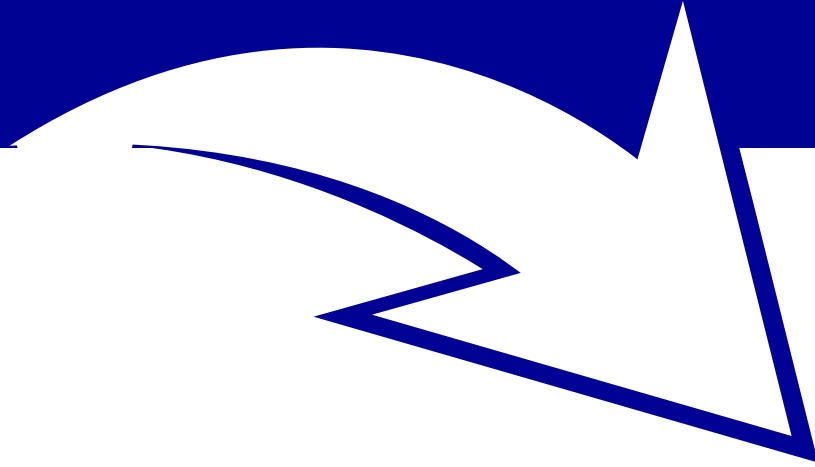


realtimepublishers.comtm

The Administrator Shortcut Guidetm To



Patch Management



Rod Trent

Chapter 3: Patch Management Tools	39
Selecting a Tool	39
Key Selection Criteria.....	39
Learning Curve	40
Ease of Use	40
Platform Support.....	40
System Targeting	41
Comprehensive Testing by Patch Management Vendor.....	41
Comprehensive Reporting	41
Product Patch Support.....	41
Patch Management Product Maturity and Stability	41
Scalability	42
Connection Sensitivity	42
Deployment Schedule.....	42
Wake-on-LAN	42
Customizable Deployment Options	43
Elevated Rights Deployment	43
Strong Customer Support.....	43
International Support	44
Product Security.....	44
Agented vs. Agentless.....	44
Systems Management	45
Cost	46
Overview of Different Types of Patch Management Applications	46
SUS Overview—Free Tool Example.....	46
SMS 2003 Overview—Enterprise Application Example	48
Prism Patch Manager Overview—Agented or Agentless Example	49
Key Comparisons for SUS, SMS, and Prism Patch Manager.....	50
Example of Using a Patch Tool	51
Summary	55

Copyright Statement

© 2004 Realtimerepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimerepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimerepublishers.com, Inc or its web site sponsors. In no event shall Realtimerepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimerepublishers.com and the Realtimerepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimerepublishers.com, please contact us via e-mail at info@realtimerepublishers.com.

Chapter 3: Patch Management Tools

This chapter discusses several considerations that are important when determining the patch management application that is right for your environment. Although each environment is different and each company's business needs will determine the specific tool-selection criteria, this chapter provides several key areas that need to be included in your fact-finding research for choosing a patch management product.

This chapter will also delve into the various patch management application types and the different methods they use to provide patch management support. To illustrate the available capabilities and features, we will explore a few of the popular tools.

Selecting a Tool

One of the major decisions of patch management is the determination of which application or toolset you will use to deploy patches. The decision must be based on several areas of focus, but ultimately you need to decide on an application that fits well into your current processes, workflow, policies, and computing environment. The application should closely follow the patch management procedures and policies that you have implemented. Paramount to selection is finding an application that is flexible enough to adjust to—without negatively impacting—business that also patches all systems successfully. In addition, the chosen patch management application should provide the ability to completely automate your processes as well as give you peace of mind, knowing that the computing environment is safe and secure.

A best practice is to determine your workflow, then decide on a patch management application, rather than buying the application and learning later that it doesn't meet your needs. Too many companies make the purchase first (usually as a result of a business management decision), then realize that the application doesn't adequately meet the needs of the environment. The patch management staff is left with an application for which the staff must develop custom workarounds to ensure that the environment is secure.

Key Selection Criteria

The following list highlights key criteria you will want to include in your selection process for a patch management application:

- Learning curve
- Ease of use
- Platform support
- System targeting
- Comprehensive testing by patch management vendor
- Comprehensive reporting
- Product patch support
- Patch management product maturity and stability
- Scalability

- Connection sensitivity
- Deployment Schedule
- Wake-on-LAN
- Customizable deployment options
- Elevated rights deployment
- Strong customer support
- International support
- Product security
- Agented vs. agentless
- Systems management
- Cost

When making your selection, apply the criteria you envisioned during your patch management policy development to these criteria (where applicable) in your decision making process.

Learning Curve

How much time will be required to learn the application? If you are looking to purchase a patch management product, it is likely that business management has already approved the purchase, which means obtaining a product is critical to the business. Thus, the product that is chosen will need to be implemented in a short timeframe after purchase. During your testing, research, and evaluation of the various products, determine the level of competence one needs to implement the product across the entire organization and how long the implementation phase will take.

Ease of Use

Another key criterion is how easy it will be to deploy patches once the patch management application is implemented. Use critical patches as a yardstick for determining how quickly you can prepare a patch for deployment throughout your organization.

Platform Support

Unless every computer in your company runs the same OS and OS revision and service level, you will want to consider how well the patch management application supports different levels of OS versions. In most companies, a diverse set of OS versions are in use every day. Some run Windows XP with SP1, while others continue to run Windows 98 or Windows NT for compatibility with older business function applications that have not been upgraded by the vendor. The patch management application must be able to support the entire environment and provide the ability to distribute patches to each computer.

System Targeting

When searching for a patch management application, include the criteria for system targeting. System targeting allows you to deploy patches to a specific selection of computers based on specific criteria. For example, the ability to deploy a patch only to the Windows XP computers in your company that have SP1 installed. Alternatively, you might want to target only a range of computers at a specific office in your company, or even a select business group such as Human Resources.

Some patch management applications also allow you to deploy to a range of IP addresses, Windows security groups, and even Active Directory (AD) containers. Determine the level of deployment control that you require and evaluate the patch management applications accordingly.

Comprehensive Testing by Patch Management Vendor

Even after Microsoft releases a patch publicly, several patch management application vendors test the patches further before authorizing them for release through their products. This feature gives an extra level of protection for the patch management application customers. If you are concerned about whether Microsoft adequately tests patches, you will want to include this criterion into your overall evaluation plan.

Comprehensive Reporting

Being able to clearly determine whether a system has been successfully patched is as critical as the ability to deploy patches. Make sure the products that you evaluate provide a built-in mechanism—or at least an available add-in or plug-in for download and use—that enables reporting. Another useful feature is the ability to customize reporting to your environment.

Product Patch Support

Most companies utilize many applications to support the business. When considering a patch management application, determine whether you need patch support for more than just the OS. If you need patch support for other applications—such as Microsoft SQL Server, Microsoft Office, or other custom applications—look for products that offer additional application support or the ability to incorporate your own patches into the distribution system.

Patch Management Product Maturity and Stability

How long has the patch management application been offered, and how long has the vendor been supporting the product? There are several major and trusted patch management products on the market; you might feel more comfortable with these products than with a newcomer to the market. In addition, consider whether the product has been specifically designed for patch management, rather than as part of an overall systems management solution. Some of the stalwart systems management solution vendors added patch management capabilities later, which means the core application is strong but the patching portion may be in its infancy.

Scalability

For small to midsized companies that don't intend to grow significantly, scalability might not be a concern. However, for large companies and those companies that intend to steadily add new workstations to the environment, determine whether the patch management product can grow with you. If you have thousands of computers to distribute patches to, you will want to make sure that any potential products are scalable.

Connection Sensitivity


Distributing patches across the network to workstations can cause excessive use of the connection. A connection-sensitive patch management product will allow you to “throttle” the amount of bandwidth it can utilize to distribute the patches. A connection-sensitive patch management product can also automatically determine the connection speed and type and use this information to either halt distribution when the connection is too slow or use methods of transferring the patches in the background. There are several products on the market that offer “drizzle” technology to allow a remote or dial-in user to receive patches over a slower connection without drastically hampering the connection speed.

Deployment Schedule

A good patch management application should offer a comprehensive scheduling component. If you have access to a scheduling system, you can prepare the patch for deployment, then configure it to start at a later date. This capability allows you to initiate the transfer of the patch from the network to the workstations during off-hours or overnight. The scheduling system allows you to minimize the impact of patches on your network and on end users' productivity. And, if something comes up before the patch starts its distribution, you can quickly alter the schedule for another time or stop the distribution completely. This functionality gives you a high level of control over the patch management process.


Wake-on-LAN

Though not always a necessary component in some organizations, if you determine that you must deploy patches at night while the computer is still connected to the network, Wake-on-LAN can be an extremely useful feature. Patch management applications with Wake-on-LAN capability enable a packet to be sent to a waiting workstation, and that packet “wakes-up” the computer so that the patches can be installed while the user is at home. When the user comes to work in the morning and boots the computer to start the day, the computer has already been patched without incurring any productivity losses.

 Wake-on-LAN is a part of Intel's Wired for Management System and is a result of the Intel-IBM Advanced Manageability Alliance. For more information, see <http://www.intel.com>.

Customizable Deployment Options

Some organization's software distribution policies require that software be installed silently, without any user interaction, and forgo a reboot until the user shuts down for the day. The patch management solution you choose should offer options that closely follow your software distribution policies. The product should enable you to customize the command-line options to meet your requirements or to alter the way the patch is distributed should a requirement change during your testing and planning.

 For a list of possible Windows patch options, see the Microsoft article "Summary of Command-Line Syntax for Software Updates" at <http://support.microsoft.com/default.aspx?scid=kb;en-us;810232>.

Elevated Rights Deployment

In NT 4.0, Win2K, and Windows XP environments, different groups of users have different levels of rights and permissions. In these environments, default users have limited access to system areas of the computer. Users without administrative rights cannot install certain patches. Determine whether the patch management products you are reviewing have the ability to install patches using the elevated rights required for a successful deployment.

Strong Customer Support

Another consideration in your patch management product selection is the support infrastructure of the solutions' vendors. The following list provides example questions to use as a basis for your evaluation; develop questions customized to your environment to best determine your vendor support requirements:

- How quickly can the vendor help you with problems with the product and/or patches?
- Does the vendor offer onsite training?
- How quickly does the vendor make patches available for the product after Microsoft (or an application vendor) has made the patches publicly available?
- What level of support is included with the purchased product?
- Are there varying levels of support depending on the number of licenses you purchase?
- Does the vendor offer a secure download for updates to the product?
- Does the purchase of the product include future updates?
- Does the vendor graciously accept feedback about the product and support?
- Will the vendor work with you to implement the product to fit your environment?

International Support

Does the product support many languages and codepages? Larger companies tend to have offices in many countries. In these scenarios, the product must be able to provide international support options; the product must:

- Enable global communication, allowing users to edit content and work in any language
- Simplify the deployment, maintenance, and support of different language releases of the OS and applications worldwide, reducing the complexity and overall cost of ownership
- Deal with a larger number of system differences from one language to another; doing so eases the maintenance and administrative effort

Product Security

Patching the computers in your organization is an effort to bring the environment within the most current level of security. Thus, the patch management product you choose must not be the weak link in the security chain. Verify that the products you evaluate include secure communications and encryption between the client and the server.

Agented vs. Agentless

There are two types of patch management products: agented and agentless. An agented solution requires that a client component is installed on the workstations and server prior to patch deployment functions being available. Agentless solutions utilize other technologies to distribute the patches to the workstations and servers. An agentless solution enables you to deploy patches immediately after installing the patch management server component.


The two types of options change the implementation and management level. With the agented solution, you must make sure that the agent is always functioning; otherwise, patches will not be distributed to the computers. This requirement can be frustrating when you have to distribute a critical patch. However, although this requirement adds an extra level of management (that is, making sure that the agents are working and the computers are communicating), agented solutions tend to offer more features such as installed patch inventory and hardware and software inventory. In addition, agentless solutions usually provide little or no support for mobile or remote systems such as laptops.

Also, agented machines are beneficial in the following situations:

- Intermittently connected laptops—Agentless solutions require the computer to be connected at the time of deployment, while agented solutions can queue the patch deployments, automatically installing the desired patch(es) the next time a connection is established.
- Computers connected over slow links—Agented solutions may offer bandwidth throttling options, making the patch process bandwidth friendly.
- RPC restricted configurations—Secured networks—such as government agencies and hospitals conforming to specific HIPAA standards—that disable RPC will benefit from agented machines. Windows XP Service Pack 2 (SP2), by default, will render agentless solutions unusable as the built-in firewall will block all incoming connections. Agented solutions work well in these hardened networks because the agent usually initiates the contact to the patch server, not vice versa.

Systems Management

If your company needs more features than a standalone patch management application can provide, consider products that offer overall management of the environment. Several systems management vendors have incorporated patch management components into their products over the past year.

 As noted earlier, spend time researching systems management packages to determine how long they have supported patch management components. Many products that have been on the market for some time might have only recently added these features; thus, the solutions' patch management components aren't as time tested as the rest of the product.

Systems management applications provide key features in addition to patch management:

- Remote computer management
- Hardware inventory
- Software inventory
- Asset management
- Software distribution
- Querying and reporting
- Workstation and server monitoring

An important factor when reviewing a systems management product is that these applications generally include software distribution components, which are useful for situations in which a patch does not follow the normal rules for deployment. For example, some patching products might not report on Outlook Express or DCOM, so you would need to employ the software distribution product (which includes reporting on these products) to distribute the patches. A standalone software distribution feature also means you can deploy any piece of software requested by the users. A patch management application cannot deploy the full Microsoft Office 2003 installation, but a software distribution solution can.

Cost

Cost is probably the ultimate deciding factor for a specific patch management application. You must weigh a product's features; the overall cost of implementation, deployment, and continued management; and the return of value against the licensing costs. If the price of purchasing the product combined with these factors exceeds the price you are willing to spend, you might need to "settle" on an alternative, lower-priced product. Choosing a product based on cost is understandable, but you need to also keep in mind that the ultimate goal for patching is to keep the environment secure. You'll need to calculate the cost of downtime, loss of data, and loss of intellectual property, then compare that data with the price of the product. In most cases, the price of the product will be considerably less than the cost of a direct, electronic attack on your company's computing assets.

There are a few "free" patching tools on the market, which would ease the cost burden of a patch management tool, but you must consider the level of support and the feature set that is included with these free tools. In addition, although a product might be labeled as free by the vendor, there are other costs associated with installing, implementing, and managing the product. For example, you might need to deploy a brand-new server with the adequate requirements and proper OS licensing, just to implement the "free" product. In most cases, you get what you pay for.

Overview of Different Types of Patch Management Applications


To give you an idea of the types of patching solutions on the market, let's explore a brief overview of Microsoft Software Update Services (SUS), Microsoft Systems Management Server (SMS), and New Boundary Technologies' Prism Patch Manager.

SUS Overview—Free Tool Example

Microsoft SUS is a no-charge add-in component for Win2K and Windows Server 2003 (WS2K3) that is designed to greatly simplify the process of keeping computers in your organization up to date with the latest critical updates, security updates, and service packs. SUS installs a Web-based application that enables administrators to quickly and reliably deploy updates to desktop and server machines running Win2K, Windows XP, and WS2K3. The updates can be synchronized from the live Windows Update servers and saved on the SUS server. Then, after approving only the updates you have tested and want to distribute, the updates can be downloaded from the SUS server by the Automatic Updates component on client machines.

SUS consists of the following downloadable components:

- Microsoft SUS—This server component is installed on a computer running Win2K Server inside your corporate firewall. SUS synchronizes with the Windows Update site to deliver all critical updates for Win2K and Windows XP. The synchronization can be automatic or completed manually by the administrator. When the updates are downloaded, you can test the updates, then decide which updates to install throughout your organization. The SUS server component is available in English and Japanese.
- Automatic Updates—This component runs on any client machine that you want to keep updated by using SUS. The Automatic Update component is included in Win2K SP3 and later, Windows XP SP1 and later, and WS2K3; it can be easily installed on Win2K SP2 and Windows XP RTM systems. This component enables your Windows servers and Windows client computers to connect to a server running SUS and receive any updates. You can control which server each Windows client should connect to as well as schedule when the client should perform all installations of critical updates—either manually or via Group Policy and AD. Automatic Updates is available in 24 languages.

 SUS does not include a built-in reporting feature, but there are several free add-ons available for download from the Internet. A couple of popular reporting tools are:

<http://www.susserver.com/Software/SUSreporting/>

<http://www.usinfinet.com/products/details.aspx?prod=3>

SUS 1.0 supports updates for Win2K SP2 and later, Windows XP Professional, and WS2K3. It does not include provisions for updates to any other Microsoft products, such as Microsoft Office, SQL Server, or Exchange Server. As many as 15,000 clients can be supported by a single SUS server. You can also use multiple SUS servers in a single environment. SUS 2.0 is due sometime during the first part of 2005 and will include support for other Microsoft products and a reporting feature. SUS 2.0 has been renamed to Windows Update Services (WUS).

SUS Resources

The following list highlights useful resources for learning about SUS and evaluating the product as a patch management solution for your environment.

SUS interactive simulation at

<http://www.microsoft.com/windowsserver2003/evaluation/demos/sims/sus/viewer.htm>

SUS Frequently Asked Questions (FAQs) at

<http://www.microsoft.com/windowsserversystem/sus/susfaq.mspx>

SUS overview white paper at <http://www.microsoft.com/windowsserversystem/sus/susoverview.mspx>

SUS deployment white paper at

<http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx>

“Updating a Small Business Server Network with SUS” at

<http://www.microsoft.com/windowsserversystem/sus/updatingsbswsus.mspx>

“Microsoft Solutions for Management: Patch Management Using Microsoft Software Update Services” at

<http://www.microsoft.com/downloads/details.aspx?FamilyId=38D7E99B-E780-43E5-AA84-CDF6450D8F99&displaylang=en>

WUS FAQs at <http://www.microsoft.com/windowsserversystem/sus/wusfaq.mspx>

SMS 2003 Overview—Enterprise Application Example

Microsoft SMS 2003 provides a comprehensive solution for change and configuration management for the Microsoft platform, enabling organizations to provide relevant software and updates to users quickly and cost-effectively. SMS 2003 provides the following key capabilities:

- Application deployment
- Asset management
- Security Patch management
- Mobility
- Windows management services integration

SMS 2003 is an agented technology. Before patches can be deployed to your workstations and servers, the SMS client (agent) must be discovered and installed, hardware and software inventory must be performed, and the computer information must be in SMS's SQL database. SMS 2.0 offered an add-on called a Feature Pack that included patch management as an option to SMS administrators. SMS 2003 is the first version to incorporate the patch management component, called Software Update Management, into the product. Software Update Management provides full support for obtaining, reviewing, testing, deploying, and monitoring patch deployments. SMS 2003 also includes special technologies for deploying updates to remote or slow-connection clients.

SMS 2003 Resources

The following list highlights resources for learning about SMS 2003 and evaluating the product as a patch management solution for your environment.

What's new in SMS 2003 at <http://www.microsoft.com/smsserver/evaluation/whatsnew/default.asp>

Product overview at <http://www.microsoft.com/smsserver/evaluation/overview/default.asp>

Product features at <http://www.microsoft.com/smsserver/evaluation/features/default.asp>

Datasheets at <http://www.microsoft.com/smsserver/evaluation/datasheets/default.asp>

Demos at <http://www.microsoft.com/smsserver/evaluation/demo/default.asp>

SMS 2003 evaluation software at <http://www.microsoft.com/smsserver/evaluation/2003/default.asp>

Capabilities at <http://www.microsoft.com/smsserver/evaluation/capabilities/default.asp>

SMS 2003 feature pack overview at
<http://www.microsoft.com/smsserver/evaluation/featurepack/default.asp>

System requirements at <http://www.microsoft.com/smsserver/evaluation/sysreqs/default.asp>

Case studies at <http://www.microsoft.com/smsserver/evaluation/casestudies/default.asp>

FAQs at <http://www.microsoft.com/smsserver/evaluation/faq/default.asp>

Reviewer's guide at <http://www.microsoft.com/smsserver/evaluation/revguide/default.asp>

Prism Patch Manager Overview—Agented or Agentless Example

New Boundary Technologies' Prism Patch Manager is a software update (patch) management solution for NT 4.0, Win2K, Windows XP, and many mission-critical applications. This product enables network administrators to perform research on the updates that are available for their systems, query systems to determine the current update or patch level, install updates from a central console, define policies concerning update installation, and verify that a previously installed update is still valid.

From the Prism Patch Manager console, users can perform the following tasks:

- Read articles about the updates (research)
- Query systems (inventory)
- Remotely install any combination of updates (deployment) for the following software products NT 4.0, Win2K, Windows XP, WS2K3, IIS, SQL Server, Exchange Server, Internet Explorer (IE), Media Player, Windows Media Services, NetMeeting, Office 2000, Office XP, Office 2003, Outlook 2000, Outlook 2002, and Microsoft Data Access Components (MDAC)
- Define policies (required updates)
- Verify installations (validation)

Prism Patch Manager provides the most comprehensive software update research, query, distribution, and validation solution, giving administrators the decision-making and policy-management solution that they need for managing the process of deploying service packs, hotfixes, and other self-installing software patches. Prism Patch Manager can be deployed using both agented and agentless options; thus, you have full control over how you want to manage the workstations and servers when deploying patches.

Prism Patch Manager Resources

The following list highlights resources for learning about Prism Patch Manager and evaluating the product as a patch management solution for your environment.

Prism Patch Manager overview at

http://www.newboundary.com/products/prismpatch/prismpatch_info.htm

Feature list at http://www.newboundary.com/products/prismpatch/ppm_features.htm

Product support knowledge base at http://www.nbtnewboundary.com/support/docs/ppm/pm_chm.htm

User's guide (Adobe Acrobat format file) at

http://www.newboundary.com/rcenter/manuals/prismpatch6_1/pm_user_guide.pdf

Deployment guide (Adobe Acrobat format file) at

http://www.newboundary.com/rcenter/manuals/prismpatch6_1/pm_deploy_guide.pdf

General discussion support forum at

<http://www.nbtnewboundary.com/forum/messages.aspx?ForumID=9>

Tips and tricks support forum at <http://www.nbtnewboundary.com/forum/messages.aspx?ForumID=10>

Features request forum at <http://www.nbtnewboundary.com/forum/messages.aspx?ForumID=12>

Evaluation download at http://www.nbtnewboundary.com/download/prismpatch/ppm_download.aspx

Key Comparisons for SUS, SMS, and Prism Patch Manager

Based on the overview of the different types of patch management applications in the previous section, Table 3.1 gives a quick overview of the differences and key features.

Product	Key Features	Agent	Requirements	Support	Price
SUS and WUS	Free download from Microsoft; Works with the Windows Update client included on the Windows OS	Yes—built-in to Windows	Win2K, WS2K3, or Windows XP	Only security and security-rollup patches, critical updates, and service packs for the supported OSs	Free download, but need an adequate server (with proper licensing) to install it on
SMS 2003	Can deploy any piece of software in addition to patches; has reporting features built-in	Yes—utilizes the SMS client, which must be installed before patches can be distributed	NT 4.0, Win2K, WS2K3, Windows XP, or Windows 98	All patches, service packs, and updates for the supported OSs; also supports patch, update, and application installations for Microsoft and other applications	See product Web site for pricing and licensing information
Prism Patch Manager	Support for non-OS systems, including legacy and third-party applications; automatic notification of patch availability; and more	Both agented and agentless	NT 4.0, Win2K, WS2K3, or Windows XP	Support for non-OS systems, including legacy and third-party applications*	See product Web site for pricing and licensing information

Table 3.1: SUS, SMS, and Prism Patch Manager comparison.

* Additionally, Prism Patch Manager is a superset of SUS and WUS. It supports everything SUS/WUS supports and it contains support back to NT and the following applications: Exchange Server, SQL Server, IIS, MDAC, Office, ISA, and XML Web Services. PPM also supports non-OS systems, including legacy and third-party applications.

Table 3.2 provides additional patch management applications and information on where you can find more information.

Patch Management Application	Information
Altiris patch management solution	http://www.altiris.com
Authentium PatchMatrix	http://www.authentium.com/
BigFix Enterprise Suite	http://www.bigfix.com/
ConfigureSoft Security Update Manager	http://www.configuresoft.com/
Ecora Patch Manager	http://www.ecora.com/ecora/
Gravity Storm Software Service Pack Manager 2000	http://www.securitybastion.com/
LanDesk Patch Manager	http://www.landesk.com/
ManageSoft Security Patch Management	http://www.managesoft.com
Quest Software Patch Management for Microsoft	http://wm.quest.com/
Shavlik Technologies HfNetChk Pro	http://www.shavlik.com/
St. Bernard Software UpdateEXPERT	http://www.stbernard.com/
PatchLink Update	http://www.patchlink.com/

Table 3.2: Patch management solutions.

Example of Using a Patch Tool

To better understand how a patch management application will work within your patch management processes, this section will describe the steps to deploy patches to your computers using an example tool that lets you easily discover and research updates (see Figure 3.1).

The screenshot displays the Prism Patch Manager application. The main window is titled "Research Mode" and shows a list of updates with columns for Name, KB Article, Description, Release Date, Install Date, Platform, and Language. The selected update is "MS02-012 Malformed Data Transfer Request May Cause the Windows SMTP Service to Stop Working". Below the list, a detailed view of the Microsoft Knowledge Base article is shown, including the title "MS02-012: A Malformed Data Transfer Request May Cause the Windows SMTP Service to Stop Working" and a "Comments?" section.

Figure 3.1: Viewing and researching updates using a third-party patch management tool.

This tool enables you to sort the information in the research pane by column. To see the article associated with a given update, click the update. The associated article will be displayed in the browser pane below.

Next, you want to download the available new updates. Perform the following steps to download updates. In the network pane, select a machine running the OS and service pack for which you want to download an update. With a machine selected in the network pane, all of the applicable updates are listed in the machine/update pane. Select the update(s) you want to download by clicking them:

- To select multiple updates, hold down the Ctrl key while selecting each update.
- To select a series of adjacent updates, click the first in the series, hold down the Shift key, and click the last one in the series.

Download the selected updates by doing one of the following:

- Open the Deployment menu, and select Download from the menu
- Right-click a selected update, and select Download from the menu (as Figure 3.2 shows)

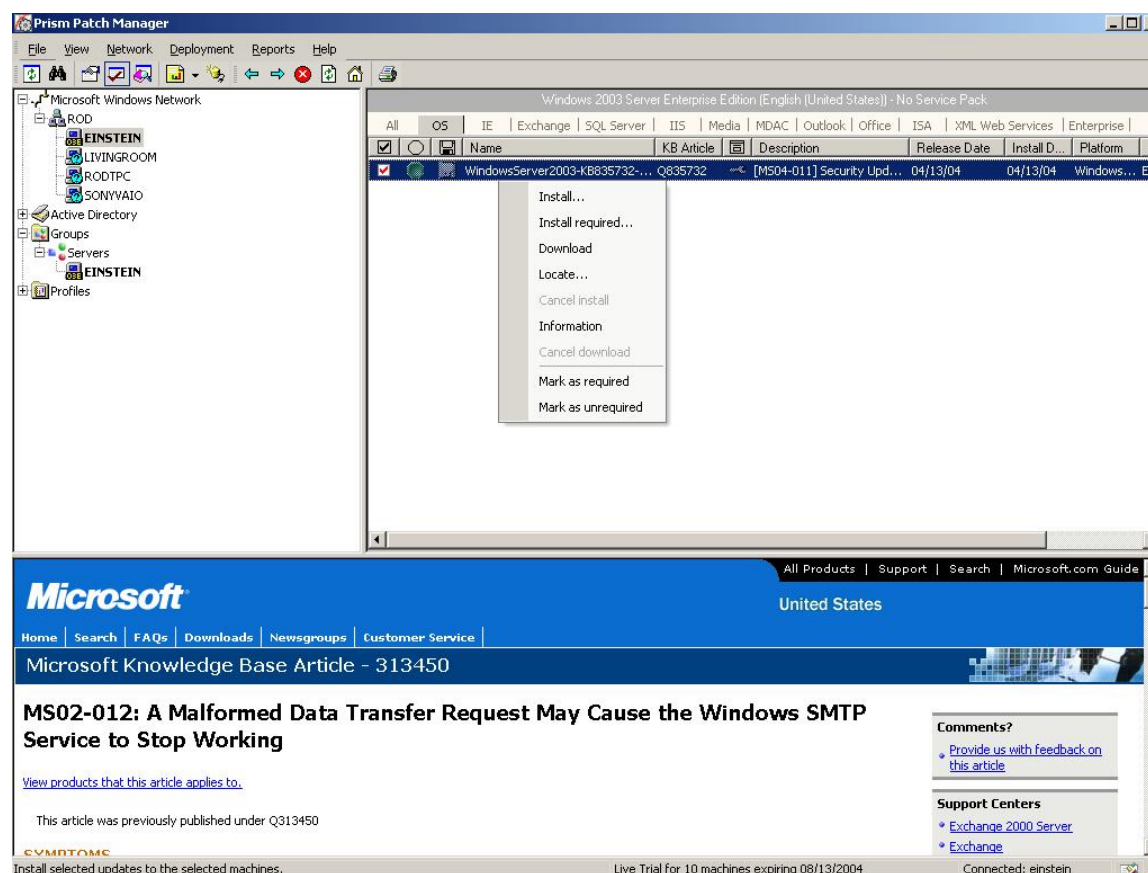


Figure 3.2: Downloading updates.

The file(s) are downloaded immediately. This particular tool indicates that an update is being downloaded by using a blue diskette with a red arrow icon. When the download of an update is complete, the download status icon is a blue diskette.

Next, you want to install (or deploy) the updates. Updates are deployed with this tool by using the machine/update pane. To start, select the machines in the network pane to which you want to install updates. After the machine(s) is selected, the applicable patches will be displayed in the machine/updates pane to the right. Identify the updates you want to install, and select them. Doing so will bring up the Installation wizard that will help you through the rest of the installation.

In the network pane, select the machines onto which you want to install an update. With one or more machines selected in the network pane, all of the applicable updates are listed in the machine/update pane. Select the update(s) you want to install by clicking on them. Install the selected updates by doing one of the following:

- Open the Deployment menu, and select Install from the menu
- Right-click any highlighted update, and select Install from the menu (as Figure 3.3 shows)

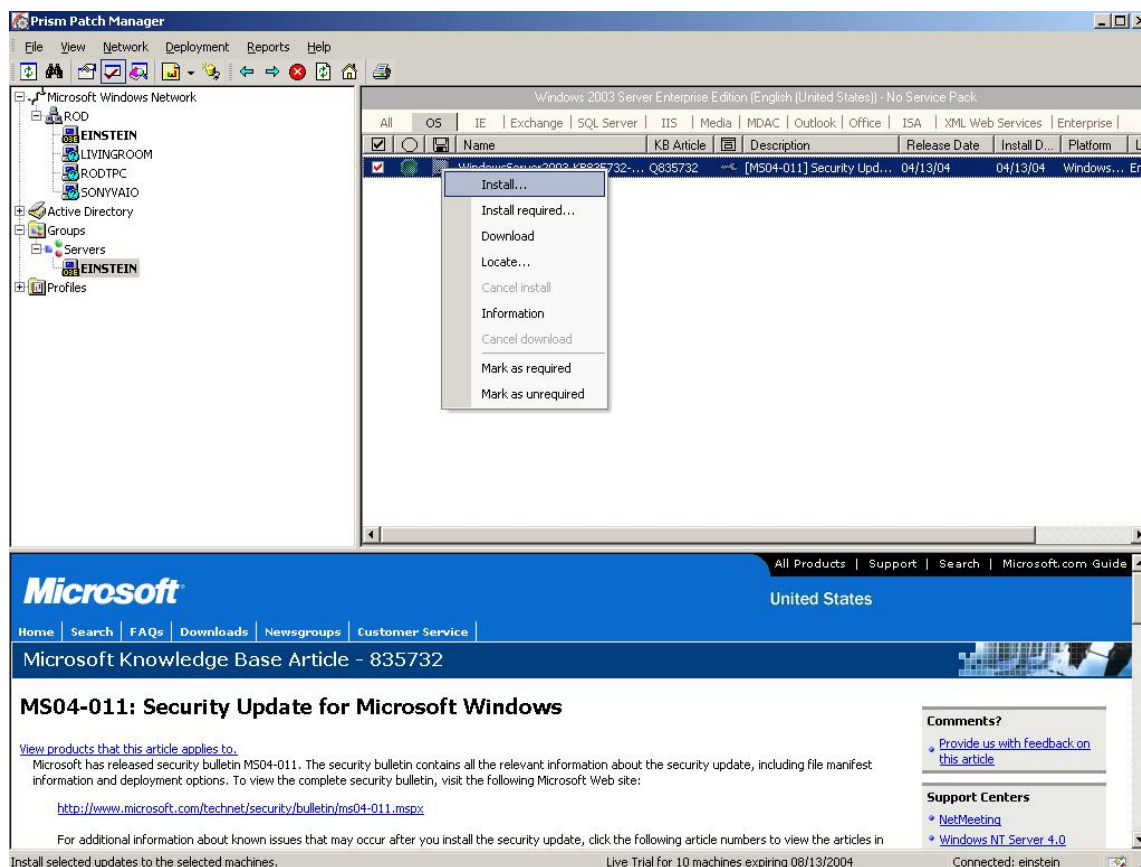


Figure 3.3: Installing updates.

This tool displays an Install Updates dialog box that shows the machines and the updates that you selected. In the Install Updates dialog box, select the desired installation options (as Figure 3.4 shows).

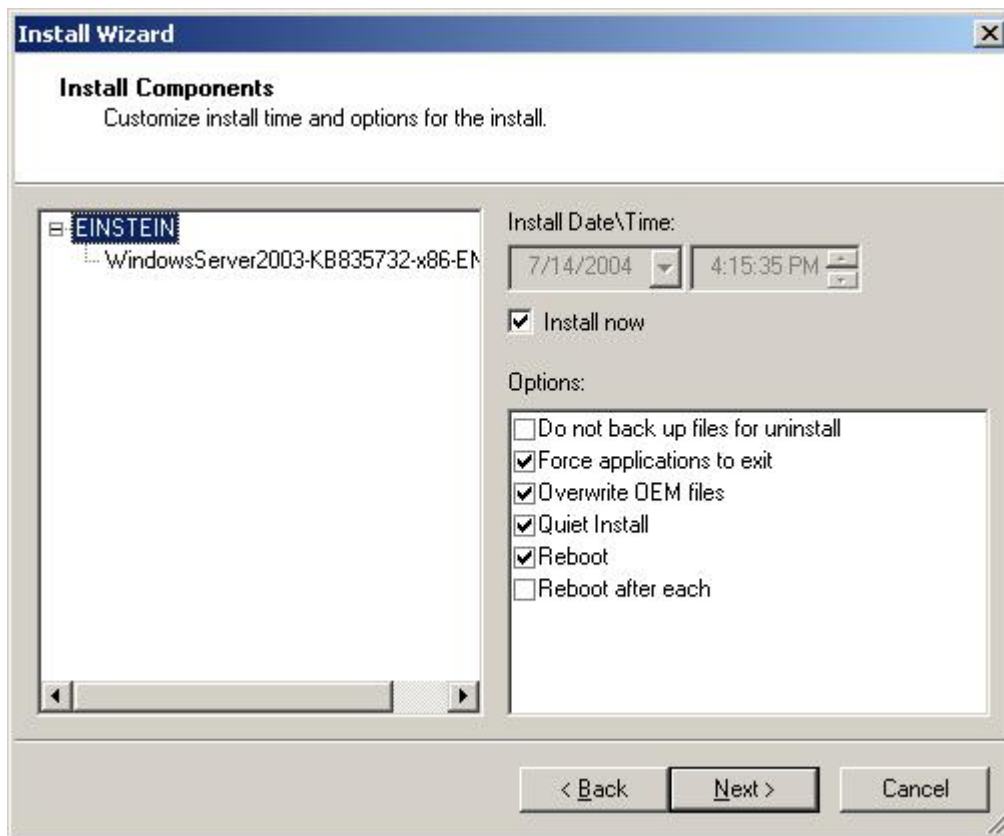


Figure 3.4: Selecting the update installation options.

These options may be different for each type of update; however, some general options that may apply to all include:

- Use the Install Date\Time field to schedule the date and time that you want the installation to commence. To change the date, select the down arrow in the field, and click the desired install date. To change the time, click the time and edit the hour and minutes individually by typing in a new value. This field is unavailable if the *Install Now* check box is selected.
- Select the *Install Now* check box to perform the installation immediately upon clicking Done.
- Select the *Do not backup files for uninstall* check box to skip saving files for a subsequent uninstall of the update.
- Select the *Force Applications to Exit* check box if you want the system to close any running applications prior to a reboot.
- Select the *Overwrite OEM Files* check box (generally for service packs) to automatically overwrite the OEM-supplied file regardless of the version in the supplied file.

- Select the *Quiet Install* check box if you want the installation to proceed with no indications on the remote machines that an installation is taking place.
- Select the *Reboot* check box if you want the target systems to automatically reboot when the install has completed.
- If you are installing more than one hotfix, select the *Reboot after each* check box if you want the machine(s) to reboot after each hotfix. This tool analyzes the set of updates that is being installed and eliminates unnecessary reboots between the installation of each update.

Click Finish. When the installation finishes, you can view the status by looking in the machine/update pane. If a green button displays in the second column, the update is installed. If a clock icon displays, the install is scheduled but has not yet completed.

Patch Management Resources

If you are looking for third-party resources for communicating issues and interacting with other individuals working with patch management products and solutions, check out the following resources:

myITforum.com at <http://myITforum.techtarget.com>

PatchManagement.org at <http://www.patchmanagement.org>

PatchTalk at <http://www.patchtalk.com/>

SUSServer.com at <http://www.susserver.com>

UpdateTalk at <http://www.updatetalk.com/>

Summary

Selecting a patch management application is a tough decision. You not only need to determine the application that you will implement but also ensure that the application will fit into your environment and your patch management processes. This chapter describes the requirements on which to base your patch management application selection, talks about the types of patch management applications, and gives you a jump-start for understanding the products available.

The ultimate goal of any patch management process is to secure the environment in the least number of steps possible. Picking the right product is crucial not only for creating a secure computing environment but also for building confidence in business management. The success of the product you choose will have far-reaching results on your career achievements.

This quick-start guide provides a roadmap for developing your patching strategies and gives you concise guidance for determining the “next-steps” in creating a process and policy that your company can rely on for years to come. Security through patching is a simple goal that requires diligence. Building a patch management process, developing a policy that becomes a company standard, and choosing the right technologies to purvey a vision is a career-building event. Let the prescriptions in this guide ensure that you are successful.