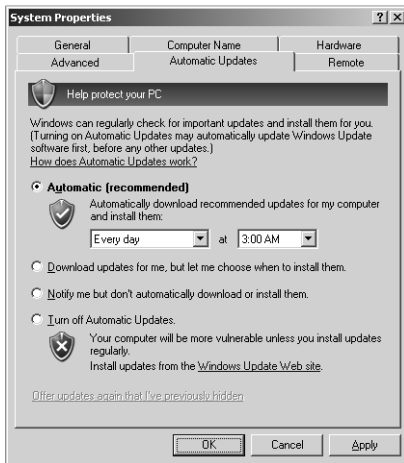


Figure 9-8 The Automatic Updates tab of the System Properties dialog box

Download Behavior

Automatic Updates supports two download behaviors:

- **Automatic** Updates are downloaded without notification to the user.
- **Notification** If Automatic Updates is configured to notify the user before downloading updates, it registers the notification of an available update in the system event log and to a logged-on administrator of the computer. If an administrator is not logged on, Automatic Updates waits for a user with administrator credentials before giving notification by means of a balloon in the notification area of the system tray.

After update downloading begins, Automatic Updates uses BITS to perform the file transfer using idle network bandwidth. BITS ensures that network performance is not hindered due to file transfer. The Automatic Updates client validates the Microsoft digital signature and examines the cyclical redundancy check (CRC) on each package before installing it.

Installation Behavior

Automatic Updates provides two options for installation:

- **Notification** Automatic Updates registers an event in the system log indicating that updates are ready for installation. Notification will wait until a local administrator is logged on before taking further action. When an administrative user is logged on, a balloon notification appears in the system tray. The administrator

clicks the balloon or the notification icon and then may select from available updates before clicking Install. If an update requires restarting the computer, Automatic Updates cannot detect additional updates that might be applicable until after the restart.

- **Automatic (Scheduled)** When updates have been downloaded successfully, an event is logged to the system event log. If an administrator is logged on, a notification icon appears and the administrator can manually launch installation at any time until the scheduled installation time.

At the scheduled installation time, an administrator who is logged on will be notified with a countdown message prior to installation and will have the option to cancel installation, in which case the installation is delayed until the next scheduled time. If a nonadministrator is logged on, a warning dialog box appears but the user cannot delay installation. If no user is logged on, installation occurs automatically. If an update requires restart, a five-minute countdown notification appears informing users of the impending restart. Only an administrative user can cancel the restart.



Tip If a computer is not turned on at the scheduled Automatic Updates installation time, installation will wait to the next scheduled time. If the computer is never on at the scheduled time, installation will not occur. Ensure that systems remain turned on to be certain that Automatic Updates install successfully, or configure the Reschedule Automatic Updates Scheduled Installations policy setting, described below.

Configuring Automatic Updates Through Group Policy

The Automatic Updates client will, by default, connect to the Microsoft Windows Update server. After you have installed WSUS in your organization, you can direct Automatic Updates to connect to specific intranet WSUS servers by configuring the registry of clients manually or by using Windows Update group policies.

To configure Automatic Updates using GPOs, open a GPO and navigate to the Computer Configuration\Administrative Templates\Windows Components\Windows Update node. The Windows Update policies are shown in Figure 9-9.

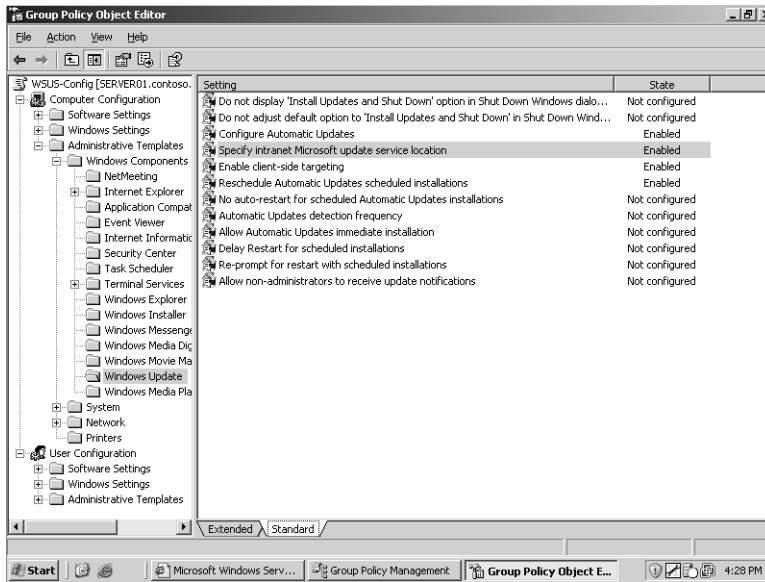


Figure 9-9 Windows Update policies



Note The Automatic Updates policies described below are supported by the newest version of the %Windir%\Inf\Wuau.inf administrative template, which is installed by default on Windows XP SP2 and Windows Server 2003 SP1. If you do not see the policies, copy Wuau.inf from an appropriate system, right-click the Administrative Templates node and choose Add/Remove Templates, click Add, and then locate the Wuau.inf template.

The following policies are available, each playing an important role in configuring effective update distribution in your enterprise:

- Specify Intranet Microsoft Update Service Location** This policy allows you to redirect Automatic Updates to a server running WSUS. You must configure the two text boxes with the URL to the WSUS server *http://serverFQDN*. If you have installed WSUS to a port other than port 80, you must include the port in the URL—for example, *http://serverFQDN:port*.



Note Be sure that any firewall, including Windows Firewall, allows inbound traffic on Transmission Control Protocol (TCP) port 80 to the WSUS server.

- Automatic Updates Detection Frequency** Automatic Updates clients poll their WSUS server every 22 hours, minus a random offset. This policy setting allows you to modify that frequency.

- **Configure Automatic Updates** When an update has been detected, you control the download and installation behavior of the client using this policy setting. There are three options: Notify For Download And Notify For Install, Auto Download And Notify For Install, and Auto Download And Schedule The Install. These options are combinations of the installation and download behaviors discussed earlier in the lesson.
- **Reschedule Automatic Updates Scheduled Installations** If installations are scheduled and the client computer is turned off at the scheduled time, the default behavior is to wait for the next scheduled time. The Reschedule Automatic Updates Scheduled Installations policy, if set to a value between 1 and 60, causes Automatic Updates to reschedule installation for the specified number of minutes after system startup.
- **Enable Client-Side Targeting** If you have configured the WSUS server for client-side targeting, you can use this policy to configure clients with a specific computer group. The client will report this group name to the WSUS server. The group must be defined on the WSUS server, as discussed in this lesson.



See Also For guidance regarding client configuration using registry settings, see the WSUS documentation, which is available along with the WSUS installation files from <http://www.microsoft.com/wsus>.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the “Questions and Answers” section at the end of this chapter.

1. You are configuring a WSUS infrastructure. One server is synchronizing metadata and content from Microsoft Update. Other servers (one in each site) are synchronizing content from the upstream WSUS server. Which of the following steps is required to complete the WSUS infrastructure?
 - a. Configure Automatic Updates clients using Control Panel on each system.
 - b. Configure GPOs to direct clients to the WSUS server in their sites.
 - c. Configure a manual content distribution point.
 - d. Approve updates using the WSUS administration page.

2. You are configuring WSUS for a group of Web servers. You want the Web servers to update themselves nightly based on a list of approved updates on your WSUS server. However, once in a while an administrator is logged on, performing late-night maintenance on a Web server, and you do not want update installation and potential restart to interfere with those tasks. What Windows Update policy configuration should you use in this scenario?
 - a. Notify For Download And Notify For Install
 - b. Auto Download And Notify For Install
 - c. Auto Download And Schedule The Install
3. You want all network clients to download and install updates automatically during night hours, and you have configured scheduled installation behavior for Automatic Updates. However, you discover that some users are turning off their machines at night, and updates are not being applied. Which policy allows you to correct this situation without changing the installation schedule?
 - a. Specify Intranet Microsoft Update Service Location
 - b. No Auto-Restart For Scheduled Automatic Updates Installations
 - c. Reschedule Automatic Updates Scheduled Installations
 - d. Configure Automatic Update

Lesson Summary

- WSUS is an intranet application that runs on IIS 6.0 and is administered through a Web-based administration site: *http://WSUS_Servername/WSUSAdmin*.
- The WSUS server synchronizes content for subscribed product types and update classifications and allows an administrator to configure approval centrally for each update. Typically, an enterprise configures WSUS to download the actual update installation files as well.
- Updates can be targeted to specific computers by defining computer groups on the WSUS servers. The membership of those groups can be managed on the server or by using client-side registry entries or Group Policy settings.
- Automatic Updates, which runs on Windows 2000, Windows XP, and Windows Server 2003, is responsible for downloading and installing updates on the client.
- Group Policy can be used to configure Automatic Updates to retrieve patches from a WSUS server rather than from the Windows Update servers. GPOs can also drive the download, installation, and restart behavior of the client computers.

Lesson 2: Service Packs

Microsoft releases service packs to consolidate critical updates, security rollups, hot-fixes, driver updates, and feature enhancements. As suggested at the beginning of this chapter, it is no longer feasible to wait until Service Pack 3 before installing Service Pack 2. You must stay current with service packs to maintain the security and integrity of your enterprise network. WSUS, discussed in the previous lesson, is capable of distributing service packs, but SUS is not. In environments where service packs are not deployed using an update infrastructure, you need to implement the skills covered in this lesson, which will allow you to deploy service packs by means of Group Policy.

After this lesson, you will be able to

- Download and extract a service pack
- Deploy a service pack with Group Policy–based software distribution

Estimated lesson time: 5 minutes

Downloading and Extracting Service Packs

When a service pack is released, Microsoft makes it available for installation and download from the Microsoft Web site. A service pack can be installed directly from a Microsoft server, in which case the client launches the service pack setup from the Microsoft site, and a small setup utility is downloaded to the client. That setup utility reconnects to the Microsoft server and controls the download and installation of the entire service pack. Service packs are generally sizeable, so performing this task machine-by-machine is not an efficient deployment strategy in all but the smallest environments.

Service packs can also be obtained on CD from Microsoft and through many Microsoft resources, such as TechNet and MSDN. Service pack CDs often include extras, such as updated administrative tools, new policy templates, and other value-added software. In an enterprise environment, it is therefore recommended to obtain the service pack media.

When you do not have access to a CD containing the service pack, and you want to deploy the service pack to more than one system, you can download the entire service pack as a single file, again from the Microsoft Web site. The service pack executable, if launched (by double-clicking, for example), triggers the installation of the service pack. This single-file version of the executable can also be *extracted* into the full folder and file structure of the service pack, just as it would be on the service pack CD, but without the value adds.

To extract a service pack, launch the executable from a command prompt with the `-x` switch. For example, to extract Windows Server 2003 SP1 for 32-bit platforms, type **WindowsServer2003-KB889101-SP1-x86-ENU.exe -x**. You will then be prompted for a folder to which the service pack is extracted. After the process is complete, you will see the full service pack folder structure contained in the target folder. You can then launch installation of the service pack, just as from the CD, by double-clicking `I386\Update\Update.exe`.

Deploying Service Packs with Group Policy

Service pack installation requires administrative credentials on the local computer unless the service pack is installed through Group Policy or Systems Management Server (SMS). Because service packs apply to systems, it is necessary to assign the service pack through computer-based, rather than user-based, Group Policy.

To distribute a service pack, create a shared folder and either extract the service pack to that folder or copy the contents of the service pack CD to the folder. Then, using the Active Directory Users And Computers snap-in, create or select an existing GPO. Click Edit and the Group Policy Object Editor console appears, focused on the selected GPO.

Expand the Computer Configuration\Software Settings node. Right-click Software Installation and choose New, then Package. Enter the path to the service pack's Update.msi file. Be certain to use a UNC format (for example, `\\Server\Share`) and *not* a local volume path, such as `Drive:Path`. In the Deploy Software dialog box, select Assigned. Close the Group Policy Object Editor console. Computers within the scope of the GPO—in the site, domain, or OU branch to which the policy is linked—automatically deploy the service pack at the next startup.



Tip Windows XP systems with Logon Optimization configured might require two restarts. Logon Optimization can be disabled by enabling the policy Always Wait For The Network At Computer Startup And Logon, found in the policy path Computer Configuration\Administrative Templates\System\Logon.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the “Questions and Answers” section at the end of this chapter.

1. What command should you use to unpack the single file download of a service pack?
 - a. Setup.exe -u
 - b. Update.exe -x
 - c. Update.msi
 - d. <Servicepackname>.exe -x
2. What type of Group Policy software deployment should be used to distribute a service pack?
 - a. Published in the Computer Configuration Software Settings
 - b. Assigned in the Computer Configuration Software Settings
 - c. Published in the User Configuration Software Settings
 - d. Assigned in the User Configuration Software Settings

Lesson Summary

- Service packs can be extracted using the -x switch.
- Group Policy can deploy service packs by assigning Update.msi through the computer configuration's software settings policy.

Lesson 3: Administering Software Licenses

The End User License Agreement (EULA) is more than just a nuisance that you must click through to begin installing a new operating system, update, or application. The EULA is a binding contract that gives you the legal right to use a piece of software. In an enterprise environment, managing software licenses is critically important. In this lesson, you will learn to use the licensing tools provided by Windows Server 2003 to register and monitor licenses and compliance.

After this lesson, you will be able to

- Understand Per Server and Per Device or Per User licensing modes
- Configure licenses using the Licensing properties in Control Panel and the Licensing administrative tool
- Create license groups

Estimated lesson time: 20 minutes



Note The Evaluation Edition of Windows Server 2003, Enterprise Edition, included on the companion CD-ROM with this book, does not support licensing. You will not be able to follow along with the examples in this lesson without purchasing the full retail version of the product.

Obtaining a Client Access License

The server license for Windows Server 2003 enables you to install the operating system on a computer, but you need a Client Access License (CAL) before a user or device is legally authorized to connect to the server. CALs are obtained in bundles, and are often but not always included in the purchase of the operating system. Keep copies of the CAL certificates and your EULAs on file in the event that your organization is audited for licensing compliance.



Tip Remember that when upgrading a server from Microsoft Windows NT 4 or Windows 2000 to Windows Server 2003, you must purchase CAL upgrades as well.

You must have a CAL for any connection to a computer running Windows Server 2003 that uses server components, which include file and print services or authentication. Very few server applications run so independently that the client/server connection does not require a CAL. The most significant exception to the CAL requirement is unauthenticated access conducted through the Internet. Where there is no exchange of credentials during

Internet access, such as users browsing your public Web site, no CAL is required. CALs are therefore not required for Windows Server 2003 Web Edition.

There are two types of CALs: Windows Device CALs, which allow a device to connect to a server regardless of the number of users who might use that device; and Windows User CALs, which allow a user to connect to a server from a number of devices. Windows Device CALs are advantageous for an organization with multiple users per device, such as shift workers. Windows User CALs make most sense for an organization with employees that access the network from multiple or unknown devices.



Note The licensing tools and the user interface do not yet distinguish between Windows User or Windows Device CALs. A device CAL is registered indirectly, using license groups.

The number of CALs you require, and how you track those licenses, depends on which client access licensing mode you pursue.

Per-Server Licensing

Per-server licensing requires a User or Device CAL for each concurrent connection. If a server is configured with 1,000 CALs, the 1,001st concurrent connection is denied access. CALs are designated for use on a particular server, so if the same 1,000 users require concurrent connections to a second server, you must purchase another 1,000 CALs.

Per-server licensing is advantageous only in limited access scenarios such as when a subset of your user population accesses a server product on very few servers. Per-server licensing is less cost-effective in a situation in which multiple users access multiple resources on multiple servers. If you are unsure which licensing mode is appropriate, select Per Server. The license agreement allows a no-cost, one-time, one-way conversion from Per Server to Per Device or Per User licensing when it becomes appropriate to do so.

Per-Device or Per-User Licensing

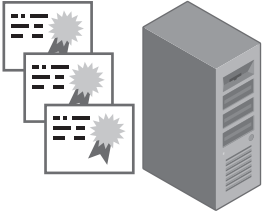
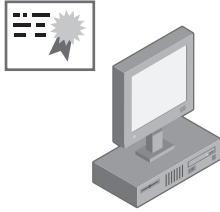
The Per Device or Per User licensing mode varies from the Per Seat scheme of previous versions of Windows. In this new mode, each device or user that connects to a server requires a CAL, but with that license, the device or user can connect to a number of servers in the enterprise. Per User or Per Device mode is generally the mode of choice for distributed computing environments in which multiple users access multiple servers.

For example, a developer who uses a laptop and two desktops would require only one Windows User CAL. A fleet of 10 Tablet PCs that are used by 30 shift workers would require only 10 Windows Device CALs.

The total number of CALs equals the number of devices or users, or a mixture thereof, that access servers. CALs can be reassigned under certain, understandable conditions—for example, a Windows User CAL can be reassigned from a permanent employee to a temporary employee while the permanent employee is on leave. A Windows Device CAL can be reassigned to a loaner device while a device is being repaired.

Per Server and Per Device or Per User licensing modes are illustrated in Table 9-1.

Table 9-1 CAL Licensing Modes

Per Server	Per User or Per Device
	
<ul style="list-style-type: none"> ■ Traditionally licensed in Per Server mode when there are few servers that require limited access. ■ The number of CALs needed is determined by the number of concurrent connections that are required. 	<ul style="list-style-type: none"> ■ Traditionally licensed in Per User or Per Device mode when there are many servers that require frequent and widespread access. ■ Usually more economical when the number of CALs needed is determined by the number of users or devices, or both, that require access to the servers.



Tip Windows Server 2003 includes Terminal Services, also known as Remote Desktop. Remote Desktop includes a two (concurrent) connection license for administrators to connect to a remote server. For Terminal Services to perform as an application server, allowing non-administrative users to connect to hosted applications, you must acquire Terminal Services CALs. Details regarding client licensing can be found at <http://www.microsoft.com/windowsserver2003/howtobuy/licensing/ts2003.msp>.

There are two utilities that will help you track and manage software licensing:

- **Licensing in Control Panel** The Control Panel Choose Licensing Mode tool, as shown in Figure 9-10, manages licensing requirements for a single computer running Windows Server 2003. You can use Licensing to add or remove CALs for a server running in per-server mode; to change the licensing mode from Per Server to Per Device or Per User; or to configure licensing replication.

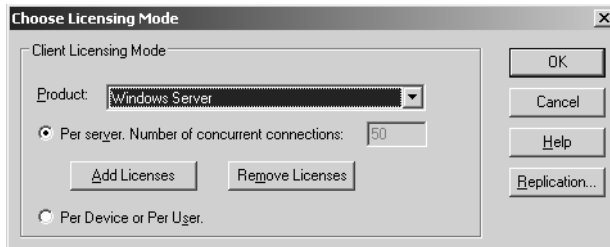


Figure 9-10 The Choose Licensing Mode tool in Control Panel

- **Licensing in Administrative Tools** The Licensing administrative tool, discussed in the next section, allows you to manage licensing for an enterprise by centralizing the control of licensing and license replication in a site-based model.

Administering Site Licensing

The License Logging service, which runs on each computer running Windows Server 2003, assigns and tracks licenses when server resources are accessed. To ensure compliance, licensing information is replicated to a centralized licensing database on a server in the site. This server is called the site license server. A site administrator, or an administrator for the site license server, can then use the Microsoft Licensing tool in Administrative Tools program group to view and manage licensing for the entire site. This new license tracking and management capability incorporates licenses not just for file and print services, but for IIS, for Terminal Services, and for BackOffice products such as Exchange or SQL Server.

The Site License Server

The site license server is typically the first domain controller created in a site. To find out what server is the license server for a site, open Active Directory Sites And Services, expand to select the Site node, and then right-click Licensing Site Settings and choose Properties. The current site license server is displayed, as shown in Figure 9-11.

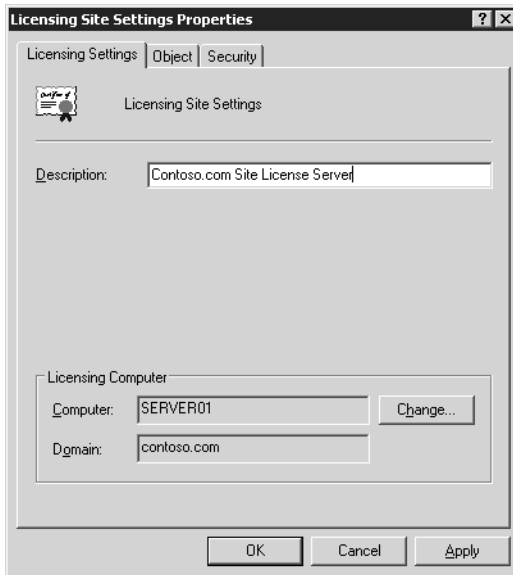


Figure 9-11 Identifying and changing the site license server

To assign the site license server role to another server or domain controller, click Change and select the desired computer. To retain the licensing history for your enterprise, you must, immediately after transferring the role, stop the License Logging service on the new license server, then copy the following files from the old to the new licensing server:

- `%Systemroot%\System32\Cpl.cfg` contains the purchase history for your organization.
- `%Systemroot%\Lls\Llsuser.lls` contains user information about the number of connections.
- `%Systemroot%\Lls\Llsmapi.lls` contains license group information.

After all files have been copied, restart the License Logging service.

Administering Site Licenses

After you have identified the site license server for a site, you can view the licensing information on that server, opening Licensing from the Administrative Tools program group. The Server Browser tab in Licensing (as shown in Figure 9-12) enables you to manage licensing for an entire site or enterprise.

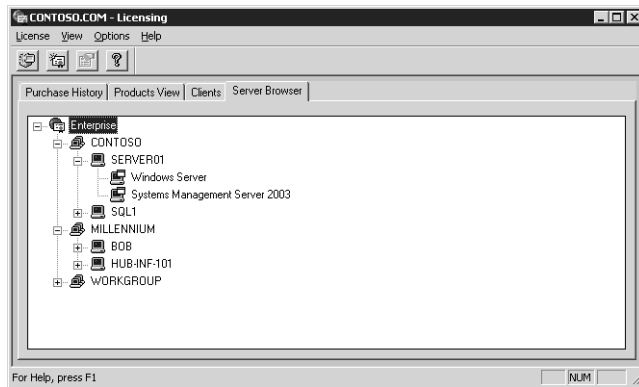


Figure 9-12 The Server Browser tab of the Microsoft Licensing administrative tool

The Server Browser page of Licensing allows you to manage any server in any site or domain for which you have administrative authority. You can locate a server and, by right-clicking it and choosing Properties, manage that server's licenses. For each server product installed on that server, you can add or remove per-server licenses. You can also, where appropriate, convert the licensing mode. Remember that per-server licensing mode issues a license when a user connects to the server product. When a user disconnects from the server product, the License Logging service makes the license available to another user.

The server properties also allow you to configure license replication, which can be set on a server using its Licensing properties in Control Panel. By default, license information is replicated from a server's License Logging Service to the site license server every 24 hours, and the system automatically staggers replication to avoid burdening the site licensing server. If you want to control replication schedules or frequency, you must manually vary the Start At time and Start Every frequency of each server replicating to a particular site license server.

To manage Per Device or Per User licensing, click Licensing from the Administrative Tools program group, then choose the New License command from the License menu. In the New Client Access License dialog box, select the server product and the number of licenses purchased. Licenses are added to the pool of licenses. As devices or users connect to the product anywhere in the site, they are allocated licenses from the pool, with one license for each device or user. After a pool of licenses is depleted, license violations occur when additional devices or users access the product.

The Purchase History tab in Licensing (as shown in Figure 9-13) provides a historical overview of licenses purchased for a site, as well as the quantity, date, and administrator associated with the addition or removal of licenses.

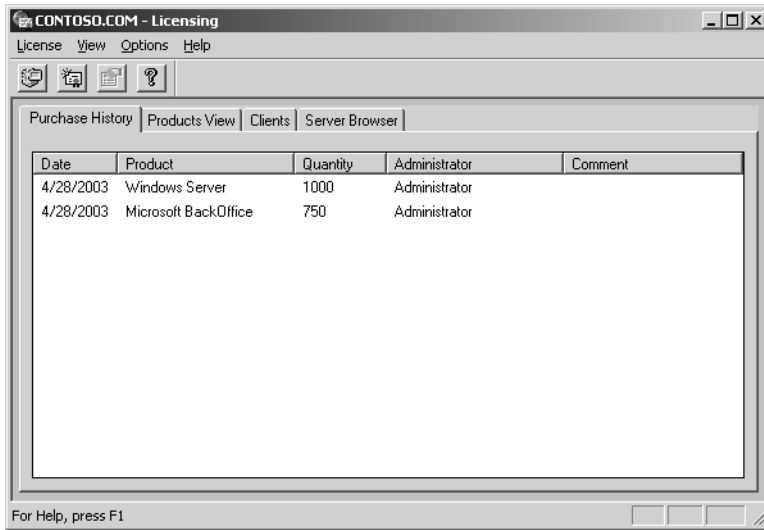





Figure 9-13 The Purchase History tab of the Microsoft Licensing administrative tool

To view cumulative information about licensing and compliance, click the Products View tab. This tab shows how many licenses have been purchased and allocated to users or devices (in Per Device or Per User mode) or the number of licenses purchased for all servers in the site and the peak connections reached to date (in Per Server mode). You can also determine compliance using the licensing status symbols shown in Table 9-2.

Table 9-2 Licensing Status Symbols

Symbol	Licensing Status
	The product is in compliance with legal licensing requirements. The number of connections is less than the number of licenses purchased.
	The product is not in compliance with legal licensing requirements. The number of connections exceeds the number of licenses purchased.
	The product has reached the legal limit. The number of connections equals the number of licenses purchased. If additional devices or users will connect to the server product, you must purchase and log new licenses.

License Groups

Per Device or Per User licensing requires one CAL for each device. However, the License Logging service assigns and tracks licenses by user name. When multiple users share one or more devices, you must create license groups, or licenses will be consumed too rapidly.

A license group is a collection of users who collectively share one or more CALs. When a user connects to the server product, the License Logging service tracks the user by name but assigns a CAL from the allocation assigned to the license group. The concept is easiest to understand with examples:

- **10 users share a single handheld device for taking inventory** A license group is created with the 10 users as members. The license group is assigned one CAL, representing the single device they share.
- **100 students occasionally use a computer lab with 10 computers** A license group is created with the 100 students as members, and is allocated 10 CALs.

To create a license group, click the Options menu and, from the Advanced menu, choose New License Group. Enter the group name and allocate one license for each client device used to access the server. The number of licenses allocated to a group should correspond to the number of devices used by members of the group.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the “Questions and Answers” section at the end of this chapter.

1. What are the valid licensing modes in Windows Server 2003? Select all that apply.
 - a. Per User
 - b. Per Server
 - c. Per Seat
 - d. Per Device or Per User
2. You are hiring a team to tackle a software development project. There will be three shifts of programmers, and each shift will include six programmers. Each programmer uses four devices to develop and test the software, which authenticates against a computer running Windows Server 2003. What is the minimum number of CALs required if the servers involved are in Per Device or Per User licensing mode?
 - a. 6
 - b. 4
 - c. 18
 - d. 24

3. What tool will allow you to identify the site license server for your site?
 - a. Active Directory Domains And Trusts
 - b. The Licensing tool in Control Panel
 - c. Active Directory Sites And Services
 - d. DNS
4. You manage the network for a team of 500 telephone sales representatives. You have 550 licenses configured in Per Device or Per User licensing mode. A new campaign is launched, and you will hire another shift of 500 reps. What do you need to do to most effectively manage license tracking and compliance?
 - a. Revoke the licenses from the existing clients
 - b. Delete the existing licenses, and then add 500 licenses
 - c. Create license groups
 - d. Convert to Per Server licenses

Lesson Summary

- Windows Server 2003 provides a new mode of licensing whereby a user can access a server product from multiple devices using one license, or a group of users can access a server product from a single device. This is called Per Device or Per User licensing.
- When more than one user accesses a server product from shared devices, add those users as a license group, and allocate licenses to that group equivalent to the number of devices.
- License information is replicated, by default every 24 hours, to the site license server.
- Licensing can be managed using the Licensing tool in Control Panel or, more centrally, using the Licensing administrative tool from the Administrative Tools program group.

Case Scenario Exercise

You are configuring an update strategy for a network consisting of 1000 clients running a mix of Windows XP and Windows 2000. Your goal is to prevent users from downloading updates directly from Microsoft Update and to create a structure in which you can approve critical patches and security rollups for distribution.

You have recently purchased desktops and laptops, and you have applied the corporate standard image to those systems. Unfortunately, the image was created a while

ago. The Windows XP image has only Service Pack 1 applied. So your first task is to update systems to the latest service pack level so that the Automatic Updates client, as well as all patches and fixes, can be installed on the computers.



Note In this hands-on scenario, you may test the results using a second computer. To do so, join the computer to the domain and move its computer account to the Desktops OU.

Exercise 1: Download and Extract the Service Pack

1. Create a folder on the C drive and name the folder ServicePack.
2. From the Microsoft download site, <http://www.microsoft.com/downloads>, or from the Windows XP site, <http://www.microsoft.com/windowsxp>, download the latest service pack. Save it to the C:\ServicePack folder.
3. Open a command prompt and type **cd C:\ServicePack** to change to the Service-Pack folder.
4. Type **WindowsXP-KB395935-SP2-ENU.exe -x**. Substitute WindowsXP-KB395935-SP2-ENU with the file name of the service pack you downloaded.
5. You will be prompted to indicate the location to which the service pack will be extracted. Type **C:\ServicePack**.
6. The service pack is extracted. Use Windows Explorer to navigate the folder structure that was created. Make note of the location of Update.exe (in the Update folder), which you use to launch installation of the service pack on a single machine, and of Update.msi (in the same folder), which you can use to deploy the service pack through Group Policy–based software distribution.

Exercise 2: Deploy the Service Pack with Group Policy

1. Share the C:\ServicePack folder with the share name ServicePack.
2. Open Active Directory Users And Computers.
3. Expand the domain and locate (or create) the Desktops OU.
4. Create a computer object in the Desktops OU called Desktop0569 to represent one of the new systems.



Note If you have a second system with which to perform this case scenario exercise, move that system's account into the Desktops OU.

5. Create a GPO called SP-Deploy.

If you are using the GPMC to manage Group Policy:

- a. Open the GPMC.
- b. Right-click the Desktops OU and choose Create And Link A GPO Here.
- c. Name the GPO **SP-Deploy**.
- d. Right-click the SP-Deploy Group Policy link and click Edit.

Otherwise:

- a. Right-click the Desktops OU and choose Properties.
- b. Click the Group Policy tab.
- c. Click New to create a new GPO. Name the object SP-Deploy.
- d. Select the SP-Deploy Group Policy link and click Edit.

The Group Policy Object Editor opens.

6. Navigate to Computer Configuration\Software Settings.
7. Right-click Software Installation, choose New, and then choose Package.
8. Type the path `\\server01.contoso.com\servicepack` and press ENTER. The browse dialog box will take you to the root of the extracted service pack.
9. Navigate to the Update.msi file you identified in the previous exercise. Select the Update.msi file and click Open.
10. Select Assigned and click OK. The package is created.
11. Close Group Policy Object Editor and the Desktop OU's Properties dialog box.
12. (Optional) If you have a second system with Windows XP, but without SP2, you can test the deployment of the service pack. Remember that computers running Windows XP are configured by default to optimize logon, so it might take two restarts before the service pack is applied. You can confirm the service pack level on a machine by clicking Start, Run, and then typing **winver**.

Exercise 3: Install WSUS

1. If IIS is not already installed, complete Exercise 1 of the Practice in Chapter 6, Lesson 4, to install IIS.
2. Navigate to <http://www.microsoft.com/wsus>.
3. Locate and download the WSUS installation package.
4. Start WSUS installation by double-clicking the downloaded file.
5. On the Welcome screen, click Next.
6. Read and accept the End User License Agreement, and then click Next.

7. On the Select Update Source screen, configure a location for WSUS to be installed if the default is not acceptable. Click Next.



Note The updates might consist of several GBs of files. If you have a slow Internet connection, or if you want to save time during this exercise, clear the option to Store Updates Locally. WSUS will not synchronize update installation files, which will reduce the requirements for free disk space and will reduce the time required for the initial synchronization of updates. However, any clients that use the WSUS server will have to download the update installation files from Microsoft Update.

8. On the Database Options page, select Install SQL Server Desktop Engine (Windows) On This Computer. Click Next.
9. On the Web Site Selection page, select Use The Existing IIS Default Web Site (recommended). Click Next.
10. On the Mirror Update Settings page, click Next.
11. A summary page appears. Confirm the configuration and click Next.
12. After installation has completed, clear the option to Launch The Web Administration Tool. Click Finish.

Exercise 4: Synchronize WSUS

1. If you are not already viewing the WSUS administration page, open Internet Explorer and navigate to *http://SERVER01/WSUSAdmin*.



Note To view the WSUS administration site, you might need to add Server01 to the Local Intranet trusted site list to access the site. Open Internet Explorer and choose Internet Options from the Tools menu. Click the Security Tab. Select Trusted Sites and click Sites. Add **Server01** and **Server01.contoso.com** to the trusted site list.

2. Below the To Do List, click the Get Started By Synchronizing Your Server link.
3. In the Update Files And Languages area, click Advanced.
4. A warning message indicates that computers will not be able to receive updates from the server during the configuration change. Click OK.
5. In the Language frame, select Download Only Those Updates That Match The Locale Of This Server.
6. A warning message indicates that you need to include all languages of all computers in your network. Click OK.
7. Click OK to close the Advanced Synchronization Options dialog box.

You will manually synchronize for this exercise. However, you can examine synchronization options by clicking Synchronize Using This Schedule. When you are finished exploring settings, click Cancel.

8. Below Tasks, click the Synchronize Now link. If you have elected to download updates to the server, synchronization might take some time.
9. After synchronization has occurred, click the Updates link in the top navigation bar.
10. Approve a small number of updates so that you can return later to experiment further with approval and automatic updates.
11. Examine other pages of the WSUS administration site. After you have familiarized yourself with the site, close Internet Explorer.

Exercise 5: Configure Automatic Updates

1. Create a GPO called WSUS-Config.

If you are using the GPMC to manage Group Policy:

- a. Open the GPMC.
- b. Right-click the domain *contoso.com* and choose Create And Link a GPO Here.
- c. Name the GPO WSUS-Config.
- d. Right-click the WSUS-Config Group Policy link and click Edit.

Otherwise:

- a. Right-click the domain *contoso.com* and choose Properties.
 - b. Click the Group Policy tab.
 - c. Click New to create a new GPO. Name the object WSUS-Config.
 - d. Select the WSUS-Config Group Policy link and click Edit.
2. Navigate to Computer Configuration\Administrative Templates\Windows Components\Windows Update.
 3. Double-click the policy: Specify Intranet Microsoft Update Service Location, and then select Enabled.
 4. In *both* text boxes, type **http://server01.contoso.com** and click OK.
 5. Double-click the policy: Configure Automatic Updates, and then select Enabled.
 6. In the Configure Automatic Updating drop-down list, choose 4-Auto Download And Schedule The Install.
 7. Confirm the installation schedule: Daily at 3:00 A.M.

8. Click OK.
9. Double-click the policy: Reschedule Automatic Updates Scheduled Installations, and then select Enabled.
10. In the Wait After System Startup (Minutes) box, type **10** and click OK.



Exam Tip The Wait After System Startup policy is used to reschedule a scheduled installation that was missed, typically when a machine was turned off at the scheduled date and time.

11. Close the Group Policy Object Editor.
12. To confirm the configuration, you can restart the server, which is also within the scope of the new policy. Open System from Control Panel and click the Automatic Updates tab. You will see that configuration options are disabled because they are now being determined by policy.

Chapter Summary

- Windows Server Update Services (WSUS) enable you to centralize and manage the approval and distribution of updates to a variety of Microsoft operating systems, servers, and applications. One or more WSUS servers host lists of approved updates and, optionally but typically, the update files themselves. Automatic Updates clients are configured, usually through GPOs, to obtain updates from intranet WSUS servers rather than from Microsoft Update.
- Service packs can be obtained free from Microsoft. If the service pack is a single file, it can be extracted from the command prompt by entering the service pack's filename followed by the -x switch.
- Service packs are deployed easily by assigning a software installation package to the computer configuration's software settings policies in a GPO. WSUS, but not SUS, supports deploying service packs through the update infrastructure.
- Tracking and managing licenses and compliance is an important part of an administrator's job. Windows Server 2003 gives you the ability to assign licenses based on concurrent connections to a specific server or to maintain a license for each device or user that connects to any number of servers in your enterprise.
- Licenses are replicated between servers' License Logging service and the site license server. The site license server can be identified using Active Directory Sites And Services, but site licensing is administered using the Licensing tool in the Administrative Tools programs group.
- A license group enables users to share one or more devices. The number of Windows Device CALs is assigned to the license group.

Exam Highlights

Before taking the exam, review the key points and terms that are presented below to help you identify topics you need to review. Return to the lessons for additional practice and review the “Further Reading” sections in Part 2 for pointers to more information about topics covered by the exam objectives.

Key Points

- Read the CD-ROM supplement regarding SUS. As of the date of publication, certification exams were focused on SUS rather than on WSUS.
- For SUS or WSUS, focus on administrative tasks, such as synchronizing, approving updates, viewing logs and events, and configuring Automatic Updates through System in Control Panel (on a stand-alone computer) or using Group Policy in a larger environment. Remember that you cannot direct a computer to an WSUS server using the Automatic Updates properties on a client. You must use Group Policy, or a registry entry, to redirect the client to an intranet server rather than to Microsoft Update.
- Be able to calculate license requirements in a variety of Per Server or Per Device or Per User scenarios. Remember that license groups allow multiple users to share one or more devices.

Key Terms

Client Access License The license that allows a user or device to connect to a server product for any functionality, including file and print service or authentication.

Per Server license mode Licenses are allocated when a user or device connects to the server or product. When the user disconnects, the license is returned to the available license pool. This mode requires sufficient licenses to support the maximum number of concurrent connections on each individual server.

Per Device or Per User mode Licenses requirements allow a single CAL to authorize a user (who may use more than one device) or a device (which may be used by more than one user) to connect to any number of servers.

license group Because the License Logging service allocates licenses based on user name and not device name, Windows Device CALs are given to a license group. A license group has one or more users, and is allocated licenses equivalent to the number of devices used by that group to connect to server products.

Questions and Answers

Page
9-25

Lesson 1 Review

1. You are configuring a WSUS infrastructure. One server is synchronizing metadata and content from Windows Update. Other servers (one in each site) are synchronizing content from the parent WSUS server. Which of the following steps is required to complete the WSUS infrastructure?
 - a. Configure Automatic Updates clients using Control Panel on each system.
 - b. Configure GPOs to direct clients to the WSUS server in their sites.
 - c. Configure a manual content distribution point.
 - d. Approve updates using the WSUS administration page.

The correct answers are b and d.

2. You are configuring WSUS for a group of Web servers. You want the Web servers to update themselves nightly based on a list of approved updates on your WSUS server. However, once in a while an administrator is logged on, performing late-night maintenance on a Web server, and you do not want update installation and potential restart to interfere with those tasks. What Windows Update policy configuration should you use in this scenario?
 - a. Notify For Download And Notify For Install
 - b. Auto Download And Notify For Install
 - c. Auto Download And Schedule The Install

The correct answer is c. You want the Web servers to update themselves, so you must schedule the installation of updates. However, an administrator always has the option to cancel the installation.

3. You want all network clients to download and install updates automatically during night hours, and you have configured scheduled installation behavior for Automatic Updates. However, you discover that some users are turning off their machines at night, and updates are not being applied. Which policy allows you to correct this situation without changing the installation schedule?
 - a. Specify Intranet Microsoft Update Service Location
 - b. No Auto-Restart For Scheduled Automatic Updates Installations
 - c. Reschedule Automatic Updates Scheduled Installations
 - d. Configure Automatic Update

The correct answer is c. Updates are automatically downloaded using background processes and idle bandwidth, but the installation is triggered by the specified schedule. If a computer is

turned off at the installation time, it waits until the next scheduled date and time. The Reschedule Wait Time policy, if set between 1 and 60, causes Automatic Updates to start update installation 1 to 60 minutes after system startup.

Lesson 2 Review

1. What command should you use to unpack the single file download of a service pack?
 - a. Setup.exe -u
 - b. Update.exe -x
 - c. Update.msi
 - d. <Servicepackname>.exe -x

The correct answer is d.

2. What type of Group Policy software deployment should be used to distribute a service pack?
 - a. Published in the Computer Configuration Software Settings
 - b. Assigned in the Computer Configuration Software Settings
 - c. Published in the User Configuration Software Settings
 - d. Assigned in the User Configuration Software Settings

The correct answer is b.

Lesson 3 Review

1. What are the valid licensing modes in Windows Server 2003? Select all that apply.
 - a. Per User
 - b. Per Server
 - c. Per Seat
 - d. Per Device or Per User

The correct answers are b and d.

2. You are hiring a team to tackle a software development project. There will be three shifts of programmers, and each shift will include six programmers. Each programmer uses four devices to develop and test the software, which authenticates against a computer running Windows Server 2003. What is the minimum number of CALs required if the servers involved are in Per Device or Per User licensing mode?
 - a. 6
 - b. 4

- c. 18
- d. 24

The correct answer is c. If you were to license based on devices, there are six times four devices, or 24 devices. It will be more cost-effective to license based on the number of users, which is 18.

3. What tool will allow you to identify the site license server for your site?
- a. Active Directory Domains And Trusts
 - b. The Licensing tool in Control Panel
 - c. Active Directory Sites And Services
 - d. DNS

The correct answer is c.

4. You manage the network for a team of 500 telephone sales representatives. You have 550 licenses configured in Per Device or Per User licensing mode. A new campaign is launched, and you will hire another shift of 500 reps. What do you need to do to most effectively manage license tracking and compliance?
- a. Revoke the licenses from the existing clients
 - b. Delete the existing licenses, and then add 500 licenses
 - c. Create license groups
 - d. Convert to Per Server licensing

The correct answer is c.