

ITPro<sup>TM</sup>  
SERIES

Windows IT Pro

 **eBooks**

Keeping Your Business  
SAFE from Attack:

# Patch Management

By Jeff Felling

**Microsoft<sup>®</sup>**



**Microsoft®**

## Contents

<b>Chapter 7 Enterprise Solutions: SMS 2003</b> .....	<b>115</b>
<b>Preparing Your Environment for SMS</b> .....	<b>116</b>
Setting Up AD .....	116
<b>Installing SMS 2003</b> .....	<b>117</b>
Configuring a Base SMS Installation .....	118
Specify the Management Point .....	118
Enable Reporting .....	118
Prepare the Deployment of the SMS Client Software .....	119
Decrease Polling Intervals and Increase Polling Frequency for Testing .....	120
Enable Client Push Installation .....	120
Specify the Account to Use for Software Distribution .....	120
<b>Client Discovery and Installation</b> .....	<b>120</b>
Review Newly Discovered Clients .....	121
Troubleshooting Missing or Unassigned Clients .....	122
Other Methods for Installing the SMS Client .....	122
Checking the SMS Client on the Client Computer .....	122
<b>Using SMS for Software Updates</b> .....	<b>123</b>
Installing the Office Update Inventory Tool .....	123
<b>Installing the Security Update Inventory Tool</b> .....	<b>125</b>
<b>SMS Vernacular: Programs, Packages, Advertisements, and Collections</b> .....	<b>126</b>
<b>Creating Your Package of Updates: Working with the Distribute Software Updates Wizard</b> .....	<b>127</b>
Advertise Your Updates .....	132
<b>SMS 2003 Reporting</b> .....	<b>134</b>
<b>Manually Refreshing the Reports</b> .....	<b>134</b>
<b>Patch Management with SMS</b> .....	<b>134</b>

## Chapter 7:

# Enterprise Solutions: SMS 2003

Staying one step ahead of new exploits of known vulnerabilities takes time and effort. At a minimum, such preparedness requires knowledge that new updates are available and that you've protected your systems with the most current updates. This book has explored processes, mechanisms, and freely available patch management technologies to assist with the triage and deployment of Windows security updates and service packs. Microsoft also offers a highly flexible commercial software patch management product: Systems Management Server. SMS 2003 Service Pack 1 (SP1) provides software update scanning of both Windows and Microsoft Office platforms, as well as detailed and customizable reports showing the status of software updates. SMS is regarded as a complex enterprise product for large organizations, but even small to midsize businesses can benefit from SMS's enhanced inventory and reporting capabilities. SMS 2003 integrates with Active Directory (AD) and for small deployments can be installed on a single server. Yet, SMS scales very well to accommodate patch management for very large enterprises.

The SMS platform does more than patch management. This powerful enterprise tool lets you centrally manage your client machines and it includes features such as hardware and software inventory, software distribution, software metering, and remote control services. It includes client-server features that recognize and accommodate remote and mobile computers and fast or slow WAN network links. In fact, it wasn't until 2002 that Microsoft added specific patch management capabilities to SMS through the SMS 2.0 Software Update Services (SUS) Feature Pack. Users of SMS 2.0 could download the feature pack for free and add inventory and deployment capabilities to their SMS infrastructure specifically tuned for patch management.

Since then, Microsoft has integrated many of the patch management features into SMS 2003 SP1. You can use SMS 2003's inventory and software distribution mechanisms to assess and install updates for both Windows Security and Microsoft Office products. SMS 2003 also supports a flexible query and reporting engine for presenting a wide variety of highly customizable update-summary data of your patch status. You might wonder what SMS offers for patch management that is different from SUS and Windows Server Update Services (WSUS). In a nutshell, SMS provides more granular targeting criteria, is cognizant of your WAN topology (so it works better for deploying patches to remote offices and mobile users), and offers broader support of software deployments. For example, instead of simply approving an update to a group of computers (like you can do with WSUS), with SMS you can deploy an update to laptops of only a particular brand or model and track the installation progress on a daily report.

To take advantage of these features and enhancements, you must first face the rather steep learning curve of successfully deploying and managing SMS 2003—especially if you have a large or complex organization. Not only is the initial deployment more complex than with SUS or WSUS, but each security update also takes more time to prepare for deployment. Fortunately, many resources are available to help answer questions you might have about this multifaceted product. For SMS 2003 planning, deployment, and administration tutorials, you can check out the Web site at

<http://www.microsoft.com/smsserver>. Also at the Microsoft Web site, you can go to the Technet Virtual Lab sessions at <http://www.microsoft.com/technet/traincert/virtuallab/sms.mspx>.

SMS 2003 provides an entire suite of systems management capabilities and this chapter will walk you through configuring a basic installation of SMS 2003 to scan and inventory, deploy, and report on the status of security updates and Microsoft Office updates.

## Preparing Your Environment for SMS

As with any new technology or application, I recommend setting up a simple test environment that is separate from any production machines. If you haven't worked with SMS, I suggest that you read about deployment considerations, recommendations, and best practices at the Microsoft Web site, <http://www.microsoft.com/smsserver>. This example is based on a Windows 2003 AD domain: all the client computers run Windows 2000 (Win2K) or later and are members of this domain. Therefore, we will use the latest SMS features such as Advanced Security and the advanced client. (These features are available to SMS 2003 installations. If you are upgrading from SMS 2.0, or running on NT 4.0 or Windows 98, then you might need to use standard security and the legacy client.) Under advanced security, all the SMS servers are in AD and SMS runs under the local system account, which reduces the number of domain accounts needed to run the program. (Integration with AD is a huge benefit of SMS 2003 over earlier versions.)

This chapter walks you through a basic SMS 2003 installation that consists of one server and a few clients. The server plays multiple roles as a primary site, a management point, distribution point, and reporting point. Before installing SMS we need to configure the server platform. On this server install Windows Server 2003 OS, Internet Information Server (IIS) 6.0, and the Background Intelligent Transfer Service (BITS) Server Extensions.

SMS 2003 uses a SQL Server database to store all its data, and for our test environment we'll install SMS onto a server running SQL Server 2000 SP3a. The client machines consist of several Windows XP workstations and a computer running Windows Server 2003. The clients are all within the same class C subnet (192.168.0.0/24) and have Internet access.

First, confirm that your SMS Server has been built as follows:

- Windows Server 2003 with all security updates applied
- Application Server with IIS 6.0 and BITS Server Extensions installed
- SQL Server 2000 with SP3a installed

## Setting Up AD

Next we need to create the user accounts that SMS will use and enable the SMS Site Server to update AD. First, let's create the account that we will use to deploy software on each client computer. Launch Active Directory Users and Computers and create a domain account (e.g., smsDeploy). This account needs to have administrative privileges on each client computer that you want to manage with SMS. (This account does not need to be a member of the Domain Admin group and, if possible, you should refrain from using that privileged group.)

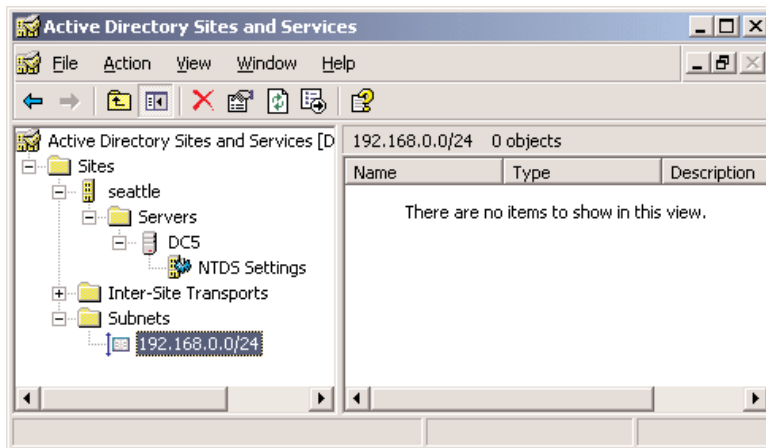
We will configure SMS 2003 to run under the advanced security option, so we need to give permissions for the primary Site Server computer to update the System container in AD. To do this, open Active Directory Users and Computers, and from the menu select View, Advanced features. Navigate to the System container, right click it, and select Properties. Select the Security tab and click

Add. In *Select Users, Computers, or Groups* make sure the Object Type includes Computers, then type the name of the computer on which you will install SMS. Click Check Names to ensure that the computer name is recognized and click OK. Now, in the group or user names list, select the name of your computer and make sure that Read, Write, Create All Child Objects, and Delete All Child Objects are selected. Next, click Advanced, select the computer account again, then click Edit. In the *Apply onto* drop down menu, select *This object and all child objects*. Click OK until you exit the dialog box.

SMS 2003 integrates with AD and leverages AD Sites to define SMS Site Boundaries. An SMS site boundary defines SMS's scope when looking for computers to manage. To define the AD Site, launch Active Directory Sites and Services from the Administrative tools. The default name of the first AD site is *Default-First-Site-Name*. You can either rename this to something that defines your site (in our example, we define the AD site name as *seattle*) or leave the default name. Next, right-click the Subnets node, and left click New Subnet to define the subnet (e.g., 192.168.0.0 with a subnet mask of 255.255.255.0). Assign that subnet to the site name by clicking on the site, then click OK. When completed your Active Directory Sites and Services will look similar to Figure 7-1.

**Figure 7-1**

*Viewing Active Directory Sites and Services after setup*



## Installing SMS 2003

Running the SMS 2003 setup program is very straightforward. From the SMS 2003 installation media, run *autorun.exe* and select to install SMS 2003 to start the installation wizard. First specify to install an SMS Primary Site. In our example, our site code is SEA, the site name is *seattle*, and the site domain is security. Next in the installation process, the setup program will ask whether to extend the AD schema for you. (You must be a member of the schema admins group to perform this step.) When prompted, choose to install SMS 2003 under Advanced Security. In the last few steps of the wizard it will create the database for you; by default it's named *SMS\_sitename* (e.g., SMS\_SEA).

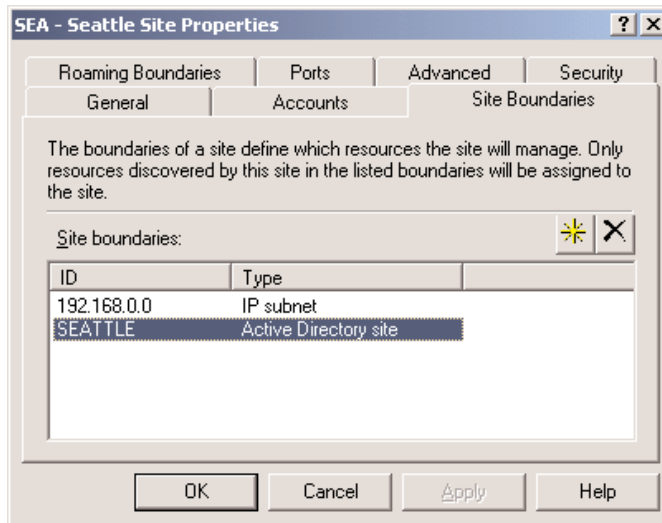
The basic installation of SMS 2003 is now complete. Now, let's make it functional.

Launch the SMS Administration console by clicking Start, All Programs, Systems Management Server, then SMS Administrator Console. From this Microsoft Management Console (MMC) you will be able to perform most of your patch management activities. Now, let's begin the base configuration of SMS.

### Configuring a Base SMS Installation

Navigate to Site Database, Site Hierarchy, right-click the Site Name, then click Properties to see the properties for the site. As Figure 7-2 shows, click the Site Boundaries tab, then click the yellow star icon to add a new Site boundary.

**Figure 7-2**  
*Adding a new site boundary*



Choose the site boundary and add the AD site that you created earlier (e.g., seattle). (You can also define a site boundary by subnet ID, but I've found that leveraging AD sites for this is more flexible and easier to manage.)

### Specify the Management Point

The clients will communicate with the SMS infrastructure through SMS Management Points. The management points are the primary point of contact for clients. By default this point is undefined and we must assign this role to our new SMS server. Navigate to Site Database, Site Hierarchy, Site Name, Site Settings, then click Site Systems. In the right pane, double-click the site name (e.g., \\SMS) to bring up the Site System Properties. Click the tab Management Point and enable the checkbox *Use this site system as a management point*.

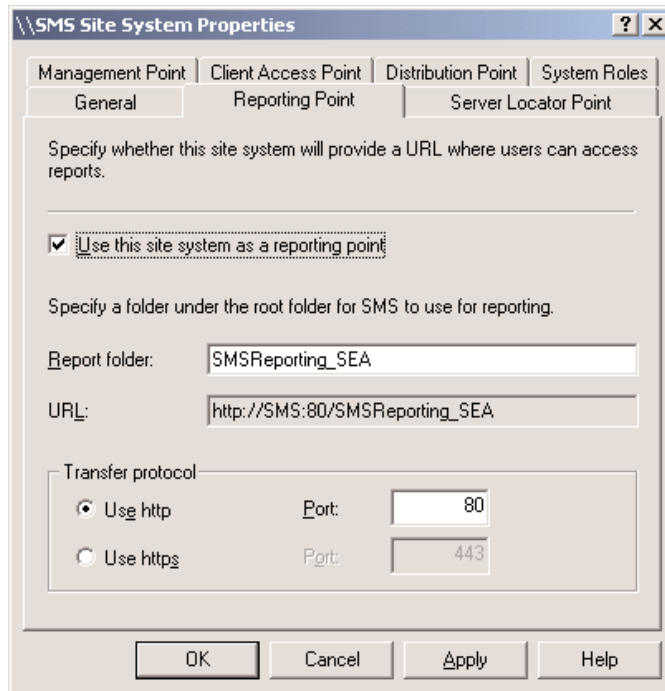
### Enable Reporting

To view reports from this SMS Server we need to define it as a Reporting Point. (If you do not have a reporting point enabled the Run reports option will be grayed out.) Navigate to Site Database, Site

Hierarchy, Site Name, Site Settings, and Site Systems. In the right pane, right-click the name of your SMS server, and left-click Properties to bring up the Site System Properties. Click the Reporting Point tab and enable the *Use this site system as a reporting point* checkbox. You can leave the defaults for the remaining values, as Figure 7-3 shows.

**Figure 7-3**

*Showing the Reporting Point settings*



Add the user accounts that you want to provide with access to the SMS reports to the SMS server's local group *SMS Reporting Users*. Adding these users is an important step because, by default, even local administrators cannot view the reports. Test the installation by opening your Web browser to [http://smsserver/SMSReporting\\_sitecode](http://smsserver/SMSReporting_sitecode). We'll look at the reports specific to patch management after we've completed the SMS configuration and used it to deploy a few patches.

### Prepare the Deployment of the SMS Client Software

Now we'll configure SMS to load the SMS Systems Management client on the computers in our test domain. Navigate to Site Database, Site Hierarchy, Site Name, Site Settings, then click Client Agents. In the right pane of the MMC, double-click the names of the agents you want to install. For patch management you need to enable the Hardware Inventory Client Agent, Software Inventory Client Agent, and Advertised Programs Client Agent. (The remaining agents are used for other SMS features.)

### **Decrease Polling Intervals and Increase Polling Frequency for Testing**

A lot of SMS functionality revolves around polling client computers for status and information. Many polling intervals are set to 1 day or 1 week by default. To facilitate testing, I recommend decreasing some of these settings to much more frequent intervals. This adjustment will let you witness changes more frequently when evaluating and using the system. For both the Software and Hardware Inventory agents decrease the time to run the inventory to a time less than the default (e.g., 1 hour). Similarly, for the Advertised Programs Client Agent, increase the polling time to a more frequent interval (e.g., 5 minutes). These settings facilitate testing while increasing network and system load. Remember to restore these settings to default values when you deploy to your production environment.

### **Enable Client Push Installation**

Now, let's configure SMS to deploy the agents to your test systems. Navigate to Site Database, Site Hierarchy, Site Name, Site Settings, then click Client Installation Methods. In the right pane, double-click the Client Push Installation and enable the checkbox *Enable Client Push Installation to assigned resources*. Also, enable the checkboxes next to the platforms on which you want to deploy the client: servers, workstations, or domain controllers (DCs).

Earlier we created a domain account with administrative permissions on the SMS client computers; now we need to specify this account in SMS. Click the Accounts tab and click the yellow star icon to add the account that will be used to install the SMS client software. Enter the domain and account name of the previously created client software deployment account (e.g., security\smsDeploy). Click OK to exit the Client Push Installation properties. With this configuration SMS 2003 will install the SMS client on any computers that are running and that SMS has discovered and assigned to this site.

### **Specify the Account to Use for Software Distribution**

In addition to installing the SMS Client software, we need to also configure an account for SMS to use to install the software updates. Navigate to Site Database, Site Hierarchy, Site Name, Site Settings, then click Component Configuration. In the right pane of the MMC, double-click Software Distribution. On the General Tab for the Advanced Client Network Access Account, click Set, enter the domain and account name of the service account you want to use for the client installation (e.g., security\smsDeploy), and enter the password. Click OK.

At this point, the majority of the configuration of our basic SMS installation is complete. Now we need to run a discovery to populate the SMS database with potential client computers. When a discovery runs, a discovery data record (DDR) is created for each object found. Because we enabled the Client Installation Push, any objects that are discovered, are within the site boundary, and can be administratively managed by the SMS computer, will be installed with the SMS client.

## **Client Discovery and Installation**

SMS 2003 retains many of the flexible discovery processes of earlier SMS versions, such as network and heartbeat discovery, but also recognizes objects in AD. So now in addition to using SNMP and other techniques to scan the network, SMS can query an AD DC directly for computer and user objects. For our test domain, we'll use the SMS Discovery Method Active Directory System Discovery to populate our collection of objects on which we want to install and manage the SMS client.

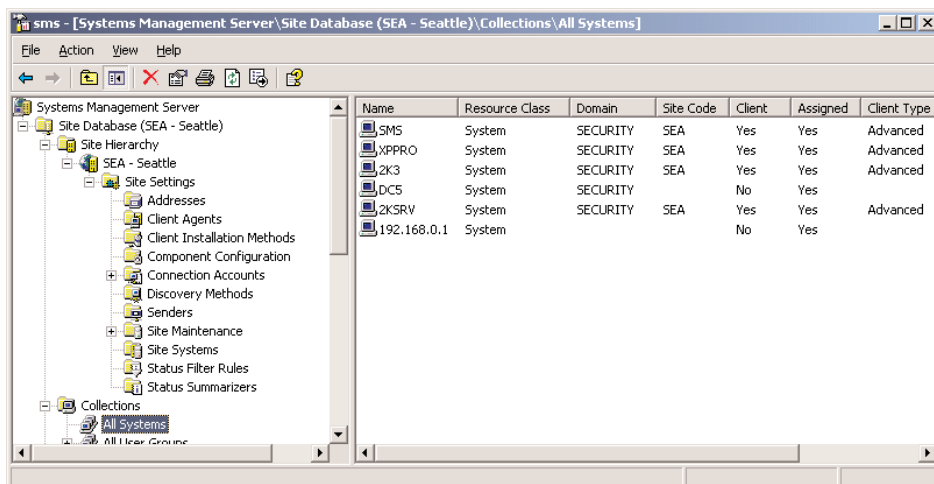
Navigate to Site Database, Site Hierarchy, Site Name, Site Settings, then click Discovery Methods. In the right pane, double-click Active Directory System Discovery. Enable the Enable Active Directory System Discovery checkbox. Click the New icon, select Local Domain, and ensure Recursive is selected. When you click OK, you will be prompted to select the container to poll. Specify the container (e.g., organizational unit—OU—or domain name) then click OK. The distinguished name (DN) of the container you selected will appear in the Active Directory System Discovery dialog box. Click the Polling Schedule tab and notice that polling occurs every day. Click the checkbox to enable Run Discovery as soon as possible. This will initiate the discovery now. SMS will create a DDR for each resource it finds and will automatically begin to deploy the client software, based on our earlier configuration.

### Review Newly Discovered Clients

Each new system discovered with DDR will be viewable in the collection *All Systems*. Navigate to the Site Database, Site Hierarchy, expand the Collections node, and click *All Systems*. Depending on the size of your network and network link speed, the computers in your specified AD container will appear in the right pane. (AD is not the only discovery method and you can use other network-oriented methods to pick up nondomain objects. However, you will not be able to use the SMS advanced client or other techniques presented in this chapter to manage these.)

If you make changes to your site definition, add new clients and follow up with a manual discovery, or change your client installation options, then you can manually update the collection membership. Under the collections node, right-click the All Systems node, left-click All Tasks, the select Update Collection Membership. An hourglass will appear next to the All Systems collection while the update is processing and you can click the Refresh button at the top of the MMC to update the status until the update has completed. In the right pane, you'll see all the computers, as Figure 7-4 shows.

**Figure 7-4**  
*Viewing the All Systems computer collection*



## ***Troubleshooting Missing or Unassigned Clients***

If following a discovery your clients are neither assigned nor have a client installed, double-check that:

- The site boundary is correctly defined. If you specified only a subnet ID, define the site boundary through AD site and make sure that AD site has been correctly associated with the correct subnets.
- The SMS Client Installation features are configured to use an account with administrative permissions on the clients.
- SMS has been configured to deploy the clients.

## ***Other Methods for Installing the SMS Client***

In the earlier configuration example we configured the Client Push Installation option Enable Client Push Installation to assigned resources to automatically deploy and install the SMS clients. You can use several other methods to install the client: by manual installation, using a logon script, through a Windows Group Policy software installation, through a software image, and more.

SMS 2003 supports two types of clients: the advanced client and the legacy client. This example supports only the advanced client because it does not have any NT 4.0 or SMS 2.0 systems. The legacy client is based on SMS 2.0, supports NT 4.0 and Windows 98, and does not have as many features as the new SMS 2003 advanced client. The advanced client offers better security; for example, it runs under the local system account on the client computer and is not dependent upon domain accounts as was the SMS 2.0 client. Also the Advanced Client supports BITS technology, which provides better support for mobile and remote users. Also, the client agents (e.g., the hardware and software inventory agents) are included in the advanced client. When using the legacy client, the client agents must be downloaded and installed separately.

If you need to manually install the SMS client, run `\\smserver\SMS_sitecode\Client\i386\ccmsetup.exe` to install the advanced client (or run `smsman.exe` to install the legacy client).

At any time you can initiate a client installation directly from the SMS Administrators console. From the list of clients in the collections node, right-click the name of the computer on which you want to install the client, and select All Tasks, Install Client. Follow the short wizard to initiate the client installation process.

## ***Checking the SMS Client on the Client Computer***

On a computer that you have installed the SMS client, open the Control Panel. If the SMS Client was successful, you will see a new program called Systems Management. Launch the Systems Management applet and confirm that it contains information about your newly installed site. Click the Components tab to verify that the components (i.e., SMS Inventory Agent, SMS Software Update Agent, and Software Distribution Agent) are installed. Also check that the client has been correctly assigned to your site. On the Advanced tab, confirm that your site is listed as the *Currently assigned to Site Code Value*. If it is not, click the Discover button or enter the site code (e.g., SEA) and click OK. The advanced client files are in `%SystemRoot%\System32\CCM`. The legacy client files are installed to `%windir%\MS\SMS`.

## Using SMS for Software Updates

Now that we've installed a base SMS platform and deployed the SMS client to our test computers, we can focus on the Software Update Management features. In this section we'll look at how to use SMS to scan for and deploy missing security updates and run reports to show the status of the updates.

SMS 2003 integrated many, but not all, of SMS 2.0 Feature Pack's patch management features. You must add two modules separately. By default, the following software update modules are installed in SMS 2003:

- The Distribute Software Updates Wizard
- The Software Updates Installation Agent
- Software Update Reports

You must download and install these add-on modules separately:

- Microsoft Office Inventory Tool for updates (officepatch\_enu.exe)
- Security Update Inventory Tool (securitypatch\_enu.exe)

You can download these two modules as a single file from the Microsoft Web site at <http://www.microsoft.com/smsserver/downloads/2003/featurepacks/suspack/default.asp>. Copy the file to your SMS site server and run it to extract the files to a directory of your choosing. To install the two scanning tools, navigate to the chosen directory, then to the directory named SMS2003SP1ScanTools\_ENU and run the two installation programs OfficePatch\_ENU.exe and SecurityPatch\_ENU.exe.

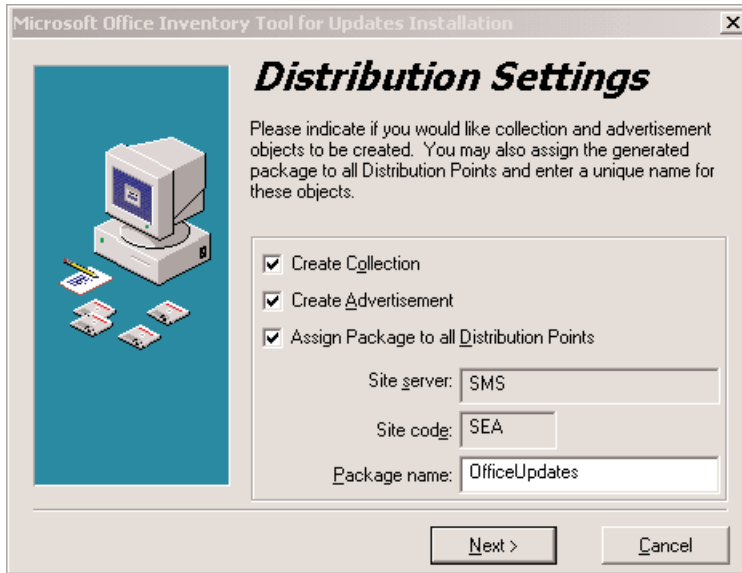
### ***Installing the Office Update Inventory Tool***

The Office Inventory Tool for Updates module is an SMS add-on that runs weekly to check the update status for Office 2003, Office XP, and Office 2000 on your SMS client machines. Both this module and the Security Update Inventory Tool module independently integrate available Microsoft utility tools for use within SMS. This integration provides a common interface and reporting mechanism for these scanning tools. SMS saves time from running these tools independently by scheduling when these tools run and collecting the results in the SMS database. Then you can use the SMS Reporting capabilities to view the update status and create new update deployment packages that install only on machines that need specific updates.

To install the Office Update Inventory Tool, run the self-installing executable file, then specify a destination directory (e.g., C:\Program Files\OfficePatch). Click Next. Because the module relies on an existing tool for the scanning process, it prompts you to download the most recent version of the tool directly from the Microsoft Web site. Click Download, and the installer will download the latest versions of invcm.exe and invcif.exe. (If your test server doesn't have direct Internet access, you must download these files separately and copy them to this machine. Search Microsoft.com for the latest version of these files. At the time of publishing, you could download invcm.exe from the Office Update Inventory Tool Version 2.1 Web site at <http://www.microsoft.com/downloads/details.aspx?FamilyID=1687c33e-d2c8-4766-937f-6e97e3e0f299&displaylang=en> and invcif.exe from the Microsoft Office Online Web site at <http://go.microsoft.com/fwlink/?linkid=19074&clcid=0x409>.) Click Next, and the installation wizard extracts and installs the tools into your SMS installation. After installing the tool, the setup wizard, which Figure 7-5 shows, walks you through the configuration.

**Figure 7-5**

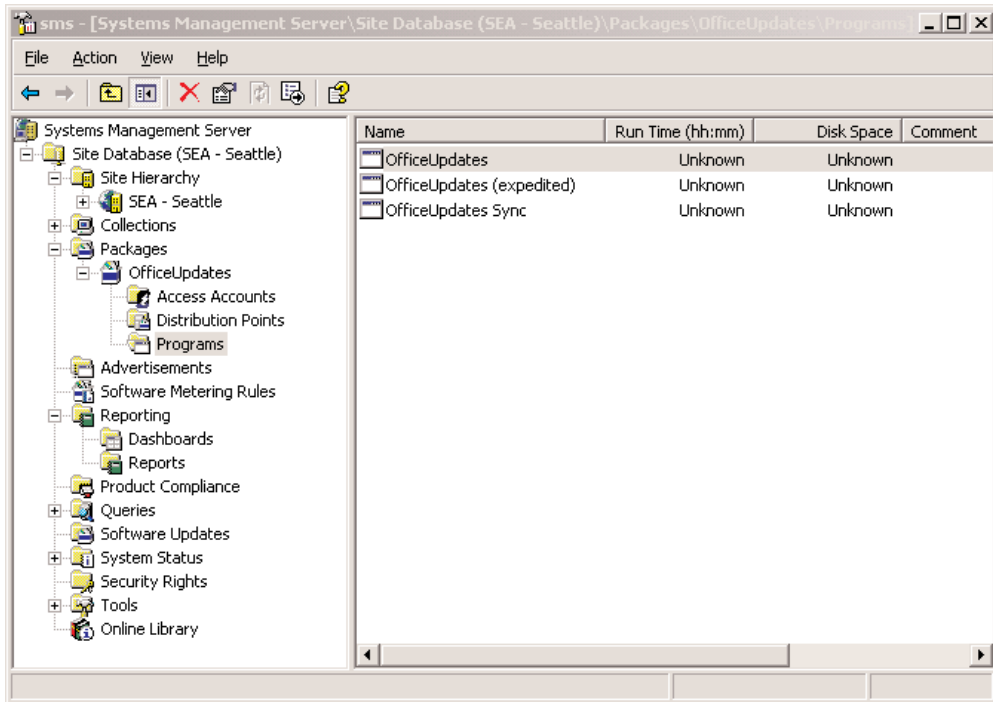
*Using the Microsoft Office Inventory Tool for Updates Installation setup wizard*



Confirm that the Create Collection, Create Advertisement, and Assign Package to all Distribution Points check boxes are selected. This tool creates a new SMS deployment package and assignment. When asked, enter a package name (such as *OfficeUpdates*), specify the names of any test computers to include in the initial advertisement, then complete the remaining steps of the wizard. Then SMS creates the programs, packages, and advertisements for the Office Update Inventory Tool.

To review the Office Update Inventory Tool module's settings, open the SMS Administrator Console, click Site Database, select Packages, and click the name of your new OfficeUpdates package (e.g., OfficeUpdates). Next, click the Programs node in which you'll find your three new programs: OfficeUpdates, OfficeUpdates (expedited), and OfficeUpdates Sync, which Figure 7-6 shows.

**Figure 7-6**  
*Showing OfficeUpdates programs in the Programs node*



Additionally, two advertisements appear in your site: OfficeUpdates and OfficeUpdates Sync. The OfficeUpdates advertisement starts the program of the same name once a week to scan your SMS client computers for installed Office components and updates. The OfficeUpdates Sync advertisement downloads new update information from Microsoft each week.

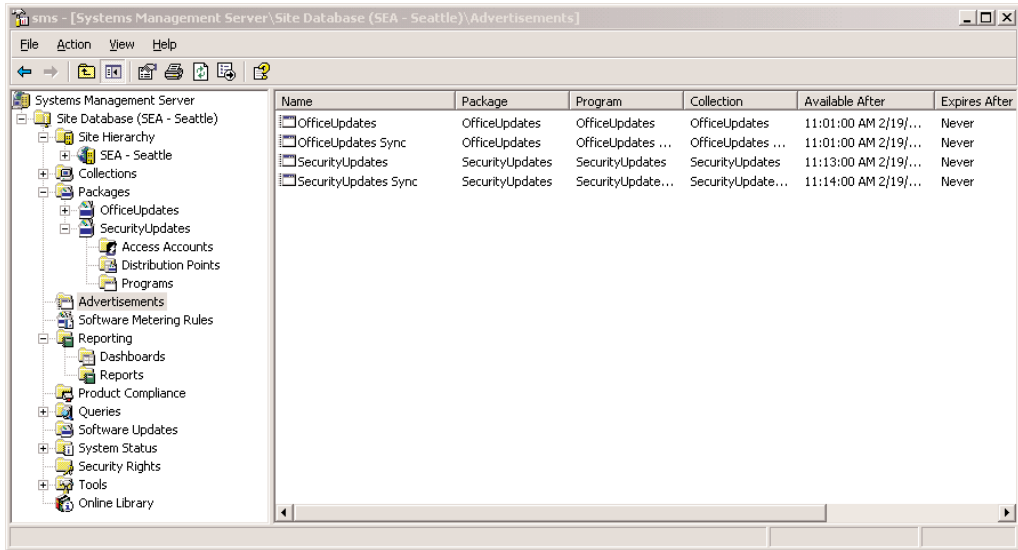
## Installing the Security Update Inventory Tool

To check for crucial OS security updates the Security Update Inventory Tool module scans a machine for installed updates and compares the results against a Microsoft database (mssecure.cab) of updates. When installed, this tool integrates into SMS and runs weekly to collect security update data from your SMS clients. As with the Office Update Inventory Tool module, you will be able to use SMS 2003's builtin reporting to view the status of the updates. Using the Distribute Software Updates Wizard, you can also create and deploy packages of updates that install on machines that need the update. SMS schedules and manages the application of the module.

Installing the Security Update Inventory Tool is similar to installing the Office Update Inventory Tool. Run the program SecurityPatch\_ENU.exe to initiate the installation wizard. Specify a destination directory for the tools (e.g., C:\Program Files\SecurityPatch). Then the tool prompts you to download the latest version of the security patch bulletin catalog file (mssecure.cab), an XML file. Continue through the wizard to install the Security Update Tool. Like with the Office Update tool, enter a name

for the Package (e.g., SecurityUpdates). Review and specify the Distribution settings, Database Updates, and a test computer. Then install the module. As Figure 7-7 shows, new SMS advertisements associated with the Security Update Inventory Tool have been added to your SMS installation.

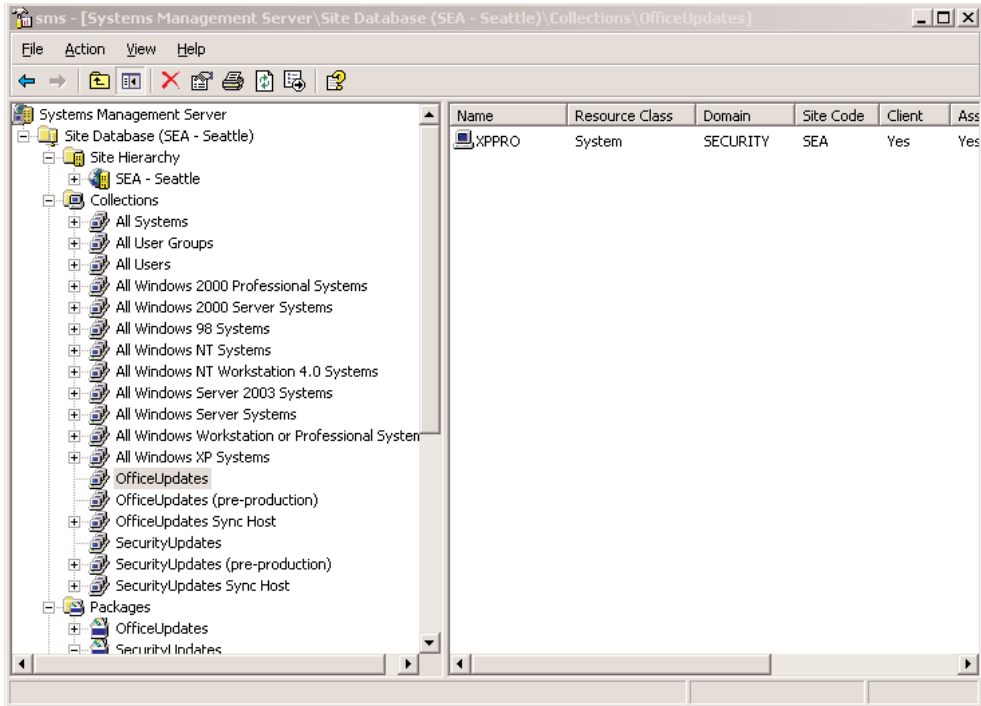
**Figure 7-7**  
*Viewing new SMS advertisements for updates*



## SMS Vernacular: Programs, Packages, Advertisements, and Collections

Before we get too far into the nuts and bolts of scheduling scans and deploying security updates, let's take a crash course in SMS lingo. In SMS vernacular, a program defines the binary application (e.g., patchinstall.exe) that describes the command line, the starting directory, and the rights under which the application runs (e.g., administrative rights). The package encapsulates multiple programs and specifies the distribution points, or locations, to deliver the package. For example, if you have geographically dispersed offices connected by a slow link, you will likely place a distribution point in each office. The package also contains information about how to deliver the programs to the distribution points: for example, whether to compress the files. An SMS advertisement schedules when a program will run and configures the program for a specific collection. Collections are logical groupings of SMS clients used to target SMS actions. For example, the Microsoft Office Update Inventory Tool module creates several collections for testing and production computers, which Figure 7-8 shows.

**Figure 7-8**  
*Showing Collections for testing and production computers*

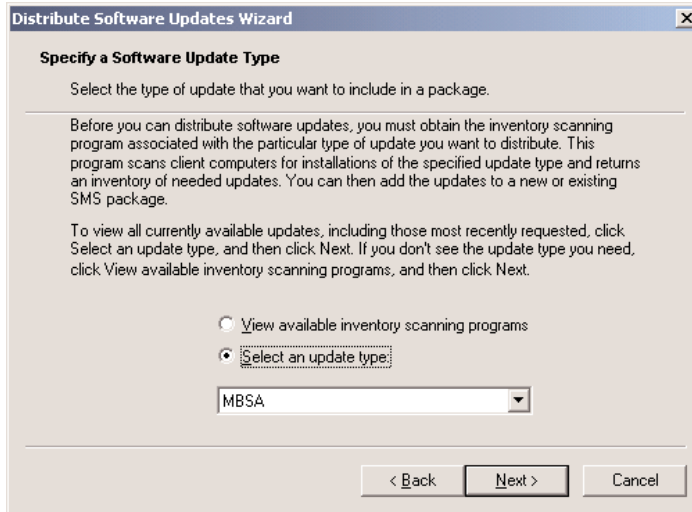


## Creating Your Package of Updates: Working with the Distribute Software Updates Wizard

The Distribute Software Updates Wizard was previously a separately installed add-on to SMS 2.0 available from the SMS Feature Pack, but it is fully integrated into SMS 2003 SP1. This module analyzes data that the Office Update Inventory Tool and the Security Update Inventory Tool modules collect, then recommends patches to install. This wizard pulls a list of applicable updates identified during an earlier run of either the Office Updated Inventory Tool or the Security Update Inventory Tool scan, then walks you through the process of downloading the updates and configuring them for deployment through SMS. Although SMS package creation can be challenging, the Distribute Software Updates Wizard eases the challenge a bit by setting the package parameters, downloading the updates, and configuring the SMS programs and packages for you.

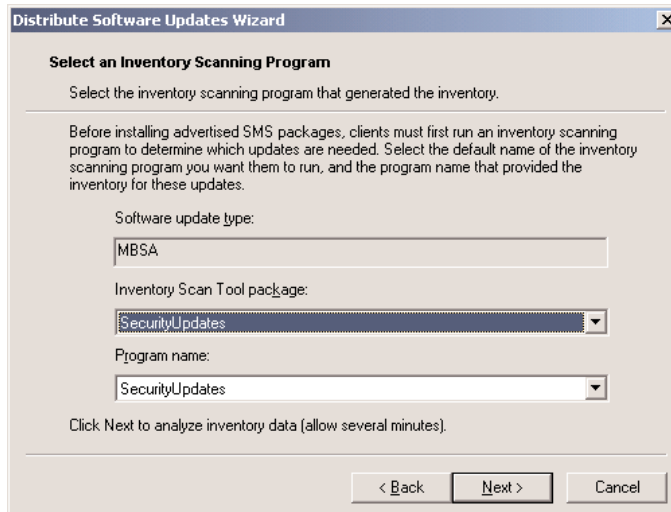
Open the SMS Administrator Console, expand Site Database, right click Software Updates, expand All Tasks, and select Distribute Software Updates to invoke the Distribute Software Updates wizard. On the first step of the wizard, select the software update type: MBSA (for Security Updates) or Microsoft Office (for Office Updates), as Figure 7-9 shows.

**Figure 7-9**  
*Selecting a software update type*



The wizard notifies you that you must create a new package; in subsequent runs, the wizard lets you edit existing packages. This new package will contain the security updates for deployment. Name your package (e.g., MyFirstSecurityUpdates) and enter the name of your organization. Next, specify the Inventory Scan Tool package and the Program name. For this example, select Security Updates for each, as Figure 7-10 shows.

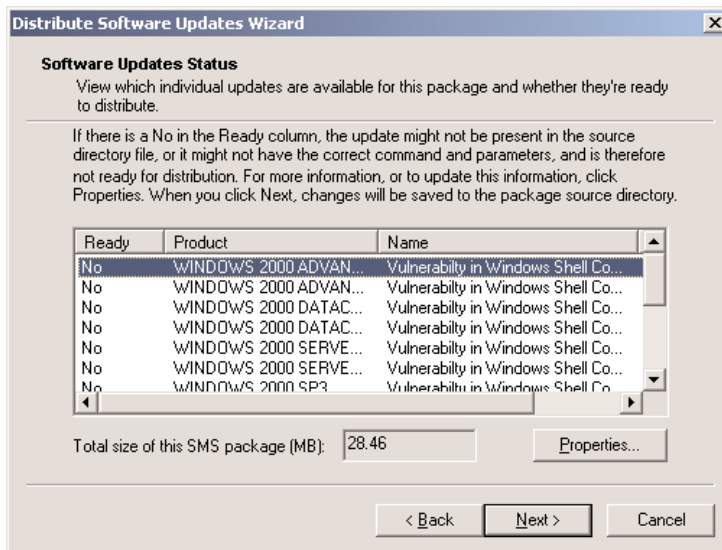
**Figure 7-10**  
*Selecting the Inventory Scan Tool package and the Program name*



The next wizard screen displays applicable security updates. The wizard generates this list by comparing the available Microsoft security updates against the results of previous security update inventory scans. Select the updates you want to include in this package. Click Next, then specify the source directory in which the update files will reside. SMS can download the updates for you and copy them to your distribution point. If a download fails, you'll need to download the update separately. At times SMS can't download an update (e.g., the URL might point to an incorrect or broken update link), so you will need to become familiar with the process of downloading updates and pointing the wizard to them. SMS sometimes stumbles as it tries to reconcile and automate the many different update formats that Microsoft offers. If the wizard fails to identify the update executable file, you must manually open the Microsoft Security Bulletin Web site, search for and download the correct version of the specific update, and copy it manually to a location that the SMS Distribute Software Updates Wizard specifies. Even with the help of the wizard selecting the individual updates, waiting for them to download then configuring them for deployment is a time consuming process compared to SUS and WSUS's simpler update process.

After downloading each patch to your distribution point, the status of each update shows *not* Ready, which Figure 7-11 shows. To make an update ready, you must specify the command-line parameters the update will use when it runs.

**Figure 7-11**  
*Showing the status of the patches*



Select each update and click Properties to view details about the update. By default, the Parameters box might be blank, as Figure 7-12 shows.

**Figure 7-12**  
*Showing a blank Parameters box*

The screenshot shows the 'Distribute Software Updates Wizard' dialog box. The fields are filled with the following information:

- Product:** WINDOWS SERVER 2003, DATACENTER EDITION GOLD
- Name:** Vulnerability in Windows Shell Could Allow Remote Code Executi
- Language:** English (United States)
- Locale ID:** 1033
- Make this update valid for all client locales
- Program:** WindowsServer2003-KB890047-x86-enu.exe
- Parameters:** (empty field)
- Binary present:** Yes
- Binary path:** http://download.microsoft.com/download/1/6/5/165c3dac-d5f6-
- QNumber of the KB article:** 890047
- Authorized on:** 2/19/2005 12:23 PM
- Coordinated Universal Time

Buttons visible include 'Information', 'Impgnt...', 'Syntax', 'Download', 'OK', 'Cancel', and 'Help'.

You must specify parameters to suppress reboots and limit user interaction (i.e., silent or quiet install). Unfortunately, as explained in earlier chapters, Microsoft employs multiple engines to deploy its updates, and each engine uses specific command-line variants. When in doubt, click Syntax to display a Microsoft Web site showing the myriad of command-line switch information about a specific update's engine or go to the Microsoft Web site at <http://support.microsoft.com/default.aspx?scid=KB;en-us;q810232>. Table 7-1 provides several command-line variants excerpted from the table at the Microsoft Web site.

**Table 7-1 SMS Software Update Command-Line Switches for Silent Installations**

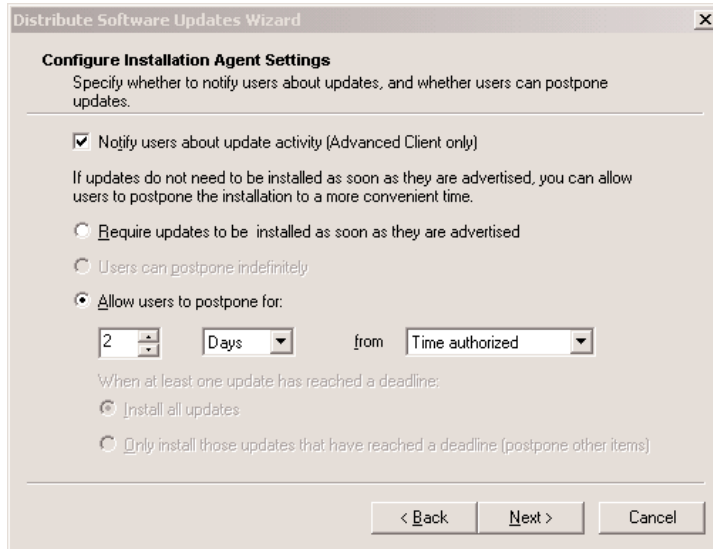
Product or Component	Command Line	Examples
Windows NT 4.0 and Windows 2000 (Win2K) SP3 and earlier		-q -z q123456i.exe -q -z
Win2K SP4 and later, and Windows XP (Switches vary depending upon update.exe version.)	/q /u /z /norestart /quiet /passive	q123456_w2k_sp4_x86_en.exe /q /u /z q123456_w2k_sp4_x86_en.exe /norestart /quiet /passive
Internet Information Services (IIS) 4.0 and 5.0	/q /z	q123456.exe /q /z q1234356_w2k_sp2_x86_en.exe /q /z
Internet Explorer (IE)	/q:a /r:n	q123456.exe /q:a /r:n
Windows Media Player (WMP)	/q:a /r:n	wm320920_71.exe /q:a /r:n
Exchange 2000 Server	/q /z	811853_enu_i386.exe /q /z
Exchange 2003 Server	/q /z	Exchange2003-KB832759-x86-enu /q /z
Office		See the SUS Feature Pack release notes and online documentation.
SQL Server 2000	/a /q DISABLESTATUS=AUTO	SQLHotfix_ENU.exe /a /q DISABLESTATUS=AUTO
Virtual Machine (VM)	/c:"javatrig.exe /exe_install /l /q" /q:a /r:n	msjavwu.exe /c:"javatrig.exe /exe_install /l /q" /q:a /r:n
Microsoft Data Access Components (MDAC), and Microsoft XML Core Services (MSXML)	/C:"dahotfix.exe /q /n" /q:a enu_Q832483_mdac_x86	/C:"dahotfix.exe /q /n" /q:a
Commerce Server		Please refer to the bulletin for the available command-line syntax.
Content Management Server (CMS)		Please refer to the bulletin for the available command-line syntax.
BizTalk Server		Please refer to the bulletin for the available command-line syntax.
Host Integration Server (HIS)		Please refer to the bulletin for the available command-line syntax.
Dell system updates or Dell component updates	No need to specify.	The correct command line is provided by the Dell update catalog.

[Note: This table is reprinted from Microsoft Knowledge Base article 810232.]

Click the *Information* button to go to an update's TechNet Web page. These pages give you quick and detailed information about specific updates. After you have added the parameters for each update, click Next to specify the distribution points that will push the package to clients. At this point in the process you can specify whether to immediately collect client inventory and postpone restarts for servers or workstations.

Lastly, configure the desired behavior of the Software Updates Installation Agent. The Software Updates Installation Agent runs on a client machine during the update package installation to ensure that you don't install redundant or unnecessary updates. This agent provides granular control over the deployment process for a set of updates. For example, you can specify the number of minutes that the process should wait for a user to accept an update before installing it automatically. This agent can also monitor update installations and cancel installations that hang or fail. As Figure 7-13 shows, you can also let users install updates at their convenience.

**Figure 7-13**  
Viewing the *Configure Installation Agent Settings* dialog box

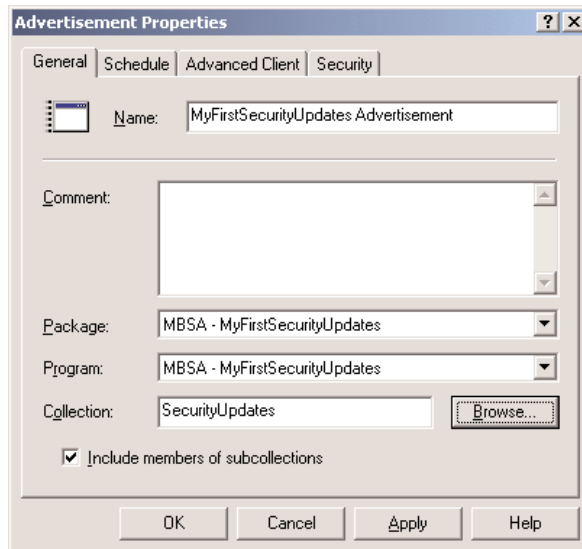


For example, you can allow users to wait 2 days before having the update install automatically or restart the system. Users like to be able to specify when to install updates, and you can rest assured that the updates will deploy. Additionally, you can configure the Installation Agent to report successful and failed installations and elect to postpone system restarts for servers and workstations. This feature is handy when you're deploying a package to a mixed group of servers and workstations and you want to reboot the workstations immediately after installing an update, but want to delay rebooting servers until you take them offline for maintenance. This last step completes the Distribute Software Updates wizard but the package will not deploy yet. We must advertise the package.

### ***Advertise Your Updates***

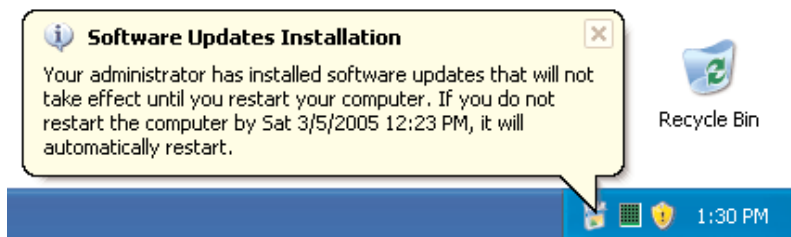
Navigate to Site Database, right click the Advertisements node, select New, then Advertisement. On the General tab, name the advertisement (e.g., MyFirstSecurityUpdates Advertisement), select the Package and Program, and enter the name of the Collection that includes the target computers for the advertisement to include. In this example, as in Figure 7-14, you can see that most of the entries are from objects we created earlier.

**Figure 7-14**  
Viewing Advertisement Properties



Also in our example, the collection SecurityUpdates includes one computer defined for testing, named *xppro*. Click the Schedule tab and define the time that you want to deploy the software. Regularly scheduled SMS advertisements are available for installation from a users Add Remove Programs control panel program. But with security updates, you will most likely want the security updates to install automatically without user interaction. To do this, you must assign the package by scheduling it for mandatory assignment. On the Schedule tab, click new mandatory assignment, and specify a time (or specify *As soon as possible*). After you click OK, you can see that your new advertisement is listed under Advertisements.

At this point you can switch over to an affected client and watch the SMS client install the new updates. Because this example is a security update, while watching task manager you will see the Microsoft Baseline Security Analyzer (*mbsacli.exe*) scan the computer before the update is installed (the security update inventory tool uses *mbsacli.exe* to scan the client computer). This scan ensures that only the necessary updates are deployed. Lastly, depending on your package preferences, your users might be presented with a dialog box instructing them to restart their computer within a specified timeframe, as Figure 7-15 shows.

**Figure 7-15***Receiving notification of an update and restart time*

Run the update and check that the patches have installed successfully. (For testing purposes, you can run MBSA on the test machine to quickly verify that the appropriate updates applied successfully.) If you encounter any problems, examine your client machine's CCM\logs directory (e.g., %windir%\system32\ccm\logs) for the patchinstall.log file. This file lists all the applicable updates for that client and which updates are authorized in that package. This step can help you determine why a particular update or package isn't installing correctly.

## SMS 2003 Reporting

SMS 2003 also includes builtin Web reports from the SMS server defined as a reporting point. Access the SMS Web Reports home page (by default this page is located at [http://smsreportserver/SMSReporting\\_sitecode](http://smsreportserver/SMSReporting_sitecode)) to view any data collected since installing the update tools and running the inventory.

## Manually Refreshing the Reports

To manually refresh report data—for example, after installing updates on a machine—you must specify a new time for the Security Update Inventory Tool and the Office Update Inventory Tool advertisement to run. When these programs finish running, you must run a hardware inventory on the client machine. On the client system, run the Systems Management applet. Click the Components tab, select the Hardware Inventory Agent, and click Start Component. This process will gather the update information from the client machine and post it to the SMS database, thereby updating the SMS Software Update reports.

Standard SMS reports include Hardware Inventory, Software Inventory, details on the SMS Site, and Status Message Reports. Patch status reports include drilldown-capable reports that show patches by machine, all patches, or patches by product. Microsoft includes many different reports that let you easily survey your organization's overall patch landscape or drill down into details about an individual patch or machine's deployment status.

## Patch Management with SMS

SMS 2003 provides a high degree of flexibility for deploying Microsoft Security updates, but it is not for the faint of heart. Although SMS is an enterprise tool, it can be used in small to midsize shops. But to use SMS successfully requires more training and configuration than Microsoft's less sophisticated products, such as SUS and WSUS. Plus the preparation of the patches for deployment is

much more hands on than with SUS, WSUS, or other commercial patch management programs. But for those that do invest the time, SMS provides a widely customizable platform from which to scan for and deploy updates and most any other software.

Remember these tips when installing SMS 2003 for patch management:

- SMS is designed to scale for very large enterprise deployments, so many of its components are modules. For a small or lab environment, install SMS on one server for basic testing of the patch deployment features.
- An SMS client must be installed on each target computer.
- Programs include the definition of the updates that you want to deploy.
- Packages define the distribution points for groups of related programs.
- Advertisements define the schedule and logistics for deploying a package—including the targeted collections.
- Collections are groups of computers based on system attributes or manually defined.
- In an SMS 2003 environment you must install the Office Update and Security Update scanning tools.
- Use SQL Server's backend, builtin queries, custom queries, and reports to generate a stunning array of views into your data.

The combination of reports, inventory tools, and targeted patch distribution that SMS offers might be compelling enough to lure non-SMS converts into the fold. Properly deployed, SMS becomes a powerful foundation for patch management.