Novell.

Novell® ZENworks® Patch Management

Powered by PatchLink Corporation

V6.0 Administration Guide

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451

http://www.novell.com

1. Patch Management Server Overview

The Patch Management Server provides a complete solution for proactive reporting, patching and updating of your network. The product includes:

- A subscription service that keeps your Patch Management Server up to date with the latest available vulnerability reports (fingerprints and signatures) and their corresponding patch files (bundled into packages).
- Using the Detection Agents throughout your network, Patch Management Server will quickly give you a detailed analysis of these fingerprints and signatures. You will quickly be able to determine the patch status of your computers.
- Based on the results of the analysis, you can easily create deployments of the report's Packages to the computers that need them. Deployments are carried out by the Deployment Agents.
- With this extensive detection mechanism, a comprehensive Inventory system is also available. You will be able to detect what operating systems, software, hardware, device drivers and services are installed on your computers.
- The Patch Management Server features a new enterprise-wide agent distribution mechanism called the **Agent Management Center**. Through the use of Deployment (Client) Agents, Package Editor, and the Agent Management Center, you can securely send software, documentation, scripts (SW, HW and Services) or any other content across your network; from small Intranets to huge Extranets, or even the Internet itself.
- **System Groups** can now be manually or automatically created according to the criteria that you establish whether by Active Directory Organizational Units (OU's), NT or Active Directory Domains, LDAP OU's, IP address ranges or geographical regions as well as the default operating system groups. With this feature, you may:
    - View the analysis of the vulnerability reports (fingerprints and signatures) based solely on the group membership.
    - View the **Inventory** based on the group membership.
    - **Deploy** patch files (or any other packages) to the entire group. The group's membership can be changed at the start of the deployment to allow the administrator complete versatility in deploying patches. After the deployment is initiated, the members of the group are given the patch packages as their agents check-in with the Patch Management Server.
    - **Lock** a group for a set of vulnerability reports, software inventory, hardware inventory, or service inventory.
    - Set a **Mandatory Baseline** for a group, so that if the compliancy analysis of vulnerability reports for a group member results in not being patched, the computer will automatically have the vulnerability's patch file deployed to it.
    - Customize the group's computer member's behavior based on the group's **Agent Policy Set** (Agent Polling Interval and Hours of Operation). An easy mechanism to allow a group's computer members to act in a specific way while not affecting the other computers registered to the system.

- The Patch Management Server contains a complete role-based security layer. A role determines what rights a user has to perform Patch Management Server functionality to the computers and groups of computers the role is assigned to. The Server contains 4 role templates to assist Administrators in designing security for the many users of your Patch Management Server System.
- The Patch Management Server provides multi-platform support for the following operating systems:

Vendor	Operating System Platform	Deployment Agent	Detection Agent
Apple	MAC OS X	X	X
IBM	AIX 5.1	X	X
Microsoft	Windows Server 2003, Web Edition	X	X
Microsoft	Windows Server 2003, Standard Edition	X	X
Microsoft	Windows Server 2003, Enterprise Edition	X	X
Microsoft	Windows Server 2003, Datacenter Edition	X	X
Microsoft	Windows XP Professional	X	X
Microsoft	Windows XP Home (Personal)	X	X
Microsoft	Windows 2000 Datacenter Server	X	X
Microsoft	Windows 2000 Advanced Server	X	X
Microsoft	Windows 2000 Server	X	X
Microsoft	Windows 2000 Professional	X	X
Microsoft	Windows NT Server 4.0, Datacenter Edition	X	X
Microsoft	Windows NT Server 4.0, Terminal Server Edition	X	X
Microsoft	Windows NT Server 4.0, Enterprise Edition	X	X
Microsoft	Windows NT Server 4.0	X	X
Microsoft	Windows NT Workstation 4.0	X	X
Microsoft	Windows ME	X	X
Microsoft	Windows 98 SE	X	X
Microsoft	Windows 98	X	X
Microsoft	Windows 95 OSR2.5	X	X
Microsoft	Windows 95 OSR2	X	X
Microsoft	Windows 95	X	X
Novell	NetWare 4.11	X	X
Novell	NetWare 4.2	X	X
Novell	Netware 5.0	X	X
Novell	NetWare 5.1	X	X
Novell	NetWare 6.0	X	X
Red Hat	Red Hat Linux 6.2	X	X
Red Hat	Red Hat Linux 7.0	X	X
Red Hat	Red Hat Linux 7.1	X	X
Red Hat	Red Hat Linux 7.2	X	X
Red Hat	Red Hat Linux 7.3	X	X
Red Hat	Red Hat Linux 8.0	X	X
Red Hat	Red Hat Linux 9.0	X	X
Sun	Solaris 2.6	X	X
Sun	Solaris 7	X	X
Sun	Solaris 8	X	X
Sun	Solaris 9	X	X

2. What's New in ZENworks Patch Management Version 6.0?

Novell® ZENworks® Patch Management 6.0, powered by PatchLink Corporation, brings an already superior patch and configuration management product to a level unsurpassed by any other solution on the market today. Many improvements and features have been added made to make ZENworks Patch Management easier to use and in the world of patch management, easier is better! The new Agent Management Center makes deploying the computer agents seamless and versatile with complete integration with Microsoft's Active Directory and LDAP directory services.

Several improvements have been made to better inform the administrator as to the status of deployments. There is also a great deal more flexibility as far as the creation of administrative computer groups is concerned. Here is a list of the major changes made in ZENworks Patch Management to make the job of patch and configuration management more versatile and easy.

Agent Management Center (See Section 3.6 for more details)

Enterprise Computer Discovery

The Agent Management Center allows the patch administrator to automatically discover computers within a specified IP address range, NT or Active Directory domain, LDAP Organizational Unit. The results of the discovery will tell the user whether the computer has the agent installed or not and allow installation on computers that do not have an Patch Management Agent running.

Application Programming Interface

A new Application Programming Interface (API) to allow the user to query the SQL database. This will provide the user with the ability to check what the status of any computer is at any particular moment.

Improved Patch Deployment

Chainable Deployments

Chainable deployments allow the administrator to define a group of patch reports to be deployed to a group of computers (many-to-many) without the need to reboot the computers after every patch. This cuts down on the number of reboots that need to be performed, thus increasing computer availability.

Better User Information

Better Search Features

The **Reports** page and all the other top level pages have increased searching functionality. For instance, on the **Reports** page, you can now search via report name/CVE number, the vulnerability status, the report impact, as well as the original group search.

Status Page

The Patch Management Server **Status** page gives users a set of comprehensive indicators on what the Server is currently doing or scheduled to do. This includes all deployments in the queue for any given period of time, status of the Discover Applicable Updates process (DAU) and a better indication as to the status of the Server subscription replication between the Subscription Host Server and the Patch Management Server.

Status Window

Patch Management Server now provides detailed agent deployment status logging allowing each sub-transaction to be logged and displayed back on the Patch Management Server.

Smarter Agents

Smarter Client Agent

The client agent now triggers the Patch Management Server to reschedule the DAU process for that particular computer anytime an end user installs any hardware or software thus giving an immediate update to Patch Management Server as to the vulnerabilities of the computer.

Smarter Discovery Agent

A new agent policy setting allows the user to run the DAU at variable speeds enabling better control of network bandwidth utilization.

Windows 2003 Server Support

True Windows 2003 Server support is provided for Web, Standard and Enterprise versions.

Note: Windows 2003 Web version supports a limited number of agents due to MSDE limitations.

3. Getting Started

Using This Guide

Use this guide as a reference to describe Patch Management Server as in what it is, what it does, and how to do it. It is best to follow this guide sequentially as you begin using Patch Management Server, as certain sections pertain to and reference others that are documented later in the manual.

Most screenshots contained in this guide were taken using Windows XP operating system set with the default (blue) color scheme. The color schemes, buttons, and other items may vary slightly on your operating environment depending on what operating system you are running and your selected theme.

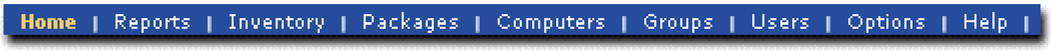
Understanding the Interface

Contained in each section of Patch Management Server, as illustrated by this document, are certain page functions and features designed either to aid the user's tasks, or to simply enhance other functions. Certain pages contain specific functions and features and these various functions and features may or may not be present depending on what page you are on. Note the **Page Functions** heading in each section to view which features are present. The standard page functions and features are broken down as follows:

Help

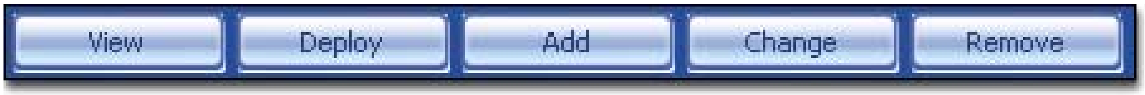
The Patch Management Server is a very comprehensive, web-based interface, designed to provide ZENworks® Patch Management users the information for what they need in a timely manner to properly patch and manage your network. It assists new users in learning the product, yet keeping all of the core functionality available for advanced users. Throughout Patch Management Server, context sensitive help is provided by clicking on the **Help** located in the top menu or the ? icon found on the top of every wizard and property page. Many of the user interfaces have fields that contain additional information that is displayed when your mouse moves over one of those fields.

Navigation Menu



The user interface provides a consistent and easy to use navigation menu, which is always present across the top portion of the screen. This navigation menu quickly takes you to the various major sections of Patch Management Server, as well as providing secondary notification of what section you are currently in. This navigation menu will behave differently based on your defined access rights associated with your user role. A section's name will not highlight or take you to the section if you do not have access to that section.

Action Menu



A variety of context sensitive actions are always located along the bottom of the page. These buttons provide quick access to all the common actions available for each page.

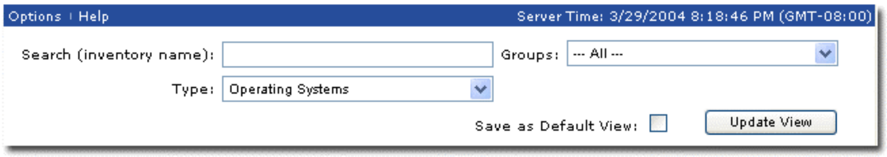
Like the navigation menu, the action menu functionality also depends on your user role (and its defined access rights) and the view you are working in (if a filter dropdown selection is applicable). If you do not have access to a button, the button will be grayed out and non-functional. Note the **Action Menu** heading in each section to view which actions are present.

Display and Hide

The display more information (⊞) and hide (⊟) information functions appear regularly throughout Patch Management Server. If the display and hide function is present on a certain page, it will be identified each section's **Page Functions**. Click on the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟, ⊞) is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

Starting with version 5.1, the filtering capability of Patch Management Server has been greatly enhanced. Now you can search, filter, and save results views as your default view for the next time you visit the page. This makes the job of finding what you are looking for much easier and less time consuming.
The advanced page search, filtering dropdown menus, and saving functions appear in various Patch Management Server pages.



Server Time: 3/29/2004 8:18:46 PM (GMT-08:00)

Search (inventory name):

Groups: --- All ---

Type: Operating Systems

Save as Default View: □

Depending on what page you are viewing determines your ability to search, filter, and save your viewable results.

For instance, you may search **Inventory** for more granular results by entering the computer name text into the **Search** field and clicking on the Update View Update View button. This will return the computer(s) having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Page search, filtering dropdown menus, and saving functionality varies depending on what page you are on. To understand the full advanced page search, filtering dropdown menus, and saving functions appearing on the Patch Management Server pages, see the respective **Page Functions** sections of this document where applicable.

Sort

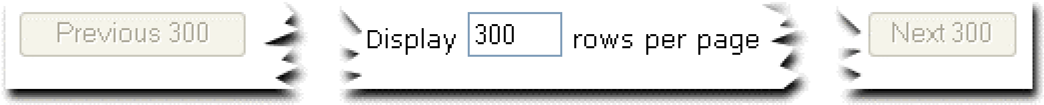
The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Display (Pagination)

Depending on the amount of items available for display and what page you are viewing, determines the display function. The Display function, if enabled, is located at the bottom above the Action Menu.



- Next: To display the next page of computers, click on the next button. If the last computer is displayed, the next button is disabled.
- Previous: To display the previous page of computers, click on the previous button. If the first computer is being displayed, the previous button is disabled.
- Computers per Page: The computer list initially displays up to 100 computers per page. To change the number of computers to display per page, enter a new number in to the Computers per Page input field. To display all computers enter a zero in the input field.

Auto Refresh

Where present and when selected, the Auto Refresh function automatically refreshes the page every 15 seconds.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Defining Access

Determining who gets access to Patch Management Server, what they can see, and what they can do is completely user-configurable. The goal of Patch Management Server Security is not to mandate how you define your security policies, but only to allow you the ability to institute your security policies effectively for Patch Management Server. Security access is determined by two mechanisms: Windows-based authentication and Patch Management Server access rights.

Windows-based Authentication

Authenticating to Patch Management Server is handled by the Windows operating system. Any user(s) who are members of a local Windows group, Patch Management Server Administrators, will gain all the necessary rights and abilities to log on to the web site. Authorization of what users can and can not do is handled by Access Rights (see below). Upon installation, the User (who is created during the installation) is given the Administrator user role, but you may remove this at any time, as long as there exists at least one user who belongs to the Administrator user role.

Patch Management Server Access Rights

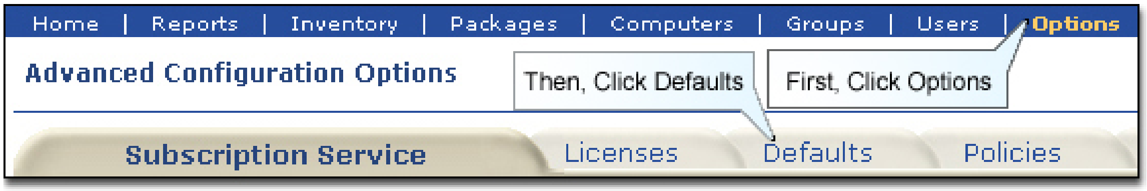
Once a user has authenticated into Patch Management Server, their assigned user role is checked to see what features (sections of Patch Management Server) and functionality (actions they can perform in those sections) they have. Each user role is assigned its own set of groups and computers (computers outside of the membership of the assigned groups) on which their access right-based functionality operates. If a user manages to get past the Windows security (Domain User who is not a member of the local Patch Management Server Administrators group for example), they will be unable to view any sections of Patch Management Server, see any groups or computers or perform any actions on them. If a user does not have access to a given section, they will be given an access denied error message.

In the Users Section, the Roles tab is where these roles are defined, while the Users tab is where you can add or remove users to Patch Management Server and assign them a user role.

Agent Behavior – Defining Your Policies

Before getting into the installation of agents on to the client computers of your network, the behavior of how those agents will act needs to be defined. At installation, the only single mechanism that defines this is found in the **Options** section, under the **Defaults** page.

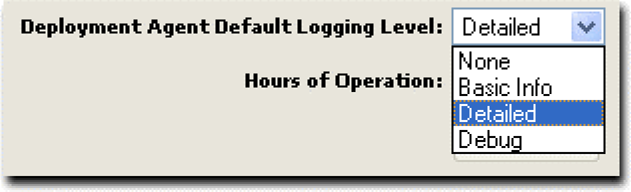
Since all of the groups are installed using the **Empty Agent Policy Set**, this is the single place that will affect your agent's behavior.


Home | Reports | Inventory | Packages | Computers | Groups | Users | Options
Advanced Configuration Options
Then, Click Defaults
First, Click Options
Subscription Service
Licenses
Defaults
Policies

There are only four individual items that make up an agent's behavior and they are all easily configurable from this page. Of the four items, three can be overridden by a group's **Agent Policy Set.**

Logging Level

Determines how much data you want your agents to save to their log files. The four options are:



Deployment Agent Default Logging Level: Detailed

Hours of Operation:

- None: only errors are logged.
- Basic Info*:* errors and the very basic information is saved. Example: when it is performing a deployment it will indicate that it had a deployment to do.
- Detailed: errors and more explanation of what the agent is doing is saved. Example: deployments, including what they deployments are, and when agent policies are changed, including what they are, are logged.
- Debug: log everything and every step the agent does. This should only be used when you are validating the agent's behavior or its actions. This mode will generate megabytes worth of data on a busy system.

Note: The agent log files are deleted every time the Refresh Inventory Data System Task is deployed to an agent.

Communication Interval

Determines how much time the agent will sleep between communication with Patch Management Server. When it communicates with Patch Management Server it is checking to see if it has any policy updates or if it has any deployments to do. This interval is critical to Patch Management Server; if the interval is too high, the agents will not get their tasks in a reasonable amount of time. If the interval is too low, Patch Management Server (and your network traffic) will constantly be busy and other agents will not be able to get their tasks. Interval rates typically vary between 15 and 60 minutes depending upon number of nodes, network architecture and bandwidth.

Hours of Operation

When enabled, this value determines when the agents shall start and stop communicating with Patch Management Server. If the agent is in the middle of a deployment and the agent's hours of operation expire (exceeds the designated stop time) it will finish what it is currently working on and continue the rest of the deployment at the next Hours of Operation interval.

Concurrent Deployment Limit

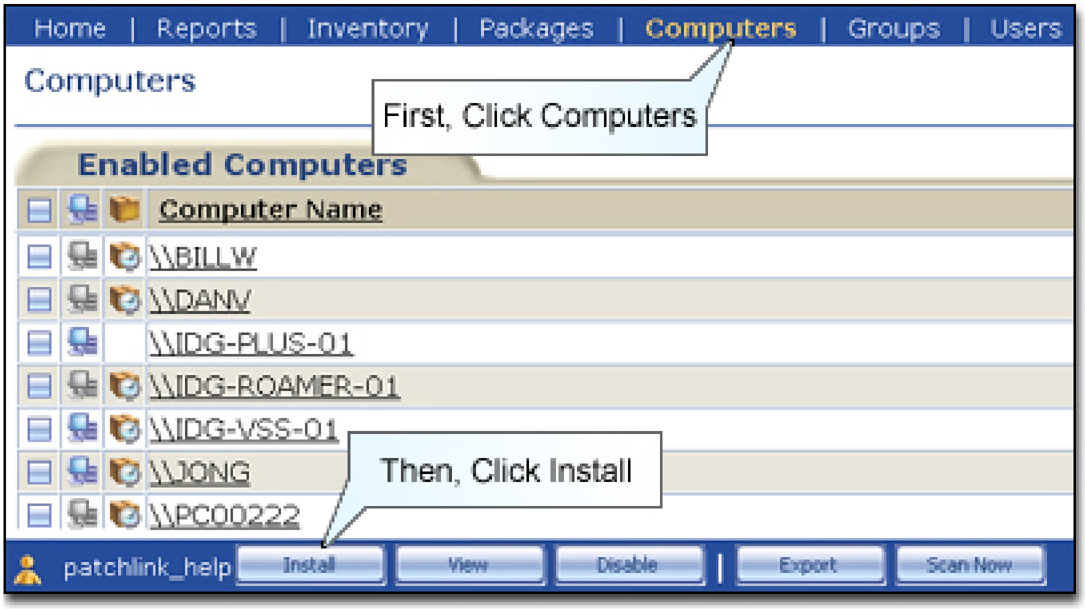
This value determines how many deployments can be given to the agents at any given time (if a deployment is scheduled for more than an hour for a particular agent, that deployment is no longer counted). This is a safeguard that will reduce the chance of any of your Patch Management Server' systems from being overloaded. This is the only value that cannot be overridden by a group's **Agent Policy Set** as it limits deployments for all agents.

Agents and Installing Them

Both the deployment (also known as **Deployment Agent**) and **Detection Agent** are bundled together and installed at the same time. The deployment agent is a service that is constantly running to ensure that when deployments are ready to start, policy changes, etc., the agent will act on them in a timely manner. The behavior of this agent is entirely defined by the agent's policies, whether the agent is using the default agent policies for Patch Management Server or the superset of the group's agent policy sets the agent is a member of. The detection agent will run only when the user on the individual computer initiates it, or the deployment agent deploys the **Discover Applicable Updates System Task**.

Installing agents is a simple function and there are various installers available to install agents on to your computers. They can be found by clicking on the **Add** button in the **Computers** section. This will initialize a screen showing the available Patch Management Agent Installers.

Note: If you cannot access the Computers section or do not have access for the Install button, speak with your Patch Management Server Administrator on obtaining access to those sections of the product.



The **Agent Installers** page displays the various installers you can use to register computers to Patch Management Server. For each agent installer, there is useful information you should read first to determine which one to use for which computers. Each agent installer is different from the operating systems it works under in pertinence to its requirements or behavior. Read each section carefully to determine the best options for your needs. If one does not work for a particular computer, check the others or access the Patch Management Server Forums to see if there is a better option available for you. Without the agents installed on your computers, you will not be able to determine what is patched and what is not patched, nor will you be able to deploy any patches.

The various agent installers are:

- Single Agent Installer for Windows (Win95 to Win2k3)
- **Single Agent Windows MSI Installer** (Win95 to Win2k3)
- Silent Agent Installer for Windows (Win95 to Win2k3)
- Domain-wide Agent Deployment Wizard for Windows (Win2k to Win2k3). Available computers are captured from the Primary Domain Controller.
- Single Agent Installer for UNIX (Solaris, Red Hat Linux)
- Single Agent Installer for NetWare (4.11 to 6)
- **PatchLink Distribution Point** - provides a quick and easy way to add remote package cache capabilities to any server computer within your wide area network. Based on the SQUID NT v2.5 open source based product, this software provides you with a turnkey content caching solution where none previously existed. It is recommended that PatchLink Distribution Point should be installed on server computers within your environment that are permanently connected to your network. Installing on a workstation is also possible, however since that workstation becomes a gateway for communication between agent computers and the Patch Management Server, it is a good idea to make sure that computer is permanently attached to the WAN and always live on the network. The default proxy port for PatchLink Distribution Point is 25253.

  Once a Distribution Point has been installed in a remote office, new agents at that location can be configured to communicate through the Distribution Point by specifying :25253 as the proxy value during agent installation. Proxy settings for existing agents can also be modified by launching the Novell® Patch Management control panel applet and pushing the "Proxy" button.

Once a computer has registered its agent against Patch Management Server, the Patch Management Server Administrator can assign it to various user roles so others can access or view it.

- See Section 10.4 for more detail on the PatchLink Distribution Point.

Agent Management Center (AMC)

The ZENworks® Patch Management Patch Management Server features a new enterprise-wide agent distribution mechanism called the **Agent Management Center (AMC)**. Through the use of Deployment (Client) Agents, Package Editor, and the Agent Management Center, you can securely send software, documentation, scripts (SW, HW and Services) or any other content across your network, from small Intranets to huge Extranets, or even the Internet itself.

The major features of the **AMC** allow you to perform network host discovery, install / uninstall Patch Management Server agents, and agent management functions including adding agents to groups or user roles, and removing agents from Patch Management Server if they have been offline for an extended period.

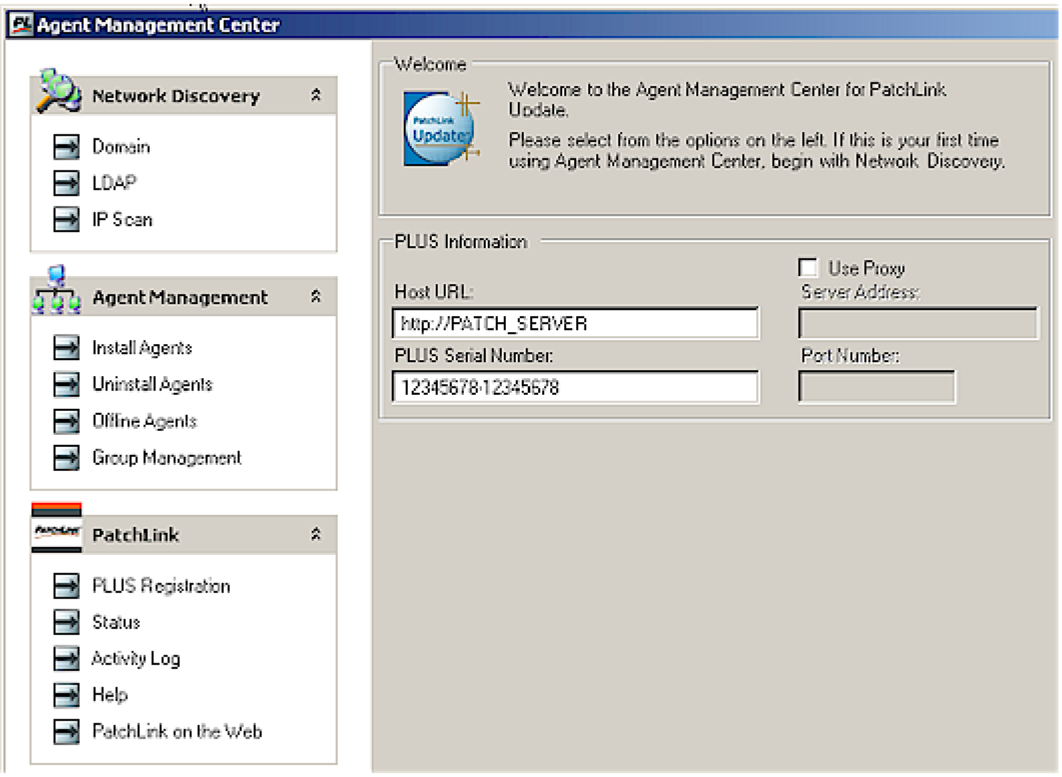
Enterprise Computer Discovery

The Agent Management Center allows the patch administrator to automatically discover computers within a specified IP address range, a Windows domain or an LDAP Organizational Unit. The results of the discovery will tell the user whether the computer has the agent installed or not and allow installation on computers that do not have a Patch Management Agent running.

Agent Installation

The AMC makes the task of agent installation easier by allowing users to selectively install the agent on a few or many computers that they choose at one time.

Agent Management Center Main Screen



Welcome to the Agent Management Center for PatchLink Update.

Please select from the options on the left. If this is your first time using Agent Management Center, begin with Network Discovery.

Host URL: http://PATCH_SERVER

PLUS Serial Number: 12345678-12345678

□ Use Proxy

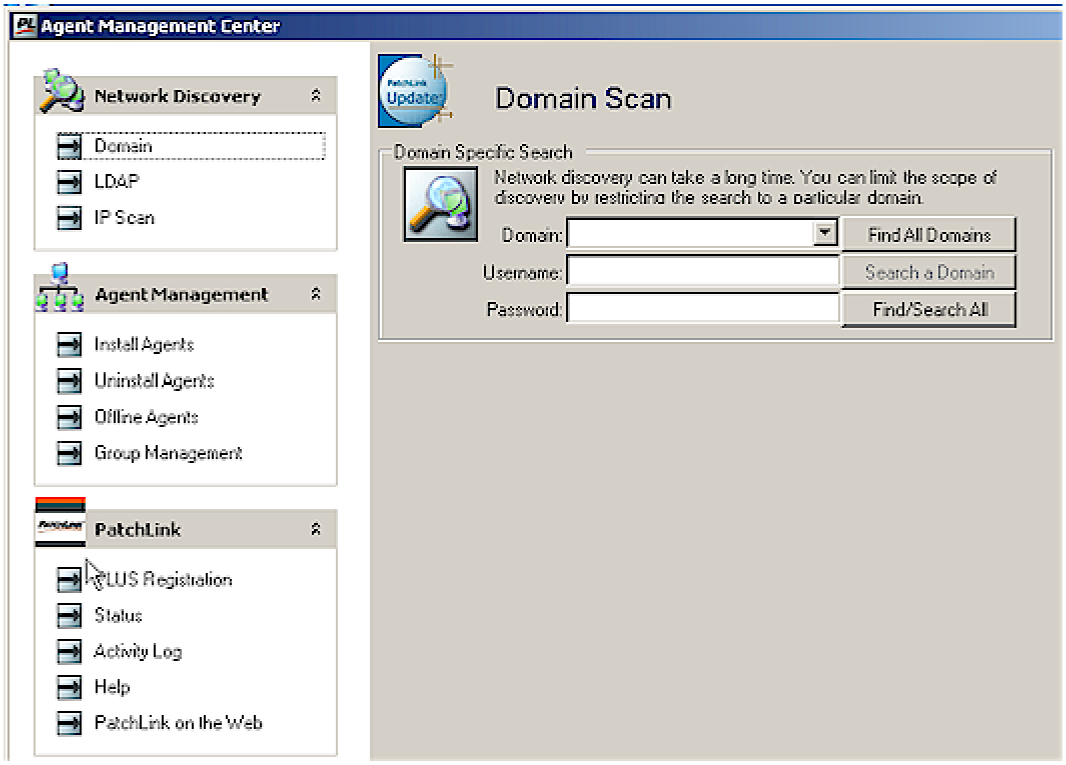
Server Address:

Port Number:

The Main Screen is the screen first displayed when deploying the AMC from the Windows/Programs menu. From this page you can choose to perform a network discovery, perform agent installation and management functions or access the Patch Management Server product registration page and other Patch Management Server functions. Information needed by the agents for use in the installation process is entered here. The Host URL for the Patch Management Server and its Patch Management Server Serial Number should be entered here before you deploy agents.

Network Discovery Section

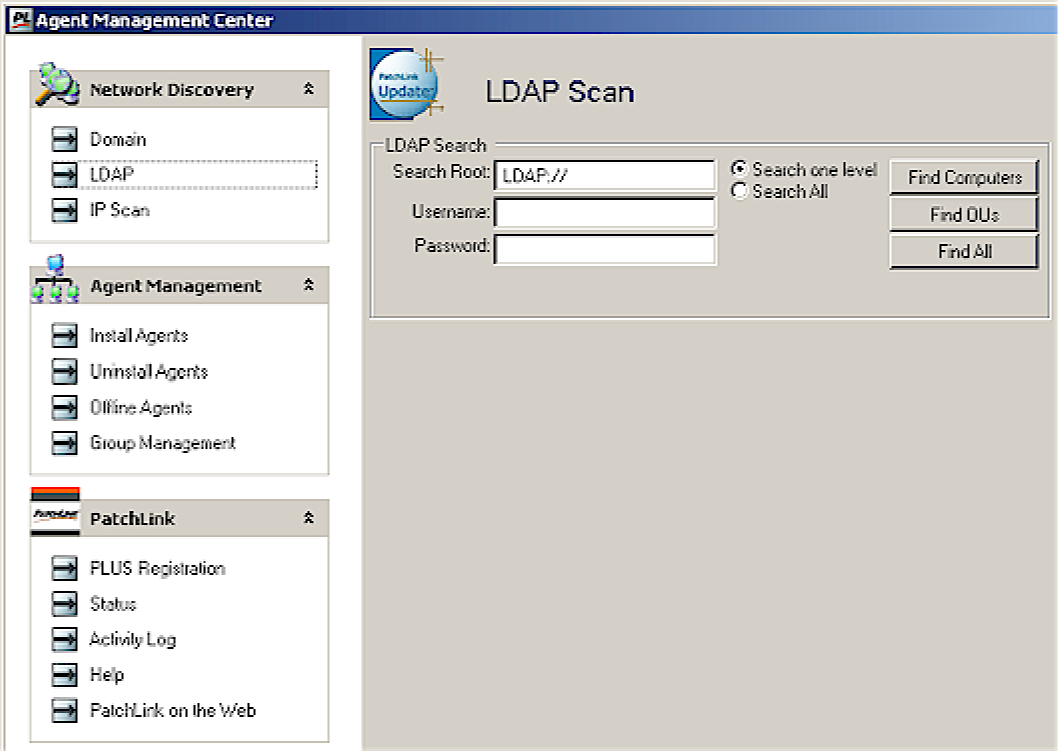
Domain Scan



Network discovery can take a long time. You can limit the scope of discovery by restricting the search to a particular domain.

The Domain Discovery screen allows you to perform a Domain Specific Search or a Search All Domains to discover all the computers in the domain. You simply enter the name of the domain in the Domain field or select the Find Domains pushbutton to find all the domains in your network.

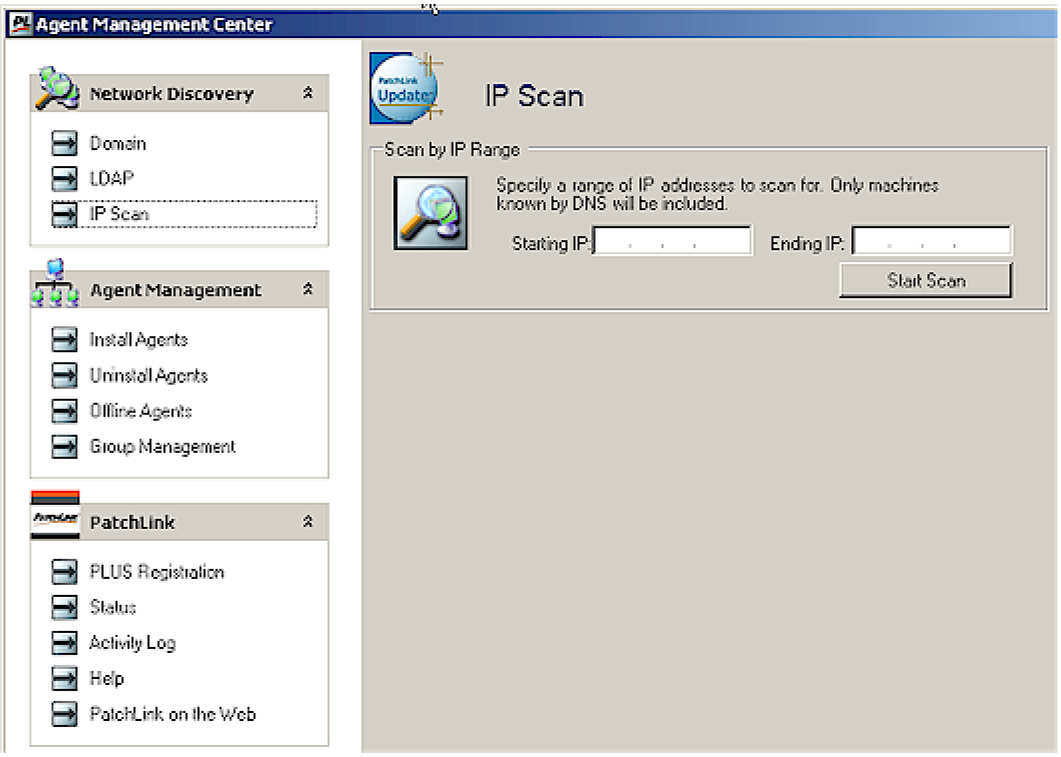
Active Directory Search and Discovery



Search Root: LDAP://
Username:
Password:
● Search one level
○ Search All

The Active Directory/LDAP Search and Discovery screen allows the user to search for computers within the directory tree from the root directory. The username and password for the Active Directory Administrator account can be entered in the corresponding fields but may not be necessary depending on your LDAP setup. All that is really needed is that your user permissions include read permission on the LDAP directory. From here you can select whether you want to only search one level or search all levels of the LDAP root. You can also choose to find computers, LDAP Organizational Units or find all the elements in the directory.

IP Address Search and Discovery



Specify a range of IP addresses to scan for. Only machines known by DNS will be included.

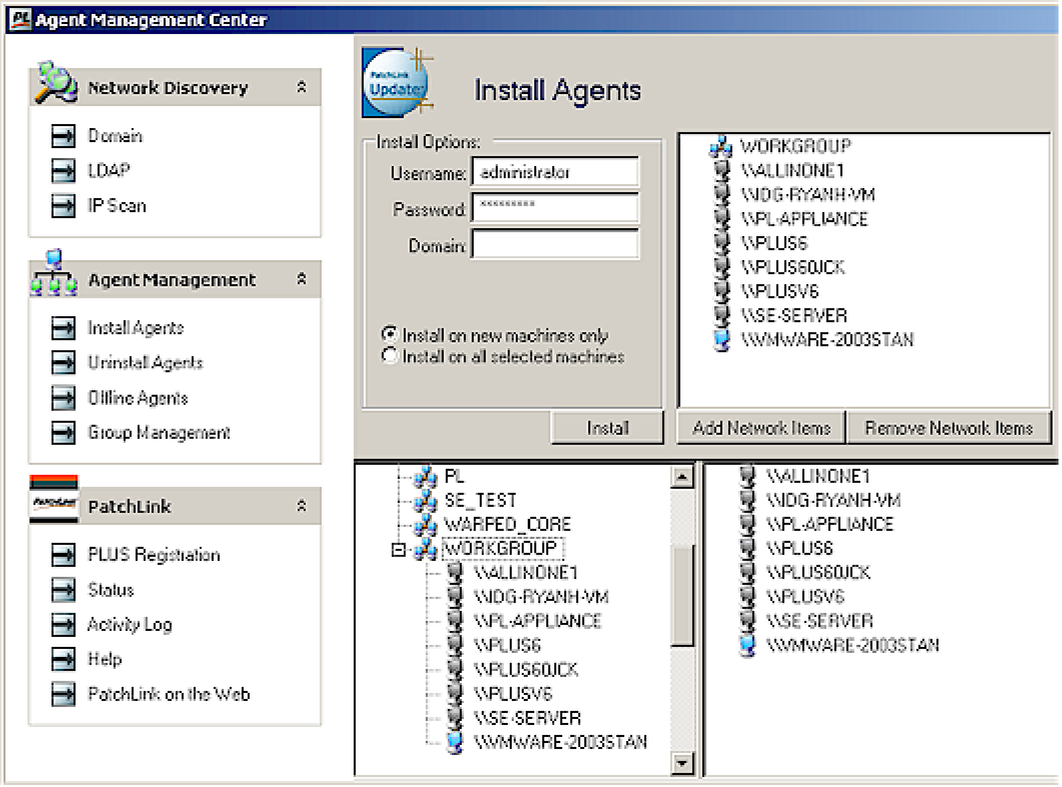
The IP Scan screen allows the user to search the network for computers by their IP addresses. The IP addresses must be registered within the Domain Name Service (DNS) of the DNS domain in order to obtain the computer name.

Enter the starting and ending IP addresses that you want to scan for and select the Start Scan pushbutton to begin your scan. Multiple ranges of IP address can be searched simultaneously.

Note: System Discovery using IP Scan will likely set off Intrusion Detection systems. Please be advised of this before you use this method in your environment and notify the appropriate security personal.

Agent Management Section

Installing Agents



Install Options:

Username: administrator

Password: *********

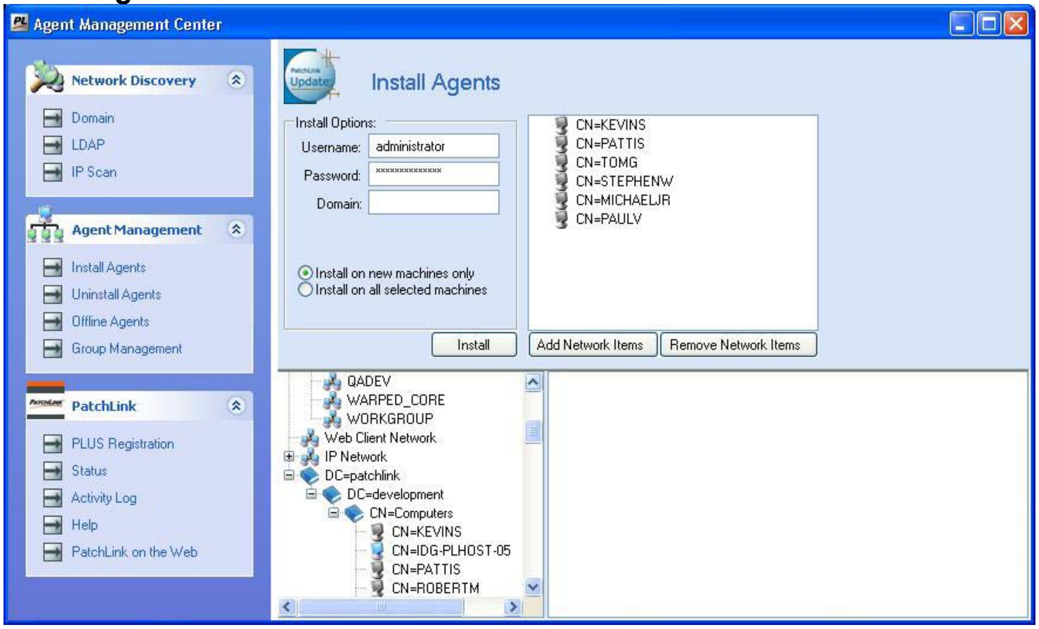
Domain:

● Install on new machines only
○ Install on all selected machines

The Install Agents screen is the place where you perform the agent install after you have discovered the computers on your network. The user entered in the Username field must have Administrator permissions in order to install the Patch Management Agent. You can choose whether you want to install on new computers only or reinstall on a previously discovered computer. You must also choose which install method for AMC to use. The recommended method of installation is using the WMI Install option but can only be used if the WMI service is running on the computer. If the WMI service is not running then you must use the Service install method.

You simply select from either of the lists below the Install pushbutton and click on the Add Network Items pushbutton to select the computers or domains you want to install the Patch Management Agent on. The computer icons that have a blue screen are computers that already have the agent installed. Computers that have a gray screen are computers that do not have the agent installed.

Installing to a Domain and an OU



Install Options:

Username: administrator

Password: **************

Domain:

● Install on new machines only
○ Install on all selected machines

CN=KEVINS
CN=PATTIS
CN=TOMG
CN=STEPHENW
CN=MICHAELJR
CN=PAULV

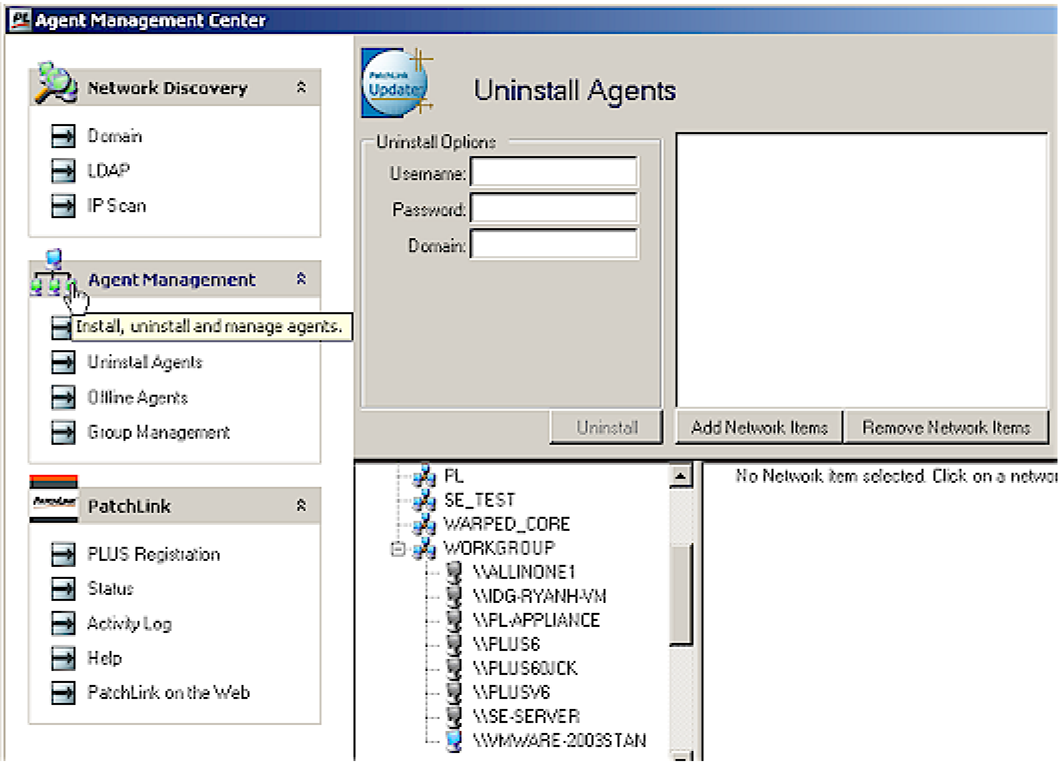
```
    QADEV
    WARPED_CORE
    WORKGROUP
  Web Client Network
⊞ IP Network
⊟ DC=patchlink
  ⊟ DC=development
    ⊟ CN=Computers
        CN=KEVINS
        CN=IDG-PLHOST-05
        CN=PATTIS
        CN=ROBERTM
```

Always start from a valid Search Root, for example…

- LDAP://development
- GC:

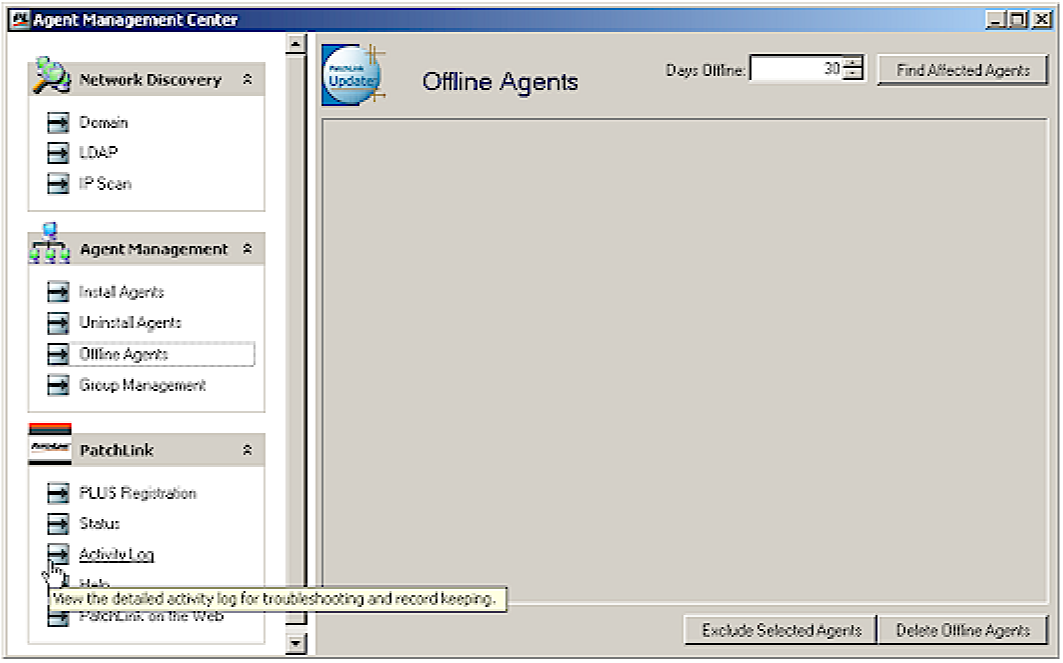
A password may or may not be needed here, depending on how security is setup in the local environment. Once a computer is found by any of the above methods, the Agent Management Center will build out the rest of the tree (parents, etc.).

Uninstalling Agents



The Uninstall Agents screen allows you to uninstall agents manually. Simply select the computer(s) that you want to uninstall from one of the two lists at the bottom, select the type of uninstall, being Standard or WMI and click the Uninstall pushbutton.

Offline Agents



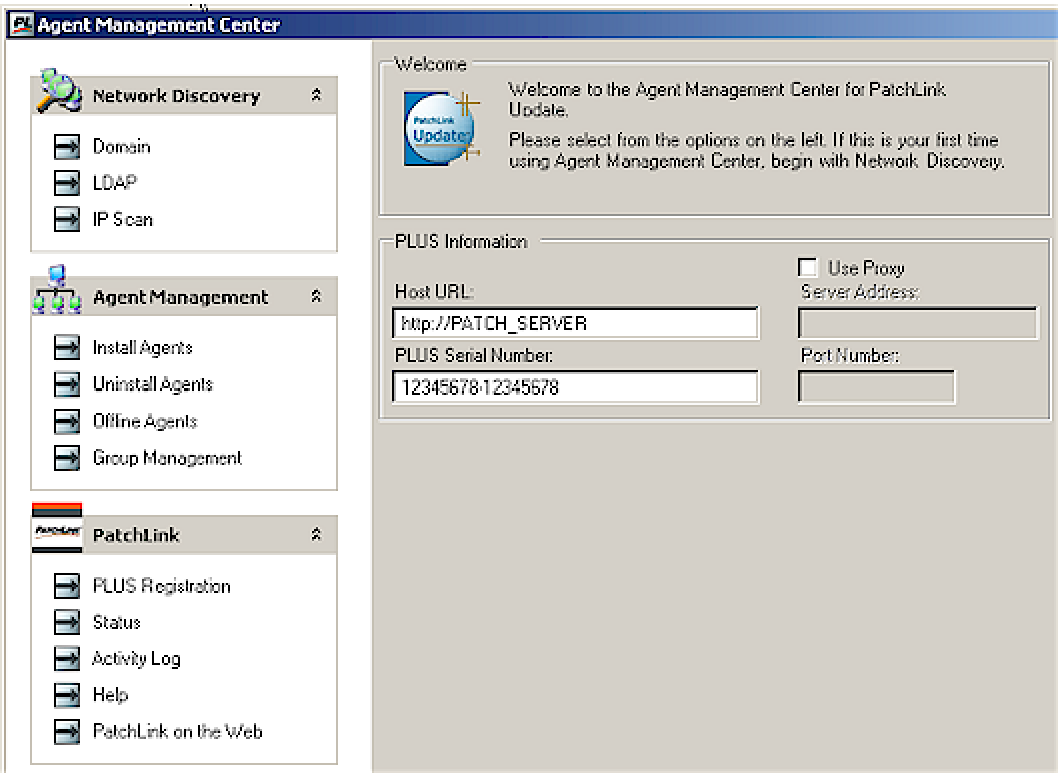
Days Offline: 30

View the detailed activity log for troubleshooting and record keeping.

The Offline Agents screen allows the patch administrator to flag computers that have not registered with the Patch Management Server for a specific number of days that is entered in the “Days offline” screen. Computers that have been offline for more that the number of days specified in the “Days offline” field will be displayed in the gray area below the “Days offline” field.

From there you simply select the computers that you want to exclude or delete and push the appropriate pushbutton.

PatchLink Section



Welcome to the Agent Management Center for PatchLink Update.

Please select from the options on the left. If this is your first time using Agent Management Center, begin with Network Discovery.

Host URL: http://PATCH_SERVER

PLUS Serial Number: 12345678-12345678

☐ Use Proxy

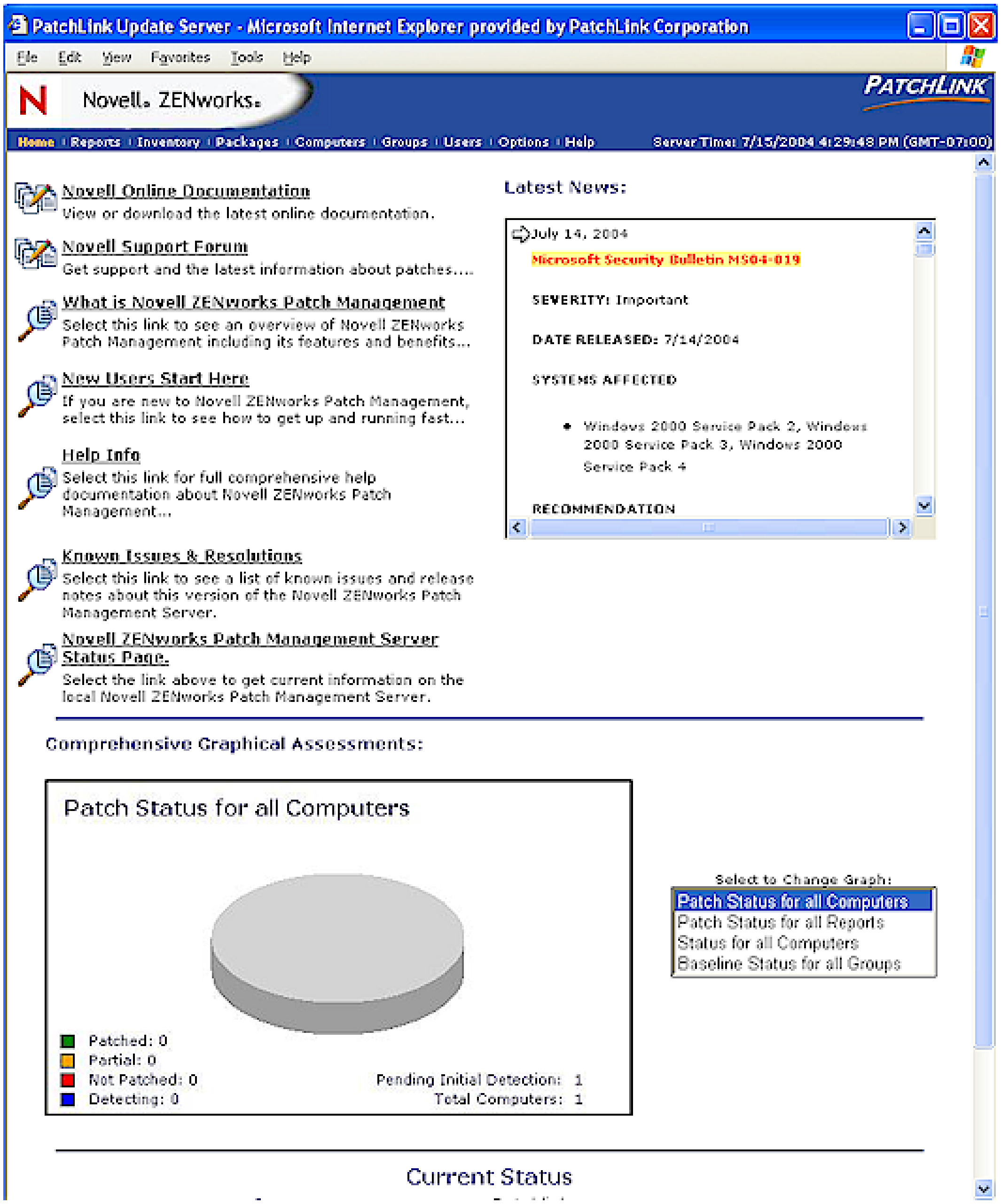
Server Address:

Port Number:

The PLUS Registration screen allows you to enter the Patch Management Server registration information needed to install agents and to access the online help pages for the AMC.

4. Patch Management Server Home Page

Novell® ZENworks® Patch Management solution gives you the ability to detect and patch your workstation and servers across your entire network. The **Home Page** gives you latest information and status about your Patch Management Server. If Patch Management Server licenses have expired, the License Expiration page will be displayed instead. From here you can access the Novell® Online Documentation, Support Forum, a Novell ZENworks Patch Management demo, New Users page, Help Files, Known Issues and Resolutions and the Patch Management Server Status Page.


PatchLink Update Server - Microsoft Internet Explorer provided by PatchLink Corporation
File Edit View Favorites Tools Help
Novell. ZENworks.
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help

Server Time: 7/15/2004 4:29:48 PM (GMT-07:00)

Novell Online Documentation
View or download the latest online documentation.

Novell Support Forum
Get support and the latest information about patches....

What is Novell ZENworks Patch Management
Select this link to see an overview of Novell ZENworks Patch Management including its features and benefits...

New Users Start Here
If you are new to Novell ZENworks Patch Management, select this link to see how to get up and running fast...

Help Info
Select this link for full comprehensive help documentation about Novell ZENworks Patch Management...

Known Issues & Resolutions
Select this link to see a list of known issues and release notes about this version of the Novell ZENworks Patch Management Server.

Novell ZENworks Patch Management Server Status Page.
Select the link above to get current information on the local Novell ZENworks Patch Management Server.

Latest News:

July 14, 2004
Microsoft Security Bulletin MS04-019

SEVERITY: Important

DATE RELEASED: 7/14/2004

SYSTEMS AFFECTED

- Windows 2000 Service Pack 2, Windows 2000 Service Pack 3, Windows 2000 Service Pack 4

RECOMMENDATION

Comprehensive Graphical Assessments:

Patch Status for all Computers

🟩 Patched: 0
🟧 Partial: 0
🟥 Not Patched: 0
🟦 Detecting: 0

Pending Initial Detection: 1
Total Computers: 1

Select to Change Graph:
Patch Status for all Computers
Patch Status for all Reports
Status for all Computers
Baseline Status for all Groups

Current Status

Novell Support Forum

The Novell Support Forum provides a location where the latest information and technical support about the Patch Management Server, its processes, functions and features are displayed. You can search through other customer questions and answers to see if their answers can assist you. Additionally, you can post your own questions and Novell Customer Service will assist you in a timely manner. Registered users can select to receive notifications when any of the different forum topics receives new activity. Select the **Novell Support Forum** link to open the Support Forum.

What is Novell® ZENworks® Patch Management?

What is Novell ZENworks Patch Management provides a detailed overview of the **Patch Management Server** system.

New Users Start Here

New User's Start Here displays a quick start user's guide to understanding the interface, defining access, agent behavior and their installation.

Help Info

Help Info provides comprehensive documentation on the Patch Management Server.

Known Issues & Resolutions

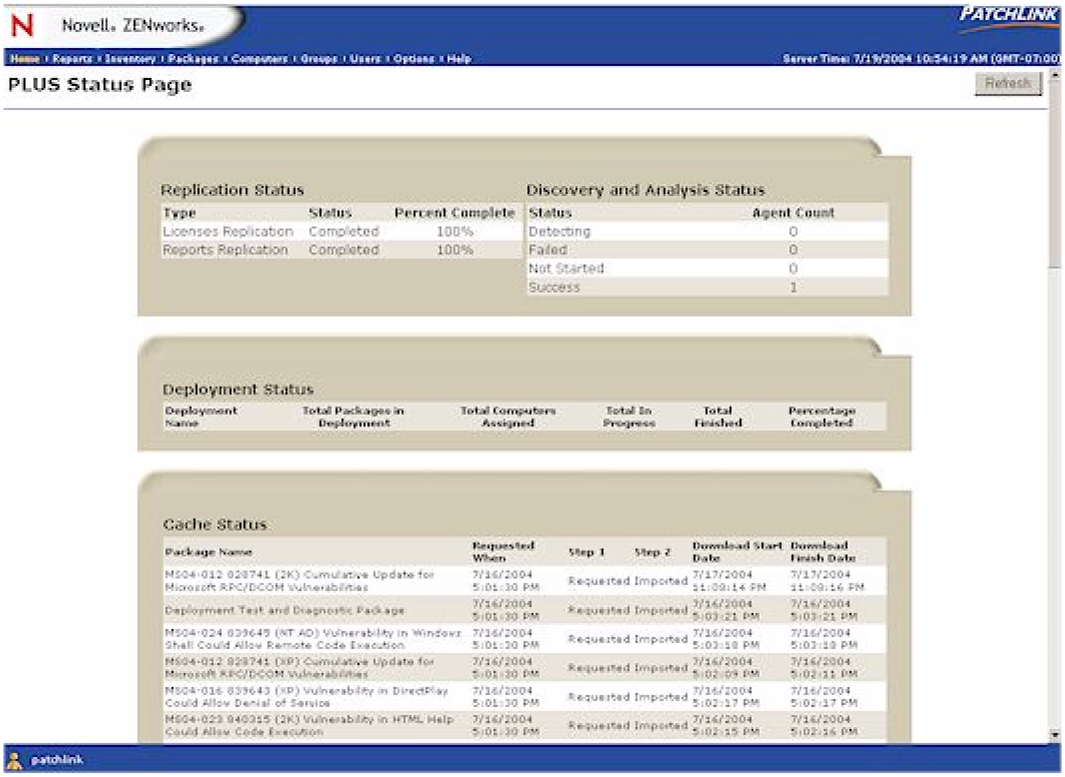
Known Issues displays a list of Known Issues, Release Notes, and Important Links about the Patch Management Server.

Patch Management Server Status Page

The Patch Management Server Status Page shows, at a glance, the **Replication Status** between the Patch Management Server and the main patch repository. The **Type** of replication, the **Status** of the replication, and the **Percent Complete** are displayed.

It also shows the current patch deployment **Discovery and Analysis Status**; showing whether a patch is being detected, has failed, has not started or was successful.

The **Deployment Status** portion of the page shows all deployment statuses so you can quickly check whether a package was deployed. Click on the **Deployment Name** link to view the computer's details.



Novell. ZENworks.
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Refresh
patchlink

Server Time: 7/19/2004 10:54:19 AM (GMT-07:00)

PLUS Status Page

Replication Status

Type	Status	Percent Complete
Licenses Replication	Completed	100%
Reports Replication	Completed	100%

Discovery and Analysis Status

Status	Agent Count
Detecting	0
Failed	0
Not Started	0
Success	1

Deployment Status

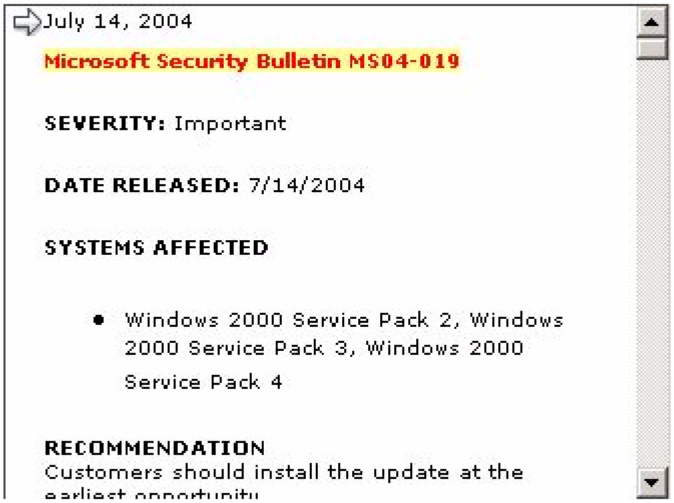
Deployment Name	Total Packages in Deployment	Total Computers Assigned	Total In Progress	Total Finished	Percentage Completed

Cache Status

Package Name	Requested When	Step 1	Step 2	Download Start Date	Download Finish Date
MS04-012 828741 (2K) Cumulative Update for Microsoft RPC/DCOM Vulnerabilities	7/16/2004 5:01:30 PM	Requested	Imported	7/17/2004 11:09:14 PM	7/17/2004 11:09:16 PM
Deployment Test and Diagnostic Package	7/16/2004 5:01:30 PM	Requested	Imported	7/16/2004 5:03:21 PM	7/16/2004 5:03:21 PM
MS04-024 839645 (NT AD) Vulnerability in Windows Shell Could Allow Remote Code Execution	7/16/2004 5:01:30 PM	Requested	Imported	7/16/2004 5:03:10 PM	7/16/2004 5:03:10 PM
MS04-012 828741 (XP) Cumulative Update for Microsoft RPC/DCOM Vulnerabilities	7/16/2004 5:01:30 PM	Requested	Imported	7/16/2004 5:02:09 PM	7/16/2004 5:02:11 PM
MS04-016 839643 (XP) Vulnerability in DirectPlay Could Allow Denial of Service	7/16/2004 5:01:30 PM	Requested	Imported	7/16/2004 5:02:17 PM	7/16/2004 5:02:17 PM
MS04-023 840315 (2K) Vulnerability in HTML Help Could Allow Code Execution	7/16/2004 5:01:30 PM	Requested	Imported	7/16/2004 5:02:15 PM	7/16/2004 5:02:16 PM

The **Cache Status** is a chronological detail of your packages downloaded into the Patch Management Server cache, including: Package Name, Requested When (Date and Time), Steps involved, Download Start Date (Date and Time), and Download Finish Date (Date and Time).

Latest News



July 14, 2004

Microsoft Security Bulletin MS04-019

SEVERITY: Important

DATE RELEASED: 7/14/2004

SYSTEMS AFFECTED

- Windows 2000 Service Pack 2, Windows 2000 Service Pack 3, Windows 2000 Service Pack 4

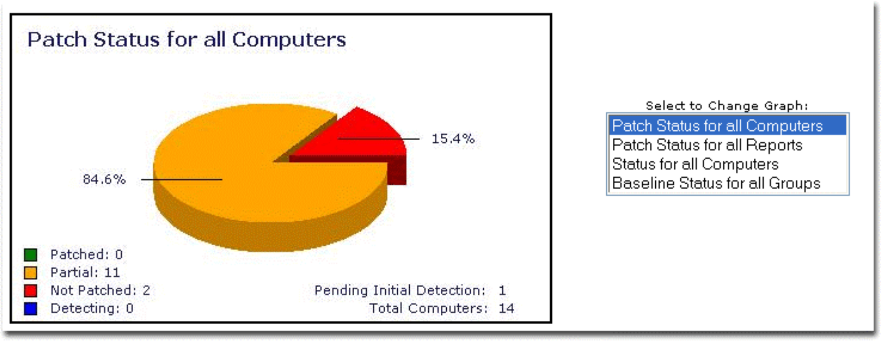
RECOMMENDATION
Customers should install the update at the earliest opportunity

This window displays the latest news, articles, announcements, and press releases from PatchLink Corporation.

Comprehensive Graphical Assessments

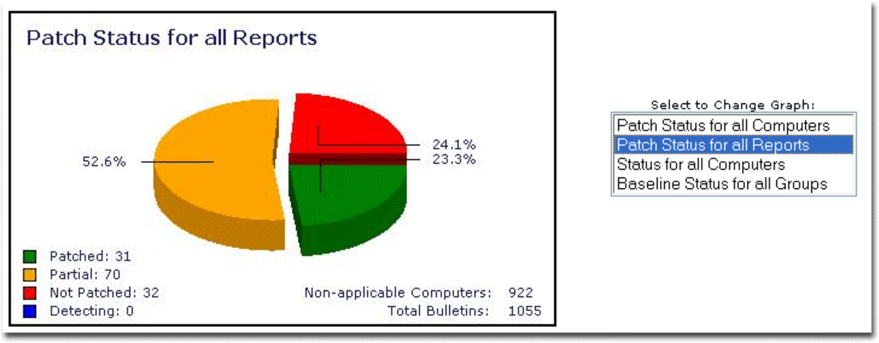
A pie chart graphical display illustrate various statuses of certain patch elements of the Patch Management Server. There are four different display views with different colors and percentages representing these various statuses. The displays are:

1. Patch Status for all Computers – displaying the status for all computers which are:


Patch Status for all Computers
15.4%
84.6%
🟩 Patched: 0
🟧 Partial: 11
🟥 Not Patched: 2
🟦 Detecting: 0
Pending Initial Detection: 1
Total Computers: 14
Select to Change Graph:
Patch Status for all Computers
Patch Status for all Reports
Status for all Computers
Baseline Status for all Groups

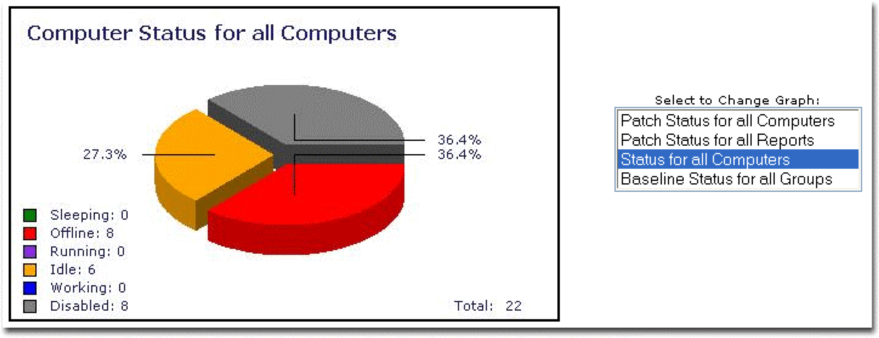
- Completely Patched
- Partially Patched
- Not Patched
- Performing the analysis detection
- Pending the initial analysis detection

2. Patch Status for all Reports – displaying the status for all vulnerability patch reports:


Patch Status for all Reports
24.1%
23.3%
52.6%
🟩 Patched: 31
🟧 Partial: 70
🟥 Not Patched: 32
🟦 Detecting: 0
Non-applicable Computers: 922
Total Bulletins: 1055
Select to Change Graph:
Patch Status for all Computers
Patch Status for all Reports
Status for all Computers
Baseline Status for all Groups

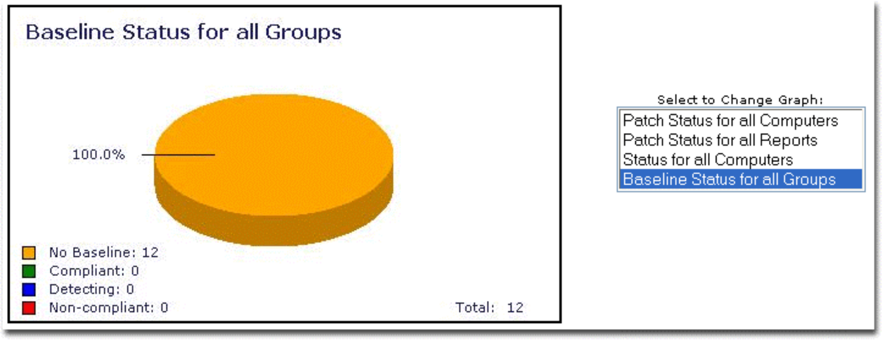
- Completely Patched
- Partially Patched
- Not Patched
- Detecting
- Reports which have no applicable computers assigned to

3. Status for all computers:



- Sleeping (outside their hours of operation)
- Detect offline or have not communicated with the Patch Management Server in over two intervals (15 minutes minimum).
- Running: currently performing the analysis detection outside the normal means (rarely occurring when the detection process happens outside of the deployment mechanism).
- Idle: Agent is communicating fine and currently not performing any tasks.
- Working: the Agent is currently working on a task.
- Disabled and unable to perform any tasks.

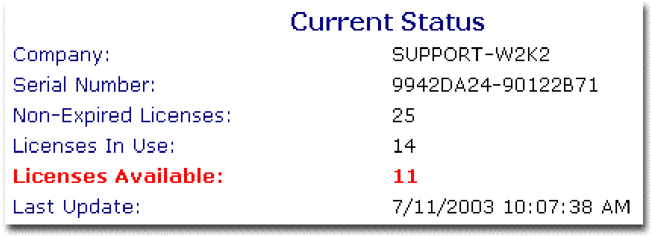
4. Compliancy Status for the Mandatory Patch Baseline Status for all Groups:



- Groups whose members are fully compliant with their baseline.
- Groups whose members are not compliant with their baseline.
- Groups whose members are in the detection and analysis process.
- Groups which have no baseline.

Current Status Information

This provides you with an overall relative condition, position or state of your Patch Management Server system.



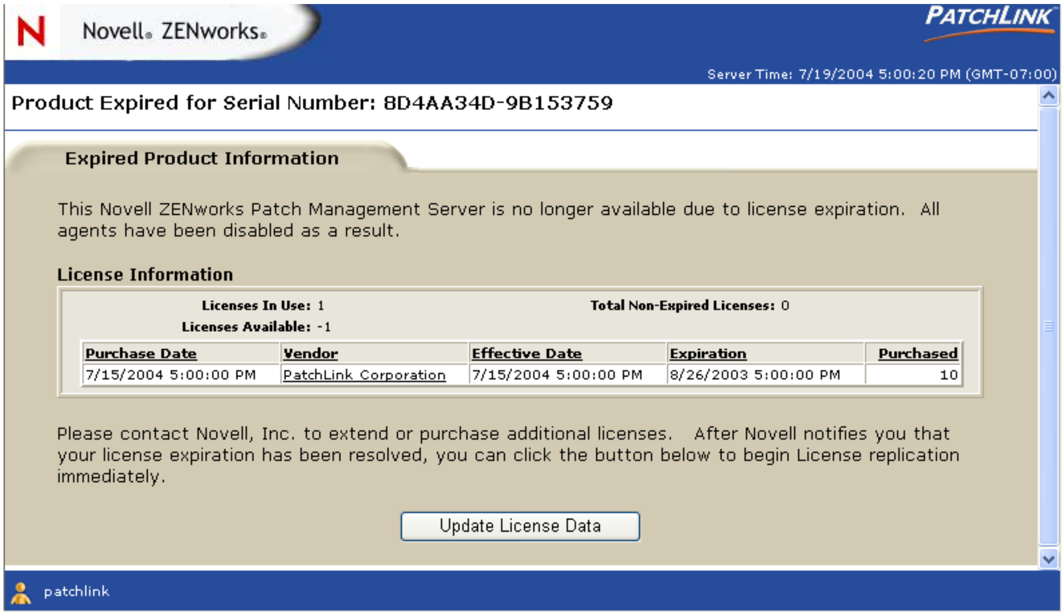
Current Status

Company:	SUPPORT-W2K2
Serial Number:	9942DA24-90122B71
Non-Expired Licenses:	25
Licenses In Use:	14
Licenses Available:	**11**
Last Update:	7/11/2003 10:07:38 AM

- Company: This is the name of the company that was entered at the time of installation.
- Serial Number: This is your Patch Management Server serial number.
- Non-Expired Licenses: This is the total number of active licenses. Each registered computer requires one license.
- Licenses in Use: This is the number of active licenses being used by registered computers.
- Licenses Available: This is the number of active and available licenses that can be used to register computers to Patch Management Server.
- Last Update: This is the date and time that the Patch Management Server last updated itself from the Subscription Host Server.

License Expiration

When Patch Management Server licenses expire, the agents will no longer be able to perform any of their tasks and the home page display is replaced with this license page. Clicking the “Update License Data” button will initiate the license verification process that connects up to the Subscription Host Server and retrieves your updated licenses. This page will automatically refresh to the home page, once your updated licenses have been saved (this usually takes 1 minute). If you need to renew your licenses or add new licenses, please contact your Novell Sales Representative.



Server Time: 7/19/2004 5:00:20 PM (GMT-07:00)

Product Expired for Serial Number: 8D4AA34D-9B153759

Expired Product Information

This Novell ZENworks Patch Management Server is no longer available due to license expiration. All agents have been disabled as a result.

License Information

Licenses In Use: 1 **Total Non-Expired Licenses:** 0

Licenses Available: -1

Purchase Date	Vendor	Effective Date	Expiration	Purchased
7/15/2004 5:00:00 PM	PatchLink Corporation	7/15/2004 5:00:00 PM	8/26/2003 5:00:00 PM	10

Please contact Novell, Inc. to extend or purchase additional licenses. After Novell notifies you that your license expiration has been resolved, you can click the button below to begin License replication immediately.

Home Page Security

The Home Page section of the Patch Management Server requires the View Home Page access right. If a user does not have the correct access the access denied error message is displayed.

The status section of the Home Page requires the View Patch Management Server Status access right. If a user does not have the correct access, this section is not displayed.

The ability to initiate the License Verification function requires the Manage Patch Management Server Licenses access right. If a user does not have the correct access, the button to initiate the verification does not appear.

Contact your Patch Management Administrator (Local Super Administrator) for more information on ZENworks® Patch Management Security.

5. Vulnerability Reports

Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |

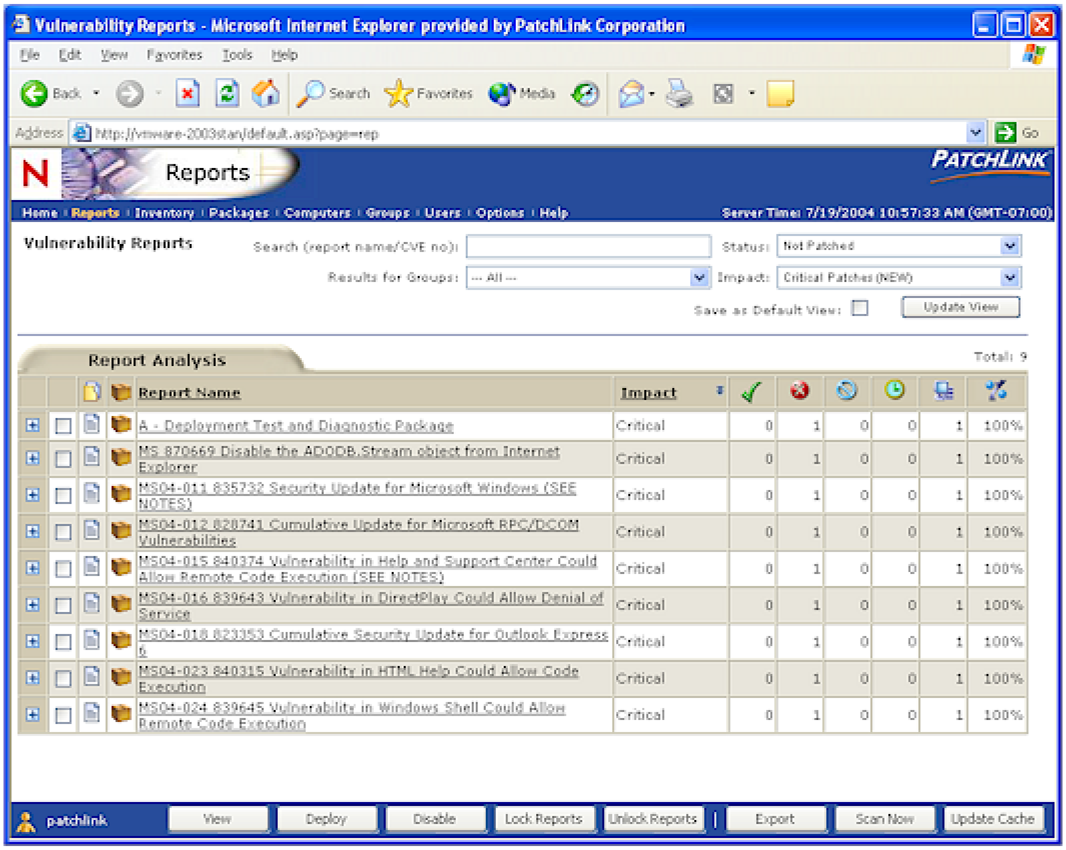
The reports page is where the majority of patch management work will be performed. It contains a listing of all patch related vulnerabilities across all the systems registered to the Patch Management Server.
It is strongly encouraged that you always manage patches from the Reports Interface, since it offers the most functionality and granularity.

A Vulnerability Report encompasses any vulnerability and how to detect it and its associated patch or patches. The detection portion of it, also called a Vulnerability Report, contains the necessary signatures and fingerprints on which to properly determine if the vulnerability is patched or not patched.

Vulnerability Report Analysis

This section displays the analysis results of the vulnerability reports during the Discover Applicable Updates process on the computer. The report analysis gives a simple top-down view of the computer in each status.

The Vulnerability Report Analysis can be seen at your network level, groups of computers level and down to a single machine level. The various statuses are detailed in this section.


Vulnerability Reports - Microsoft Internet Explorer provided by PatchLink Corporation
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://vmware-2003stan/default.asp?page=rep Go
Reports
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Update View
View
Deploy
Disable
Lock Reports
Unlock Reports
Export
Scan Now
Update Cache
patchlink

Server Time: 7/19/2004 10:57:33 AM (GMT-07:00)

Vulnerability Reports

Search (report name/CVE no):

Status: Not Patched

Results for Groups: --- All ---

Impact: Critical Patches (NEW)

Save as Default View: □

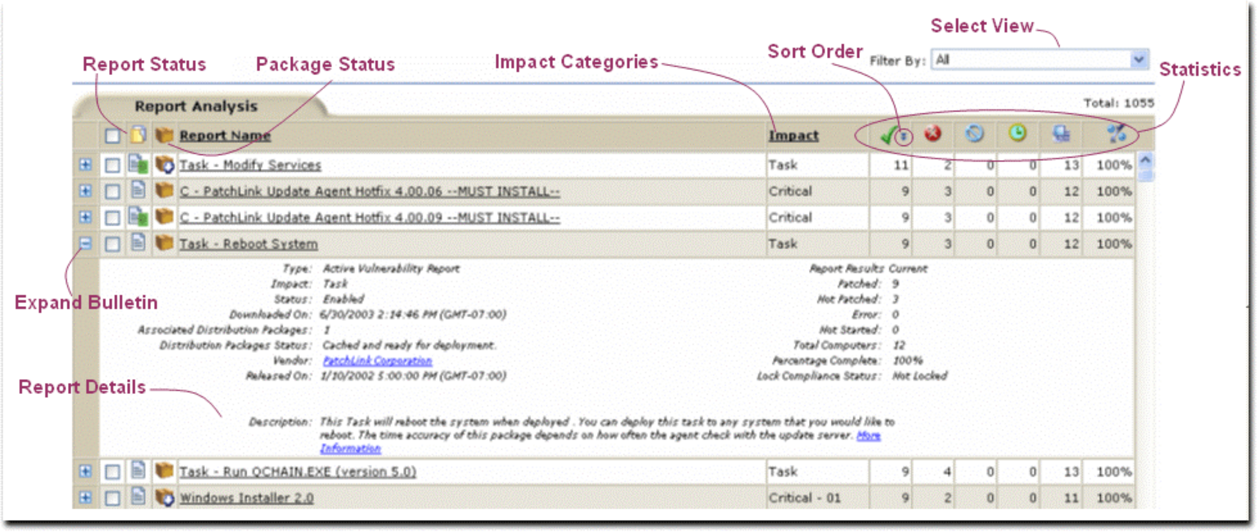
Report Analysis

Total: 9

				Report Name	Impact	✓	✗	⊘	🕒	🖥	%
⊞	□			A - Deployment Test and Diagnostic Package	Critical	0	1	0	0	1	100%
⊞	□			MS 870669 Disable the ADODB.Stream object from Internet Explorer	Critical	0	1	0	0	1	100%
⊞	□			MS04-011 835732 Security Update for Microsoft Windows (SEE NOTES)	Critical	0	1	0	0	1	100%
⊞	□			MS04-012 828741 Cumulative Update for Microsoft RPC/DCOM Vulnerabilities	Critical	0	1	0	0	1	100%
⊞	□			MS04-015 840374 Vulnerability in Help and Support Center Could Allow Remote Code Execution (SEE NOTES)	Critical	0	1	0	0	1	100%
⊞	□			MS04-016 839643 Vulnerability in DirectPlay Could Allow Denial of Service	Critical	0	1	0	0	1	100%
⊞	□			MS04-018 823353 Cumulative Security Update for Outlook Express 6	Critical	0	1	0	0	1	100%
⊞	□			MS04-023 840315 Vulnerability in HTML Help Could Allow Code Execution	Critical	0	1	0	0	1	100%
⊞	□			MS04-024 839645 Vulnerability in Windows Shell Could Allow Remote Code Execution	Critical	0	1	0	0	1	100%

A report illustrates a detection mechanism to determine if something is installed or configured in a certain way. For most reports, it is to determine if a patch, service pack, or device driver is installed on a computer. The total number of reports for each view is displayed at the upper right top.

Clicking on a vulnerability report will display the detailed results of the analysis. This is the same as in selecting a vulnerability report and clicking on the **View** button.



Filter By: All

Report Analysis

Total: 1055

				Report Name	Impact	✓	✗	⊘	🕒	🖥	%
⊞	□			Task - Modify Services	Task	11	2	0	0	13	100%
⊞	□			C - PatchLink Update Agent Hotfix 4.00.06 --MUST INSTALL--	Critical	9	3	0	0	12	100%
⊞	□			C - PatchLink Update Agent Hotfix 4.00.09 --MUST INSTALL--	Critical	9	3	0	0	12	100%
⊟	□			Task - Reboot System	Task	9	3	0	0	12	100%
⊞	□			Task - Run QCHAIN.EXE (version 5.0)	Task	9	4	0	0	13	100%
⊞	□			Windows Installer 2.0	Critical - 01	9	2	0	0	11	100%

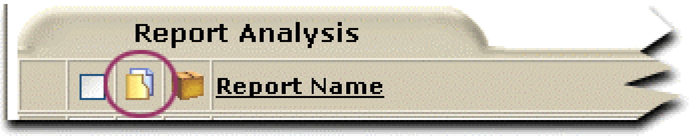
Task - Reboot System details:

Type: Active Vulnerability Report
Impact: Task
Status: Enabled
Downloaded On: 6/30/2003 2:14:46 PM (GMT-07:00)
Associated Distribution Packages: 1
Distribution Packages Status: Cached and ready for deployment.
Vendor: PatchLink Corporation
Released On: 1/10/2002 5:00:00 PM (GMT-07:00)

Report Results Current
Patched: 9
Not Patched: 3
Error: 0
Not Started: 0
Total Computers: 12
Percentage Complete: 100%
Lock Compliance Status: Not Locked

Description: *This Task will reboot the system when deployed . You can deploy this task to any system that you would like to reboot. The time accuracy of this package depends on how often the agent check with the update server.* More Information

Vulnerability Report Statuses & Types



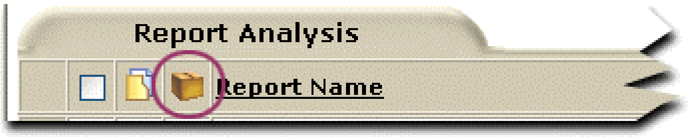
The status of a report is indicated by the following icons:

Beta	New	Current	Status Description
📄B	📄	📄	This is an active vulnerability report.
🔒📄B	🔒📄	🔒📄	This report has been locked and is in compliance.
🔒📄B ✗	🔒📄 ✗	🔒📄 ✗	This report has been locked and is out of compliance.
📄B	📄	📄	This report has been disabled.

Additional information about the status of the associated distribution package is displayed upon hovering your mouse pointer over the icon.

- Beta: This vulnerability report has been released to the BETA community.
- New: This vulnerability report has been downloaded from the Subscription Host Server and has arrived since you started your Patch Management Server session.
- Current: This is a current vulnerability report that has been downloaded from the Subscription Host Server before you started your Patch Management Server session.

Package Cache Status & Types



A vulnerability report may have any number of distribution packages associated with it. A distribution package contains the patch to fix the vulnerability. Each distribution package may be cached (downloaded) from the Subscription Host Server to Patch Management Server. They may be cached automatically if the vulnerability's impact is critical or if a deployment has been created to deploy the package(s). The package cache status icon is a hyperlink. By clicking on the icon, you will initialize a list of the individual packages that are associated with that report.

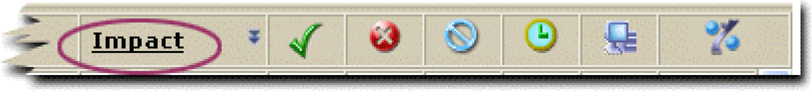
Current	New	Status Description
📦➜	📦➜	At least one of the packages is being deployed.

📦	📦	The packages are cached and ready for deployment.
⏬	⏬	At least one of the packages is being cached from the Subscription Host Server.
📦	📦	At least one of the packages has not been cached.

Additional information about the status of the associated distribution package is displayed upon hovering your mouse pointer over the icon.

- New: This distribution package has been released and its metadata has been downloaded from the Subscription Host Server since you began your Patch Management Server session.
- Current: This distribution package has been released and its metadata has been downloaded from the Subscription Host Server before you began your Patch Management Server session.

Vulnerability Report Impact



The agent list initially sorts by Impact alphanumerically in ascending order. To change the way to sort by another field (other than report or package status) click on the field name. To reverse the alphanumeric sort from ascending to descending, click on field name again.

Critical

The manufacturer or PatchLink has determined that this patch is critical and should be installed as soon as possible. Most of the recent security updates fall in to this category. The patches for this category are automatically downloaded and stored on the Patch Management Server.

Critical - 01

The manufacturer or PatchLink has determined that this patch is critical and should be installed as soon as possible. The patches for this category are not automatically downloaded and stored.

Critical - 05

The manufacturer or PatchLink has determined that this patch is critical and should be installed as soon as possible. Most of the superceded security updates fall in to this category. The patches for this category are not automatically downloaded and stored.

Recommended

The manufacturer or PatchLink has determined that this patch, while not critical or security related is useful and should be applied to maintain the health of your computers.

Informational

The manufacturer or PatchLink has determined that this patch is useful, though does not contain any changes that are necessary for day to day operations. Documentation updates are an example of the patches in this category.

Detection

These reports contain signatures that are common to multiple vulnerabilities. They contain no associated patches are only used in the detection process.

Software

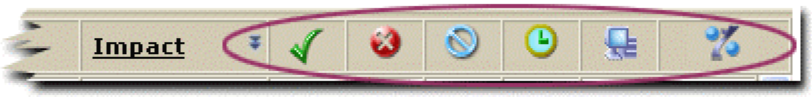
These reports contain the fingerprints and signatures for which Software Applications are based. They determine if the prerequisites are met for the installation of these applications.

Task

This category contains tasks which administrators may use to run various detection or deployment tasks across their network.

Statistics

The right-hand side of the report entry contains columns which illustrate the current result statistics for the computers which have been scanned in addition to the overall percentage completion of all computers which the detection report will be scanned.



Result	Result Definition
✓	Total number of computers that are patched.
✖	The total number of computers that are not patched.
🛇	The total number of computers that produced an error while determining the patch status for the vulnerability.
🕒	The total number of computers that are still waiting for the report analysis to finish.
🖥	The total number of computers that have met the prerequisites for the vulnerability.
%	The percentage of computers that have finished the vulnerability analysis.

You may sort by Ascending (default view) or Descending order by clicking on the corresponding results definition icon.

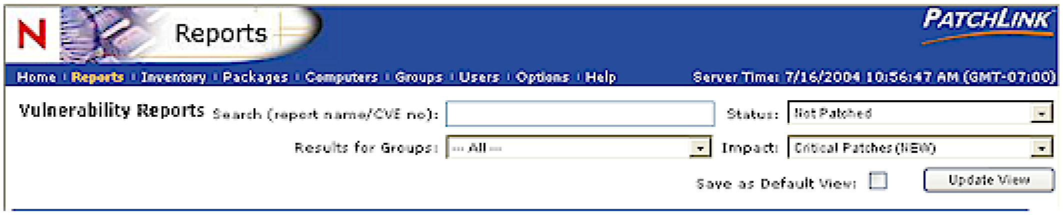
Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟, ⊞) is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Reports page header.


N
Reports
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Update View

Server Time: 7/16/2004 10:56:47 AM (GMT-07:00)

Vulnerability Reports

Search (report name/CVE no):

Status: Not Patched

Results for Groups: --- All ---

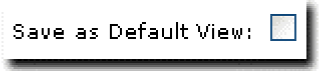
Impact: Critical Patches (NEW)

Save as Default View: □

- **Search**

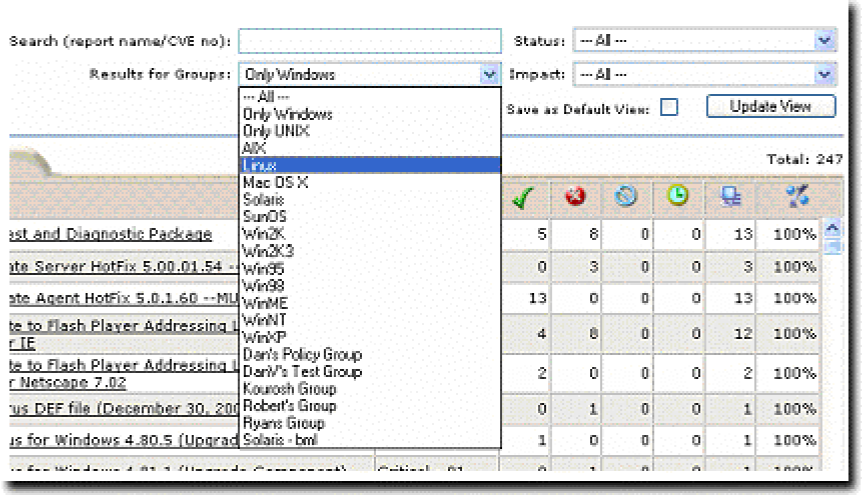
You may search reports for more granular results by entering the report name (CVE; Common Vulnerabilities and Exposures) text into the **Search** field and clicking on the Update View Update View button.

This will return the report(s) having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Save as Default View: □

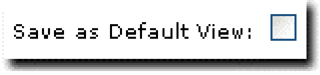
- **Results for Groups**
  Filter by **Groups** using the dropdown menu and click on the Update View Update View button.



Search (report name/CVE no):
Results for Groups: Only Windows
Status: --- All ---
Impact: --- All ---
Save as Default View: □
Update View
Total: 247

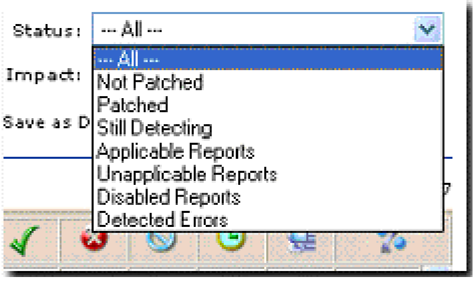
est and Diagnostic Package	5	8	0	0	13	100%
ate Server HotFix 5.00.01.54 --	0	3	0	0	3	100%
ate Agent HotFix 5.0.1.60 --MU	13	0	0	0	13	100%
te to Flash Player Addressing L r IE	4	8	0	0	12	100%
te to Flash Player Addressing L r Netscape 7.02	2	0	0	0	2	100%
us DEF file (December 30, 200	0	1	0	0	1	100%
is for Windows 4.80.5 (Upgrad	1	0	0	0	1	100%

This will return the report(s) having the selected group. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



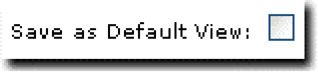
Save as Default View: □

- **Status**
  Filter by Report Statuses using the dropdown menu and click on the Update View Update View button.



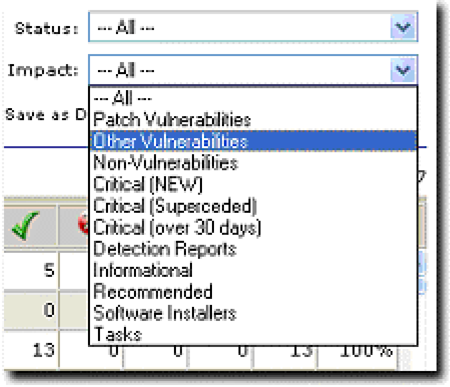
Status: --- All ---
Impact:
Save as D

This will return the report(s) having the selected status.   You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.


Save as Default View: □

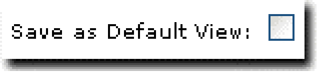
- **Impact**
  Filter by Report Impact levels using the dropdown menu and click on the Update View Update View button.

  This is extremely useful when you want to find or display only the Reports that, for example, are Critical (NEW).


Status: -- All --

Impact: -- All --

This will return the report(s) having the selected impact. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.


Save as Default View: □

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

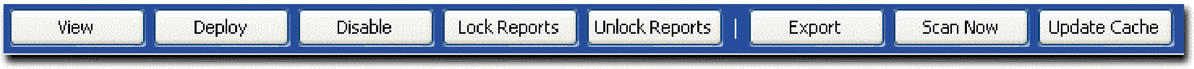
Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



View

The reports filter controls which vulnerability reports to display. There are three options to choose from: Vulnerability Reports that have computers applicable to them, Disabled Vulnerability Reports or view All Vulnerability Reports.

Deploy

This creates a deployment for the selected vulnerability report. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

Disable

This removes the selected enabled vulnerability reports from being able to be scanned during the Discover Applicable Updates process from all levels of the system (network level down to the individual computer level).

Enable

This re-enables the scanning ability for the selected disabled vulnerability reports during the Discover Applicable Updates process.

Lock Reports

Selecting a report(s) and clicking on the lock button will save the current vulnerability report analysis values. When the analysis is again displayed this data is compared to the current data to determine if the vulnerability report is in or out of compliance. If the vulnerability report is out of compliance, the vulnerability report is highlighted in red.

Unlock Reports

Selecting a locked report(s) and clicking on the unlock button will clear out the vulnerability report's locked data.

Export

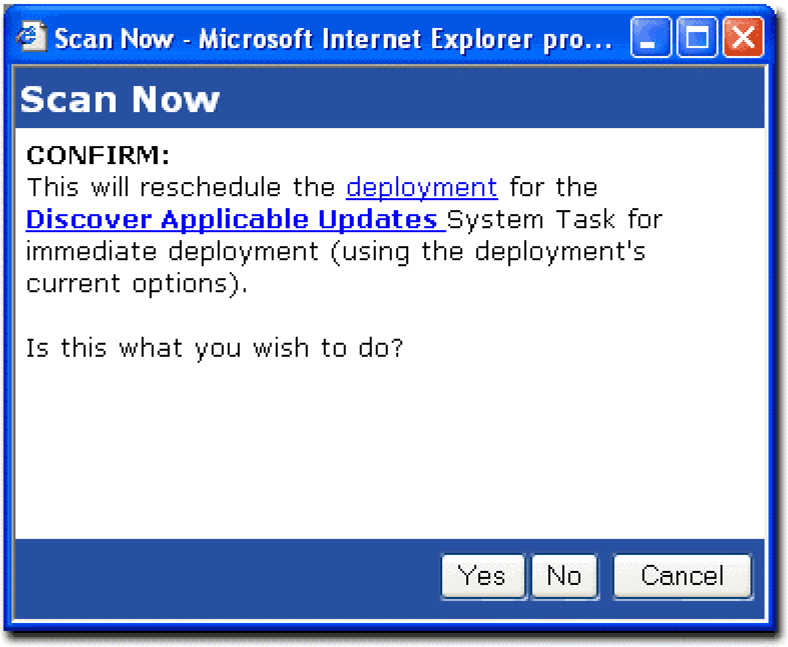
Export the vulnerability report analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates System Task** deployment for immediate execution to all selected computers.

To initialize (choose) all computers, click on **Scan Now** button without selecting any computers.

If you choose not to select any computers, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the computers.

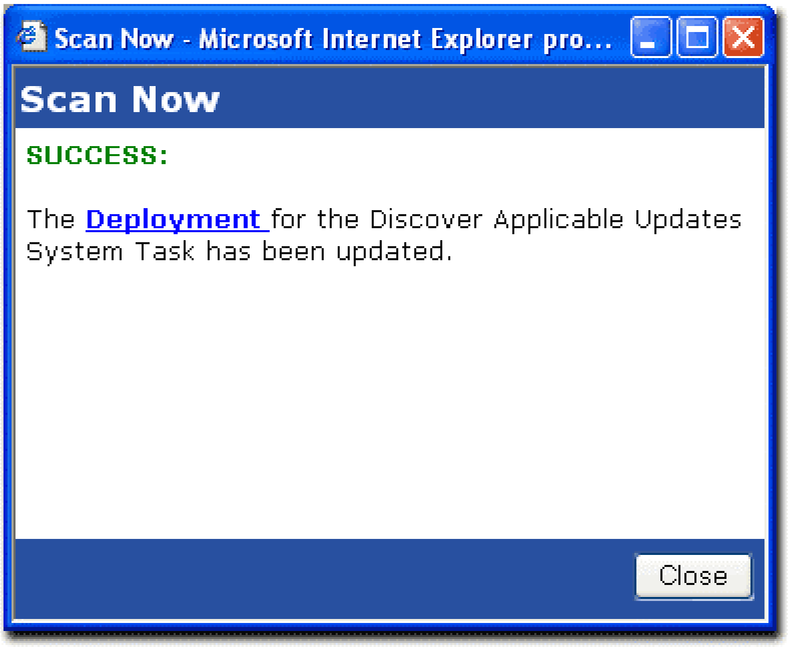


Scan Now

CONFIRM:
This will reschedule the deployment for the Discover Applicable Updates System Task for immediate deployment (using the deployment's current options).

Is this what you wish to do?

To reschedule the **Discover Applicable Updates**, select Yes



Scan Now

SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

The Patch Management Server will reschedule the selected computer(s), initialize a screen stating its success and provide a deployment link to initialize a new screen with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the screen, the Computers page will be refreshed. Previously selected deployment options are maintained

Update Cache

Update Cache initiates the process to cache (or re-cache) the associated distribution packages for the selected vulnerability reports.

Vulnerability Report Analysis Security

The Reports section of the Patch Management Server requires the View Reports Page access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the detailed report analysis requires the View Report Details access right. If a user does not have the correct access, the hyperlink will not be shown and the View button is disabled.

To be able to change the filter from detected vulnerability reports to disabled or all requires the Change Report Filter access right. If a user does not have the correct access, the filter will not have any options to choose from.

To be able to view the associated distribution packages for a given vulnerability report requires the View Packages access right. If a user does not have the correct access, the link on the package status image is disabled.

To be able to create a deployment based on the report analysis requires the Deploy Reports access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to enable or disable vulnerability reports from being available by the Discover Applicable Updates process requires the Manage Reports access right. If a user does not have the correct access, the Enable and Disable buttons are disabled.

To be able to lock or unlock the selected vulnerability reports requires the Manage UI Report Locks access right. If a user does not have the correct access, the Lock and Unlock buttons are disabled.

To export all of the vulnerability report analysis's to a comma-separated value (CSV) file requires the Export Report Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the Discover Applicable Updates process for all of the computers registered to the Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

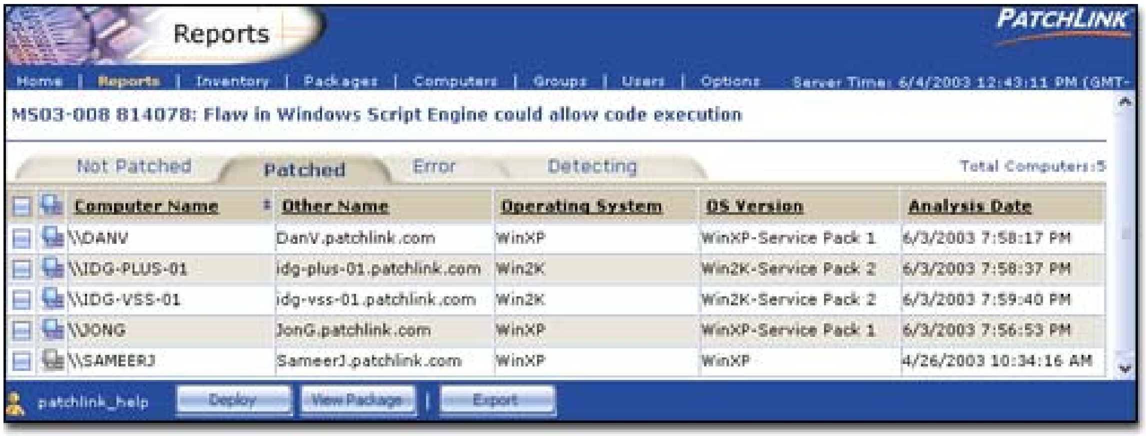
To cache the associated distribution of the selected vulnerability reports requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

Vulnerability Report Analysis Details

Each patch displayed is reported as required based on your unique configuration of systems. By clicking the report link, a full list of all computers that require the patch in question will be displayed. From there, the patch can be easily deployed.

From the Reports Homepage, click on the **Report Name Link** to view the analysis of the vulnerability report.

The analysis results of the vulnerability report are detailed and separated into four tabbed displays. The name of the tab represents status for those computers in the report analysis.



Server Time: 6/4/2003 12:43:11 PM (GMT-

MS03-008 814078: Flaw in Windows Script Engine could allow code execution

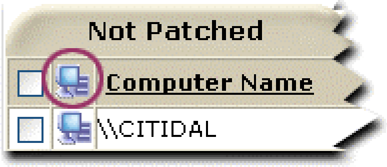
Total Computers:5

Computer Name	Other Name	Operating System	OS Version	Analysis Date
\\DANV	DanV.patchlink.com	WinXP	WinXP-Service Pack 1	6/3/2003 7:58:17 PM
\\IDG-PLUS-01	idg-plus-01.patchlink.com	Win2K	Win2K-Service Pack 2	6/3/2003 7:58:37 PM
\\IDG-VSS-01	idg-vss-01.patchlink.com	Win2K	Win2K-Service Pack 2	6/3/2003 7:59:40 PM
\\JONG	JonG.patchlink.com	WinXP	WinXP-Service Pack 1	6/3/2003 7:56:53 PM
\\SAMEERJ	SameerJ.patchlink.com	WinXP	WinXP	4/26/2003 10:34:16 AM

Analysis Results

- Not Patched: These computers were detected as needing the vulnerability patch.
- Patched: These computers were detected as being patched for the vulnerability.
- Error: These computers produced an error while determining the patch status for the vulnerability.
- Detecting: These computers are either in the process of determining the patch status for the vulnerability or waiting for the detection and analysis process to begin.

Agent Status



Status	Description
🖥	This is an idle deployment agent.
🖥🕒	This deployment agent is idle and has deployments in its work queue.
💤	The agent is sleeping as it is outside of its hours of operation.
💤🕒	The agent is sleeping as it is outside its hours of operation and has deployments in its work queue.
🖥➡	This agent is currently working on a deployment.
🔍	This is an active detection agent that does not correspond to a registered deployment agent.
🟥	The agent is considered to be offline as it has not contacted PLUS in more than two intervals (minimum of 15 minutes).
🟥🕒	The agent is considered to be offline as it has not contacted PLUS in more than two intervals (minimum of 15 minutes) and has deployments in its work queue.
🖥	This agent has been disabled.

Additional information may be displayed by hovering your mouse pointer over the icon.

Agent Information

- Host Name: This displays the name of the computer.
- Other Name: This displays either the DNS name for the computer or its IP address if it does not have an assigned DNS name.
- Operating System: This displays the abbreviated the operating system name
- OS Version: This displays additional operating system version information.
- Last Reported Date: This is the date the agent last ran the Discover Applicable Updates process.

Page Functions

Sort

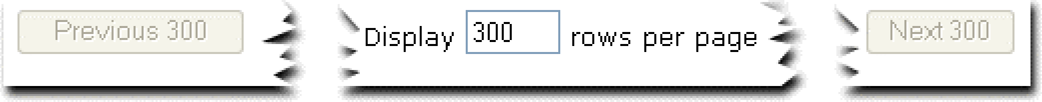
The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Display (Pagination)

Depending on the amount of items available for display and what page you are viewing, determines the display function. The Display function, if enabled, is located at the bottom above the Action Menu.

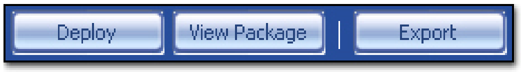


- Next: To display the next page of computers, click on the next button. If the last computer is displayed, the next button is disabled.
- Previous: To display the previous page of computers, click on the previous button. If the first computer is being displayed, the previous button is disabled.
- Computers per Page: The computer list initially displays up to 100 computers per page. To change the number of computers to display per page, enter a new number in to the Computers per Page input field. To display all computers enter a zero in the input field.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Deploy

This invokes the Deployment Wizard and allows you to create a deployment for the selected vulnerability report. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

View Package

This displays the associated distribution packages for the vulnerability report.

Export

Export the vulnerability report analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is selected and sorted on.

Vulnerability Report Analysis Security

The Report Analysis Details section of Patch Management Server requires the View Report Details access right. If a user does not have the correct access the access denied error message is displayed.

To be able to create a deployment based on the report analysis requires the Deploy Reports access right. If a user does not have the correct access, the Deploy button is disabled.

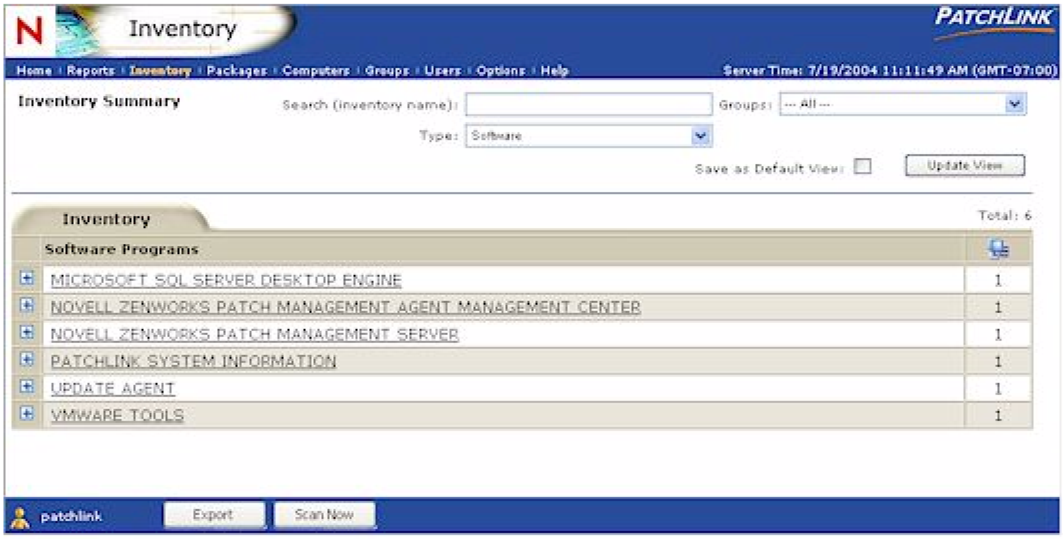
To be able to view the associated distribution packages for a given vulnerability report requires the View Packages access right. If a user does not have the correct access, the View Package button is disabled.

To export the vulnerability report analysis to a comma-separated value (CSV) file requires the Export Report Data access right. If a user does not have the correct access, the Export button is disabled.

6. Inventory

The Patch Management Server has the capability to determine what patch is applicable to what machine and has strong inventory capabilities for all the software, hardware, operating system and services on a system. The inventory reports all Operating System, Installed Software, Hardware and their device drivers, and Services from a network perspective down to the single machine level.

Clicking the ⊞ will display the list of computers containing this inventory item. Clicking the ⊟ will hide this list from view. The computer list is refreshed each time it is displayed. The alternative method to obtain this list is to click on the name of the inventory item and the page will be refreshed with this list.



Server Time: 7/19/2004 11:11:49 AM (GMT-07:00)

Inventory Summary

Search (inventory name):

Groups: --- All ---

Type: Software

Save as Default View: □

Inventory

Total: 6

	Software Programs	
⊞	MICROSOFT SQL SERVER DESKTOP ENGINE	1
⊞	NOVELL ZENWORKS PATCH MANAGEMENT AGENT MANAGEMENT CENTER	1
⊞	NOVELL ZENWORKS PATCH MANAGEMENT SERVER	1
⊞	PATCHLINK SYSTEM INFORMATION	1
⊞	UPDATE AGENT	1
⊞	VMWARE TOOLS	1

patchlink

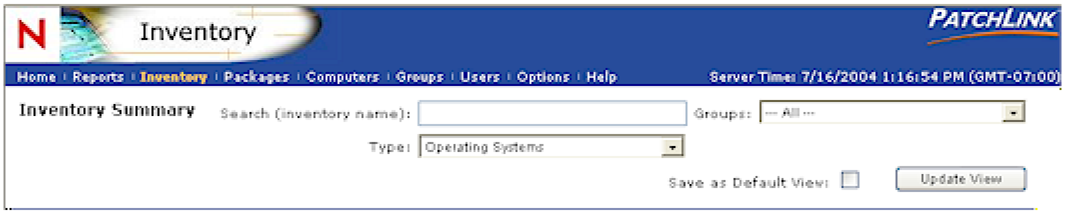
Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟,⊞) is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Inventory Summary page header.


Inventory
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Server Time: 7/16/2004 1:16:54 PM (GMT-07:00)
Inventory Summary
Search (inventory name):
Save as Default View: □
Update View

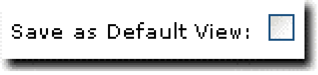
Groups: --- All ---

Type: Operating Systems

- Search

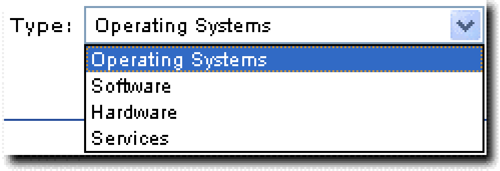
You may search inventory for more granular results by entering the inventory name text into the **Search** field and clicking on the Update View button.

This will return the inventory having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- Type

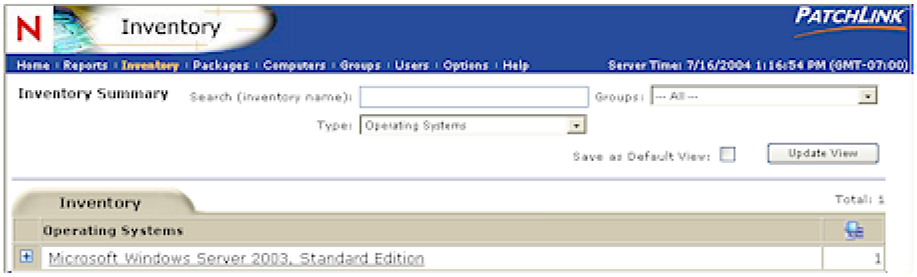
Filter by Type using the pull down menu and click on the Update View button.



This allows you to search for Operating Systems, Software, Hardware and Services.

- Operating Systems View

Displays the full operating system platform names and the number of instances, or times this operating system was detected.


Inventory
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Server Time: 7/16/2004 1:16:54 PM (GMT-07:00)
Inventory Summary
Search (inventory name):
Save as Default View: □
Update View
Inventory

Groups: --- All ---

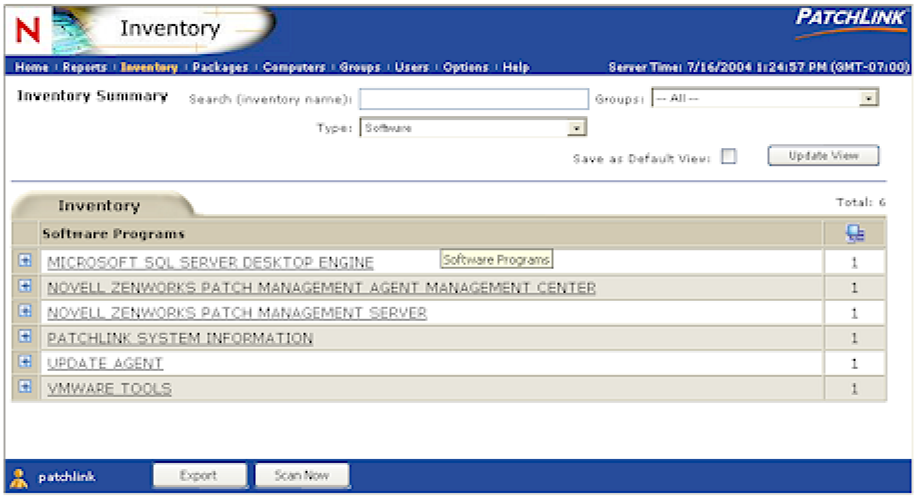
Type: Operating Systems

Total: 1

Operating Systems	
⊞ Microsoft Windows Server 2003, Standard Edition	1

- Software View

Displays the installed software applications and the number of instances, or times this software application was detected.



Inventory

PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help

Server Time: 7/16/2004 1:24:57 PM (GMT-07:00)

Inventory Summary

Search (inventory name):

Groups: -- All --

Type: Software

Save as Default View: □

Inventory

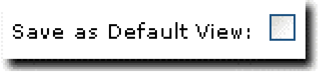
Total: 6

	Software Programs	
⊞	MICROSOFT SQL SERVER DESKTOP ENGINE	1
⊞	NOVELL ZENWORKS PATCH MANAGEMENT AGENT MANAGEMENT CENTER	1
⊞	NOVELL ZENWORKS PATCH MANAGEMENT SERVER	1
⊞	PATCHLINK SYSTEM INFORMATION	1
⊞	UPDATE AGENT	1
⊞	VMWARE TOOLS	1

Software Programs
This displays the name of the software application. Click the ⊞ for a software application to display the list of computers for that application. Click on the ⊟ to close this list.

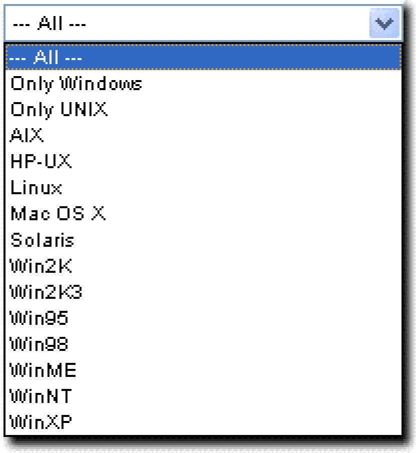
Number of Instances
The number of times this software application was detected.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Save as Default View: □

- Groups
  Filter by Group using the pull down menu and click on the Update View Update View button.



--- All ---

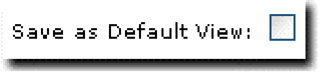
- --- All ---
- Only Windows
- Only UNIX
- AIX
- HP-UX
- Linux
- Mac OS X
- Solaris
- Win2K
- Win2K3
- Win95
- Win98
- WinME
- WinNT
- WinXP

This allows the user to search on any user defined or server defined groups that exist.

- Operating Systems
  Displays the selected or filtered operating system.

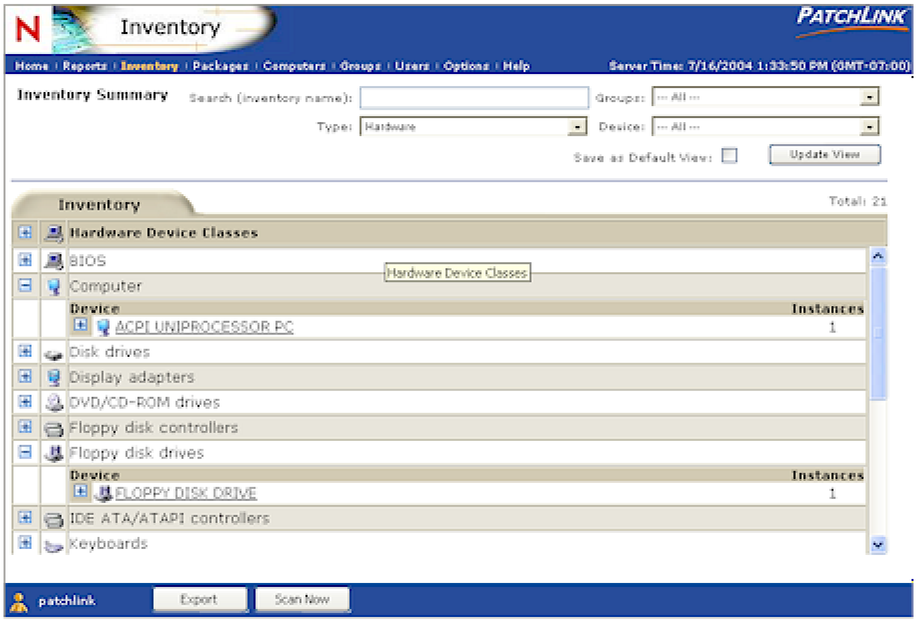
- Number of Instances
  This displays the number of times this operating system platform has been detected. For displaying the Operating System Inventory for a single computer, this is always one.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Save as Default View: □

- Hardware View
  Displays the client Hardware devices.


Inventory
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Update View
Export
Scan Now
patchlink

Server Time: 7/16/2004 1:33:50 PM (GMT-07:00)

Inventory Summary

Search (inventory name):
Groups: -- All --
Type: Hardware
Device: -- All --
Save as Default View: □

Inventory — Total: 21

⊞ Hardware Device Classes
⊞ BIOS
⊟ Computer

Device	Instances
⊞ ACPI UNIPROCESSOR PC	1

⊞ Disk drives
⊞ Display adapters
⊞ DVD/CD-ROM drives
⊞ Floppy disk controllers
⊟ Floppy disk drives

Device	Instances
⊞ FLOPPY DISK DRIVE	1

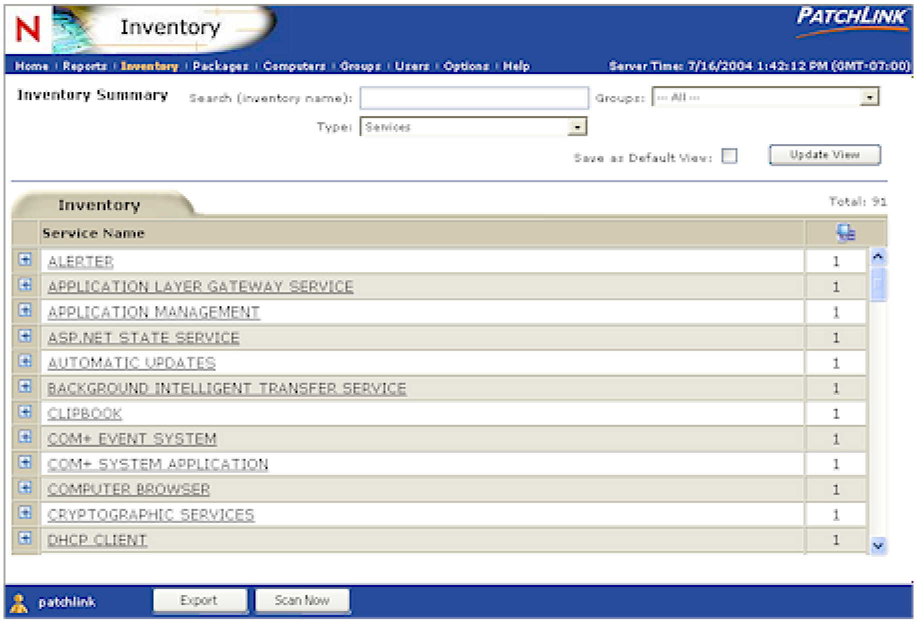
⊞ IDE ATA/ATAPI controllers
⊞ Keyboards

- Hardware Device Class
  Hardware is separated into device classes such as disk drives, processors, network adapters, etc. Click the ⊞ to display the list of devices for each class, or click on the ⊞ to display them all (for a long list of devices this may take a few moments to generate). Click the ⊟ to close this list.

- Device
  A device is a specific piece of hardware, such as a “Microsoft USB IntelliMouse Optical”. Click the ⊞ for a device to display the list of computers for that device. Click the ⊟ to close this list.

- Number of Instances
  An Instance is a specifically detected device or installed driver. A computer may contain multiple instances of a installed device or driver. For example, a computer may contain a video graphics adapter that contains multiple video sources and destinations in which each source or destination is discovered as multiple instances of the same device or driver.

- Services View
  Displays the detected services that may or may not be running.


Inventory
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help

Server Time: 7/16/2004 1:42:12 PM (GMT-07:00)

Inventory Summary

Search (inventory name):

Groups: --- All ---

Type: Services

Save as Default View: □

Total: 91

Service Name	
ALERTER	1
APPLICATION LAYER GATEWAY SERVICE	1
APPLICATION MANAGEMENT	1
ASP.NET STATE SERVICE	1
AUTOMATIC UPDATES	1
BACKGROUND INTELLIGENT TRANSFER SERVICE	1
CLIPBOOK	1
COM+ EVENT SYSTEM	1
COM+ SYSTEM APPLICATION	1
COMPUTER BROWSER	1
CRYPTOGRAPHIC SERVICES	1
DHCP CLIENT	1

- Service Name
  This displays the name of the service.

- Number of Instances
  The number of times this service was detected.

Action Menu

Export

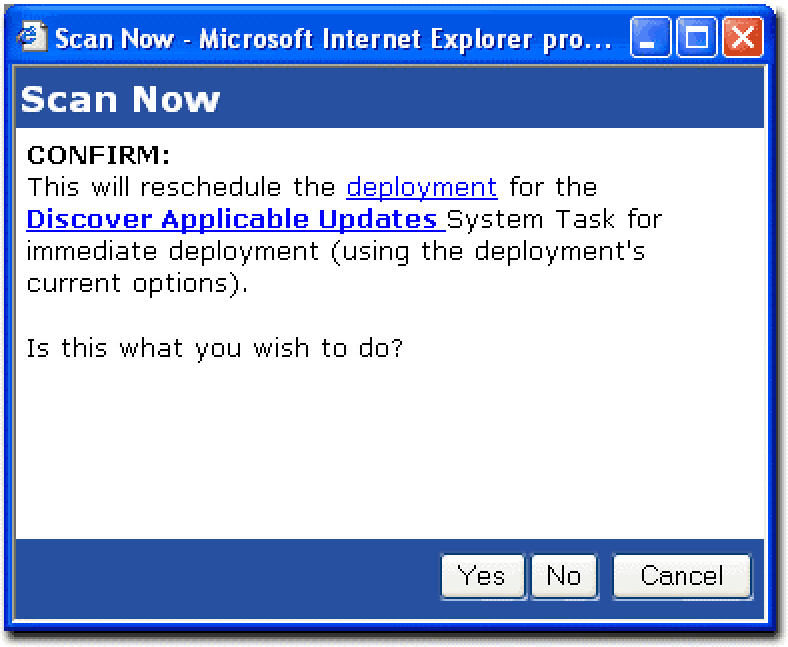
Export the filtered inventory data to a comma-separated value (CSV) file.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected computers.

To initialize (choose) all computers, click the **Scan Now** button without selecting any computers.

If you choose not to select any computers, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the computers.

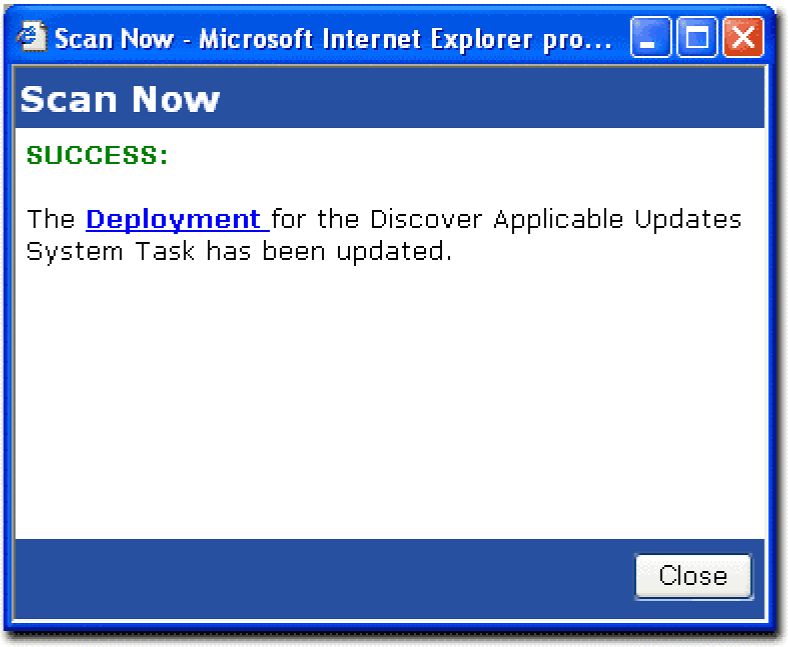


Scan Now

CONFIRM:
This will reschedule the deployment for the Discover Applicable Updates System Task for immediate deployment (using the deployment's current options).

Is this what you wish to do?

To reschedule the **Discover Applicable Updates**, select Yes.



Scan Now

SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

The Patch Management Server will reschedule the selected computer(s), initialize a screen stating its success and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the pop-up window, the Computers page will be refreshed and initialized. Previously selected deployment options are maintained.

Discovered Inventory Security

The Inventory section of the Patch Management Server requires the View Inventories access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the Software inventory requires the View Software Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Hardware inventory requires the View Hardware Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Services inventory requires the View Services Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the list of computers on which an inventory belongs to requires the View Computers access right. If a user does not have the correct access, the hyperlink on the inventory item is not disabled and the ⊞ function is disabled.

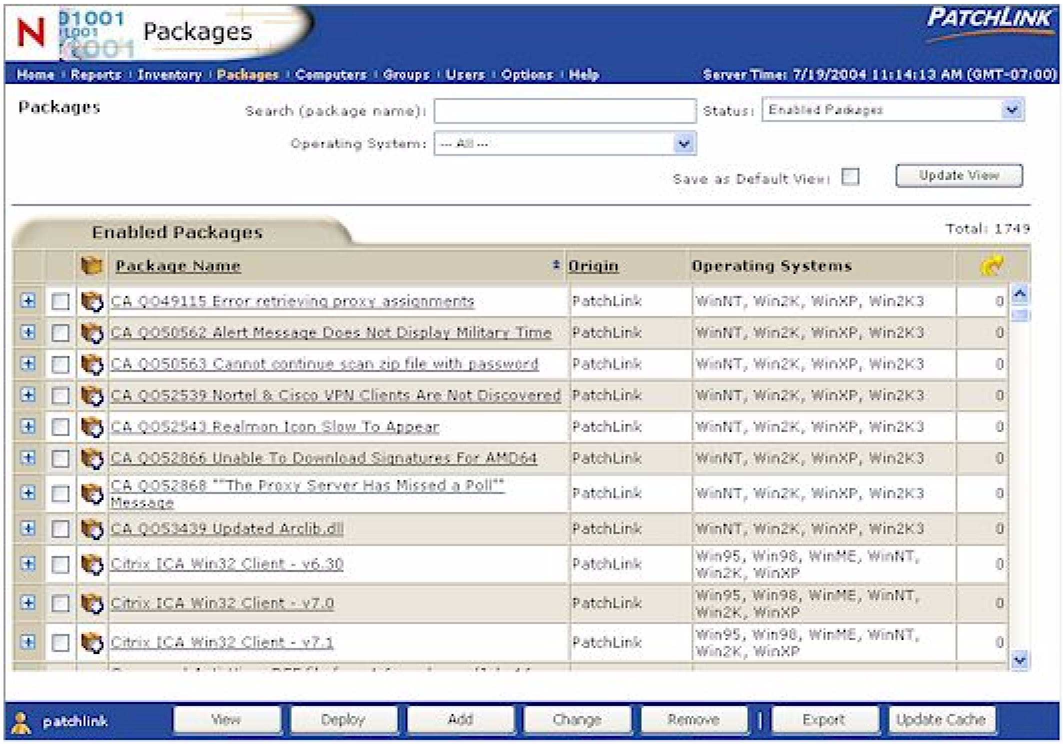
To export the inventory to a comma-separated value (CSV) file requires the Export Inventory Data access right. If a user does not have the correct access, the Export button is disabled.

7. Packages

Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |

Distribution Packages contain all the actual patch software and executable code used for patch deployment. Vulnerability Reports may contain several patch packages that will be deployed in a specific order. You can create custom packages from this page that do not require the patented Patch Fingerprinting technology. The ability to create custom packages demonstrates the software distribution capabilities of ZENworks® Patch Management Server as well as other tasks that you may require.

Distribution packages will contain whatever you want to deploy on a computer or group. A distribution package can run tasks or scripts, install software applications, place files (or directories of files) to a specified location, change the configuration of an application or service, or various other things that can be done in an unattended manner. The majority of the packages contain the patches for vulnerabilities, defects or bugs. If you would like to create your own patch, application or script package, see Section 8; Creating and Editing Packages: Package Editor Wizard and Section 9; Deploying Packages: Schedule Deployment Wizard for more information on custom packages.


N
01001
Packages
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
patchlink
View
Deploy
Add
Change
Remove
Export
Update Cache

Server Time: 7/19/2004 11:14:13 AM (GMT-07:00)

Packages

Search (package name):

Status: Enabled Packages

Operating System: --- All ---

Save as Default View: □ Update View

Enabled Packages

Total: 1749

		Package Name	Origin	Operating Systems	
⊞	□	CA QO49115 Error retrieving proxy assignments	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
⊞	□	CA QO50562 Alert Message Does Not Display Military Time	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
⊞	□	CA QO50563 Cannot continue scan zip file with password	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
⊞	□	CA QO52539 Nortel & Cisco VPN Clients Are Not Discovered	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
⊞	□	CA QO52543 Realmon Icon Slow To Appear	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
⊞	□	CA QO52866 Unable To Download Signatures For AMD64	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
⊞	□	CA QO52868 ""The Proxy Server Has Missed a Poll"" Message	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
⊞	□	CA QO53439 Updated Arclib.dll	PatchLink	WinNT, Win2K, WinXP, Win2K3	0
⊞	□	Citrix ICA Win32 Client - v6.30	PatchLink	Win95, Win98, WinME, WinNT, Win2K, WinXP	0
⊞	□	Citrix ICA Win32 Client - v7.0	PatchLink	Win95, Win98, WinME, WinNT, Win2K, WinXP	0
⊞	□	Citrix ICA Win32 Client - v7.1	PatchLink	Win95, Win98, WinME, WinNT, Win2K, WinXP	0

Package Information

Package Name

This displays the name of the distribution package. Clicking on the distribution package will display the deployments for that distribution package.

The package and Deployment details are as follows:

- Distribution Package Name
- Origin
- Status
- Cache Status
- Cache Request Status
- Deployment Availability
- OS Platforms
- The user who created this distribution package
- The date the distribution package was created
- The user who last modified the distribution package
- When the distribution package was last modified
- The date when a deployment was last created for this distribution package Version
- Total number of directories found in the package
- Total number of files found in the package
- Total size of the compressed package size (in KB)
- Total number of prescripts
- Total number of postscripts
- Total number of command-line scripts
- Total number of dependant distribution packages
- Total number of idle deployments
- Total number of running deployments
- Total number of deployments that failed
- Total number of deployments that were fully successful
- Total number of deployments for this distribution package
- Description of the distribution package
- Any additional Notes (if applicable)

Origin

This displays where this distribution package was distributed from.

Operating Systems

This displays operating system platforms that this distribution package can deploy to.

Deployments

The number of deployments previously created for this distribution package.

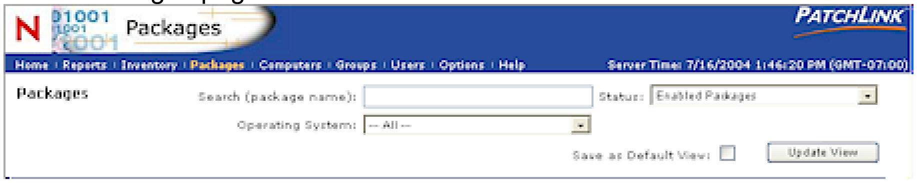
Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟, ⊞) is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Packages page header.


N
Packages
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Packages
Update View

Server Time: 7/16/2004 1:46:20 PM (GMT-07:00)

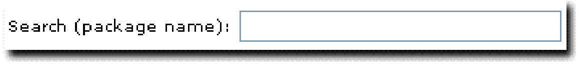
Search (package name):

Status: Enabled Packages

Operating System: -- All --

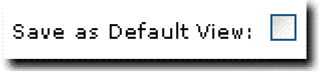
Save as Default View: □

- Search
  You may search packages for more granular results by entering the package text into the **Search** field and clicking on the Update View Update View button.



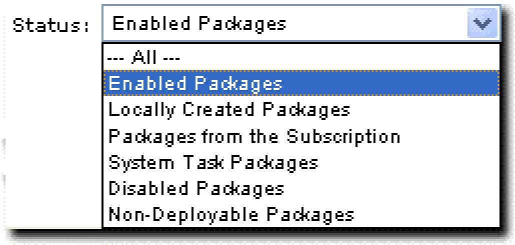
Search (package name):

This will return the package(s) having the name of the entered text.   You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



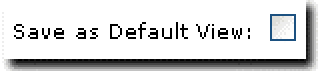
Save as Default View: □

- Status
  Filter by package status using the dropdown menu and click on the Update View Update View button.



Status: Enabled Packages

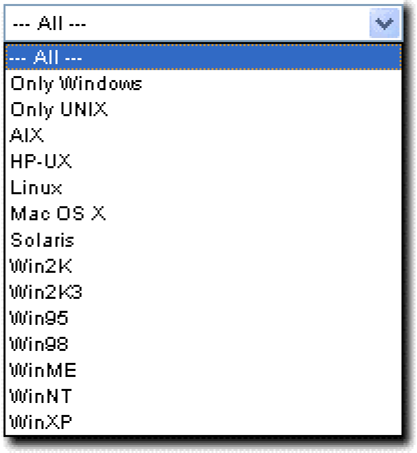
You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Save as Default View: □

- Operating Systems

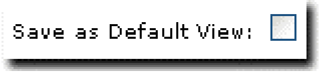
Filter by Operating Systems using the dropdown menu and click on the Update View Update View button.



--- All ---

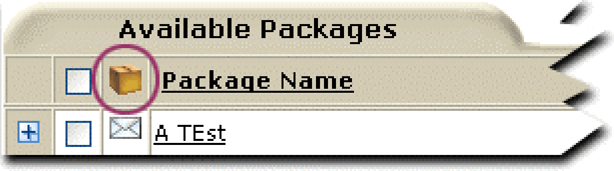
- --- All ---
- Only Windows
- Only UNIX
- AIX
- HP-UX
- Linux
- Mac OS X
- Solaris
- Win2K
- Win2K3
- Win95
- Win98
- WinME
- WinNT
- WinXP

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Save as Default View: □

Package Statuses & Types



Available Packages

	□	📦	Package Name
⊞	□	✉	A TEst

New	Current	Tasks	Local	Description
📦	📦	⚙		The package is not cached.
⏲	⏲	⏲		The package has been scheduled to be cached or is in the process of being cached.
📦	📦	⚙		An error occurred while trying to cache the package.
📦	📦	⚙	✉	The package is cached and ready for deployment.
📦	📦	⚙	✉	The package is currently deploying (animated).
📦	📦	⚙	✉	The package is disabled.

New

This distribution package has been released and its metadata has been downloaded from the Subscription Host Server since you began your Patch Management Server session.

Current

This distribution package has been released and its metadata has been downloaded from the Subscription Host Server before you began your Patch Management Server session.

Tasks

This is a system task distribution package.

Local

This is a locally created distribution package.
See Section 9; Deploying Packages: Schedule Deployment Wizard for more information on custom packages.

Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟,⊞) is only available for Microsoft Internet Explorer at this time.

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

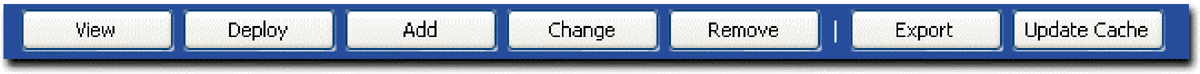
Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



View

This displays additional information about the distribution package. In this view you can also click to view the distribution package's deployments.

Deploy

This creates a deployment for the selected distribution package. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

Add

Create a new local distribution package See Section 8; Creating and Editing Packages: Package Editor Wizard for more information.

Change

Change a local distribution package. See Section 8; Creating and Editing Packages: Package Editor Wizard for more information.

Remove

This removes any non-System Task selected distribution packages. The Patch Management Server will re-download the package metadata (and not the files or scripts) for any deleted PatchLink provided distribution package (via the Patch Management Server's subscription service). The Patch Management Server will only cache the package if it is critical or being requested by a deployment.

Export

Export the distribution package list (and their information) to a comma-separated value (CSV) file. The order of the data is based on what the current display is sorted on.

Update Cache

Initiates the process to cache (or re-cache) for the selected distribution packages. If no distribution packages are selected this will re-cache all of the previously cached distribution packages.

Distribution Packages Security

The Distribution Packages section of the Patch Management Server requires the View Packages access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the deployments for a distribution package requires the View Deployments access right. If a user does not have the correct access the hyperlink on the Package Name will not be displayed.

To be able to create a deployment for a selected distribution package requires the Deploy packages access right. If a user does not have the correct access the Deploy button is disabled.

To be able to create, change or remove distribution packages requires the Manage Packages access right. If a user does not have the correct access the Add, Change and Remove buttons are disabled.

To export all of the distribution packages and their information to a comma-separated values (CSV) file requires the Export Package Data access right. If a user does not have the correct access the Export button is disabled.

To cache the selected (or re-cache all of the previously cached) distribution packages requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

Deployments

A Deployment, in its simplest form, allows a Patch to be downloaded by a Deployment Agent, so it can install it. In more generic terms, a Deployment is the encompassing instructions around a Distribution Package that describes to the Deployment Agent how to deploy the package. The contents of the Distribution Package contain all the other necessary information (info, files and scripts) required to actually perform whatever needs to be done: install this patch executable, stop this service, validate a system condition, change a database entry, etc.

Deployments can be created throughout the product, but basically encompass three main areas: Report-based Deployments, Package-based Deployments and a Group's Mandatory Baseline.

Report-based Deployments

A Vulnerability Report contains multiple associated distribution packages and the target package to be deployed depends on the assigned computers. As a computer goes through the Discover Applicable Updates process, it is assigned Vulnerability Reports to scan as the Patch Management Server determines they are applicable to the computer. Based on these results, a User has the ability to determine which computers to deploy the "Patch" (Vulnerability Fix) to. Behind the scenes, the Patch Management Server goes through and makes sure that the computers get assigned the correct Distribution Package.

Package-based Deployments

A Distribution Package is assigned a single operating system, thus only those computers whose operating system matches are able to perform the deployment. Package-based Deployments are the easiest to create, though they do not give you the granularity to tell the User which computers really apply to this patch (or package) or not.

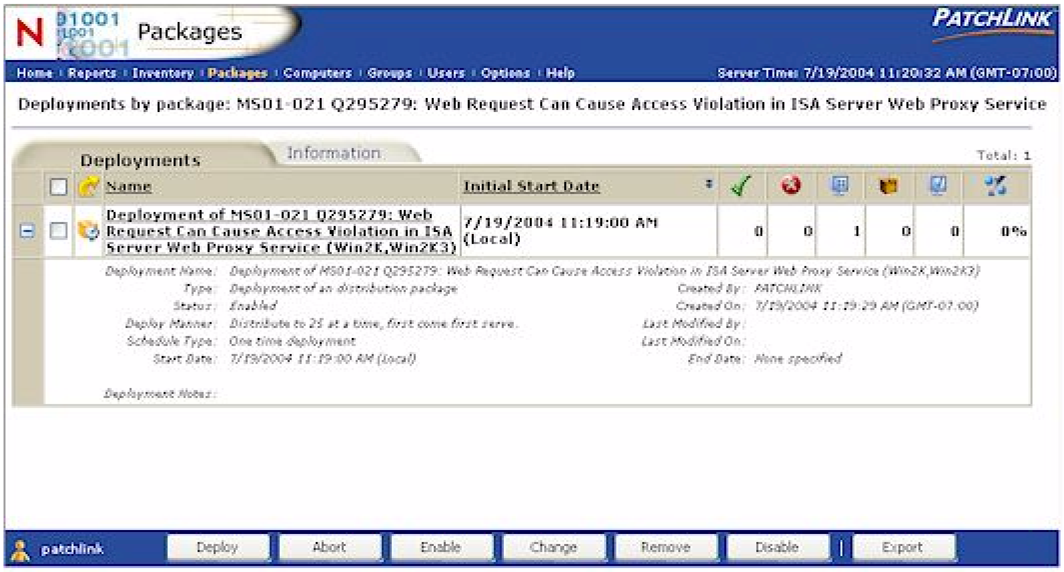
Group Mandatory Baseline

A group contains a feature called its Mandatory Baseline, or the ability to define a baseline of Vulnerability Reports or Locally-created Distribution Packages as being the base set of patches and other packages that must be installed for the group's computer members. In terms of Vulnerability Reports, a Mandatory Baseline will continually check to verify and validate that the patch is actually installed; if it is not, it will deploy the necessary distribution package to get it to be installed.

Select a specific **Package Name** link from the Package Name column to view information and deployment details.

The package deployments section displays all of the deployments that have been created for the distribution package.

The Distribution Packages section displays all of the packages that the Patch Management Server has available to it, various functions to manage them, and the number of Deployments created to deploy a package.



Packages
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Server Time: 7/19/2004 11:20:32 AM (GMT-07:00)

Deployments by package: MS01-021 Q295279: Web Request Can Cause Access Violation in ISA Server Web Proxy Service

Deployments
Information
Total: 1

	☐		Name	Initial Start Date	✓					
⊟	☐		Deployment of MS01-021 Q295279: Web Request Can Cause Access Violation in ISA Server Web Proxy Service (Win2K,Win2K3)	7/19/2004 11:19:00 AM (Local)	0	0	1	0	0	0%

Deployment Name: Deployment of MS01-021 Q295279: Web Request Can Cause Access Violation in ISA Server Web Proxy Service (Win2K,Win2K3)

Type:	Deployment of an distribution package	Created By:	PATCHLINK
Status:	Enabled	Created On:	7/19/2004 11:19:29 AM (GMT-07:00)
Deploy Manner:	Distribute to 25 at a time, first come first serve.	Last Modified By:	
Schedule Type:	One time deployment	Last Modified On:	
Start Date:	7/19/2004 11:19:00 AM (Local)	End Date:	None specified

Deployment Notes:

Clicking the ⊞ will display additional information about the deployment. Clicking the ⊟ will hide this information from view. The information is refreshed each time it is displayed. The deployment information contains:

Deployment name	The name of the deployment
Type	Deployment for which type of a package
Status	This can be: ○ Enabled ○ Disabled ○ Paused
Deploy manner	The manner in which this deployment occurred. It can be ○ Sequential ○ Parallel ○ First come first serve ○ Distribute to # of computers at a time
Schedule type	This can be: ○ Recurring ○ One time
Start date	The date and time this deployment was started
Deployment Notes	Additional information about the deployment
Created by	The user who created this deployment
Created on	The date and time this deployment was created
Last modified by	The user who modified this deployment last
Last modified on	The date and time this deployment was last modified
End date	The date and time the deployment was completed

Select a specific **Deployments Package Name** to view deployment details.

Deployment Types and Status

New	Current	Local	System Task	Mandatory Group	Description
📦	📦	✉	⚙	M	Deployment with no assigned computers.
📦➜	📦➜	✉➜	⚙➜	M➜	Deployment currently deploying (animated).
📦🕓	📦🕓	✉🕓	⚙🕓	M🕓	Deployment waiting to start.
📦✓	📦✓	✉✓	⚙✓	M✓	Deployment which all of the assigned computers and groups have finished successfully.
📦✗	📦✗	✉✗	⚙✗	M✗	Deployment in which at least one computer finished unsuccessfully.
📦	📦	✉	⚙	M	Deployment that is disabled.

- New: A new deployment is a deployment that has been created since you logged on to your current session.
- Current: A deployment that was created before you logged on to your current session.
- Local: A deployment is of a locally created distribution package.
- System Task: A system task deployment contains a system task distribution package to perform required or PatchLink provided tasks. These deployments may include automated schedules in which the membership of the deployment may not be modified, though the schedule may.
- Mandatory Group: A deployment is created through the mandatory baseline for a group. This deployment is automatically created and managed through the mandatory baseline process.

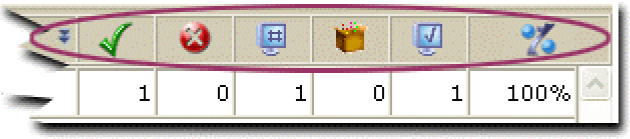
Name

The name assigned to the deployment.

Initial Start Date

The schedule date the deployment is to begin. For recurring deployments this is the first scheduled date of the deployment.

Statistics



✓	✗	#	📦	✓	%
1	0	1	0	1	100%

The right-hand side of the report entry contains columns which illustrates the current result statistics for deployments by package.

Result	Result Definition
✓	The total number of computers or groups that finished the deployment successfully.
❌	The total number of computers or groups that finished the deployment unsuccessfully.
🖥	The total number of computers or groups that are assigned the deployment.
📦	The total number of computers or groups that are in process of executing the deployment.
🖥	The total number of computers or groups that finished the deployment.
%	The percentage of the computers or groups that finished the deployment.

Deployment Summary

This view illustrates the overall information about this particular distribution package including its content, deployment status, etc.

Deployments of a package are designated by the following types:

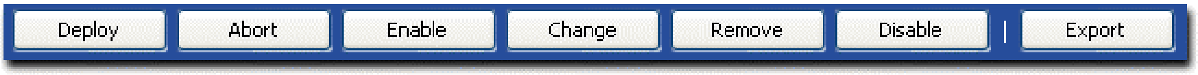
Result	Result Definition
M	Deployment of a mandatory baseline item for a group.
📦	Deployment of a distribution package (provided by PatchLink).
📦	Deployment of a new distribution package (provided by PatchLink).
⚙	Deployment of a new distribution package (provided by PatchLink).
✉	Deployment of a locally-created distribution package.

Each deployment has the following states, depending upon the status results of the deployment (using a distribution package deployment for the deployment type).

Result	Result Definition
📦	This deployment has not started.

➜	This deployment is currently in progress. (animated)
✓	This deployment has finished and all targets of the deployment came back as they deployed the package successfully.
✗	This deployment has finished and at least one of targets of the deployment came back as it deployed the package unsuccessfully.
■	This deployment has been disabled or put on hold.

Action Menu



Deploy

Deploys the current (selected) package. This will launch the Deployment Wizard. You can quickly schedule a package for deployment or distribution to computers with Client Agents from this wizard. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

Note: You will **not** be allowed to create new deployments of System Task Packages from PatchLink (only modify their schedule).

Abort

To abort one or more deployments:

- Select one or more deployments.
- Click the Abort button at the bottom of the page.

This will cancel one or more deployments. The computers that have already received the package will not be affected and any other computers will show that the package deployment was aborted before the deployment could occur.

Note: You will **not** be allowed to abort deployments of System Task Packages from PatchLink.

Enable

Click on the Enable button to enable a paused or a disabled deployment. The deployment will then be scheduled to occur according to its schedule type and manner.

Change

This will launch the Deployment Wizard, allowing you to make modifications to any deployment. All deployments can be changed, including deployments of System Task Packages from PatchLink. Note that System Task Packages are automatically assigned to computers, so removing a computer from a deployment of a System Task Package will have no effect (the computer will be re-assigned to the deployment by the Patch Management Server). See Section 8; Creating and Editing Packages: Package Editor Wizard for more information.

Remove

Removes the selected disabled deployments. To remove one or more deployment entries:

- Select one or more deployments
- Click the Remove button.

This will delete the selected package deployments from your Patch Management Server. Removing a deployment will have no affect on computers that have already received the deployment.

Note: you will not be allowed to remove deployments of System Task Packages from PatchLink.

Disable

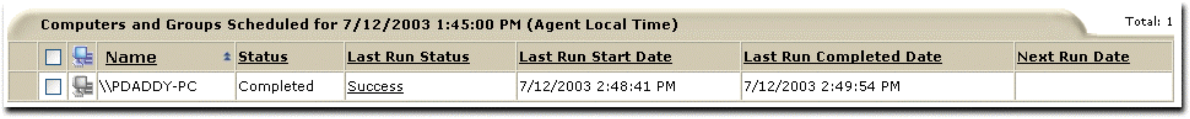
Disables the deployment. The deployment will be paused and no longer deployed to the assigned computers.

Export

Export the deployment data to a comma-separated value (CSV) file.

Deployment Details

The deployment details section displays the assigned computers and groups and the status of the deployment for each. To view the group membership results for the deployment, click on the name of the group, then select that specific deployment package's **Name** link.

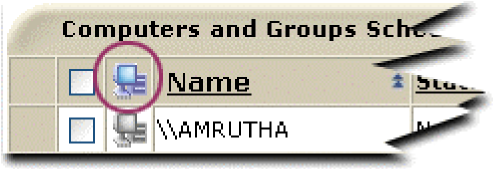


Computers and Groups Scheduled for 7/12/2003 1:45:00 PM (Agent Local Time)

Total: 1

□		Name	Status	Last Run Status	Last Run Start Date	Last Run Completed Date	Next Run Date
□	🖥	\\PDADDY-PC	Completed	Success	7/12/2003 2:48:41 PM	7/12/2003 2:49:54 PM	

Computer Status



Computers and Groups Sche

□	🖥	Name
□	🖥	\\AMRUTHA

Status	Description
🖥	This is an enabled deployment agent.
💤	The agent is sleeping as it is outside its hours of operation.
🔍	This is an enabled detection agent that does not correspond to a registered deployment agent.
🖥	The agent is considered to be offline as it has not contacted the Patch Management Server in more than two intervals (minimum of 15 minutes).

🖥	This agent has been disabled.

Name

This displays the name of the computer or group. The name of the group is also a hyperlink. Clicking the link will display the members of the group and the status of the deployment for each.

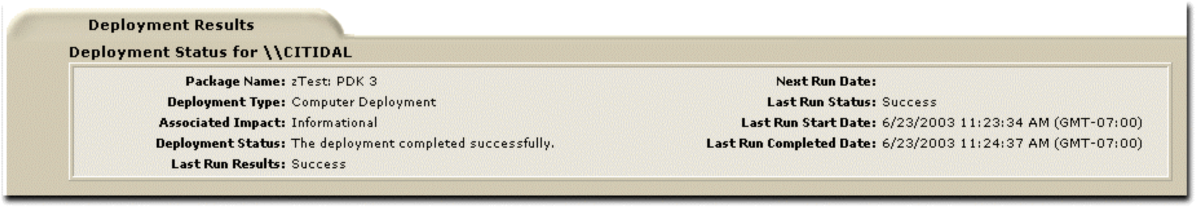
Status

This displays the status of the deployment for the computer or group.

Status	Description
Not Started	The computer or group has not started the deployment. • The deployment start time has not been reached. • The computer has not contacted the Patch Management Server since the start of the deployment. • The deployment limit was full the last time the computer contacted the Patch Management Server. It will try again on its next interval.
In Progress	The computer or the group has started the deployment.
Not Running	The computer or group has finished at least the first occurrence of this recurring deployment, but the next instance of this deployment has not started.
Not Scheduled	Computer members of a group are not assigned the deployment for a group deployment until the computer has contacted the Patch Management Server once the deployment start time has been reached.
Obtaining Package	The Patch Management Server is currently downloading the necessary distribution packages for the deployment. Once they have been cached (and the deployment start time has been reached), the computers will be able to download perform the deployment.
Completed	All computers and groups have finished the deployment.
Disabled	The specific computer or group assignment for this deployment has been disabled.

Last Run Status (link)

This displays the status message from the last time this computer or group performed the deployment. Once the deployment has been performed, the specific results of the deployment for that computer can be displayed by clicking on the status text.



Deployment Results

Deployment Status for \\CITIDAL

Package Name:	zTest: PDK 3	**Next Run Date:**	
Deployment Type:	Computer Deployment	**Last Run Status:**	Success
Associated Impact:	Informational	**Last Run Start Date:**	6/23/2003 11:23:34 AM (GMT-07:00)
Deployment Status:	The deployment completed successfully.	**Last Run Completed Date:**	6/23/2003 11:24:37 AM (GMT-07:00)
Last Run Results:	Success		

- Package Name: This displays the name of the distribution package that was deployed.
- Deployment Type:

  This displays the deployment type.
- Associated Impact: This displays the impact of the associated vulnerability report, if the distribution package is associated to one.
- Deployment Status: This displays the overall deployment status information.
- Last Run Results: This displays the results of the last time the computer performed the deployment.
- Next Run Date: This displays the date when the computer is to perform the deployment again, if the deployment is recurring.
- Last Run Status: This displays the status of the last time the computer performed the deployment.
- Last Run Start Date: This displays the date when the computer last started the deployment.
- Last Run Completed Date: This displays the date when the computer last finished the deployment.

Last Run Start Date

This displays the date when the computer or group last started the deployment.

Last Run Completed Date

This displays the date when the computer or group finished the last deployment.

Next Run Date

This displays the date when the computer is to perform the next deployment.

Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟,⊞) is only available for Microsoft Internet Explorer at this time.

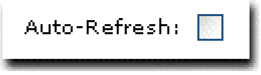
Sort ⤓

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Auto Refresh

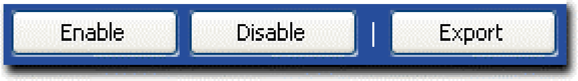


Where present and when selected, the Auto Refresh function automatically refreshes the page every 15 seconds.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Enable

This enables the selected disabled deployment assignments.

Disable

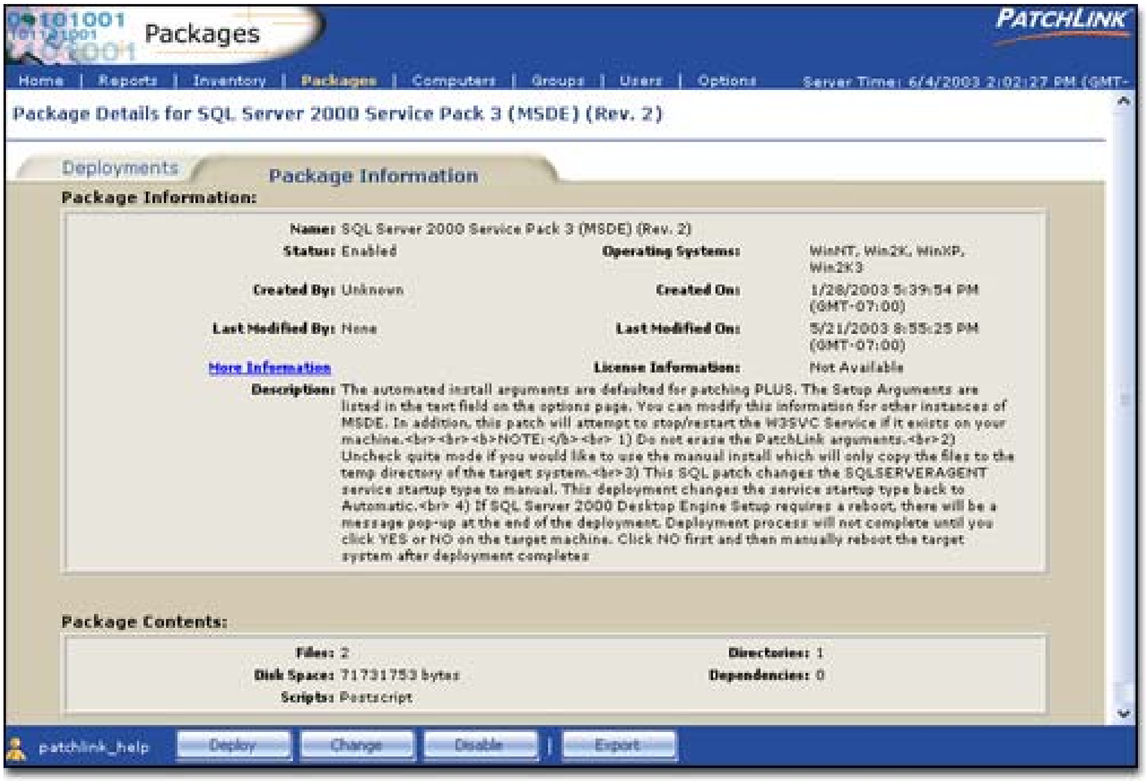
This disables the selected enabled deployment assignments. Disabled deployment assignments cause the individual deployment for the agent or group to not be performed while not affecting the overall deployment. Recurring mandatory baseline-based deployment assignments will automatically be disabled after the deployment has failed three times.

Export

Export the deployment status and details to a comma-separated value (CSV) file. The order of the data is based what the view is sorted on.

Package Information

Click on the Information tab to display the information about the distribution package. The Information section is broken down into two sections: Package Information and Package Content.


Packages
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options
Server Time: 6/4/2003 2:02:27 PM (GMT-
Deployments
Package Information
patchlink_help
Deploy
Change
Disable
Export

Package Details for SQL Server 2000 Service Pack 3 (MSDE) (Rev. 2)

Package Information:

Name: SQL Server 2000 Service Pack 3 (MSDE) (Rev. 2)

Status: Enabled

Operating Systems: WinNT, Win2K, WinXP, Win2K3

Created By: Unknown

Created On: 1/28/2003 5:39:54 PM (GMT-07:00)

Last Modified By: None

Last Modified On: 5/21/2003 8:55:25 PM (GMT-07:00)

More Information

License Information: Not Available

Description: The automated install arguments are defaulted for patching PLUS. The Setup Arguments are listed in the text field on the options page. You can modify this information for other instances of MSDE. In addition, this patch will attempt to stop/restart the W3SVC Service if it exists on your machine.

<b>NOTE:</b>
 1) Do not erase the PatchLink arguments.
2) Uncheck quite mode if you would like to use the manual install which will only copy the files to the temp directory of the target system.
3) This SQL patch changes the SQLSERVERAGENT service startup type to manual. This deployment changes the service startup type back to Automatic.
 4) If SQL Server 2000 Desktop Engine Setup requires a reboot, there will be a message pop-up at the end of the deployment. Deployment process will not complete until you click YES or NO on the target machine. Click NO first and then manually reboot the target system after deployment completes

Package Contents:

Files: 2

Directories: 1

Disk Space: 71731753 bytes

Dependencies: 0

Scripts: Postscript

Package Information

- Name: This displays the name of the distribution package.
- Status: This displays the status of the distribution package.
- Operating Systems: This displays the operating system platforms that this distribution package can deploy to.
- Created By: This displays the user who created the distribution package.
- Created On: This displays when the distribution package was created.
- Last Modified By: This displays the user who last modified the distribution package.
- Last Modified On: This displays when the distribution package was last modified on.
- More Information: This hyperlink will bring up a browser window with a page that displays more information about the distribution package or the vulnerability.
- License Information: If the distribution package requires a license to be agreed to, then this hyperlink will bring up that license page in a browser window. The license will have to be agreed to before (done when creating a deployment for it) a deployment can be created for the package.
- Description: This contains additional information about the distribution package or the patch contained inside.

Package Contents

- Files: This displays the number of files that are downloaded when the distribution package is deployed.

- Directories: This displays the number of directories that are created if they do not exist when the distribution package is deployed.
- Disk Space: This displays the compressed size of the distribution package.
- Dependencies: This displays the number of other distribution packages, which must be installed prior to this distribution in order to be deployed.
- Scripts: This displays the scripts that the distribution package contains.

Action Menu

Deploy

This creates a new deployment of the distribution package.

Change

This allows a User to change the local deployment package. See Section 8; Creating and Editing Packages: Package Editor Wizard for more information.

Disable

Disable the distribution package from being able to be deployed. If the distribution package is already disabled, this button will not be displayed.

Enable

Enable a distribution package so it can be deployed. If the distribution package is already enabled, this button will not be displayed. This enables the selected disabled deployments so they are now available for computer deployment agents to obtain.

Export

Export the deployment data to a comma-separated value (CSV) file.

8. Creating and Editing Packages: Package Editor Wizard

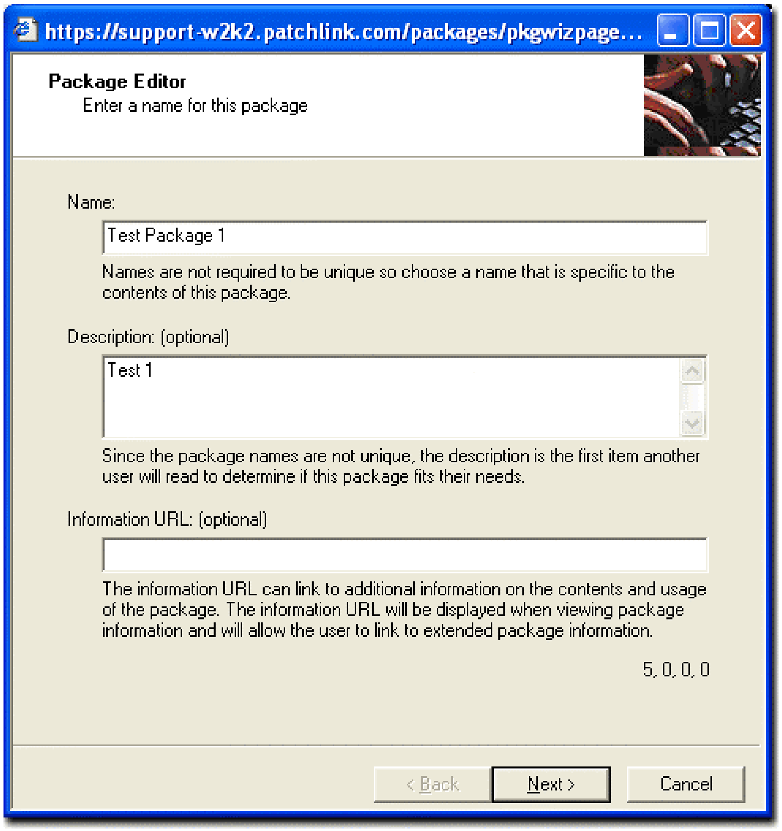
The Package Editor steps through the process of creating or editing packages.

Notes:

- Always test the package within your test network of computers to make sure that there are no unexpected problems before deploying.
- The package editor is an ActiveX control and requires Internet Explorer 5.0 or higher.
- If the Package Editor control has not already been installed on the local browser, it will be downloaded and installed. Once the package editor control has been installed, it will not be downloaded again.

Create or Edit Package

From the **Packages** homepage, click the **Add** button (or the Edit button if you wish to change a previously created package) on the **Action Menu**. The package editor screen is initialized.



https://support-w2k2.patchlink.com/packages/pkgwizpage...

Package Editor

Enter a name for this package

Name:

Test Package 1

Names are not required to be unique so choose a name that is specific to the contents of this package.

Description: (optional)

Test 1

Since the package names are not unique, the description is the first item another user will read to determine if this package fits their needs.

Information URL: (optional)

The information URL can link to additional information on the contents and usage of the package. The information URL will be displayed when viewing package information and will allow the user to link to extended package information.

5, 0, 0, 0

Screen Functions

- Skip

  The **Skip the Introduction** checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Package Editor Wizard is initialized.

- Back

  The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.

- Next

  The **Next** button initializes the wizard's next screen.

- Cancel

  The **Cancel** button closes the wizard.

Name:

Enter a name or title for your package. The name is required and you will not be able to move to the next page of the wizard until a name has been entered. Make your package names descriptive but short and remember that two or more packages may have the same name. You may change this name at a later time by modifying this package.

Description:

An optional description allows you to specify further information about the package. A good practice would be to add additional information as the package is modified, or to provide cautions and/or warnings to the potential user.

- Deployment Options:

  To include a deployment option to indicate a manual installation of the patch is required, please type in ***(manual install)*** in the description field.

  A number of additional deployment options are available here by including them in with the flags delimiter. To add these, add ***(PLFlags: flag list goes here)*** to the description field.

-y	Perform an uninstall (can be used with -m or -q)
-f	Force other applications to close at shutdown
-n	Do not back up files for uninstall
-z	Do not restart the computer when the installation is done
-q	Use quiet mode, no user interaction is required
-m	Use unattended Setup mode
-l	List installed hotfixes
-1	Force the script to reboot when the installation is done
-2	The installer may reboot
-yd	This option (uninstall) is available on the deployment wizard

-fd This option (Force other applications to close) is available on the deployment wizard
-nd This option (Do not backup) is available on the deployment wizard
-zd This option (do not restart) is available on the deployment wizard
-qd This option (quiet mode) is available on the deployment wizard
-md This option (unattended mode) is available on the deployment wizard
-ld This option (list mode) is available on the deployment wizard
-1d This option (force reboot) is available on the deployment wizard (and it is controlled by the script)
-PLDO Deploy only, do not run the script just drop the files
-PLNP Do not show a popup to the user

Notes:

- Many setup and installation packages are different and thus, the above flags are likely to change from package to package.

- To add different flags, simply type in their code. There is an input box available in the deployment wizard to allow the user to see the flags not displayed above.

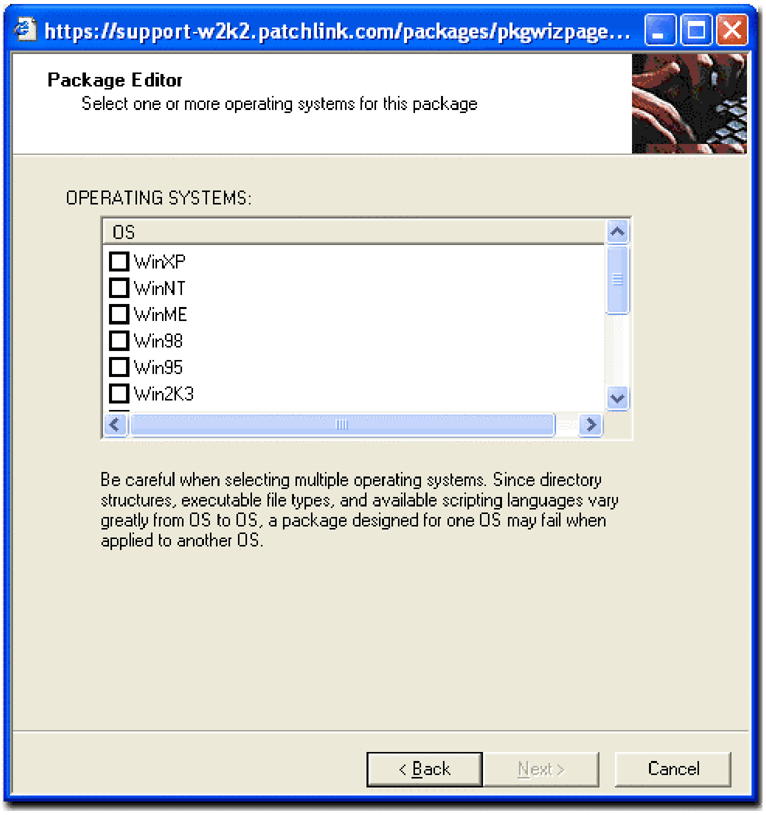
Information URL

The optional information URL can link to additional information on the contents and usage of the package. The information URL will be displayed when viewing package information and will allow the user to link to extended package information.

Click on the **Next** button to initialize the wizard's next screen, which allows you to select operating systems

Operating Systems

The Operating Systems screen allows you to select which Operating Systems you wish to deploy the package to.



https://support-w2k2.patchlink.com/packages/pkgwizpage...
Package Editor
Select one or more operating systems for this package
OPERATING SYSTEMS:
OS
□ WinXP
□ WinNT
□ WinME
□ Win98
□ Win95
□ Win2K3
< Back
Next >
Cancel

Be careful when selecting multiple operating systems. Since directory structures, executable file types, and available scripting languages vary greatly from OS to OS, a package designed for one OS may fail when applied to another OS.

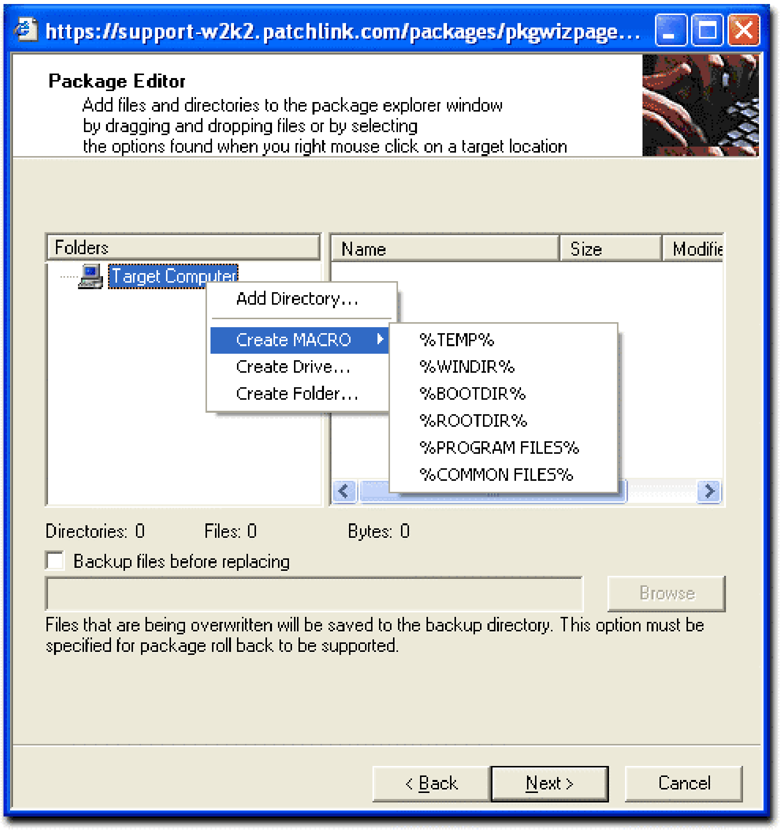
To select an Operating System, click in the checkbox to the left of the Operating System name. You can not click on the **Next** button until you have chosen at least one Operating System.

Note:
Be careful when selecting multiple Operating Systems. Since directory structures, executable file types, and available scripting languages vary greatly from Operating System to Operating System, a package designed for one Operating System may fail when applied to another Operating System.

After you have selected the operating system(s) you wish to deploy to, click the **Next** button.

Adding Files

The File Editor screen allows you to add files to the package and describe where the files will be installed when the package is deployed to the computers on your network.



https://support-w2k2.patchlink.com/packages/pkgwizpage...

Package Editor

Add files and directories to the package explorer window by dragging and dropping files or by selecting the options found when you right mouse click on a target location

Directories: 0 Files: 0 Bytes: 0

□ Backup files before replacing

Files that are being overwritten will be saved to the backup directory. This option must be specified for package roll back to be supported.

A Windows Explorer type window initializes with a directory tree on the left starting at "Target Computer" and a file list on the right. Initially, these are both empty except for the "Target Computer" in the tree view. The Target Computer folder signifies the computer(s) on which this package will be installed. It is automatically created for you and cannot be deleted.

You can begin to add files and/or directories to the package by either:

- Right-Mouse clicking on the "Target Computer" and selecting one of the options from the popup menu.
- Drag directories from a Windows Explorer or My Computer window onto the Target Computer.
- You can also drag files from a Windows Explorer or My Computer window onto any drive or directory in the tree view or into the file list.

Note:
We recommend using the temp directory when delivering the package to your target computer. The files will be deployed to %systemroot%\temp directory (c:\winnt\temp on Windows 2000 Computers).

Once the files you want in the package have been added, or while you are adding them, you can create the directory structure for the package. You can right mouse click on most of the items in either window for options on adding, renaming, or deleting items. You can also drag and drop items from one place on the tree to another or from one window to another in much the same way you would in Windows Explorer. The Right-Mouse Click options are:

Add Directory

This option will bring up a file system browse window, where you can select which directory you wish to add. This option is always available.

Add Files

This option will bring up a file system browser window, where you can select which files you wish to add. This option only becomes available once there is a directory level created (or added) under Target Computer.

Create MACRO

You may create Folders from what are referred to as Macros. Any macro name can be created by placing matching % sign's around a word when using the **Create Folder** option. The file editor allows you to create common macros by using the **Create Macro** option when right-mouse clicking on the Target Computer. Macros can be environment variables that are defined in the System Environment or special macros that only the Client Agent can expand. The following are a few examples of common macros:

%TEMP% The *operating system* temp directory location. *%TEMP%*is a macro that is guaranteed to exist on most systems. If it's not found in the *operating system* environment then it is created. *%TEMP%* typically expands to c:\Windows\Temp, c:\Temp, c:\WinNT\Temp, or /tmp depending on *operating system* and configuration.

%WINDIR% The *operating system* windows directory location. *%WINDIR%* typically expands to c:\Windows.

%BOOTDIR% The *operating system* boot directory location. *%BOOTDIR%* typically expands to c:\.

%ROOTDIR% The *operating system* root directory location. *%ROOTDIR%* typically expands to c:\.

%PROGRAM FILES% The *operating system* program files location. *%PROGRAM FILES%* typically expands to c:\Program Files.

%COMMON FILES% The *operating system* common files location. *%COMMON FILES%* typically expands to c:\Program Files\Common Files.

Not all macros are available on all *Operating Systems*. Please only choose the macros that are available for the operating systems and configurations you are using. This option only becomes available on the directory level directly under *Target Computer*.

Create Drive

If your standard computer installation uses drives other C:\ or this package will be deployed to computers that use drives other than C:\, you can add drives to the package by right mouse clicking on the Target Computer and selecting the Create

Drive option. Once the drive is created you can drag and drop the files or folders as needed to create the correct directory structure.

Create Folder

This option brings up an input window. This window allows you to type in the directory name you wish to create. This option is always available.

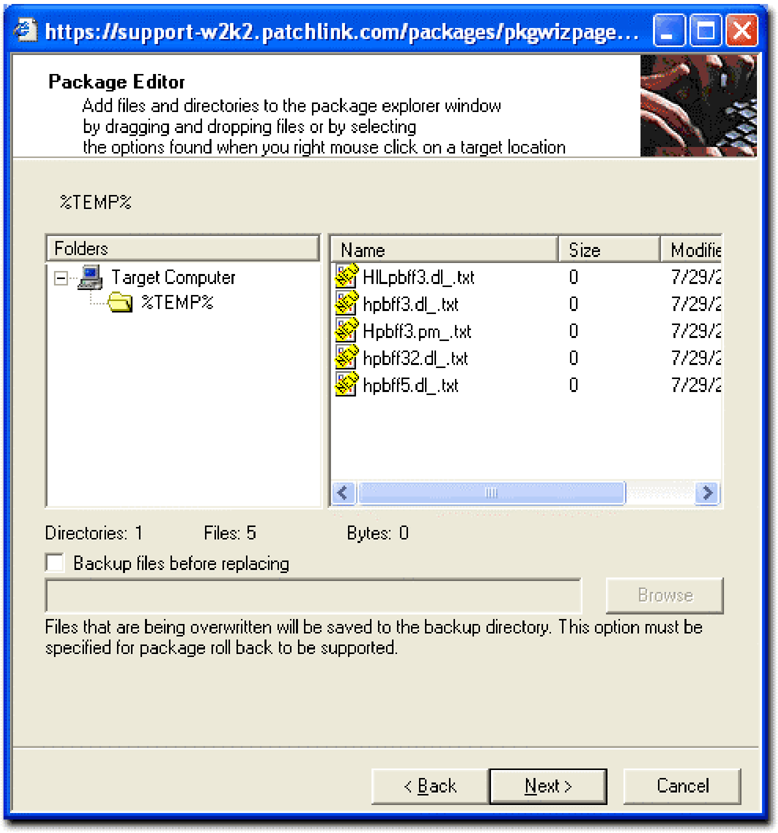
Delete

This option will delete the directory or file you have right-mouse clicked on. This option is only available on directories or files under the Target Computer.

Rename

This option will rename the directory or file you have right-mouse clicked on. This option is only available on directories or files under the Target Computer.

You may place files in any Drive, Folder, or Macro Folder you create. You can rename any file or folder. The package editor will keep track of where the original files were found. No changes will be made to the path names or file names on the computer on which the package editor is running as you are building a representation of where the files will be installed when the package is deployed.



https://support-w2k2.patchlink.com/packages/pkgwizpage...

Package Editor

Add files and directories to the package explorer window by dragging and dropping files or by selecting the options found when you right mouse click on a target location

%TEMP%

Name	Size	Modifie
HILpbff3.dl_.txt	0	7/29/2
hpbff3.dl_.txt	0	7/29/2
Hpbff3.pm_.txt	0	7/29/2
hpbff32.dl_.txt	0	7/29/2
hpbff5.dl_.txt	0	7/29/2

Directories: 1 Files: 5 Bytes: 0

□ Backup files before replacing

Files that are being overwritten will be saved to the backup directory. This option must be specified for package roll back to be supported.

Note:
Please delete all directories that you do not want installed when the package is deployed as the empty directories will be created on the target computer.

Backup Directory

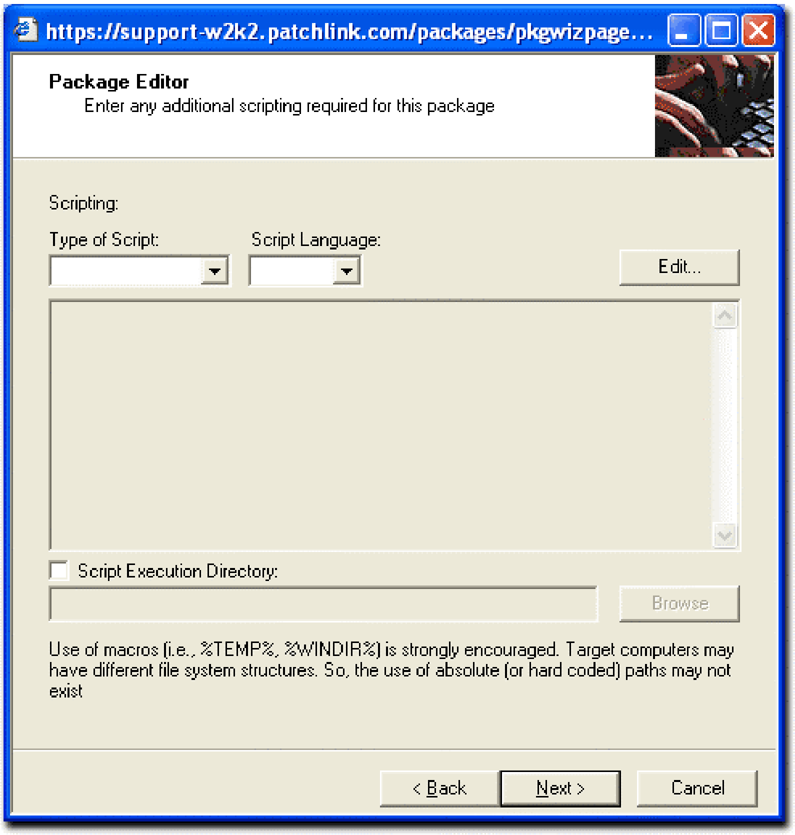
Select "Backup files before replacing" if you wish to create a backup of the files that you are adding to the package. With a backup enabled, when the agent downloads a file it will check to see if the file already exists on the machine. If it does exist the agent will first copy the original file to the backup location then replace the file with the new version from the package. Enter the backup directory path in the text box below the option or use the *Browse* button to search for the path.

Click on the **Next** button to initialize the wizard's next screen, which allows you to create scripts to run at deployment time

Create Scripts

The Create Scripts screen allows you to create scripts that will be run on the computer during the deployment process. A software package can have up to three scripts, one of each type. Scripts are executed in the follow sequence:

- Pre-Script
- Files are downloaded and copied to target locations
- Command Line Script
- Post-Script



https://support-w2k2.patchlink.com/packages/pkgwizpage...

Package Editor

Enter any additional scripting required for this package

Scripting:

Type of Script:

Script Language:

□ Script Execution Directory:

Use of macros (i.e., %TEMP%, %WINDIR%) is strongly encouraged. Target computers may have different file system structures. So, the use of absolute (or hard coded) paths may not exist

Script Types

- Pre-Script

  The Pre-Script can be used to test for a condition of the machine, shutdown a service, etc. For example; you can stop the package rollout in the pre-script by using the SetReturnCode in the PLCCAgent script object. Pre-Scripts can take the form of VBScript or JScript.

- Command Line

  Command Line Scripts are often used to launch executables. The format is the same as a standard CMD or BAT file.

- Post-Script

  Post-Script can be used for any clean-up operations, delete files, start services, run a installer, etc. Post-Scripts can take the form of VBScript or JScript.

Script Editor

- Script Type

  Select the type of script you would like to execute from the Type of Script dropdown box.

- Script Language

  Select scripting type from the Script Language dropdown box.

- Script Execution Directory

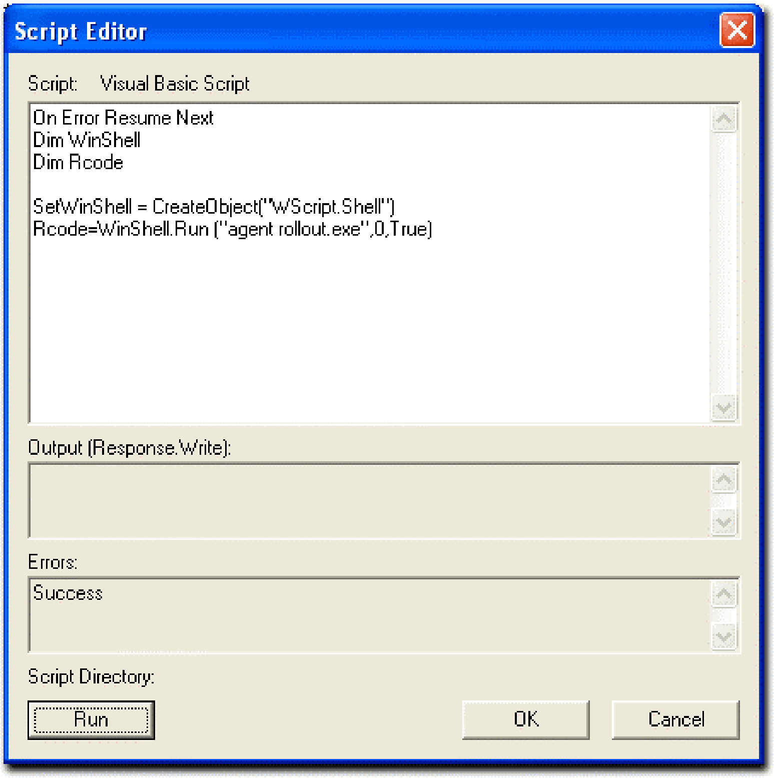
  Select Script Execution Directory if you want your script to run somewhere other than the default location. Enter the backup directory path in the text box below the option or use the **Browse** button to search for the path.

- Edit Script

  Click the **Edit** button. This will display the Script Editor dialog.

  > **Note:**
  > We recommend using a VB Script to tell the agent what to do with the package.
  >
  > Click the **Edit** Button to create your script.

Here is a simple VB Script below that will just execute the package once the package gets delivered to the target computer.



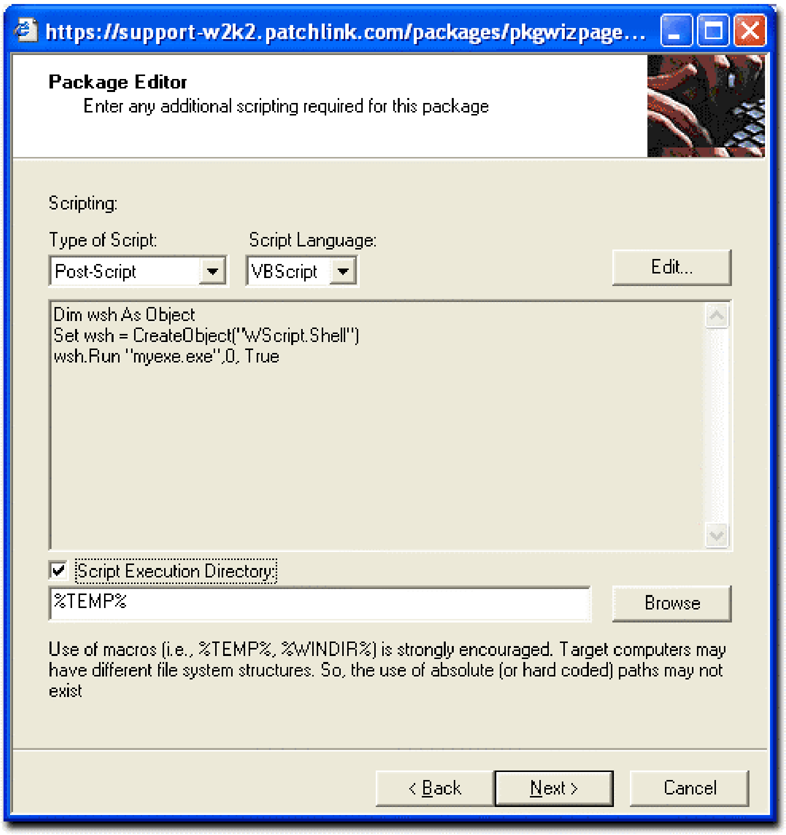
```
On Error Resume Next
Dim WinShell
Dim Rcode

SetWinShell = CreateObject("WScript.Shell")
Rcode=WinShell.Run ("agent rollout.exe",0,True)
```

Output (Response.Write):

Errors: Success

Script Directory:

Test the script by click the **Run** button on the bottom left corner. View the **Errors** field: If the results read “success,” click the **OK** button to close his window and the **Next** button to initialize the next window. If you get a failure message, correct your script until a success message is achieved.



Package Editor

Enter any additional scripting required for this package

Scripting:

Type of Script: Post-Script

Script Language: VBScript

```
Dim wsh As Object
Set wsh = CreateObject("WScript.Shell")
wsh.Run "myexe.exe",0, True
```

☑ Script Execution Directory: %TEMP%

Use of macros (i.e., %TEMP%, %WINDIR%) is strongly encouraged. Target computers may have different file system structures. So, the use of absolute (or hard coded) paths may not exist

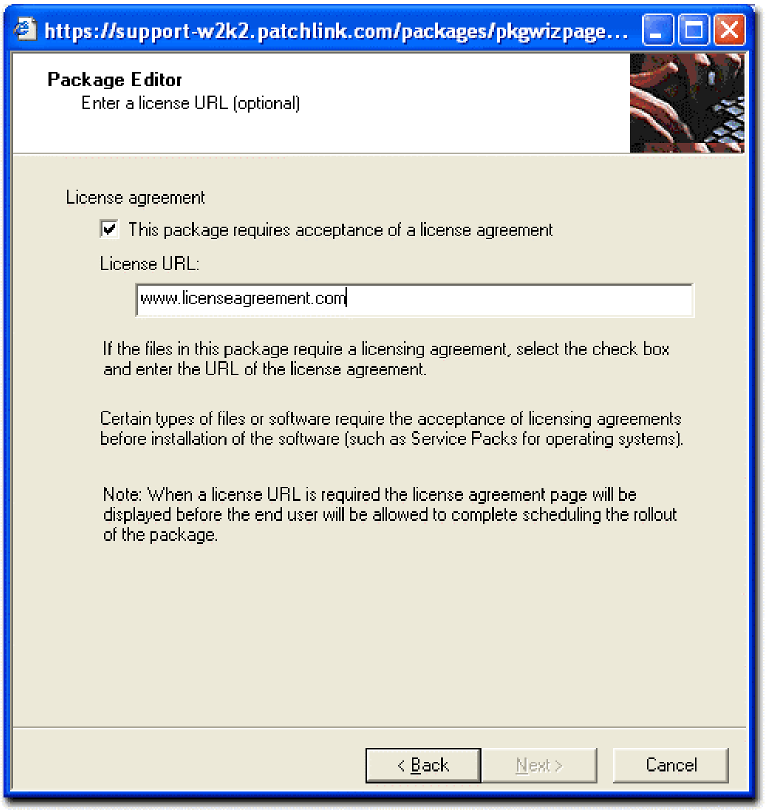
Click the Next button to initialize the wizard’s next screen, which allows you to select package dependencies.

License URL

The License Agreement screen allows you to enter in an optional License URL, which can link to licensing information for the contents of the package.

This is not normally used for packages that are in-house file distributions. It is primarily for packages containing items such as operating system service packs, device drivers, etc. The License URL will be displayed when viewing package information and will allow the user to link to the license information.

Simply select the License Agreement checkbox and type in the URL destination address of the License Agreement.



Package Editor

Enter a license URL (optional)

License agreement

☑ This package requires acceptance of a license agreement

License URL:

www.licenseagreement.com

If the files in this package require a licensing agreement, select the check box and enter the URL of the license agreement.

Certain types of files or software require the acceptance of licensing agreements before installation of the software (such as Service Packs for operating systems).

Note: When a license URL is required the license agreement page will be displayed before the end user will be allowed to complete scheduling the rollout of the package.

When scheduling a deployment of the package, the license page will be displayed, and the end user will be required to click the Accept button to complete scheduling the deployment.

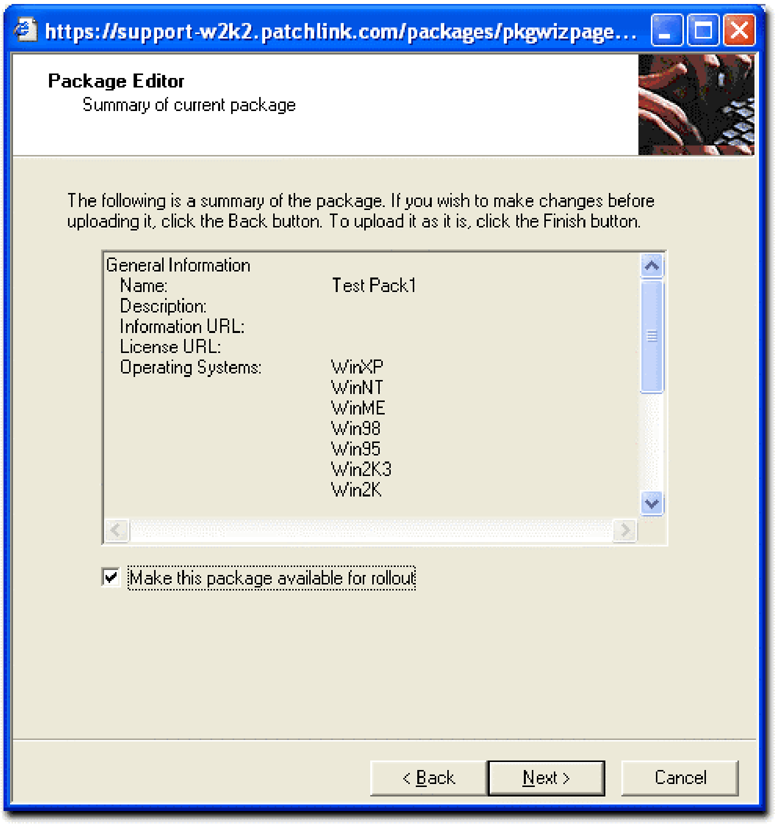
After entering the License URL (optional), click the Next button to initialize the wizard's next screen, which is a summary of the package.

Note:

If you select the License Agreement checkbox, you must type in the URL destination address of the License Agreement to initialize the **Next** button.

Summary

The Summary screen displays a simple summary of the package before the package created or the changes are committed.



Package Editor
Summary of current package

The following is a summary of the package. If you wish to make changes before uploading it, click the Back button. To upload it as it is, click the Finish button.

```
General Information
  Name:                     Test Pack1
  Description:
  Information URL:
  License URL:
  Operating Systems:        WinXP
                            WinNT
                            WinME
                            Win98
                            Win95
                            Win2K3
                            Win2K
```

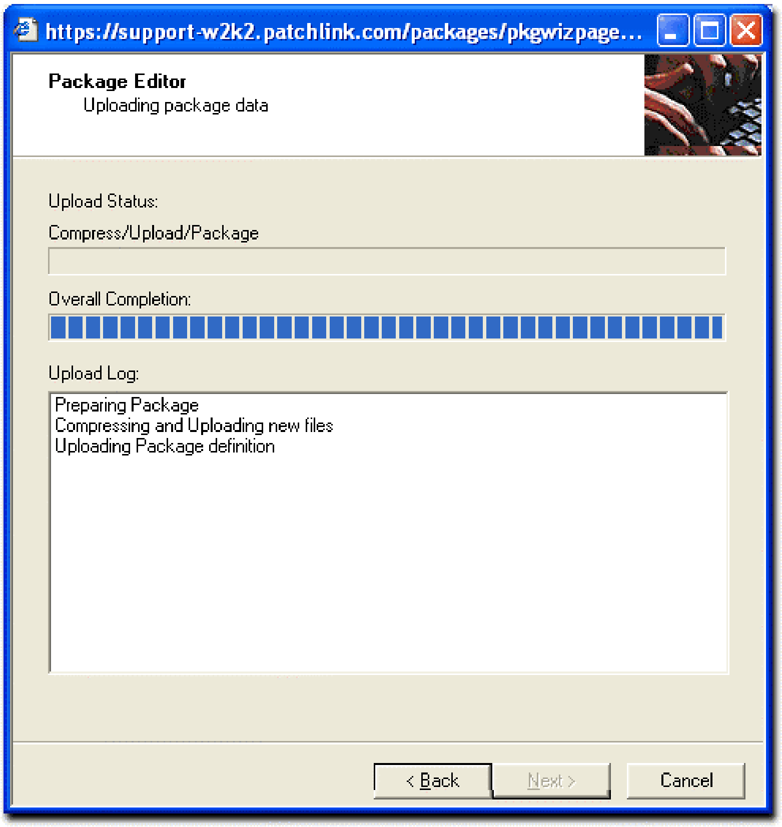
☑ Make this package available for rollout

Selecting the **Make this package available for rollout** checkbox, will enable the package to show up in the list of available packages / available for deployment (once the package is created). You may wish to de-select this item if you are creating a skeleton package that will have additional files or details added at a later date or do not wish to have the package scheduled for deployment at this time.

Click the **Next** button to initialize the wizard’s next screen, which will commit the changes, create the package, and upload the package data.

Upload

The Upload screen appears verifying that the data is unpacking and uploading.



Package Editor

Uploading package data

Upload Status:

Compress/Upload/Package

Overall Completion:

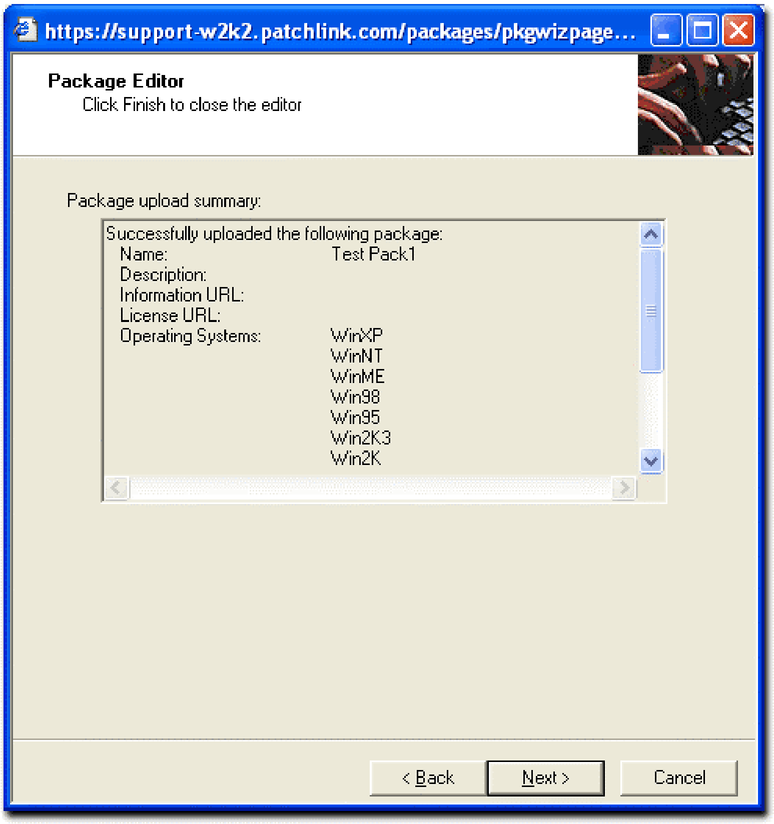
Upload Log:

```
Preparing Package
Compressing and Uploading new files
Uploading Package definition
```

Once the Upload is complete, the **Next** button will initialize. Click the **Next** button to initialize the Updated Summary screen.

Updated Summary

The final screen displays a simple summary on the saving of the package, and whether it was successful or failed. If a failure occurred, the error code and description will be displayed.



Package Editor

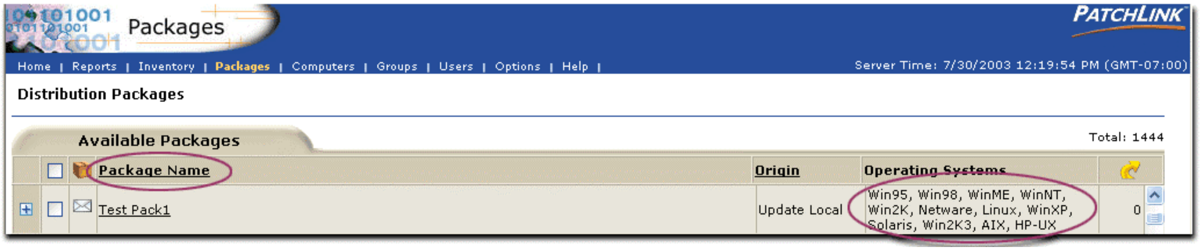
Click Finish to close the editor

Package upload summary:

```
Successfully uploaded the following package:
   Name:                Test Pack1
   Description:
   Information URL:
   License URL:
   Operating Systems:   WinXP
                        WinNT
                        WinME
                        Win98
                        Win95
                        Win2K3
                        Win2K
```

Click the **Finish** button to close the wizard and complete the operation.

Upon refreshing of the **Packages** page, you can view your package by the name you gave it upon creating it, and view the operating systems that you chose to deploy to during the patch building process.



Packages
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |

Server Time: 7/30/2003 12:19:54 PM (GMT-07:00)

Distribution Packages

Available Packages

Total: 1444

	□		Package Name	Origin	Operating Systems	
⊞	□	✉	Test Pack1	Update Local	Win95, Win98, WinME, WinNT, Win2K, Netware, Linux, WinXP, Solaris, Win2K3, AIX, HP-UX	0

9. Deploying Packages: Schedule Deployment Wizard

Use this section in congruence with Section 7; Packages, as Section 8 describes the intricacies of packages, deployments, events and statistics, while Section 9 focuses on the physicality of the actual package deployment.

After the Patch Management Server is installed and agents are deployed, it is necessary to conduct some analysis of the vulnerabilities present within the computers on your network.

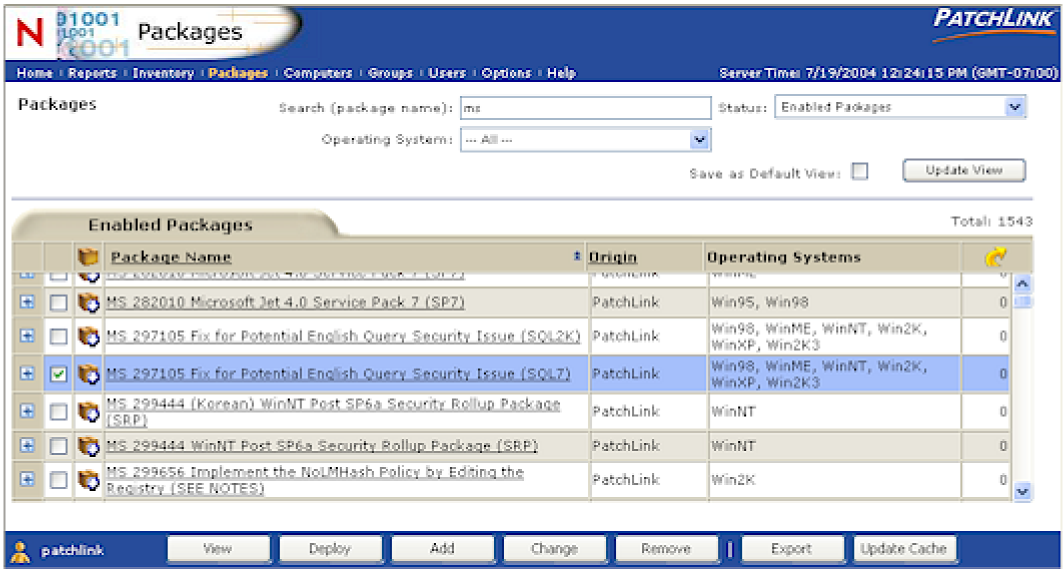
When conducting initial remediation, it is wise to begin with service packs and cumulative patches first, as this will significantly decrease the number of individual patches that need deployment.

Once the necessary computers are fully patched, it will only be necessary to deploy the new patches that are made available each week.

The Deployment Wizard steps through the process of selecting computers that will receive that package, select a one time or recurring deployment, and select the date and time to deploy the package.

Note:
Always test the package within your test network of computers to make sure that there are no unexpected problems before deploying.

Select the patch you wish to deploy by clicking on the bulletin hyperlink.



Server Time: 7/19/2004 12:24:15 PM (GMT-07:00)

Packages

Search (package name): ms

Status: Enabled Packages

Operating System: --- All ---

Save as Default View: □

Enabled Packages

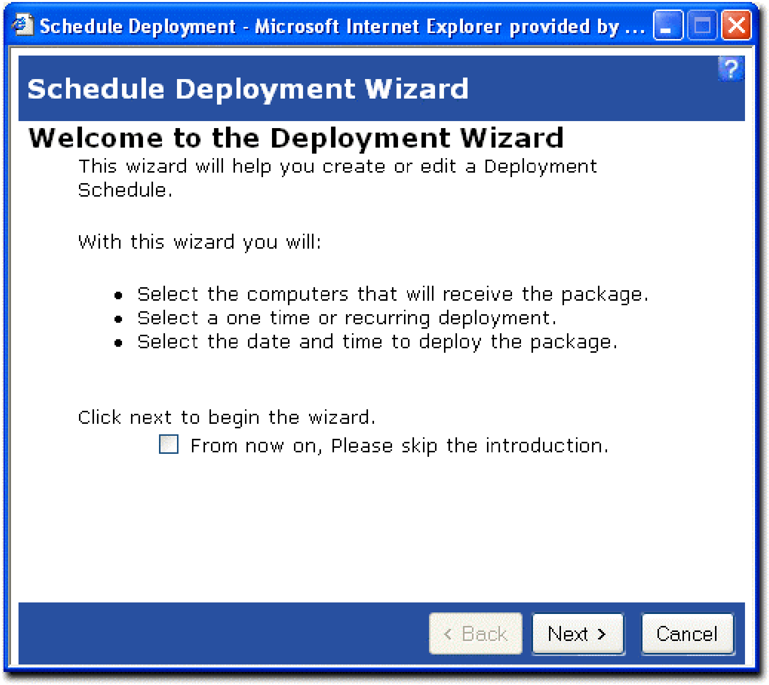
Total: 1543

		Package Name	Origin	Operating Systems	
⊞	□	MS 282010 Microsoft Jet 4.0 Service Pack 7 (SP7)	PatchLink	Win95, Win98	0
⊞	□	MS 297105 Fix for Potential English Query Security Issue (SQL2K)	PatchLink	Win98, WinME, WinNT, Win2K, WinXP, Win2K3	0
⊞	☑	MS 297105 Fix for Potential English Query Security Issue (SQL7)	PatchLink	Win98, WinME, WinNT, Win2K, WinXP, Win2K3	0
⊞	□	MS 299444 (Korean) WinNT Post SP6a Security Rollup Package (SRP)	PatchLink	WinNT	0
⊞	□	MS 299444 WinNT Post SP6a Security Rollup Package (SRP)	PatchLink	WinNT	0
⊞	□	MS 299656 Implement the NoLMHash Policy by Editing the Registry (SEE NOTES)	PatchLink	Win2K	0

From the list of computers that require this patch, click the checkbox next to the item to select, and click on the **Deploy** button to launch the **Schedule Deployment Wizard**

Welcome

The welcome screen appears.



Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

Welcome to the Deployment Wizard

This wizard will help you create or edit a Deployment Schedule.

With this wizard you will:

- Select the computers that will receive the package.
- Select a one time or recurring deployment.
- Select the date and time to deploy the package.

Click next to begin the wizard.

□ From now on, Please skip the introduction.

Screen Functions

- Skip

  The Skip the Introduction checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Schedule Deployment Wizard is initialized.

- Back

  The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.

- Next

  The **Next** button Initializes the wizard's next screen; the package selection page. This screen will appear if you have not previously selected something to deploy. If you have selected a vulnerability report or package, then the next button will take you directly the next screen; the individual computer and computer group selection page.

- Cancel

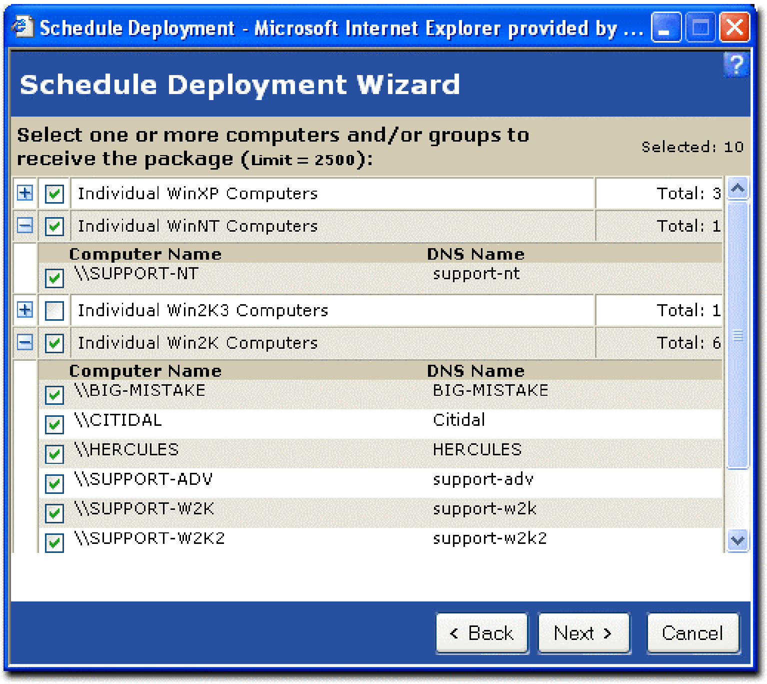
  The **Cancel** button closes the wizard.

Click the **Next** button to initialize the **Package Selection** screen.

Package Deployment Target Selection Actions

This screen displays a list of all individual computers and computer groups that you can deploy to based upon:

- The operating system supported by the package or vulnerability report being deployed.
- The agents which the vulnerability report are applicable to (only if deploying a vulnerability report).



Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

Select one or more computers and/or groups to receive the package (Limit = 2500):

Selected: 10

⊞	☑	Individual WinXP Computers	Total: 3
⊟	☑	Individual WinNT Computers	Total: 1
		Computer Name	**DNS Name**
	☑	\\SUPPORT-NT	support-nt
⊞	□	Individual Win2K3 Computers	Total: 1
⊟	☑	Individual Win2K Computers	Total: 6
		Computer Name	**DNS Name**
	☑	\\BIG-MISTAKE	BIG-MISTAKE
	☑	\\CITIDAL	Citidal
	☑	\\HERCULES	HERCULES
	☑	\\SUPPORT-ADV	support-adv
	☑	\\SUPPORT-W2K	support-w2k
	☑	\\SUPPORT-W2K2	support-w2k2

In addition to the individual computers and system-created computer groups, there is a list of all the user created computer groups present on the Patch Management Server. For system and user based group deployments, the determination of which member computers get the deployment is only determined at the start of the deployment.

Initially, the operating systems, the system groups and the user groups are displayed along with the total number of client agents associated with each of them.

To select all computers of a given operating system, click in the checkbox next to each operating system category. (Limit = 2500)

Click the ⊞ to display and select additional or individual computers within a group. All of the computers for that category will be displayed by computer name and DNS name. Hovering the mouse over the computer name will display the description and hovering over the DNS name will display the IP address. If there is no DNS name provided, the IP address will be displayed.

A deployment requires that at least one computer is selected. The wizard will not advance to the next step until at least one computer is selected. If the wizard is being used to deploy a package associated with a report, then the computers that were selected from the report page will be selected automatically.

At the top right corner of the wizard, the total number of selected computers will be displayed.

If launching the deployment wizard from the report page when the report does not have a package associated with it, it will be possible to select a package or packages that do not cover all of the operating systems of the computers. In this case, only the computers that match the operating systems of the package will be added to the deployment.

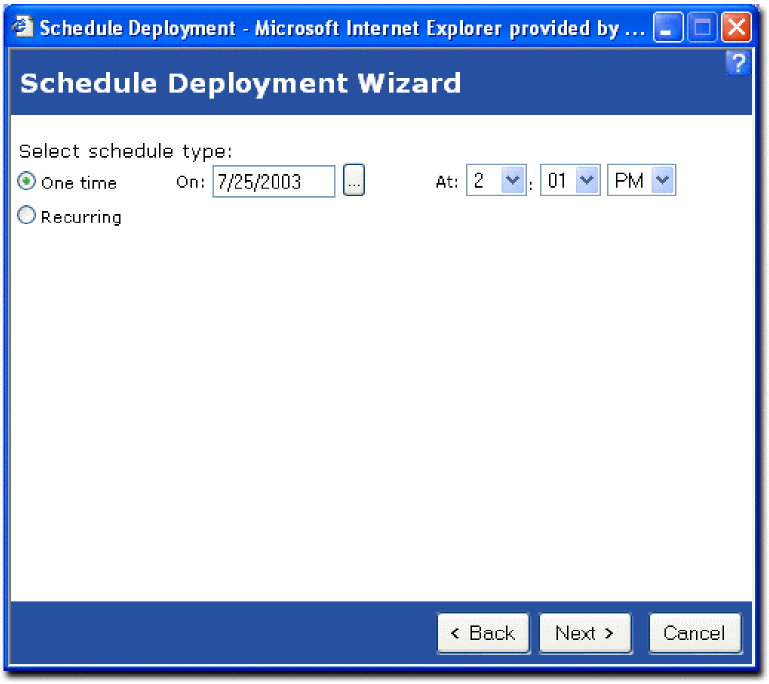
Notes:
This screen does not show up if you have previously selected the package or vulnerability report to deploy.

Selecting the checkbox selects all computers in the group.

Click on the **Next** button to initialize the **Deployment Schedule** screen.

Deployment Schedule

The Deployment Schedule screen contains scheduling information.


Schedule Deployment - Microsoft Internet Explorer provided by ...
Schedule Deployment Wizard
?
< Back
Next >
Cancel

Select schedule type:

● One time On: 7/25/2003 ... At: 2 : 01 PM

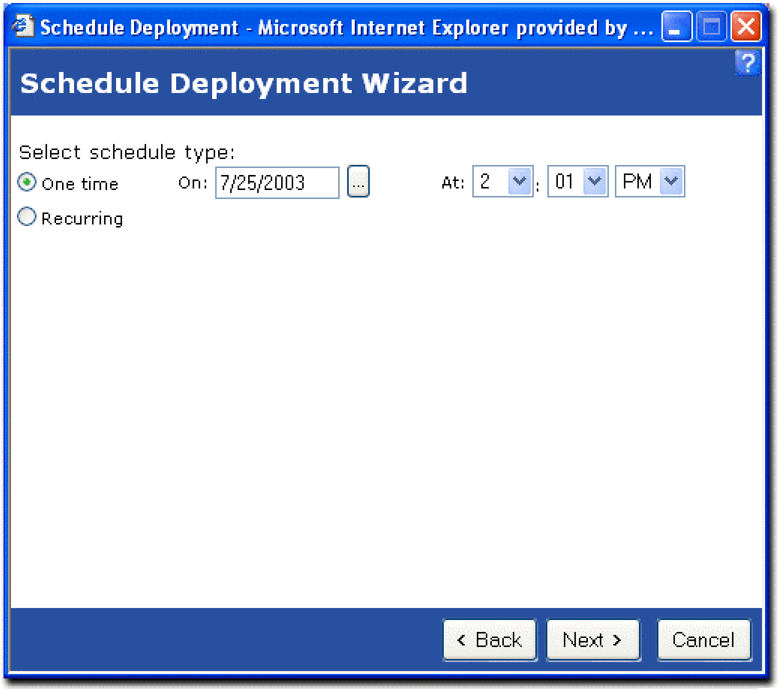
○ Recurring

Schedules can be one of the two types:

One Time: (Default)

A one time schedule will start deployments on the selected day at the selected time. If a one time deployment is scheduled for a date and time in the past, then the computers will start the deployment the next time they contact the Patch Management Server.

Note: A Select schedule type of **At Registration** appears at the initial deployment of Packages screen. This allows you to deploy the packages upon them registering to a Patch Management Server. An **At Registration** task is only valid for System Packages and will run when a client agent registers at the server. The **At Registration** option is only shown for System Package distributions.

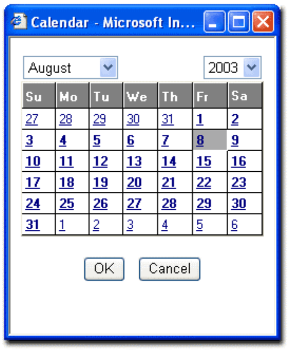

Schedule Deployment - Microsoft Internet Explorer provided by ...
?
< Back
Next >
Cancel

Schedule Deployment Wizard

Select schedule type:

● One time On: 7/25/2003 ... At: 2 : 01 PM

○ Recurring



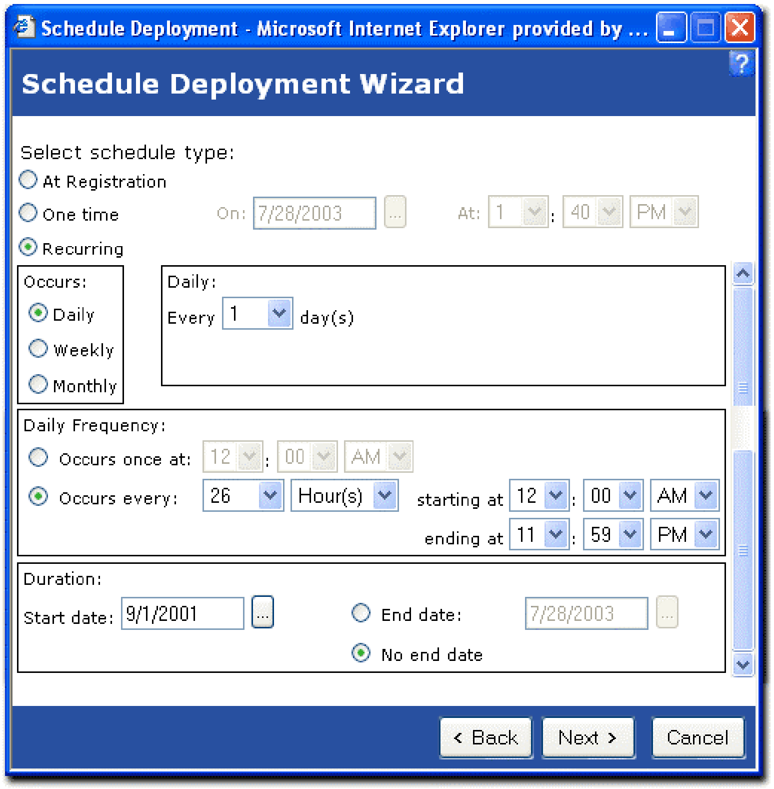
August 2003

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Click on the Calendar Launch Button ... to initialize the calendar and set the desired date. Click on the hour, minute, and AM/PM drop down menus to select the desired time.

Recurring

A recurring task will start on the given start date and will occur at the given interval and will stop if a stop day is specified. Click on the radio button to initialize the recurring task window.



Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

Select schedule type:

○ At Registration

○ One time   On: 7/28/2003 ...   At: 1 : 40 PM

● Recurring

Occurs:
○ Daily (selected ●)
○ Weekly
○ Monthly

Daily:
Every 1 day(s)

Daily Frequency:
○ Occurs once at: 12 : 00 AM
● Occurs every: 26 Hour(s)   starting at 12 : 00 AM
ending at 11 : 59 PM

Duration:
Start date: 9/1/2001 ...   ○ End date: 7/28/2003 ...
● No end date

Recurring deployments can be scheduled to occur either:

- Daily
- Weekly (You can choose the days in a week when you want the task to recur.)
- Monthly You can choose from a day number in a month (first day in the month’s chosen) or a day in a week of every month (first Monday in the month’s chosen)

Each of these can also be scheduled to occur at a specific time during the day or recurring several times during the day at a given interval and between certain hours. Finally each of these can be scheduled to end on a given day or continue with no ending date.

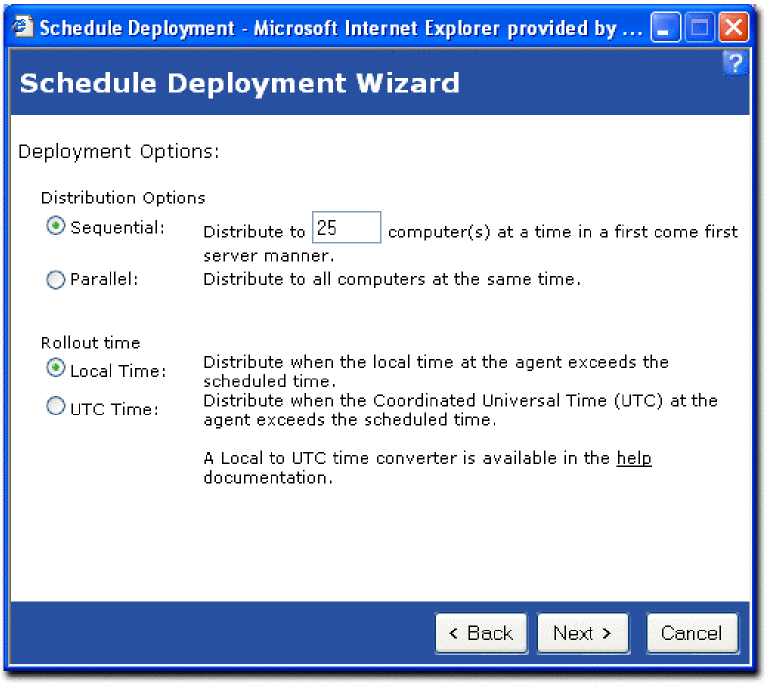
- At Registration

  An “at registration” task is only valid for System Packages and will run when a client agent registers at the server. The “at registration” option is only shown for System Package distributions.

After you have made or modified your schedule selections, click the **Next** button to initialize the **Deployment Options** screen.

Deployment Options

A deployment has two very distinct sets of options to define how the deployment is going to behave. These sets of options are: Distribution and Rollout Time.



Schedule Deployment - Microsoft Internet Explorer provided by ...
Schedule Deployment Wizard
?
< Back
Next >
Cancel

Deployment Options:

Distribution Options

● Sequential: Distribute to 25 computer(s) at a time in a first come first server manner.

○ Parallel: Distribute to all computers at the same time.

Rollout time

● Local Time: Distribute when the local time at the agent exceeds the scheduled time.

○ UTC Time: Distribute when the Coordinated Universal Time (UTC) at the agent exceeds the scheduled time.

A Local to UTC time converter is available in the help documentation.

Distribution Options

- Sequential

  Only deploy to a maximum number computers at a time, on a first-come first-serve basis. The maximum limit is configurable for all deployments and is defaulted to 25 computers. If a computer takes longer than an hour to complete the deployment, it is no longer counted against the limit (example: the computer may have been turned off). As computers finish the deployment other computers will begin to receive the deployment, as long as the maximum number is not exceeded.

  A sequential deployment will both limit the bandwidth required from the server and infrastructure, as well as halt the deployment should an error occur to a bad patch or other deployment problem.

- Parallel

  Deploy to all computers as they communicate with the Patch Management Server to get their next deployment

  Use the parallel option if bandwidth is not a consideration, and automatic halt features are not required.

Rollout Time Options

A deployment will only be given to a computer when the computer's given time has exceeded the start time of the deployment.

- Local Time

  Local time will vary depending on the time zone of your location (daylight savings time may apply). When the computer communicates with the Patch Management Server, the local time of the computer is checked to see if there are any deployments available. If you have three computers (each in their own time zone) that communicate with the Patch Management Server at the same time, each start the deployment when their local time has exceeded the start time of the deployment. Simply put, they will each start the deployment at different times with respect to the Patch Management Server.

- UTC Time

  Coordinated Universal Time (UTC), is a standardized measurement of time that does not depend on your local time zone. The time in one geographical location is exactly the same time in another. UTC is also known as World Time, Z Time, or Zulu Time. When the computer communicates with the Patch Management Server, the UTC time of the computer is checked to see if there are any deployments available. If you have three computers (each in their own time zone) that contacted the Server at the same time, each will start when the UTC time has exceeded the start time of the deployment. Simply put, they will each start the deployment at the same time with respect to the Patch Management Server.

Notes:

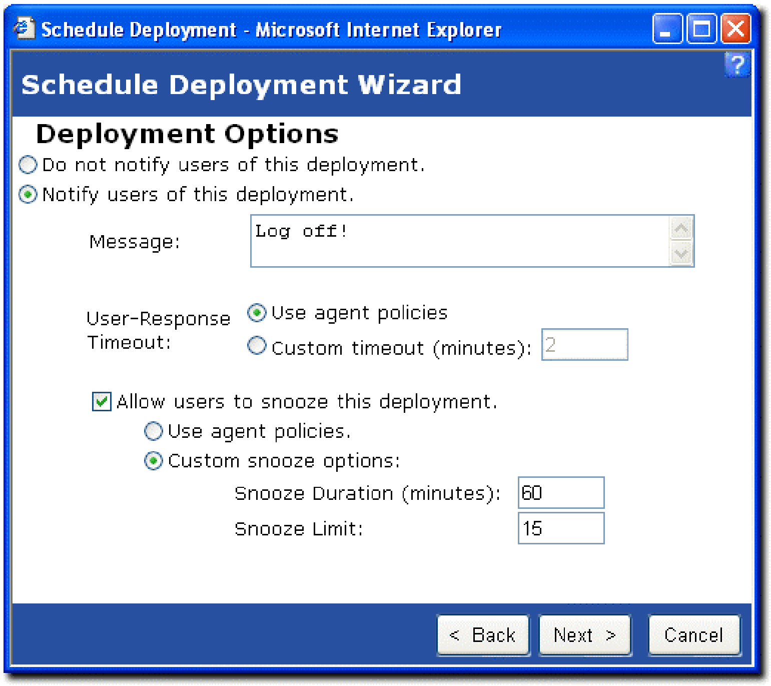
- The start time for both of these deployment types depend on the time given by the computer; so the accuracy of the computer's internal clock is important. Hence, when a computer's internal clock is slow, fast or incorrectly set, the scheduled start time of the deployment for that computer is affected.

- Deployments created to a group will always default the time to UTC since the determination of which members of the group get the deployment is not calculated until the start of the deployment.

After you have made your option selections, click the **Next** button to initialize the next **Deployment Options** screen.

Deployment Options

The **Deployment Options** screen initializes. Here you can select additional deployment options, notes, or details.



Schedule Deployment - Microsoft Internet Explorer

Schedule Deployment Wizard

Deployment Options

○ Do not notify users of this deployment.

● Notify users of this deployment.

Message: Log off!

User-Response Timeout: ● Use agent policies ○ Custom timeout (minutes): 2

☑ Allow users to snooze this deployment.

○ Use agent policies.

● Custom snooze options:

Snooze Duration (minutes): 60

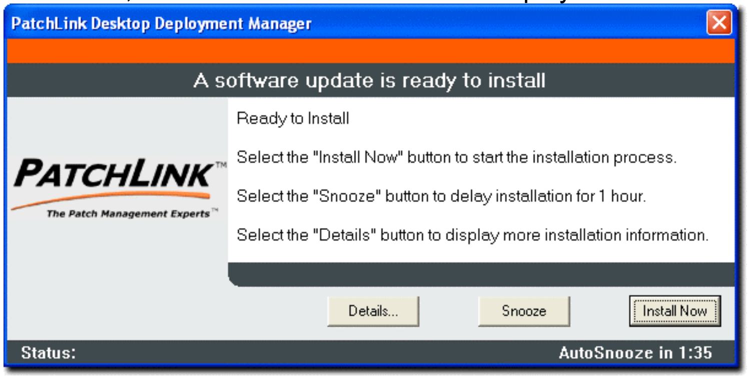
Snooze Limit: 15

Do not notify users of this deployment

If selected, the user will not be notified of the deployment, it will happen automatically.

Notify users of this deployment

If selected, the user will be notified of the deployment



PatchLink Desktop Deployment Manager

A software update is ready to install

Ready to Install

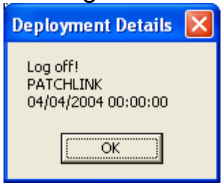
Select the "Install Now" button to start the installation process.

Select the "Snooze" button to delay installation for 1 hour.

Select the "Details" button to display more installation information.

Status: AutoSnooze in 1:35

Message: a message may be inserted into the message text field to alert the user.



Deployment Details

Log off!
PATCHLINK
04/04/2004 00:00:00

User Response Timeout:

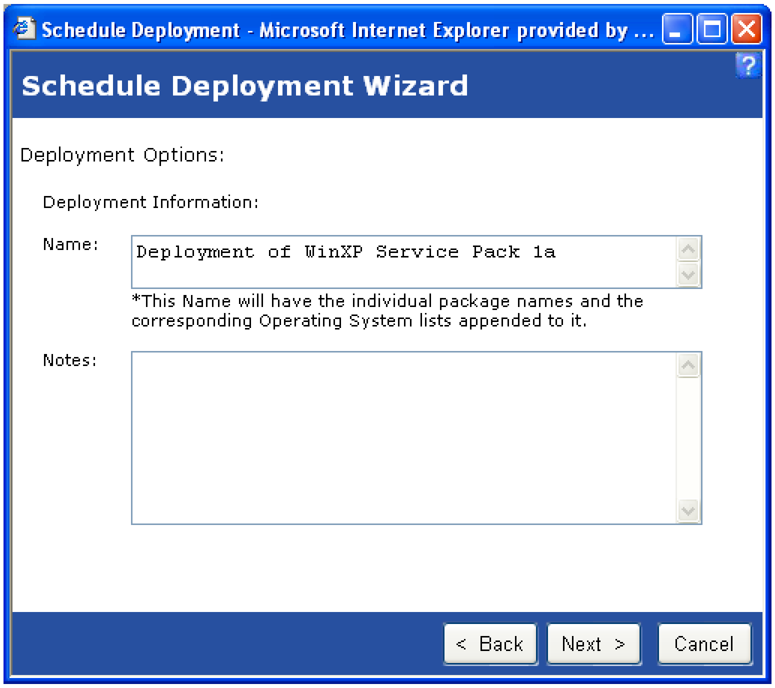
Use Agent Policies: if selected, this uses agent polices will use the pre defined agent policies.

Custom Timeout (minutes): if selected, a minute duration may be input into this field to allow a timeout user response period. If not addressed by the user in the inserted time, the package will be deployed.

After you have made your option selections, click the **Next** button to initialize the next **Deployment Options** screen.

Deployment Options

The **Deployment Options** screen initializes. Here you can select additional deployment options, notes, or details.



Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

Deployment Options:

Deployment Information:

Name: Deployment of WinXP Service Pack 1a

*This Name will have the individual package names and the corresponding Operating System lists appended to it.

Notes:

- Name: This is the name given to this deployment. The name given should be descriptive enough to summarize the deployment. This is required.

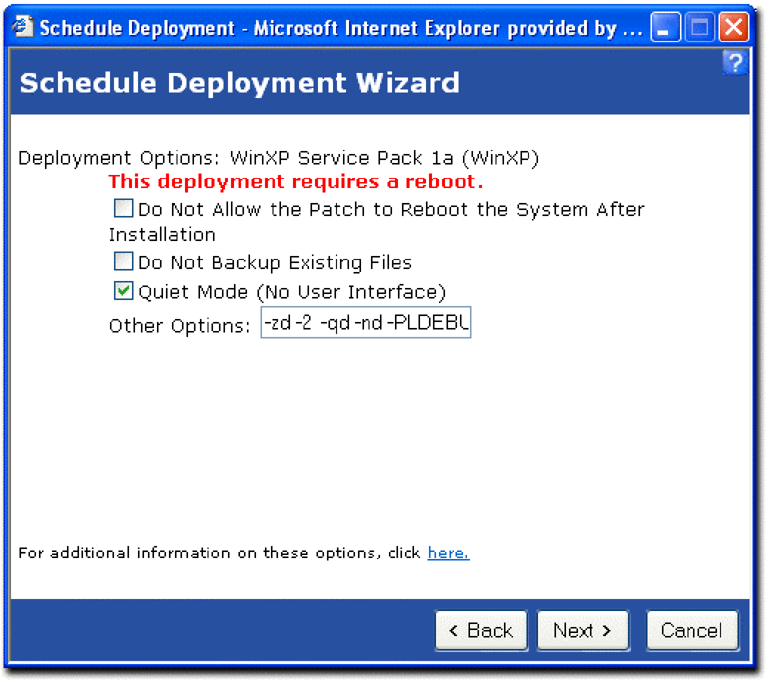
- Notes: This includes any additional information about the deployment that you want to note down like the expected results of this deployment, the effect that this deployment can have on any future deployments.

  If there are no package flag options to choose from for the item you are deploying, clicking the **Next** button initializes the License Agreement Page **or** the Deployment Information Page, depending if there is a license agreement for what you are deploying.

Click the **Next** button to initialize an additional Deployment Options screen.

Deployment Flags

Deployment options include options related specifically to the installation process during the deployment. The deployment comes pre-configured with these options to optimize the deployment's performance. These options are selected based on the behavior of the package's installer program and previous testing by PatchLink personnel. If more than one deployment package is available for deployment, then there will be multiple screens that you must go through to verify these options. These deployment options are placed in to a variable used by the deployment's post script.



Schedule Deployment - Microsoft Internet Explorer provided by ...
?

Schedule Deployment Wizard

Deployment Options: WinXP Service Pack 1a (WinXP)

This deployment requires a reboot.

☐ Do Not Allow the Patch to Reboot the System After Installation

☐ Do Not Backup Existing Files

☑ Quiet Mode (No User Interface)

Other Options: -zd -2 -qd -nd -PLDEBL

For additional information on these options, click here.

Hotfix Setup Programs

See Microsoft Windows 2000 Hotfix Installation and Deployment Guide for additional information on Microsoft specific command-line parameters for Hotfix Setup Programs. These options are:

- **This deployment requires a reboot.**

This item shows up only if the package which is being installed may require a reboot of the operating system in order to finish the deployment. This reboot function is not controlled by the deployment script, but can be turned off by selecting the **Do Not Reboot** checkbox

- Uninstall (When available from vendor)

  This option will tell the package's installer to uninstall the package from the selected computers.

  Note:
  If multiple packages replace the same file and you want to successfully return your system to its original state, you must remove the most recently installed package first.
- Force Applications Close

  This option will tell the package's installer to force all applications to close when the computer is in the shutdown process.
- Force a Reboot

  This option will tell the deployment script that a reboot *must* be performed before this deployment is complete.

  Notes:
- The script is controlling the reboot in this situation and a reboot will occur regardless if the installer requires it or not.
- This option can not be selected if the Do Not Reboot option is checked.

Do Not Reboot

This option will tell the package's installer to not reboot once the package is installed on to the computer. If the notice that the deployment requires a reboot is shown it is recommended that you do not select this option. If this option is selected anyway, do NOT install any additional programs until a reboot happens. Do not expect the package to be available until a reboot occurs, since many installations require a reboot to finish the installation process.

Note:
This option can not be selected if the **Force a Reboot** option is checked

Do Not Backup Existing Files

This option will tell the package's installer to not backup the existing files. These files are used by the uninstaller. Do not select this option if you wish to uninstall the package at a later time.

The installer controls this action and should not be confused with the deployment backup option, which will only back up the deployment package (not the installed files from the package).

Quiet Mode (No User Interface)

This option will tell the package's installer to function in quiet mode. This mode will not produce any user interfaces (in case any user is logged on to the computer at the deployment time) or require user interaction during the deployment process.

Unattended Setup Mode

This option will tell the package's installer to function in unattended mode. This option does not require any user interaction during the deployment process.

List Installed Hotfixes

This option will tell the package's installer to return a list of installed hotfixes on the computer.

Note:
The Detection Agent and Inventory function provide an additional, more in-depth, listing of what is installed on to a computer.

Other Options

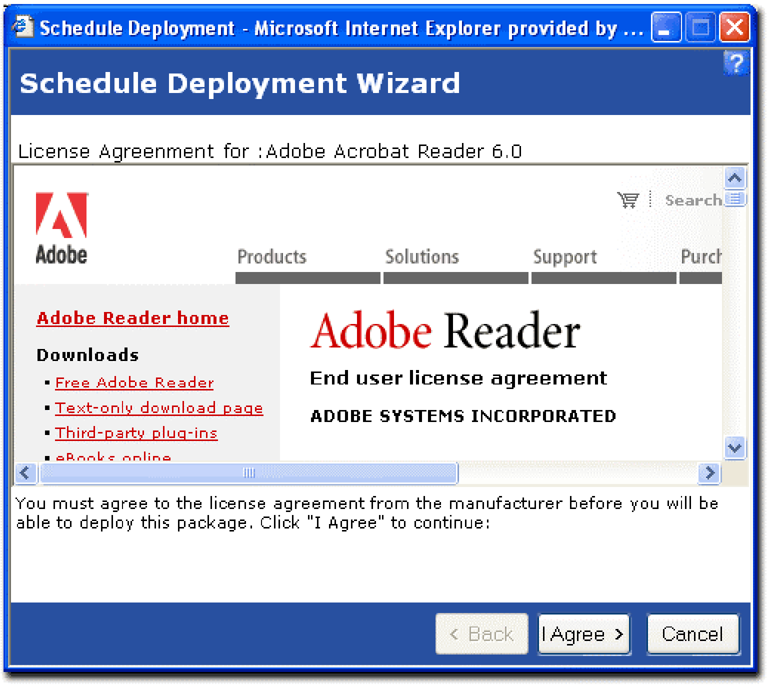
This field will display the list of other extra flags that may be used for the specific deployment, but are not generic enough for all deployments to allow it to be added as a separate flag. Generally this is used for customer deployments or special case scenarios.

Note:
The *-2* flag is often found here to indicate that the deployment's installer program may require a reboot depending if the operating system requires it.

Click the **Next** button to initialize the wizard’s next screen, which handles license validation if this package requires one. If the package does not require a license validation, the **Next** button initializes the wizard’s next screen, which allows you to define some deployment information.

Schedule Deployment Wizard: License Information

The Deployment Wizard License Information page is displayed only when a license URL is associated with the package being deployed. It will show the license URL in an imbedded frame.


Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

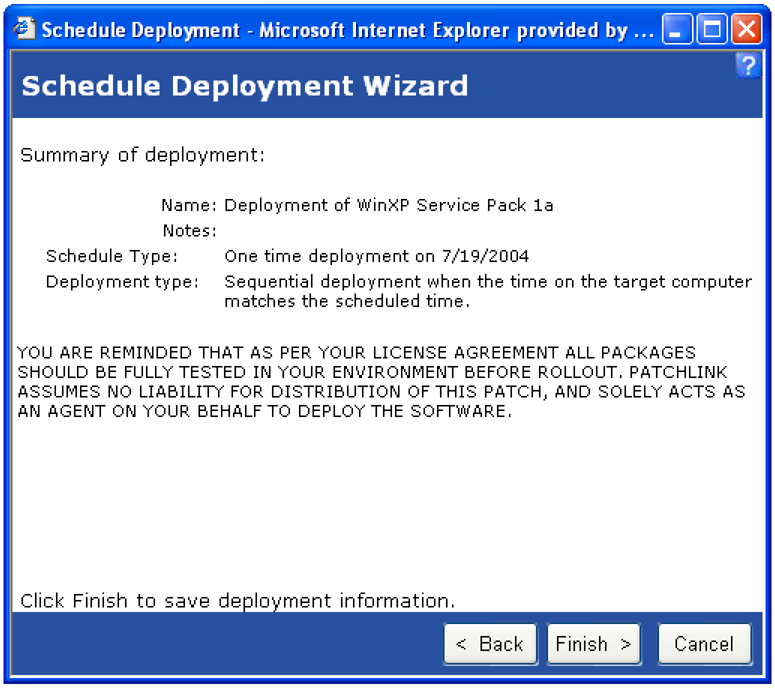
License Agreement for :Adobe Acrobat Reader 6.0

You must agree to the license agreement from the manufacturer before you will be able to deploy this package. Click "I Agree" to continue:

Click the **I Agree** button to accept the terms and initialize the wizard’s next screen, where you can define some deployment information

Summary

The Deployment Verification displays a simple summary of the deployment to be initialized. If any of this information is incorrect, press the **Back** button to change the values. If everything is correct, press the button **Finish** to have the wizard create the deployment.



Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

Summary of deployment:

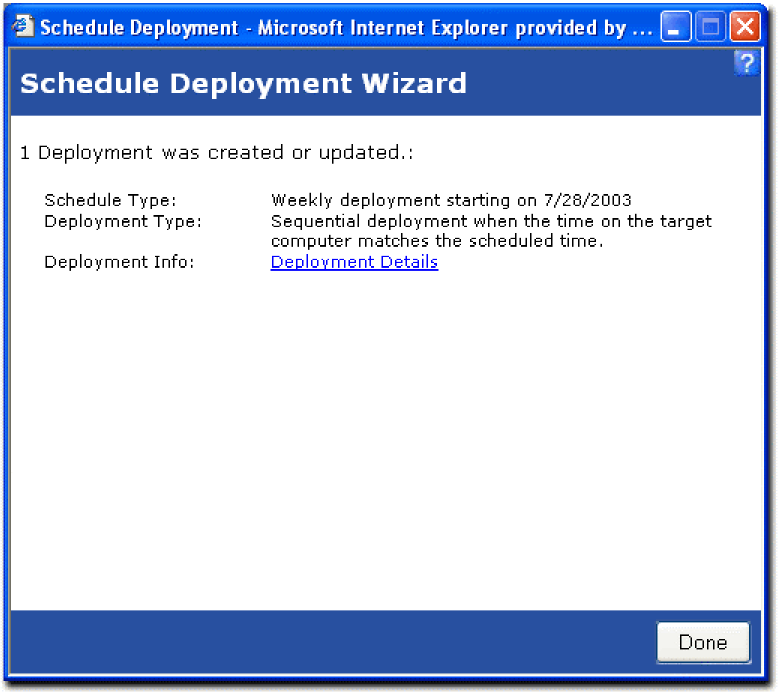
Name: Deployment of WinXP Service Pack 1a
Notes:
Schedule Type: One time deployment on 7/19/2004
Deployment type: Sequential deployment when the time on the target computer matches the scheduled time.

YOU ARE REMINDED THAT AS PER YOUR LICENSE AGREEMENT ALL PACKAGES SHOULD BE FULLY TESTED IN YOUR ENVIRONMENT BEFORE ROLLOUT. PATCHLINK ASSUMES NO LIABILITY FOR DISTRIBUTION OF THIS PATCH, AND SOLELY ACTS AS AN AGENT ON YOUR BEHALF TO DEPLOY THE SOFTWARE.

Click Finish to save deployment information.

Verification

The verification screen displays the results of the deployment creation process.



Schedule Deployment - Microsoft Internet Explorer provided by ...

Schedule Deployment Wizard

1 Deployment was created or updated.:

Schedule Type: Weekly deployment starting on 7/28/2003
Deployment Type: Sequential deployment when the time on the target computer matches the scheduled time.
Deployment Info: Deployment Details

Screen Functions

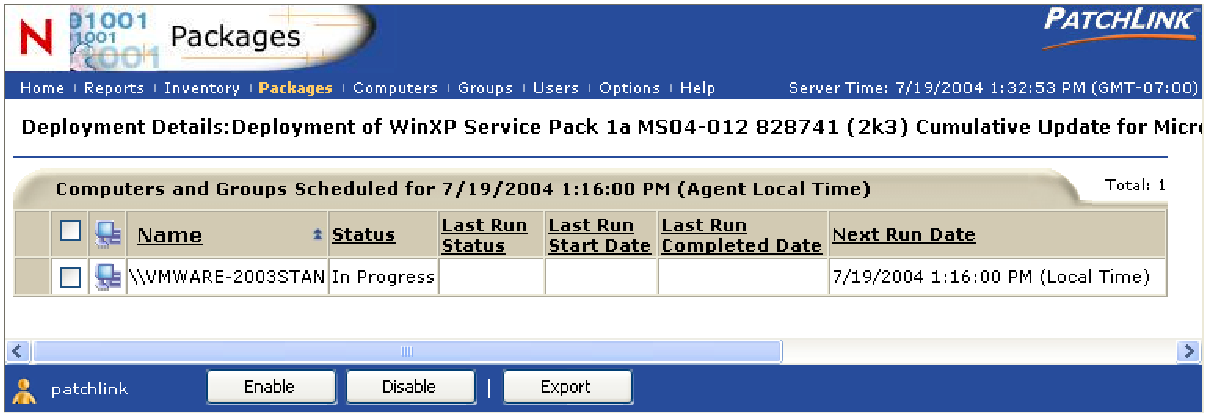
- Done

Closes the wizard and initializes the Deployment Details screen

- Deployment Details Link

  Provides details of the deployment

Upon selection of the **Done** button, the deployment details page automatically refreshes and displays the assigned computers and groups and the status of the deployment for each. To view the group membership results for the deployment, click on the name of the group.


Packages
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
patchlink
Enable
Disable
Export

Server Time: 7/19/2004 1:32:53 PM (GMT-07:00)

Deployment Details:Deployment of WinXP Service Pack 1a MS04-012 828741 (2k3) Cumulative Update for Micr

Computers and Groups Scheduled for 7/19/2004 1:16:00 PM (Agent Local Time)

Total: 1

	☐		Name	Status	Last Run Status	Last Run Start Date	Last Run Completed Date	Next Run Date
	☐		\\VMWARE-2003STAN	In Progress				7/19/2004 1:16:00 PM (Local Time)

Package Deployments Security

The package deployments section of ZENworks® Patch Management Server requires the View Deployment Status access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the information about a distribution package requires the View Packages access right. If a user does not have the correct access, the hyperlink on the Information tab is not enabled.

To be create a deployment for the distribution package requires the Deploy Packages access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to change, disable, enable, abort or remove a deployment(s) requires the Manage Deployments access right. If a user does not have the correct access, the Change, Disable, Enable, Abort and Remove buttons are disabled.

To be able to change the deployment of the Discover Applicable Updates System Task requires the Manage System Tasks access right. If a user does not have the correct access, they will receive a message indicating they do not have access.

To be able to export the distribution package’s information to a comma-separated value (CSV) file requires the Export Deployment Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Distribution Packages Security

The Distribution Packages section of ZENworks® Patch Management Server requires the View Packages access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the deployments for a distribution package requires the View Deployments access right. If a user does not have the correct access the hyperlink on the Package Name will not be displayed.

To be able to create a deployment for a selected distribution package requires the Deploy packages access right. If a user does not have the correct access the Deploy button is disabled.

To be able to create, change or remove distribution packages requires the Manage Packages access right. If a user does not have the correct access the Add, Change and Remove buttons are disabled.

To export all of the distribution packages and their information to a comma-separated values (CSV) file requires the Export Package Data access right. If a user does not have the correct access the Export button is disabled.

To cache the selected (or re-cache all of the previously cached) distribution packages requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

Package Information Security

The distribution package information section of the Patch Management Server requires the View Packages access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the deployments of the distribution package requires the View Deployments access right. If a user does not have the correct access, the hyperlink on the Deployments tab is not enabled.

To be create a deployment for the distribution package requires the Deploy Packages access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to change a local distribution package requires the Manage Packages access right. If a user does not have the correct access, the Change button is disabled.

To be able to disable or enable a distribution package requires the Manage Packages access right. If a user does not have the correct access, the Enable and Disable buttons are disabled.

To be able to export the distribution package's information to a comma-separated value (CSV) file requires the Export Package Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Deployments Details Security

The Deployment Details section of the Patch Management Server requires the View Deployment Statuses access right. If a user does not have the correct access, the access denied error message is displayed.

To enable and disable a deployment assignment requires the Manage Deployments access right. If a user does not have the correct access, the enable and disable buttons are disabled.

To export the deployment details data requires the Export Deployment Data access right. If a user does not have the correct access, the export button is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Deployments Results Security

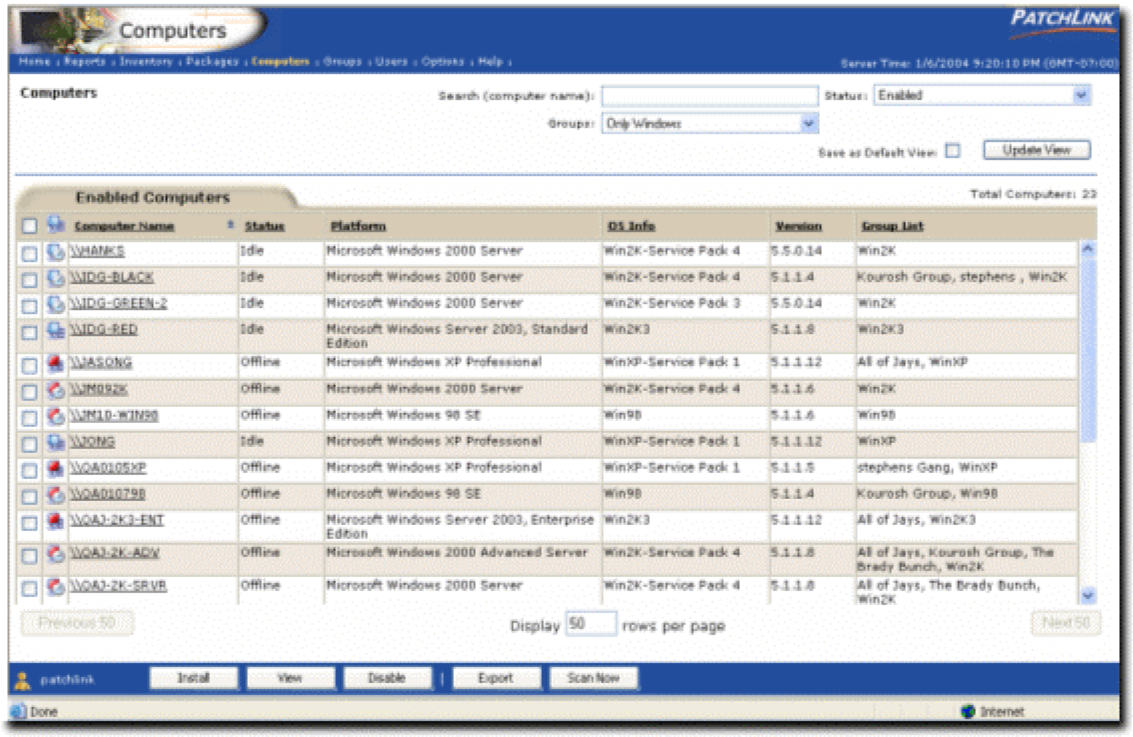
The Deployment Results section of the Patch Management Server requires the View Deployment Statuses access right. If a user does not have the correct access, the access denied error message is displayed.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

10. Computers

Home | Reports | Inventory | Packages | **Computers** | Groups | Users | Options | Help |

The computers section of the Patch Management Server displays all computers which have an agent registered against the Server. Clicking on a computer name will allow you to display a computer's specific information.



Server Time: 1/6/2004 9:20:10 PM (GMT-07:00)

Computers

Search (computer name):

Status: Enabled

Groups: Only Windows

Save as Default View: □

Enabled Computers

Total Computers: 22

□	Computer Name	Status	Platform	OS Info	Version	Group List
□	\\HANKS	Idle	Microsoft Windows 2000 Server	Win2K-Service Pack 4	5.5.0.14	Win2K
□	\\IDG-BLACK	Idle	Microsoft Windows 2000 Server	Win2K-Service Pack 4	5.1.1.4	Kourosh Group, stephens , Win2K
□	\\IDG-GREEN-2	Idle	Microsoft Windows 2000 Server	Win2K-Service Pack 3	5.5.0.14	Win2K
□	\\IDG-RED	Idle	Microsoft Windows Server 2003, Standard Edition	Win2K3	5.1.1.8	Win2K3
□	\\JASONG	Offline	Microsoft Windows XP Professional	WinXP-Service Pack 1	5.1.1.12	All of Jays, WinXP
□	\\JM092K	Offline	Microsoft Windows 2000 Server	Win2K-Service Pack 4	5.1.1.6	Win2K
□	\\JM10-WIN98	Offline	Microsoft Windows 98 SE	Win98	5.1.1.6	Win98
□	\\JONG	Idle	Microsoft Windows XP Professional	WinXP-Service Pack 1	5.1.1.12	WinXP
□	\\QA0105XP	Offline	Microsoft Windows XP Professional	WinXP-Service Pack 1	5.1.1.5	stephens Gang, WinXP
□	\\QA01079B	Offline	Microsoft Windows 98 SE	Win98	5.1.1.4	Kourosh Group, Win98
□	\\QAJ-2K3-ENT	Offline	Microsoft Windows Server 2003, Enterprise Edition	Win2K3	5.1.1.12	All of Jays, Win2K3
□	\\QAJ-2K-ADV	Offline	Microsoft Windows 2000 Advanced Server	Win2K-Service Pack 4	5.1.1.8	All of Jays, Kourosh Group, The Brady Bunch, Win2K
□	\\QAJ-2K-SRVR	Offline	Microsoft Windows 2000 Server	Win2K-Service Pack 4	5.1.1.8	All of Jays, The Brady Bunch, Win2K

Display 50 rows per page

Computer Information Columns

Computer Name

This displays the name of the computer. Click on the computer name to display specific information about the computer.

Status

This displays the status of the computer.

Platform

This displays the operating system platform the computer is running.

OS Info

This displays additional information about the operating system the computer is running.

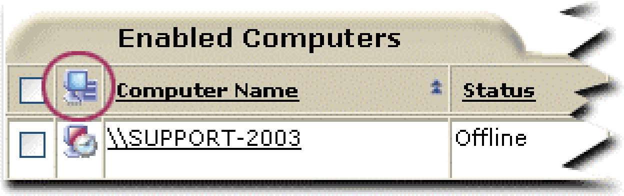
Version

This displays the version of the agent running on the computer.

Group List

This displays the list of groups that the computer is a member of.

Agent Status



Enabled Computers

□	🖥	Computer Name	Status
□	🖥	\\SUPPORT-2003	Offline

Status	Description
🖥	This is an idle deployment agent.
🖥	This deployment agent is idle and has deployments
🖥	The agent is sleeping as it is outside its hours of operation.
🖥	The agent is sleeping as it is outside its hours of operation and has deployments in its work queue.
🖥	This agent is currently working on a deployment (animated)
🔍	This is an enabled detection agent that does not correspond to a registered deployment agent*.
🖥	The agent is considered to be offline as it has not contacted the Patch Management Server in more than two intervals (minimum of 15 minutes).
🖥	The agent is considered to be offline as it has not contacted the Patch Management Server in more than two intervals (minimum of 15 minutes) and has deployments in
🖥	This agent has been disabled.

Additional information may be displayed by hovering your mouse pointer over an enabled icon.

To display additional information about the computer, click on the name of the actual computer. This performs the same function as selecting the computer and clicking on the View button on the Action Menu.

* This usually means that either the deployment agent was removed from the Patch Management Server or there has been a problem in registering the deployment agent. For more information on this check the agent installation section.

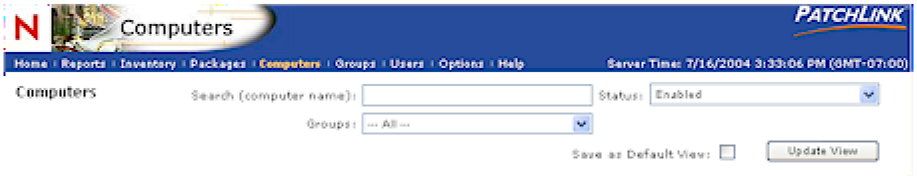
Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟, ⊞) is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Computers page header.


N
Computers
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Update View

Server Time: 7/16/2004 3:33:06 PM (GMT-07:00)

Computers

Search (computer name):

Status: Enabled

Groups: --- All ---

Save as Default View: □

- Search

Search (computer name):

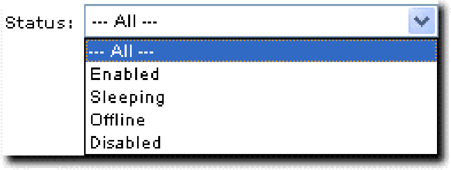
You may search computers for more granular results by entering the computer name text into the **Search** field and clicking on the Update View Update View button.

This will return the computer having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Save as Default View: □

- Status

Filter by status using the dropdown menu and click on the Update View Update View button.

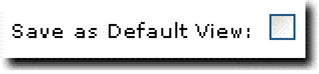


Status: --- All ---

--- All ---
Enabled
Sleeping
Offline
Disabled

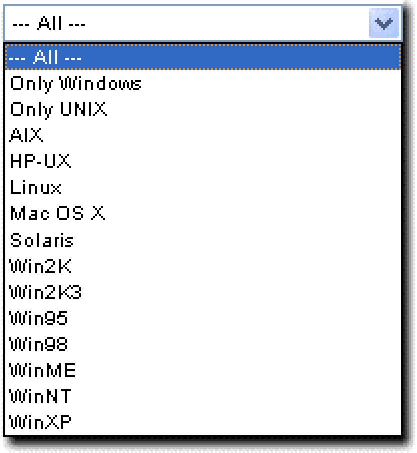
This allows the user to search on enabled, sleeping, offline, and disabled systems that exist.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



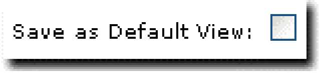
Save as Default View: □

- Groups
  Filter by group using the dropdown menu and click on the Update View button.



This allows the user to search on any user-defined or server-defined groups that exist.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Sort

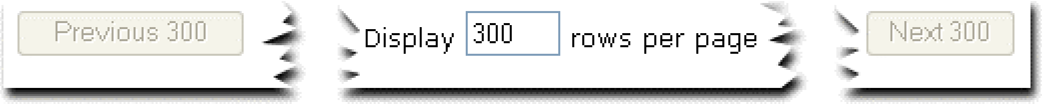
The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Display

Depending on the amount of items available for display and what page you are viewing determines the display function located at the bottom of enabled pages above the Action Menu.



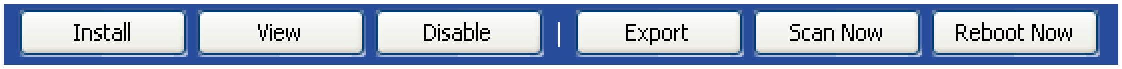
- Next: To display the next page of computers, click on the next button. If the last computer is displayed, the next button is disabled.
- Previous: To display the previous page of computers, click on the previous button. If the first computer is being displayed, the previous button is disabled.

- Computers per Page: The computer list initially displays up to 100 computers per page. To change the number of computers to display per page, enter a new number in to the Computers per Page input field. To display all computers enter a zero in the input field.

Checkboxes

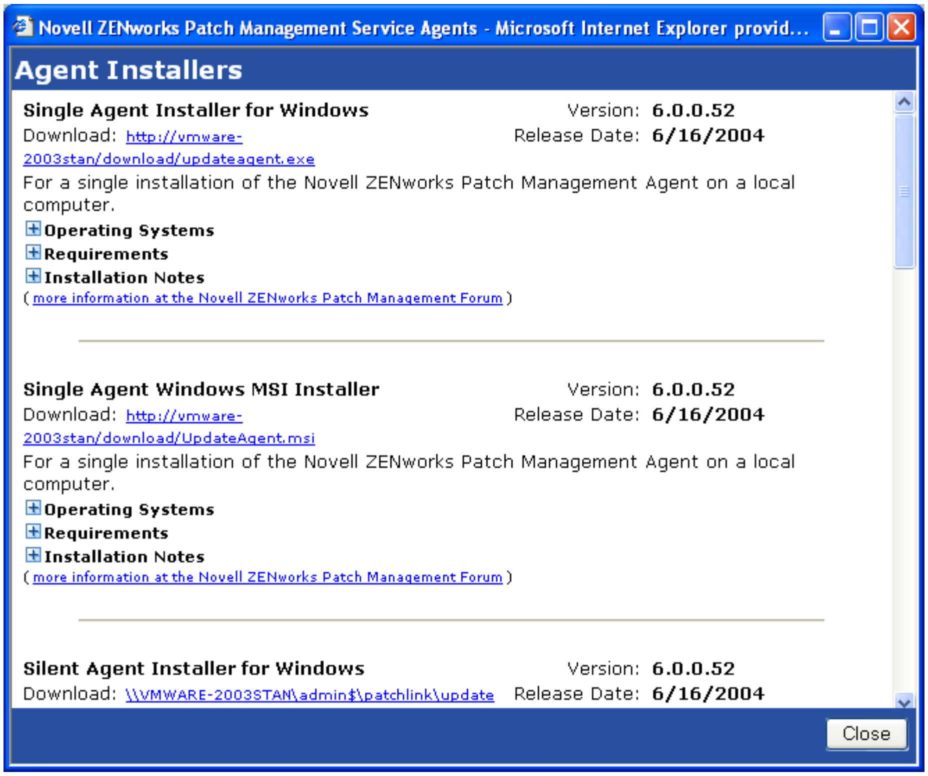
Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Install

Click on the Install button to display the list of agent installers that can be used to register computers to the Patch Management Server. See Section 3.6, Agent Management Center for more details on Agents and installing them.


Novell ZENworks Patch Management Service Agents - Microsoft Internet Explorer provid...
Close

Agent Installers

Single Agent Installer for Windows Version: **6.0.0.52**
Download: http://vmware-2003stan/download/updateagent.exe Release Date: **6/16/2004**
For a single installation of the Novell ZENworks Patch Management Agent on a local computer.
⊞ **Operating Systems**
⊞ **Requirements**
⊞ **Installation Notes**
(more information at the Novell ZENworks Patch Management Forum)

Single Agent Windows MSI Installer Version: **6.0.0.52**
Download: http://vmware-2003stan/download/UpdateAgent.msi Release Date: **6/16/2004**
For a single installation of the Novell ZENworks Patch Management Agent on a local computer.
⊞ **Operating Systems**
⊞ **Requirements**
⊞ **Installation Notes**
(more information at the Novell ZENworks Patch Management Forum)

Silent Agent Installer for Windows Version: **6.0.0.52**
Download: \\VMWARE-2003STAN\admin$\patchlink\update Release Date: **6/16/2004**

Silent installer

The Silent Installer is designed for use with log in scripts. The program is stored on a public directory. A sample log in script can be found on the Patch Management Server, which demonstrates how it is most effectively used.

MSI installer

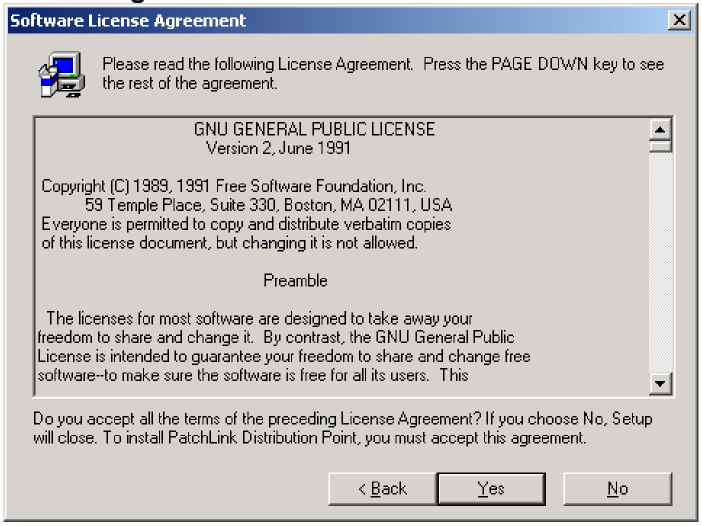
The MSI installer is designed for windows networks that use the windows software installer mechanism. The MSI installer can be edited to include the Patch Management Server name and serial number. In this way, the agent can be deployed through the use of Group Policy Objects

PatchLink Distribution Point

- Running the Installation
  The PatchLink Distribution Point install executable is called PLDISTPT.EXE and can be downloaded by logging in to the web based administration interface and clicking on the Computers section of the product, then pushing the Install button on the bottom left of that screen and selecting the download link for “PatchLink Distribution Point 2.0”.

  Once the setup program is downloaded, double click or run the PLDISTPT.EXE file on the computer on which the Distribution Point is to be installed.

License Agreement



Software License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This

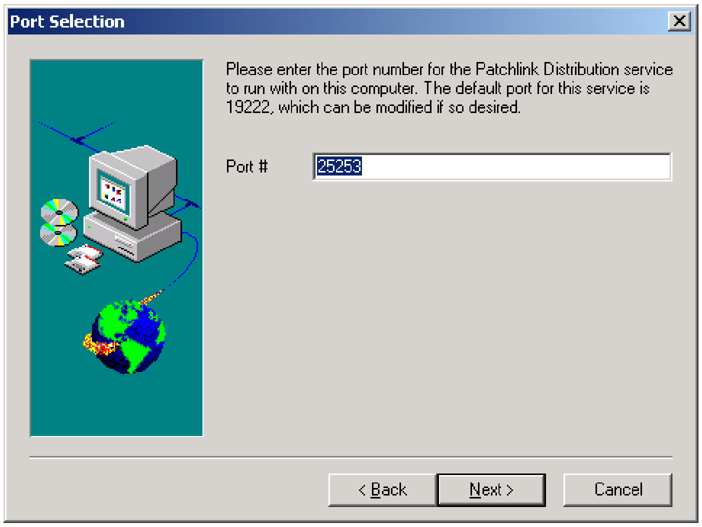
Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install PatchLink Distribution Point, you must accept this agreement.

The first screen of the installation program displays the GNU GENERAL PUBLIC LICENSE agreement under which you are entitled to use this piece of software, which has been derived from the SQUID for NT Version 2.5 product.

Please note that this open source license agreement applies only to the PatchLink Distribution Point product. All other parts of the Novell® ZENworks® Patch Management solution are covered by your existing EULA and/or MLA license documents.

Press YES to acknowledge the license agreement.

Selection of Port



Please enter the port number for the Patchlink Distribution service to run with on this computer. The default port for this service is 19222, which can be modified if so desired.

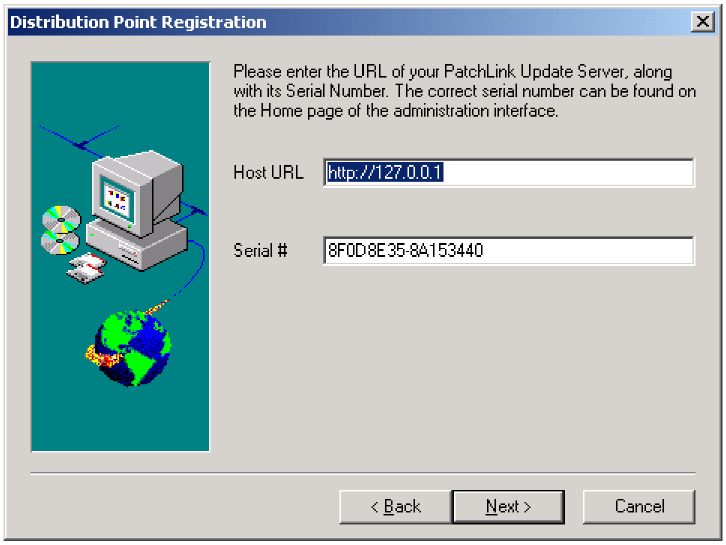
Port # 25253

The PatchLink Distribution Point installation requires that you select a TCP/IP port that this service can run on. Typical proxy service ports are 8080, 8081 and so forth. By default this port value is set to 25253 – however you can specify any numeric value that you wish that doesn't conflict with other known services that you are using on this box.

Enter the desired port number, or accept the default value.

Press Next to continue.

Registration Parameters



Please enter the URL of your PatchLink Update Server, along with its Serial Number. The correct serial number can be found on the Home page of the administration interface.

Host URL http://127.0.0.1

Serial # 8F0D8E35-8A153440

The Distribution Point installer will attempt to register this proxy with its corresponding Patch Management server.

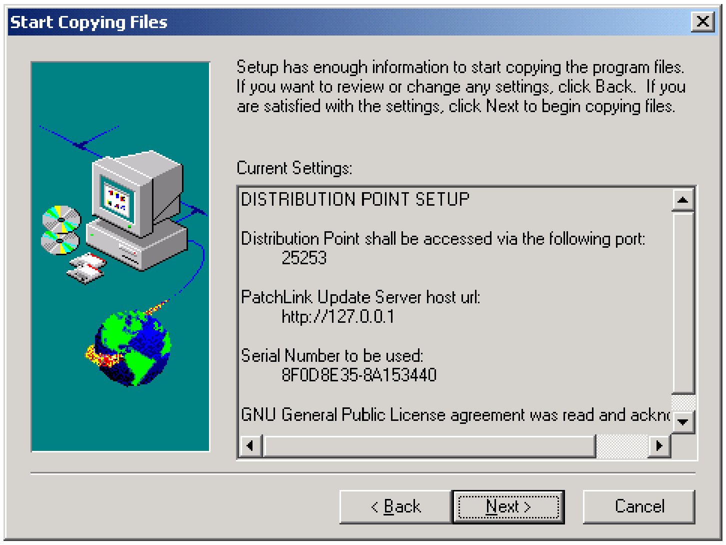
We recommend that you enter your Patch Management Server URL and Serial Number at this time so that registration can be completed – if you choose not to enter this information correctly or do not know the information; your new Distribution Point will not be included on the list of distribution points supplied to Agent computers during network path optimization tasks.

Enter the Subscription Host URL (optional)

Enter the Serial Number (optional)

Press Next to continue.

Confirmation



Start Copying Files

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
DISTRIBUTION POINT SETUP

Distribution Point shall be accessed via the following port:
        25253

PatchLink Update Server host url:
        http://127.0.0.1

Serial Number to be used:
        8F0D8E35-8A153440

GNU General Public License agreement was read and ackn(
```

This screen merely confirms your chosen installation parameters. If you wish to change any of the listed values, press Back and make your modifications at this time.

Press Next to complete installation.

Post Installation Configuration

Once installation is completed, the program files and configuration files can be found in the **C:\program files\patchlink\Distribution Point** sub-directory on the target computer. The service that has been installed and automatically started on the computer is called **PatchLink_Distribution.**

The PatchLink_Distribution service can be started and stopped like any other Windows service by going to Control Panel -> Administrative Tools -> Services. Note that when the service is running, agents may obtain their patch files from the Distribution Point – however when the service is stopped or the computer is offline for any reason (power management, suspend mode, etc) all agent communications will be suspended through that Distribution Point. For this reason we recommend that a dedicated computer that is permanently connected to the network backbone should be used for a Distribution Point.

Advanced configuration options can now be modified, if so desired, by editing the two configuration files located in the **C:\program files\patchlink\Distribution Point\etc** subdirectory:

SQUID.CONF	- which contains all cache configuration parameters
MIME.CONF	- controls what content types are handled

These options are explained in detail in the next two sections.

Cache Configuration Options – SQUID.CONF

NOTE: The following list is a relevant subset of all available options. Refer to SQUID.CONF.DEFAULT for a complete listing of all available options for the product.

It is not recommended that you alter the default configuration options set by the installation program, and doing so may require you to have to re-install if you require support from the Novell® Support team.

Network Options

http_port

The socket addresses where SQUID will listen for HTTP client requests. You may specify multiple socket addresses. There are three forms: port alone, hostname with port, and IP address with port. If you specify a hostname or IP address, then SQUID binds the socket to that specific address. This replaces the old 'tcp_incoming_address' option. Most likely, you do not need to bind to a specific address, so you can use the port number alone.

The default port number is 3128.

If you are running SQUID in accelerator mode, then you probably want to listen on port 80 also, or instead.

The -a command line option will override the *first* port number listed here. That option will NOT override an IP address, however.

You may specify multiple socket addresses on multiple lines.

If you run SQUID on a dual-homed machine with an internal and an external interface then we recommend you to specify the internal address:port in http_port. This way SQUID will only be visible on the internal address.

icp_port:

The port number where SQUID sends and receives ICP queries to and from neighbor caches. Default is 3130. To disable use "0". May be overridden with -u on the command line.

htcp_port

The port number where SQUID sends and receives HTCP queries to and from neighbor caches. Default is 4827. To disable use "0".

mcast_groups

This tag specifies a list of multicast groups which your server should join to receive multicasted ICP queries.

NOTE! Be very careful what you put here! Be sure you understand the difference between an ICP _query_ and an ICP _reply_. This option is to be set only if you want to RECEIVE multicast queries. Do NOT set this option to SEND multicast ICP (use cache_peer for that). ICP replies are always sent via unicast, so this option does not affect whether or not you will receive replies from multicast group members.

You must be very careful to NOT use a multicast address which is already in use by another group of caches.

If you are unsure about multicast, please read the Multicast chapter in the SQUID FAQ (http://www.SQUID-cache.org/FAQ/).

Usage: mcast_groups 239.128.16.128 224.0.1.20

By default, SQUID doesn't listen on any multicast groups.

udp_incoming_address
udp_outgoing_address

udp_incoming_address is used for the ICP socket receiving packets from other caches. udp_outgoing_address is used for ICP packets sent out to other caches. The default behavior is to not bind to any specific address.

A udp_incoming_address value of 0.0.0.0 indicates that SQUID should listen for UDP messages on all available interfaces.

If udp_outgoing_address is set to 255.255.255.255 (the default) then it will use the same socket as udp_incoming_address. Only change this if you want to have ICP queries sent using another address than where this SQUID listens for ICP queries from other caches.

NOTE, udp_incoming_address and udp_outgoing_address can not have the same value since they both use port 313

Options Which Affect the Neighbor Selection Algorithm

cache_peer

To specify other caches in a hierarchy, use the format:

```
cache_peer hostname type http_port icp_port
```

For example,

```
                              proxy  icp
          hostname            type     port   port  options
          -------------------- -------- ----- -----  -----------
cache_peer parent.foo.net       parent    3128  3130  [proxy-only]
cache_peer sib1.foo.net         sibling   3128  3130  [proxy-only]
cache_peer sib2.foo.net         sibling   3128  3130  [proxy-only]

      type:  either 'parent', 'sibling', or 'multicast'.

proxy_port:  The port number where the cache listens for proxy
             requests.

  icp_port:  Used for querying neighbor caches about
             objects.  To have a non-ICP neighbor
             specify '7' for the ICP port and make sure the
             neighbor machine has the UDP echo port
             enabled in its /etc/inetd.conf file.

   options: proxy-only
             weight=n
             ttl=n
             no-query
             default
             round-robin
             multicast-responder
             closest-only
             no-digest
             no-netdb-exchange
             no-delay
             login=user:password | PASS | *:password
             connect-timeout=nn
             digest-url=url
             allow-miss
             max-conn

             use 'proxy-only' to specify that objects fetched
             from this cache should not be saved locally.

             use 'weight=n' to specify a weighted parent.
             The weight must be an integer.  The default weight
             is 1, larger weights are favored more.

             use 'ttl=n' to specify a IP multicast TTL to use
             when sending an ICP queries to this address.
             Only useful when sending to a multicast group.
             Because we don't accept ICP replies from random
             hosts, you must configure other group members as
             peers with the 'multicast-responder' option below.

             use 'no-query' to NOT send ICP queries to this
             neighbor.

             use 'default' if this is a parent cache which can
```

be used as a "last-resort." You should probably only use 'default' in situations where you cannot use ICP with your parent cache(s).

use 'round-robin' to define a set of parents which should be used in a round-robin fashion in the absence of any ICP queries.

'multicast-responder' indicates that the named peer is a member of a multicast group. ICP queries will not be sent directly to the peer, but ICP replies will be accepted from it.

'closest-only' indicates that, for ICP_OP_MISS replies, we'll only forward CLOSEST_PARENT_MISSes and never FIRST_PARENT_MISSes.

use 'no-digest' to NOT request cache digests from this neighbor.

'no-netdb-exchange' disables requesting ICMP RTT database (NetDB) from the neighbor.

use 'no-delay' to prevent access to this neighbor from influencing the delay pools.

use 'login=user:password' if this is a personal/workgroup proxy and your parent requires proxy authentication.
Note: The string can include URL escapes (i.e. %20 for spaces). This also means that % must be written as %%.

use 'login=PASS' if users must authenticate against the upstream proxy. This will pass the users credentials as they are to the peer proxy. This only works for the Basic HTTP authentication sheme. Note: To combine this with proxy_auth both proxies must share the same user database as HTTP only allows for one proxy login.
Also be warned that this will expose your users proxy password to the peer. USE WITH CAUTION

use 'login=*:password' to pass the username to the upstream cache, but with a fixed password. This is meant to be used when the peer is in another administrative domain, but it is still needed to identify each user.
The star can optionally be followed by some extra information which is added to the username. This can be used to identify this proxy to the peer, similar to the login=username:password option above.

use 'connect-timeout=nn' to specify a peer specific connect timeout (also see the peer_connect_timeout directive) use 'digest-url=url' to tell SQUID to fetch the cache digest (if digests are enabled) for this host from the specified URL rather than the SQUID default location.

use 'allow-miss' to disable SQUID's use of only-if-cached when forwarding requests to siblings. This is primarily useful when icp_hit_stale is used by the sibling. To extensive use of this option may result in forwarding loops, and you should avoid having two-way peerings with this option. (for example to deny peer usage on requests from peer by denying cache_peer_access if the source is a peer)

use 'max-conn' to limit the amount of connections SQUID may open to this peer.

NOTE: non-ICP neighbors must be specified as 'parent'.

cache_peer_domain

Use to limit the domains for which a neighbor cache will be queried. Usage:

```
cache_peer_domain cache-host domain [domain ...]
cache_peer_domain cache-host !domain
```

For example, specifying

```
    cache_peer_domain parent.foo.net        .edu
```

has the effect such that UDP query packets are sent to 'bigserver' only when the requested object exists on a server in the .edu domain. Prefixing the domainname with '!' means that the cache will be queried for objects NOT in that domain.

NOTE: * Any number of domains may be given for a cache-host, either on the same or separate lines.
* When multiple domains are given for a particular cache-host, the first matched domain is applied.
* Cache hosts with no domain restrictions are queried for all requests.
* There are no defaults.
* There is also a 'cache_peer_access' tag in the ACL section.

neighbor_type_domain

usage: neighbor_type_domain neighbor parent|sibling domain domain ...

Modifying the neighbor type for specific domains is now possible. You can treat some domains differently than the the default neighbor type specified on the 'cache_peer' line. Normally it should only be necessary to list domains which should be treated differently because the default neighbor type applies for hostnames which do not match domains listed here.

EXAMPLE:

```
cache_peer  parent cache.foo.org 3128 3130
neighbor_type_domain cache.foo.org sibling .com .net
neighbor_type_domain cache.foo.org sibling .au .de
```

icp_query_timeout (msec)

Normally SQUID will automatically determine an optimal ICP query timeout value based on the round-trip-time of recent ICP queries. If you want to override the value determined by SQUID, set this 'icp_query_timeout' to a non-zero value. This value is specified in MILLISECONDS, so, to use a 2-second timeout (the old default), you would write:

```
icp_query_timeout 2000
```

maximum_icp_query_timeout (msec)

Normally the ICP query timeout is determined dynamically. But sometimes it can lead to very large values (say 5 seconds). Use this option to put an upper limit on the dynamic timeout value. Do NOT use this option to always use a fixed (instead of a dynamic) timeout value. To set a fixed timeout see the 'icp_query_timeout' directive.

mcast_icp_query_timeout (msec)

For Multicast peers, SQUID regularly sends out ICP "probes" to count how many other peers are listening on the given multicast address. This value specifies how long SQUID should wait to count all the replies. The default is 2000 msec, or 2 seconds.

dead_peer_timeout (seconds)

This controls how long SQUID waits to declare a peer cache as "dead." If there are no ICP replies received in this amount of time, SQUID will declare the peer dead and not expect to receive any further ICP replies. However, it continues to send ICP queries, and will mark the peer as alive upon receipt of the first subsequent ICP reply.

This timeout also affects when SQUID expects to receive ICP replies from peers. If more than 'dead_peer' seconds have passed since the last ICP reply was received, SQUID will not expect to receive an ICP reply on the next query. Thus, if your time between requests is greater than this timeout, you will see a lot of requests sent DIRECT to origin servers instead of to your parents.

hierarchy_stoplist

A list of words which, if found in a URL, cause the object to be handled directly by this cache. In other words, use this to not query neighbor caches for certain objects. You may list this option multiple times.

no_cache
A list of ACL elements which, if matched, cause the request to not be satisfied from the cache and the reply to not be cached. In other words, use this to force certain objects to never be cached.

You must use the word 'DENY' to indicate the ACL names which should NOT be cached.

We recommend you to use the following two lines.

```
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
```

Options which affect the Cache Size

cache_mem (bytes)
NOTE: THIS PARAMETER DOES NOT SPECIFY THE MAXIMUM PROCESS SIZE. IT ONLY PLACES A LIMIT ON HOW MUCH ADDITIONAL MEMORY SQUID WILL USE AS A MEMORY CACHE OF OBJECTS. SQUID USES MEMORY FOR OTHER THINGS AS WELL. SEE THE SQUID FAQ SECTION 8 FOR DETAILS.

'cache_mem' specifies the ideal amount of memory to be used for:

* In-Transit objects
* Hot Objects
* Negative-Cached objects

Data for these objects are stored in 4 KB blocks. This parameter specifies the ideal upper limit on the total size of 4 KB blocks allocated. In-Transit objects take the highest priority.

In-transit objects have priority over the others. When additional space is needed for incoming data, negative-cached and hot objects will be released. In other words, the negative-cached and hot objects will fill up any unused space not needed for in-transit objects.

If circumstances require, this limit will be exceeded. Specifically, if your incoming request rate requires more than 'cache_mem' of memory to hold in-transit objects, SQUID will exceed this limit to satisfy the new requests. When the load decreases, blocks will be freed until the high-water mark is reached. Thereafter, blocks will be used to store hot objects.

cache_swap_low (percent, 0-100)
cache_swap_high (percent, 0-100)
The low- and high-water marks for cache object replacement. Replacement begins when the swap (disk) usage is above the low-water mark and attempts to maintain utilization near the low-water mark. As swap utilization gets close to high-water

mark object eviction becomes more aggressive. If utilization is close to the low-water mark less replacement is done each time.

Defaults are 90% and 95%. If you have a large cache, 5% could be hundreds of MB. If this is the case you may wish to set these numbers closer together.

maximum_object_size (bytes)

Objects larger than this size will NOT be saved on disk. The value is specified in kilobytes, and the default is 4MB. If you wish to get a high BYTES hit ratio, you should probably increase this (one 32 MB object hit counts for 3200 10KB hits). If you wish to increase speed more than your want to save bandwidth you should leave this low.

NOTE: if using the LFUDA replacement policy you should increase this value to maximize the byte hit rate improvement of LFUDA! See replacement_policy below for a discussion of this policy.

minimum_object_size (bytes)

Objects smaller than this size will NOT be saved on disk. The value is specified in kilobytes, and the default is 0 KB, which means there is no minimum.

maximum_object_size_in_memory (bytes)

Objects greater than this size will not be attempted to kept in the memory cache. This should be set high enough to keep objects accessed frequently in memory to improve performance whilst low enough to keep larger objects from hoarding cache_mem .

ipcache_size (number of entries)

ipcache_low (percent)

ipcache_high (percent)

The size, low-, and high-water marks for the IP cache.

fqdncache_size (number of entries)

Maximum number of FQDN cache entries.

cache_replacement_policy

The cache replacement policy parameter determines which objects are evicted (replaced) when disk space is needed.

lru : SQUID's original list based LRU policy

heap GDSF : Greedy-Dual Size Frequency

heap LFUDA: Least Frequently Used with Dynamic Aging

heap LRU : LRU policy implemented using a heap

Applies to any cache_dir lines listed below this.

The LRU policies keeps recently referenced objects.

The heap GDSF policy optimizes object hit rate by keeping smaller popular objects in cache so it has a better chance of getting a hit. It achieves a lower byte hit rate than LFUDA though since it evicts larger (possibly popular) objects.

The heap LFUDA policy keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate since one large, popular object will prevent many smaller, slightly less popular objects from being cached.

Both policies utilize a dynamic aging mechanism that prevents cache pollution that can otherwise occur with frequency-based replacement policies.

NOTE: if using the LFUDA replacement policy you should increase the value of maximum_object_size above its default of 4096 KB to to maximize the potential byte hit rate improvement of LFUDA.

For more information about the GDSF and LFUDA cache replacement policies see http://www.hpl.hp.com/techreports/1999/HPL-1999-69.html and http://fog.hpl.external.hp.com/techreports/98/HPL-98-173.html.

memory_replacement_policy
The memory replacement policy parameter determines which objects are purged from memory when memory space is needed.

See cache_replacement_policy for details.

Logfile PathNames and Cache Directory

cache_dir
You can specify multiple cache_dir lines to spread the cache among different disk partitions.

Type specifies the kind of storage system to use. Only "ufs" is built by default. To eanble any of the other storage systems see the --enable-storeio configure option.

'Directory' is a top-level directory where cache swap files will be stored. If you want to use an entire disk for caching, then this can be the mount-point directory. The directory must exist and be writable by the SQUID process. SQUID will NOT create this directory for you.

The ufs store type:

"ufs" is the old well-known SQUID storage format that has always been there.

cache_dir ufs Directory-Name Mbytes L1 L2 [options]

'Mbytes' is the amount of disk space (MB) to use under this directory. The default is 100 MB. Change this to suit your configuration. Do NOT put the size of your disk drive here. Instead, if you want SQUID to use the entire disk drive, subtract 20% and use that value.

'Level-1' is the number of first-level subdirectories which will be created under the 'Directory'. The default is 16.

'Level-2' is the number of second-level subdirectories which

will be created under each first-level directory. The default
is 256.

The aufs store type:

"aufs" uses the same storage format as "ufs", utilizing
POSIX-threads to avoid blocking the main SQUID process on
disk-I/O. This was formerly known in SQUID as async-io.

cache_dir aufs Directory-Name Mbytes L1 L2 [options]

see argument descriptions under ufs above

The awin32 store type:

"awin32" uses the same storage format as "ufs", utilizing
WIN32-threads to avoid blocking the main SQUID process on
disk-I/O. This was formerly known in SQUID as async-io.

cache_dir awin32 Directory-Name Mbytes L1 L2 [options]

see argument descriptions under ufs above

The diskd store type:

"diskd" uses the same storage format as "ufs", utilizing a
separate process to avoid blocking the main SQUID process on
disk-I/O.

cache_dir diskd Directory-Name Mbytes L1 L2 [options] [Q1=n] [Q2=n]

see argument descriptions under ufs above

Q1 specifies the number of unacknowledged I/O requests when SQUID
stops opening new files. If this many messages are in the queues,
SQUID won't open new files. Default is 64

Q2 specifies the number of unacknowledged messages when SQUID
starts blocking. If this many messages are in the queues,
SQUID blocks until it recevies some replies. Default is 72

The coss store type:

block-size=n defines the "block size" for COSS cache_dir's.
SQUID uses file numbers as block numbers. Since file numbers
are limited to 24 bits, the block size determines the maximum
size of the COSS partition. The default is 512 bytes, which
leads to a maximum cache_dir size of 512<<24, or 8 GB. Note
that you should not change the coss block size after SQUID
has written some objects to the cache_dir.

Common options:

read-only, this cache_dir is read only.

max-size=n, refers to the max object size this storedir supports.
It is used to initially choose the storedir to dump the object.
Note: To make optimal use of the max-size limits you should order
the cache_dir lines with the smallest max-size value first and the
ones with no max-size specification last.

Note that for coss, max-size must be less than COSS_MEMBUF_SZ
(hard coded at 1 MB).

cache_access_log

Logs the client request activity. Contains an entry for
every HTTP and ICP queries received. To disable, enter "none".

cache_log

Cache logging file. This is where general information about
your cache's behavior goes. You can increase the amount of data
logged to this file with the "debug_options" tag below.

cache_store_log

Logs the activities of the storage manager. Shows which
objects are ejected from the cache, and which objects are
saved and for how long. To disable, enter "none". There are
not really utilities to analyze this data, so you can safely
disable it.

cache_swap_log

Location for the cache "swap.log." This log file holds the
metadata of objects saved on disk. It is used to rebuild the
cache during startup. Normally this file resides in each
'cache_dir' directory, but you may specify an alternate
pathname here. Note you must give a full filename, not just
a directory. Since this is the index for the whole object
list you CANNOT periodically rotate it!

If %s can be used in the file name then it will be replaced with a
a representation of the cache_dir name where each / is replaced
with '.'. This is needed to allow adding/removing cache_dir
lines when cache_swap_log is being used.

If have more than one 'cache_dir', and %s is not used in the name
then these swap logs will have names such as:

```
cache_swap_log.00
cache_swap_log.01
cache_swap_log.02
```

The numbered extension (which is added automatically)
corresponds to the order of the 'cache_dir' lines in this
configuration file. If you change the order of the 'cache_dir'
lines in this file, then these log files will NOT correspond to

the correct 'cache_dir' entry (unless you manually rename them). We recommend that you do NOT use this option. It is better to keep these log files in each 'cache_dir' directory.

emulate_httpd_log on|off

The Cache can emulate the log file format which many 'httpd' programs use. To disable/enable this emulation, set emulate_httpd_log to 'off' or 'on'. The default is to use the native log format since it includes useful information that SQUID-specific log analyzers use.

log_ip_on_direct on|off

Log the destination IP address in the hierarchy log tag when going direct. Earlier SQUID versions logged the hostname here. If you prefer the old way set this to off.

mime_table

Pathname to SQUID's MIME table. You shouldn't need to change this, but the default file contains examples and formatting information if you do.

log_mime_hdrs on|off

The Cache can record both the request and the response MIME headers for each HTTP transaction. The headers are encoded safely and will appear as two bracketed fields at the end of the access log (for either the native or httpd-emulated log formats). To enable this logging set log_mime_hdrs to 'on'.

useragent_log

SQUID will write the User-Agent field from HTTP requests to the filename specified here. By default useragent_log is disabled.

referer_log

SQUID will write the Referer field from HTTP requests to the filename specified here. By default referer_log is disabled.

pid_filename

A filename to write the process-id to. To disable, enter "none".

debug_options

Logging options are set as section,level where each source file is assigned a unique section. Lower levels result in less output, Full debugging (level 9) can result in a very large log file, so be careful. The magic word "ALL" sets debugging levels for all sections. We recommend normally running with "ALL,1".

log_fqdn on|off

Turn this on if you wish to log fully qualified domain names in the access.log. To do this SQUID does a DNS lookup of all IP's connecting to it. This can (in some situations) increase latency, which makes your cache seem slower for interactive browsing.

client_netmask
A netmask for client addresses in logfiles and cachemgr output.
Change this to protect the privacy of your cache clients.
A netmask of 255.255.255.0 will log all IP's in that range with
the last digit set to '0'.

Options for Tuning the Cache

wais_relay_host
wais_relay_port
Relay WAIS request to host (1st arg) at port (2 arg).

request_header_max_size (KB)
This specifies the maximum size for HTTP headers in a request.
Request headers are usually relatively small (about 512 bytes).
Placing a limit on the request header size will catch certain
bugs (for example with persistent connections) and possibly
buffer-overflow or denial-of-service attacks.

request_body_max_size (KB)
This specifies the maximum size for an HTTP request body.
In other words, the maximum size of a PUT/POST request.
A user who attempts to send a request with a body larger
than this limit receives an "Invalid Request" error message.
If you set this parameter to a zero (the default), there will
be no limit imposed.

refresh_pattern
usage: refresh_pattern [-i] regex min percent max [options]

By default, regular expressions are CASE-SENSITIVE. To make
them case-insensitive, use the -i option.

'Min' is the time (in minutes) an object without an explicit
expiry time should be considered fresh. The recommended
value is 0, any higher values may cause dynamic applications
to be erroneously cached unless the application designer
has taken the appropriate actions.

'Percent' is a percentage of the objects age (time since last
modification age) an object without explicit expiry time
will be considered fresh.

'Max' is an upper limit on how long objects without an explicit
expiry time will be considered fresh.

```
options: override-expire
    override-lastmod
    reload-into-ims
    ignore-reload
```

override-expire enforces min age even if the server sent a Expires: header. Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

override-lastmod enforces min age even on objects that was modified recently.

reload-into-ims changes client no-cache or ``reload'' to If-Modified-Since requests. Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

ignore-reload ignores a client no-cache or ``reload'' header. Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

Basically a cached object is:

FRESH if expires < now, else STALE
STALE if age > max
FRESH if lm-factor < percent, else STALE
FRESH if age < min
else STALE

The refresh_pattern lines are checked in the order listed here. The first entry which matches is used. If none of the entries match, then the default will be used.

Note, you must uncomment all the default lines if you want to change one. The default setting is only active if none is used.

Suggested default:

```
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320
```

quick_abort_min (KB)
quick_abort_max (KB)
quick_abort_pct (percent)
The cache by default continues downloading aborted requests which are almost completed (less than 16 KB remaining). This may be undesirable on slow (e.g. SLIP) links and/or very busy caches. Impatient users may tie up file descriptors and bandwidth by repeatedly requesting and immediately aborting downloads.

When the user aborts a request, SQUID will check the quick_abort values to the amount of data transfered until then.

If the transfer has less than 'quick_abort_min' KB remaining, it will finish the retrieval.

If the transfer has more than 'quick_abort_max' KB remaining, it will abort the retrieval.

If more than 'quick_abort_pct' of the transfer has completed, it will finish the retrieval.

If you do not want any retrieval to continue after the client has aborted, set both 'quick_abort_min' and 'quick_abort_max' to '0 KB'.

If you want retrievals to always continue if they are being cached then set 'quick_abort_min' to '-1 KB'.

negative_ttl time-units

Time-to-Live (TTL) for failed requests. Certain types of failures (such as "connection refused" and "404 Not Found") are negatively-cached for a configurable amount of time. The default is 5 minutes. Note that this is different from negative caching of DNS lookups.

positive_dns_ttl time-units

Time-to-Live (TTL) for positive caching of successful DNS lookups. Default is 6 hours (360 minutes). If you want to minimize the use of SQUID's ipcache, set this to 1, not 0.

negative_dns_ttl time-units

Time-to-Live (TTL) for negative caching of failed DNS lookups.

range_offset_limit (bytes)

Sets a upper limit on how far into the the file a Range request may be to cause SQUID to prefetch the whole file. If beyond this limit then SQUID forwards the Range request as it is and the result is NOT cached.

This is to stop a far ahead range request (lets say start at 17MB) from making SQUID fetch the whole object up to that point before sending anything to the client.

A value of -1 causes SQUID to always fetch the object from the beginning so that it may cache the result. (2.0 style)

A value of 0 causes SQUID to never fetch more than the client requested. (default)

Timeout Values

connect_timeout time-units

Some systems (notably Linux) can not be relied upon to properly time out connect(2) requests. Therefore the SQUID process enforces its own timeout on server connections. This parameter specifies how long to wait for the connect to complete. The default is two minutes (120 seconds).

peer_connect_timeout time-units

This parameter specifies how long to wait for a pending TCP connection to a peer cache. The default is 30 seconds. You may also set different timeout values for individual neighbors with the 'connect-timeout' option on a 'cache_peer' line.

read_timeout time-units

The read_timeout is applied on server-side connections. After each successful read(), the timeout will be extended by this amount. If no data is read again after this amount of time, the request is aborted and logged with ERR_READ_TIMEOUT. The default is 15 minutes.

request_timeout

How long to wait for an HTTP request after initial connection establishment.

persistent_request_timeout

How long to wait for the next HTTP request on a persistent connection after the previous request completes.

client_lifetime time-units

The maximum amount of time that a client (browser) is allowed to remain connected to the cache process. This protects the Cache from having a lot of sockets (and hence file descriptors) tied up in a CLOSE_WAIT state from remote clients that go away without properly shutting down (either because of a network failure or because of a poor client implementation). The default is one day, 1440 minutes.

NOTE: The default value is intended to be much larger than any client would ever need to be connected to your cache. You should probably change client_lifetime only as a last resort. If you seem to have many client connections tying up filedescriptors, we recommend first tuning the read_timeout, request_timeout, persistent_request_timeout and quick_abort values.

half_closed_clients

Some clients may shutdown the sending side of their TCP connections, while leaving their receiving sides open. Sometimes, SQUID can not tell the difference between a half-closed and a fully-closed TCP connection. By default, half-closed client connections are kept open until a read(2) or write(2) on the socket returns an error.

Change this option to 'off' and SQUID will immediately close client connections when read(2) returns "no more data to read."

pconn_timeout

Timeout for idle persistent connections to servers and other proxies.

ident_timeout

Maximum time to wait for IDENT lookups to complete.

If this is too high, and you enabled IDENT lookups from untrusted users, then you might be susceptible to denial-of-service by having many ident requests going at once.

shutdown_lifetime time-units

When SIGTERM or SIGHUP is received, the cache is put into "shutdown pending" mode until all active sockets are closed. This value is the lifetime to set for all open descriptors during shutdown mode. Any active clients after this many seconds will receive a 'timeout' message.

Administrative Parameters

cache_mgr

Email-address of local cache manager who will receive mail if the cache dies. The default is "webmaster."

cache_effective_user
cache_effective_group

If the cache is run as root, it will change its effective/real UID/GID to the UID/GID specified below. The default is to change to UID to nobody and GID to the default group of nobody.

If SQUID is not started as root, the default is to keep the current UID/GID, and only the GID can be changed to any of the groups the user starting SQUID is member of. Note that if SQUID is not started as root then you cannot set http_port to a value lower than 1024.

visible_hostname

If you want to present a special hostname in error messages, etc, then define this. Otherwise, the return value of gethostname() will be used. If you have multiple caches in a cluster and get errors about IP-forwarding you must set them to have individual names with this setting.

unique_hostname

If you want to have multiple machines with the same 'visible_hostname' then you must give each machine a different 'unique_hostname' so that forwarding loops can be detected.

hostname_aliases

A list of other DNS names that your cache has.

Options for the Cache Registration Service

This section contains parameters for the (optional) cache announcement service. This service is provided to help cache administrators locate one another in order to join or create cache hierarchies.

An 'announcement' message is sent (via UDP) to the registration service by SQUID. By default, the announcement message is NOT SENT unless you enable it with 'announce_period' below.

The announcement message includes your hostname, plus the following information from this configuration file:

http_port
icp_port
cache_mgr

All current information is processed regularly and made available on the Web at http://www.ircache.net/Cache/Tracker/.

announce_period

This is how frequently to send cache announcements. The default is `0' which disables sending the announcement messages.

To enable announcing your cache, just uncomment the line below.

To enable announcing your cache, just uncomment the line below.
announce_period 1 day

announce_host
announce_file
announce_port

announce_host and announce_port set the hostname and port number where the registration message will be sent.

Hostname will default to 'tracker.ircache.net' and port will default default to 3131. If the 'filename' argument is given, the contents of that file will be included in the announce message.

Miscellaneous

dns_testnames

The DNS tests exit as soon as the first site is successfully looked up

This test can be disabled with the -D command line option.

logfile_rotate

Specifies the number of logfile rotations to make when you type 'SQUID -k rotate'. The default is 10, which will rotate with extensions 0 through 9. Setting logfile_rotate to 0 will disable the rotation, but the logfiles are still closed and re-opened. This will enable you to rename the logfiles yourself just before sending the rotate signal.

Note, the 'SQUID -k rotate' command normally sends a USR1 signal to the running SQUID process. In certain situations (e.g. on Linux with Async I/O), USR1 is used for other purposes, so -k rotate uses another signal. It is best to get in the habit of using 'SQUID -k rotate' instead of 'kill -USR1 <pid>'.

append_domain

Appends local domain name to hostnames without any dots in them. append_domain must begin with a period.

Be warned that there today is Internet names with no dots in them using only top-domain names, so setting this may cause some Internet sites to become unavailable.

tcp_recv_bufsize (bytes)

Size of receive buffer to set for TCP sockets. Probably just as easy to change your kernel's default. Set to zero to use the default buffer size.

err_html_text

HTML text to include in error messages. Make this a "mailto" URL to your admin address, or maybe just a link to your organizations Web page.

To include this in your error messages, you must rewrite the error template files (found in the "errors" directory). Wherever you want the 'err_html_text' line to appear, insert a %L tag in the error template file.

deny_info

Usage: deny_info err_page_name acl
or deny_info http://... acl
Example: deny_info ERR_CUSTOM_ACCESS_DENIED bad_guys

This can be used to return a ERR_ page for requests which do not pass the 'http_access' rules. A single ACL will cause the http_access check to fail. If a 'deny_info' line exists for that ACL then SQUID returns a corresponding error page.

You may use ERR_ pages that come with SQUID or create your own pages and put them into the configured errors/ directory.

Alternatively you can specify an error URL. The browsers will then get redirected (302) to the specified URL. %s in the redirection URL will be replaced by the requested URL.

Alternatively you can tell SQUID to reset the TCP connection by specifying TCP_RESET.

memory_pools on|off

If set, SQUID will keep pools of allocated (but unused) memory available for future use. If memory is a premium on your system and you believe your malloc library outperforms SQUID routines, disable this.

memory_pools_limit (bytes)

Used only with memory_pools on:
memory_pools_limit 50 MB

If set to a non-zero value, SQUID will keep at most the specified limit of allocated (but unused) memory in memory pools. All free() requests that exceed this limit will be handled by your malloc library. SQUID does not pre-allocate any memory, just safe-keeps objects that otherwise would be free()d. Thus, it is safe to set memory_pools_limit to a reasonably high value even if your configuration will use less memory.

If not set (default) or set to zero, SQUID will keep all memory it can. That is, there will be no limit on the total amount of memory used for safe-keeping.

To disable memory allocation optimization, do not set memory_pools_limit to 0. Set memory_pools to "off" instead.

An overhead for maintaining memory pools is not taken into account when the limit is checked. This overhead is close to four bytes per object kept. However, pools may actually _save_ memory because of reduced memory thrashing in your malloc library.

forwarded_for on|off

If set, SQUID will include your system's IP address or name in the HTTP requests it forwards. By default it looks like this:

```
X-Forwarded-For: 192.1.2.3
```

If you disable this, it will appear as

```
X-Forwarded-For: unknown
```

log_icp_queries on|off

If set, ICP queries are logged to access.log. You may wish do disable this if your ICP load is VERY high to speed things up or to simplify log analysis.

icp_hit_stale on|off

If you want to return ICP_HIT for stale cache objects, set this option to 'on'. If you have sibling relationships with caches in other administrative domains, this should be 'off'. If you only have sibling relationships with caches under your control, then it is probably okay to set this to 'on'.

If set to 'on', then your siblings should use the option "allow-miss" on their cache_peer lines for connecting to you.

minimum_direct_hops

If using the ICMP pinging stuff, do direct fetches for sites which are no more than this many hops away.

minimum_direct_rtt

If using the ICMP pinging stuff, do direct fetches for sites which are no more than this many rtt milliseconds away.

cachemgr_passwd

Specify passwords for cachemgr operations.

Usage: cachemgr_passwd password action action ...

Some valid actions are (see cache manager menu for a full list):

```
5min
60min
asndb
authenticator
cbdata
client_list
comm_incoming
config *
counters
delay
digest_stats
dns
events
filedescriptors
fqdncache
histograms
http_headers
info
io
ipcache
mem
menu
netdb
non_peers
objects
offline_toggle *
pconn
peer_select
redirector
refresh
server_list
shutdown *
store_digest
storedir
utilization
via_headers
vm_objects
```

* Indicates actions which will not be performed without a valid password, others can be performed if not listed here.

To disable an action, set the password to "disable".

To allow performing an action without a password, set the password to "none".

Use the keyword "all" to set the same password for all actions.

Example:
cachemgr_passwd secret shutdown
cachemgr_passwd lesssssssecret info stats/objects
cachemgr_passwd disable all

store_avg_object_size (kbytes)
Average object size, used to estimate number of objects your cache can hold. See doc/Release-Notes-1.1.txt. The default is 13 KB.

store_objects_per_bucket
Target number of objects per bucket in the store hash table. Lowering this value increases the total number of buckets and also the storage maintenance rate. The default is 50.

client_db on|off
If you want to disable collecting per-client statistics, then turn off client_db here.

netdb_low
netdb_high
The low and high water marks for the ICMP measurement database. These are counts, not percents. The defaults are 900 and 1000. When the high water mark is reached, database entries will be deleted until the low mark is reached.

netdb_ping_period
The minimum period for measuring a site. There will be at least this much delay between successive pings to the same network. The default is five minutes.

query_icmp on|off
If you want to ask your peers to include ICMP data in their ICP replies, enable this option.

If your peer has configured SQUID (during compilation) with '--enable-icmp' then that peer will send ICMP pings to origin server sites of the URLs it receives. If you enable this option then the ICP replies from that peer will include the ICMP data (if available). Then, when choosing a parent cache, SQUID will choose the parent with the minimal RTT to the origin server. When this happens, the hierarchy field of the access.log will be "CLOSEST_PARENT_MISS". This option is off by default.

test_reachability on|off
When this is 'on', ICP MISS replies will be ICP_MISS_NOFETCH instead of ICP_MISS if the target host is NOT in the ICMP

database, or has a zero RTT.

buffered_logs on|off

cache.log log file is written with stdio functions, and as such it can be buffered or unbuffered. By default it will be unbuffered. Buffering it can speed up the writing slightly (though you are unlikely to need to worry unless you run with tons of debugging enabled in which case performance will suffer badly anyway..).

reload_into_ims on|off

When you enable this option, client no-cache or ``reload'' requests will be changed to If-Modified-Since requests. Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

see also refresh_pattern for a more selective approach.

always_direct

Usage: always_direct allow|deny [!]aclname ...

Here you can use ACL elements to specify requests which should ALWAYS be forwarded directly to origin servers. For example, to always directly forward requests for local servers use something like:

```
acl local-servers dstdomain my.domain.net
always_direct allow local-servers
```

To always forward FTP requests directly, use

```
acl FTP proto FTP
always_direct allow FTP
```

NOTE: There is a similar, but opposite option named 'never_direct'. You need to be aware that "always_direct deny foo" is NOT the same thing as "never_direct allow foo". You may need to use a deny rule to exclude a more-specific case of some other rule. Example:

```
acl local-external dstdomain external.foo.net
acl local-servers dstdomain  .foo.net
always_direct deny local-external
always_direct allow local-servers
```

This option replaces some v1.1 options such as local_domain and local_ip.

never_direct

Usage: never_direct allow|deny [!]aclname ...

never_direct is the opposite of always_direct. Please read the description for always_direct if you have not already.

With 'never_direct' you can use ACL elements to specify requests which should NEVER be forwarded directly to origin servers. For example, to force the use of a proxy for all requests, except those in your local domain use something like:

```
acl local-servers dstdomain .foo.net
acl all src 0.0.0.0/0.0.0.0
never_direct deny local-servers
never_direct allow all
```

or if SQUID is inside a firewall and there is local intranet servers inside the firewall then use something like:

```
acl local-intranet dstdomain .foo.net
acl local-external dstdomain external.foo.net
always_direct deny local-external
always_direct allow local-intranet
never_direct allow all
```

This option replaces some v1.1 options such as inside_firewall and firewall_ip.

header_access

Usage: header_access header_name allow|deny [!]aclname ...

WARNING: Doing this VIOLATES the HTTP standard. Enabling this feature could make you liable for problems which it causes.

This option replaces the old 'anonymize_headers' and the older 'http_anonymizer' option with something that is much more configurable. This new method creates a list of ACLs for each header, allowing you very fine-tuned header mangling.

You can only specify known headers for the header name. Other headers are reclassified as 'Other'. You can also refer to all the headers with 'All'.

For example, to achieve the same behaviour as the old 'http_anonymizer standard' option, you should use:

```
header_access From deny all
header_access Referer deny all
header_access Server deny all
header_access User-Agent deny all
header_access WWW-Authenticate deny all
header_access Link deny all
```

Or, to reproduce the old 'http_anonymizer paranoid' feature you should use:

```
header_access Allow allow all
header_access Authorization allow all
header_access WWW-Authenticate allow all
header_access Cache-Control allow all
header_access Content-Encoding allow all
header_access Content-Length allow all
header_access Content-Type allow all
header_access Date allow all
header_access Expires allow all
header_access Host allow all
header_access If-Modified-Since allow all
header_access Last-Modified allow all
header_access Location allow all
header_access Pragma allow all
header_access Accept allow all
header_access Accept-Charset allow all
header_access Accept-Encoding allow all
header_access Accept-Language allow all
header_access Content-Language allow all
header_access Mime-Version allow all
header_access Retry-After allow all
header_access Title allow all
header_access Connection allow all
header_access Proxy-Connection allow all
header_access All deny all
```

By default, all headers are allowed (no anonymizing is performed).

header_replace

Usage: header_replace header_name message
Example: header_replace User-Agent Nutscrape/1.0 (CP/M; 8-bit)

This option allows you to change the contents of headers denied with header_access above, by replacing them with some fixed string. This replaces the old fake_user_agent option.

By default, headers are removed if denied.

icon_directory

Where the icons are stored. These are normally kept in c:/SQUID/share/icons

error_directory

If you wish to create your own versions of the default (English) error files, either to customize them to suit your language or company copy the template English files to another directory and point this tag at them.

maximum_single_addr_tries

This sets the maximum number of connection attempts for a host that only has one address (for multiple-address hosts, each address is tried once).

The default value is three tries, the (not recommended)
maximum is 255 tries. A warning message will be generated
if it is set to a value greater than ten.

snmp_port

SQUID can now serve statistics and status information via SNMP.
By default it listens to port 3401 on the machine. If you don't
wish to use SNMP, set this to "0".

snmp_access

Allowing or denying access to the SNMP port.

All access to the agent is denied by default.
usage:

snmp_access allow|deny [!]aclname ...

Example:

```
 snmp_access allow snmppublic localhost
 snmp_access deny all
```

snmp_incoming_address
snmp_outgoing_address

Just like 'udp_incoming_address' above, but for the SNMP port.

```
snmp_incoming_address          is used for the SNMP socket receiving
                        messages from SNMP agents.
snmp_outgoing_address          is used for SNMP packets returned to SNMP
                        agents.
```

The default snmp_incoming_address (0.0.0.0) is to listen on all
available network interfaces.

If snmp_outgoing_address is set to 255.255.255.255 (the default)
then it will use the same socket as snmp_incoming_address. Only
change this if you want to have SNMP replies sent using another
address than where this SQUID listens for SNMP queries.

NOTE, snmp_incoming_address and snmp_outgoing_address can not have
the same value since they both use port 3401.

as_whois_server

WHOIS server to query for AS numbers. NOTE: AS numbers are
queried only when SQUID starts up, not for every request.

MIME Type Configuration Options

The MIME.CONF file associates filename extensions (for servers or services that don't automatically include them – like FTP) with a mime type and a graphical icon. Content-Encoding names are taken directly from section 3.1 of RFC2068 (HTTP/1.1)

This file has the following format information on each line:

RegEx Content-type icon name content-encoding transfer-mode

Here are a couple of examples from the default file:

```
\.bin$      application/macbinary anthony-unknown.gif  -          image
\.exe$      application/octet-stream       anthony-unknown.gif  -          image
\.pdf$      application/pdf         anthony-unknown.gif  -
```

It is unlikely that you will wish to modify the default MIME encoding that come in the shipped version of this product.

Cache Testing and Troubleshooting

Testing your PatchLink Distribution Point content caching solution

Setup 1: Deploy the PatchLink Distribution Point package to designated local patch storage server.

When deployed the package be will auto configured:

a) Setup cache folders
b) Configured to utilize port 25253

Setup 2: Verify that the Cache Server is Caching.

1. Point your web browser at the cache-ip and port 25253
2. Surf the web -- make sure you have no problems going thru the cache and hitting www.cnn.com, www.southcitygrill.com, etc.
3. Allow anonymous access to the updatestorage folder with directory browsing enabled via IIS
4. Browse to this location and right click "save as" on a few patches...do the same one twice
5. Check the c:\program files\patchlink\distribution point\var\logs directory and view the access.log, there will be TCP_HIT and TCP_MISS status lines:
   a. MISS <--- file not in cache
   b. HTTP_HIT <--- file pulled locally and not from upstream wire

Step Three: If all that works... test the agent...

1. Set the agent via control panel to use cache-ip address and the port 25253
2. Log into the Patch Management Server, and set the server's communication interval, under options, to 1 minute
3. Watch the log, (about 3 lines every 1 minute)… communication is working
4. Deploy the "A - Deployment Test and Diagnostic Package" to the agent
5. Watch the access.log file "AND" the local \windows\temp or \WINNT\temp directory for a text file to appear.
6. You should see a GET request in the LOG with a TCP-MISS
7. Deploy the same patch... watch the log
8. You should see a TCP_MEM_HIT <<< it's only a 1k file… it's a memory cached hit...
9. You can deploy any other patch and when you get to the additional flags field add –pldo (-pldo means just move the patch to the temp dir but don't execute)
10. Verify by watching access.log and looking at the temp dir for a .exe file or text file
11. Delete the file in temp dir.
12. Redo deployment... look for a TCP_HIT in the access.log

To remove the PatchLink Distribution Point server from the installed server:

```
Cd c:\program files\patchlink\distribution point\sbin
squid.exe –n patchlink_distribution –r
```

Troubleshooting

```
CD c:\program files\patchlink\distribution point\sbin
```

Execute the following to create the cache directories and get things set up:

```
squid.exe -f c:/progra~1/patchli~1/distrib~1/etc/squid.conf -z
```

Check to see if there are any errors in the Event Log.

Execute the following to manually run the PatchLink Distribution Point application:

```
squid.exe -f c:/progra~1/patchli~1/distrib~1/etc/squid.conf
```

Look in c:\program files\patchlink\distribution point\VAR\CACHE.LOG if the Squid process dies. See what it says if there are any other mis-configurations.
Fix any mis-configurations or problems and retry these Trouble shooting steps.

Other supported operating systems

Linux agent versions

ZENworks® Patch Management supports several distributions of Red Hat Linux including:

- 7.0, 7.1, 7.2, 7.3
- 8.0
- 9.0

The Linux agent requires the Java Runtime Environment (JRE) v1.2.2 or above, and can only be installed in single agent mode.

UNIX versions

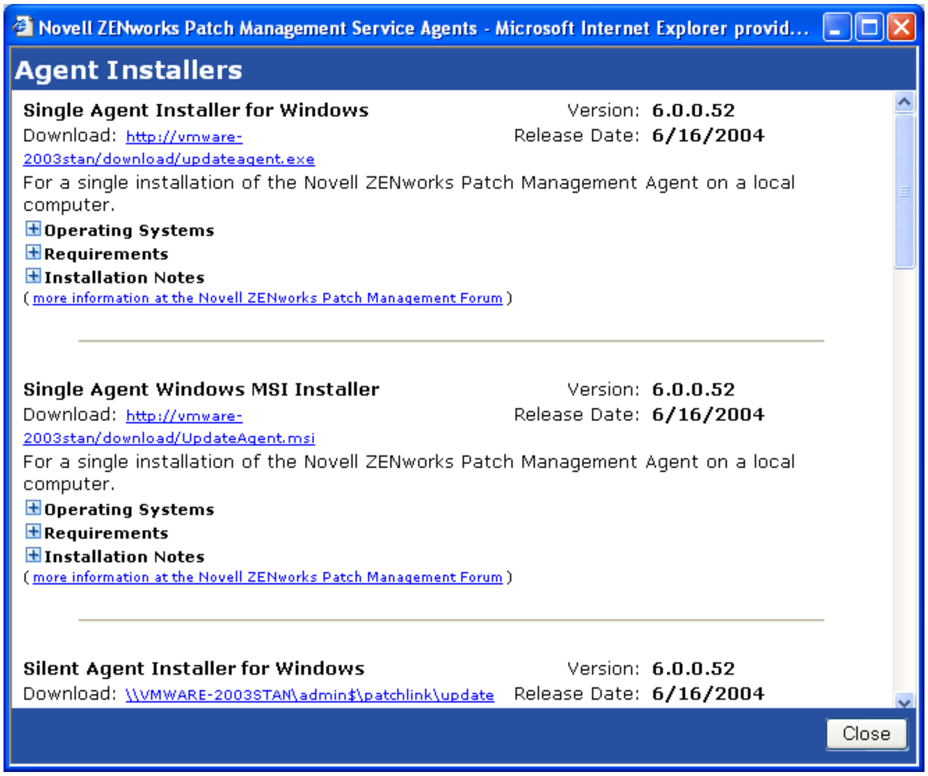
Like Linux, the UNIX requires JRE v1.2.2 and above. The following operation systems are supported:

- Solaris
- v2.5, v2.6,v 2.7, v7, and v8

Single Agent

The Single Agent Installer is used to manually add a single computer to the managed computers list. This is most often used in the case of stand alone computers.

The agent installer screen contains links to all of the agent installations and additional information on Operating Systems, Requirements, and Installation Notes.



Novell ZENworks Patch Management Service Agents - Microsoft Internet Explorer provid...

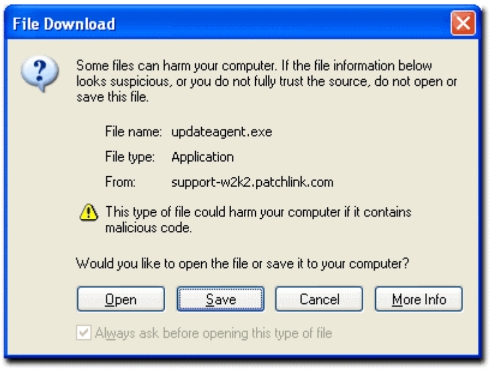
Agent Installers

Single Agent Installer for Windows Version: **6.0.0.52**
Download: http://vmware-2003stan/download/updateagent.exe Release Date: **6/16/2004**
For a single installation of the Novell ZENworks Patch Management Agent on a local computer.
⊞ **Operating Systems**
⊞ **Requirements**
⊞ **Installation Notes**
(more information at the Novell ZENworks Patch Management Forum)

Single Agent Windows MSI Installer Version: **6.0.0.52**
Download: http://vmware-2003stan/download/UpdateAgent.msi Release Date: **6/16/2004**
For a single installation of the Novell ZENworks Patch Management Agent on a local computer.
⊞ **Operating Systems**
⊞ **Requirements**
⊞ **Installation Notes**
(more information at the Novell ZENworks Patch Management Forum)

Silent Agent Installer for Windows Version: **6.0.0.52**
Download: \\VMWARE-2003STAN\admin$\patchlink\update Release Date: **6/16/2004**

- Select the Single Agent Installer for Windows link.



File Download

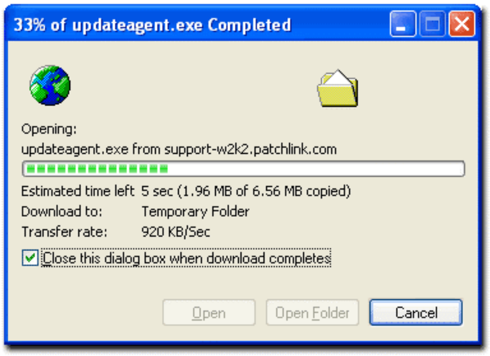
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: updateagent.exe
File type: Application
From: support-w2k2.patchlink.com

This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

- Click on the **Open** button

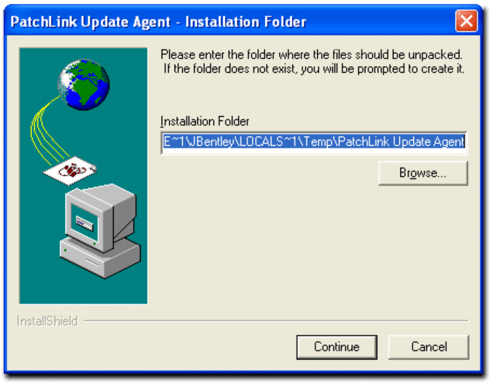


33% of updateagent.exe Completed

Opening:
updateagent.exe from support-w2k2.patchlink.com

Estimated time left 5 sec (1.96 MB of 6.56 MB copied)
Download to: Temporary Folder
Transfer rate: 920 KB/Sec
☑ Close this dialog box when download completes

- Select the destination directory for the installation files, and click on the **Continue**.

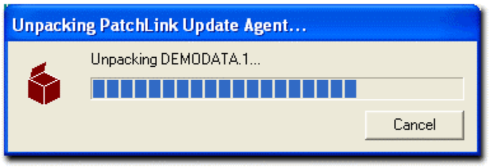


PatchLink Update Agent - Installation Folder

Please enter the folder where the files should be unpacked. If the folder does not exist, you will be prompted to create it.

Installation Folder: E~1\JBentley\LOCALS~1\Temp\PatchLink Update Agent

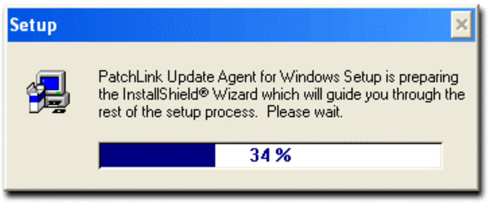
- Files Unpack



Unpacking PatchLink Update Agent...

Unpacking DEMODATA.1...

- Files Setup

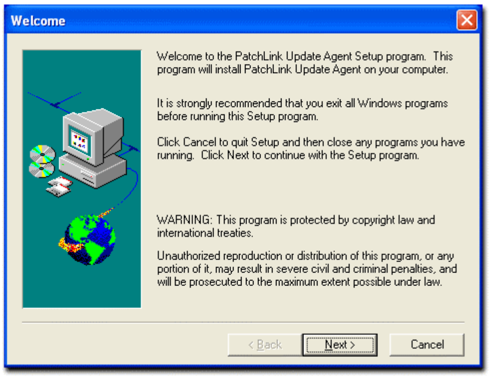


Setup

PatchLink Update Agent for Windows Setup is preparing the InstallShield® Wizard which will guide you through the rest of the setup process. Please wait.

34 %

- Read the Welcome screen and click **Next** to continue.



Welcome

Welcome to the PatchLink Update Agent Setup program. This program will install PatchLink Update Agent on your computer.

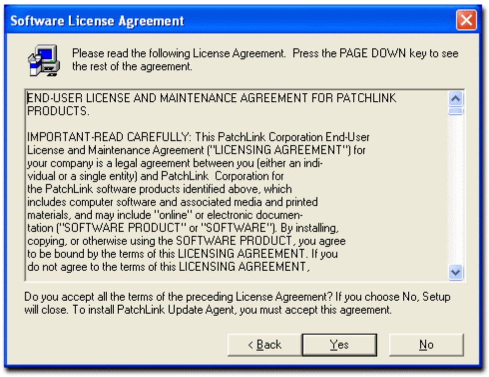
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

- Read the license agreement, and click “Yes” to continue



Software License Agreement

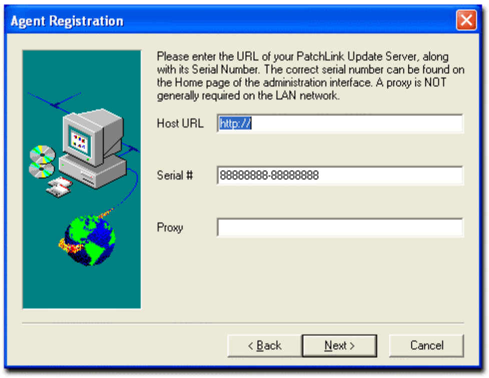
Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

END-USER LICENSE AND MAINTENANCE AGREEMENT FOR PATCHLINK PRODUCTS.

IMPORTANT-READ CAREFULLY: This PatchLink Corporation End-User License and Maintenance Agreement ("LICENSING AGREEMENT") for your company is a legal agreement between you (either an individual or a single entity) and PatchLink Corporation for the PatchLink software products identified above, which includes computer software and associated media and printed materials, and may include "online" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this LICENSING AGREEMENT. If you do not agree to the terms of this LICENSING AGREEMENT,

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install PatchLink Update Agent, you must accept this agreement.

- Enter the “Host URL”, “Serial #”, and “Proxy” server address, then click “Next” to continue.



Agent Registration

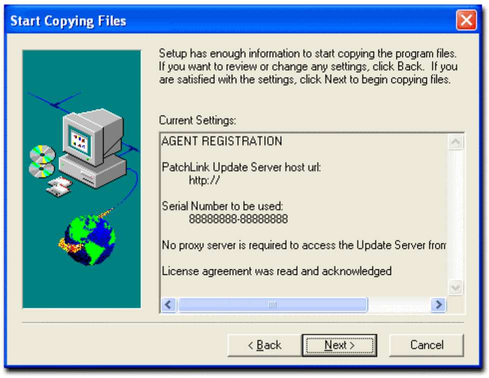
Please enter the URL of your PatchLink Update Server, along with its Serial Number. The correct serial number can be found on the Home page of the administration interface. A proxy is NOT generally required on the LAN network.

Host URL: http://

Serial #: 88888888-88888888

Proxy:

- Confirm the installation settings, and click “Next” to continue.



Start Copying Files

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

AGENT REGISTRATION

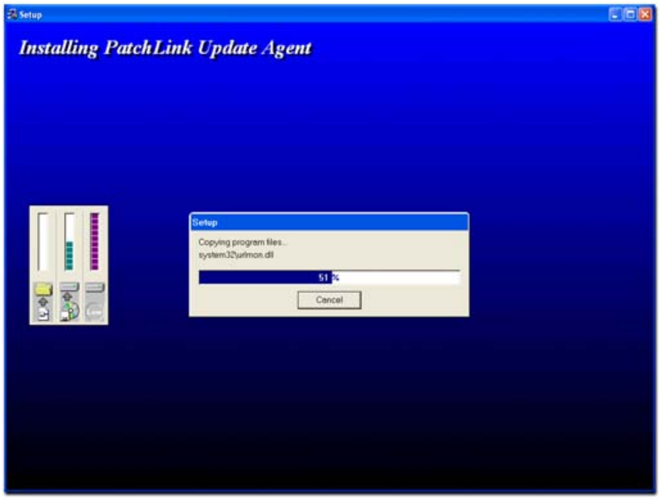
PatchLink Update Server host url:
http://

Serial Number to be used:
88888888-88888888

No proxy server is required to access the Update Server from

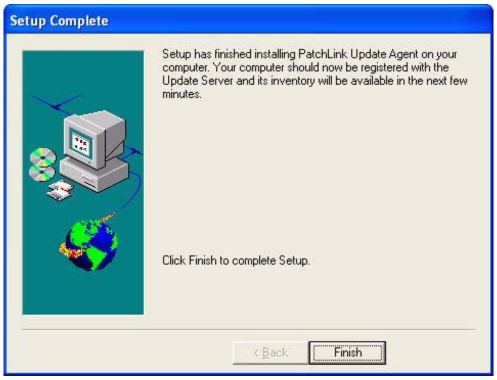
License agreement was read and acknowledged

- Patch Management Agent Installs.



Copying program files...
system32\urlmon.dll

- Click **Finish** to complete the installation



Setup has finished installing PatchLink Update Agent on your computer. Your computer should now be registered with the Update Server and its inventory will be available in the next few minutes.

Click Finish to complete Setup.

View

To display additional information about the computer, select a computer and click on the View button. This performs the same function as clicking on the name of the computer.

Enable

To enable selected disabled computers, click on the Enable button.

Disable

To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.

Export

Export the computer list data to a comma-separated value (CSV) file. The filter and order of the data is based on what the Computer List view is selected and sorted on.

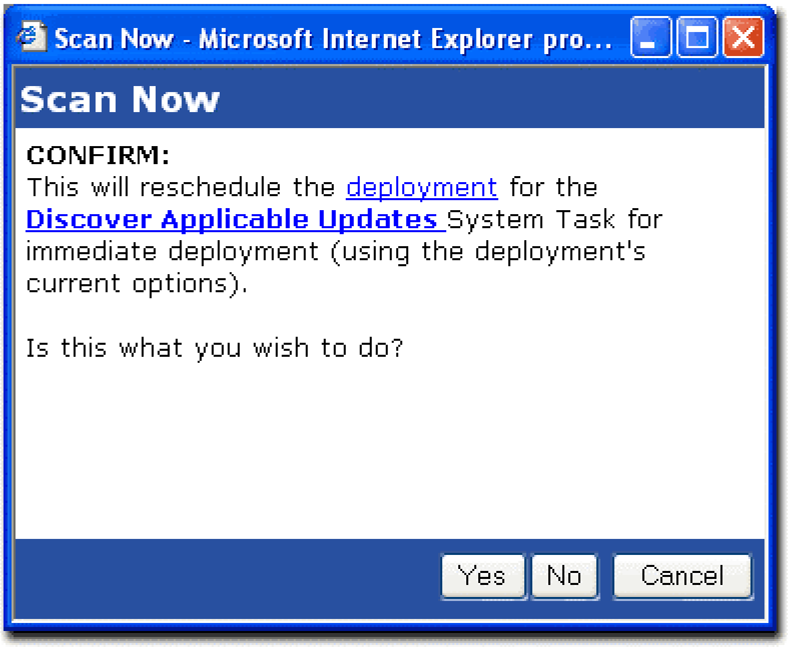
This may display only a certain number of computers per page, the export will save all computer data based on your selected filter.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected computers.

To initialize (choose) all computers, click the **Scan Now** button without selecting any computers.

If you choose not to select any computers, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the computers.

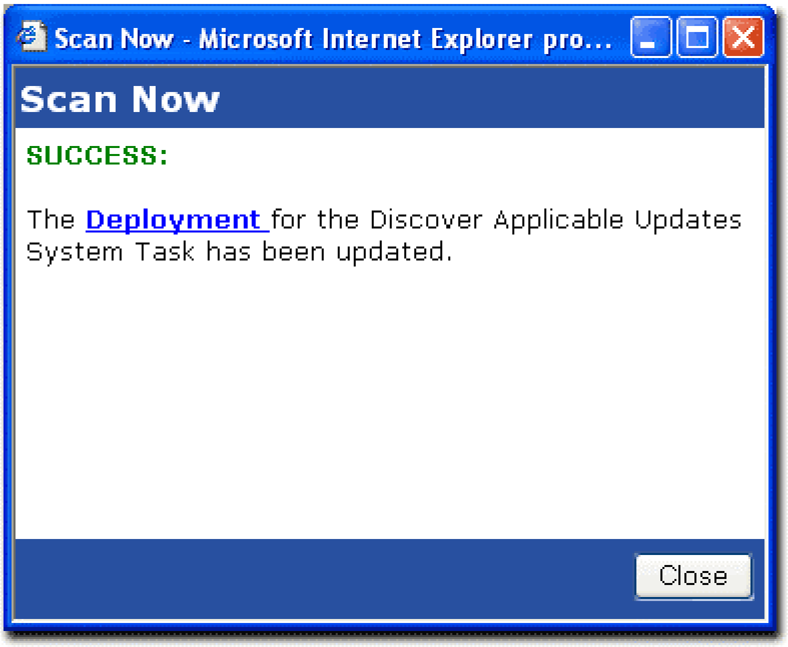


Scan Now

CONFIRM:
This will reschedule the deployment for the Discover Applicable Updates System Task for immediate deployment (using the deployment's current options).

Is this what you wish to do?

To reschedule the **Discover Applicable Updates**, select Yes.



Scan Now

SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

The Patch Management Server will reschedule the selected computer(s)'s membership (or all computers' memberships), initialize a screen stating its success and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the screen, the Computers page will be refreshed and initialized. Previously selected deployment options are maintained.

Computers Security

The Computer List section of the Patch Management Server requires the View Computers access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to be able display the agent installers' page requires the Install Computers access right. If a user does not have the correct access, the Install button is displayed. Once a computer registers against the Patch Management Server a Patch Management Administrator must give access to that computer to other user security roles.

To be able to enable, disable, and remove computers requires the Manage Computers access right. If a user does not have the correct access, the Enable, Disable, and Remove buttons are disabled.

To export the computer data to a comma-separated value (CSV) file requires the Export Computer Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

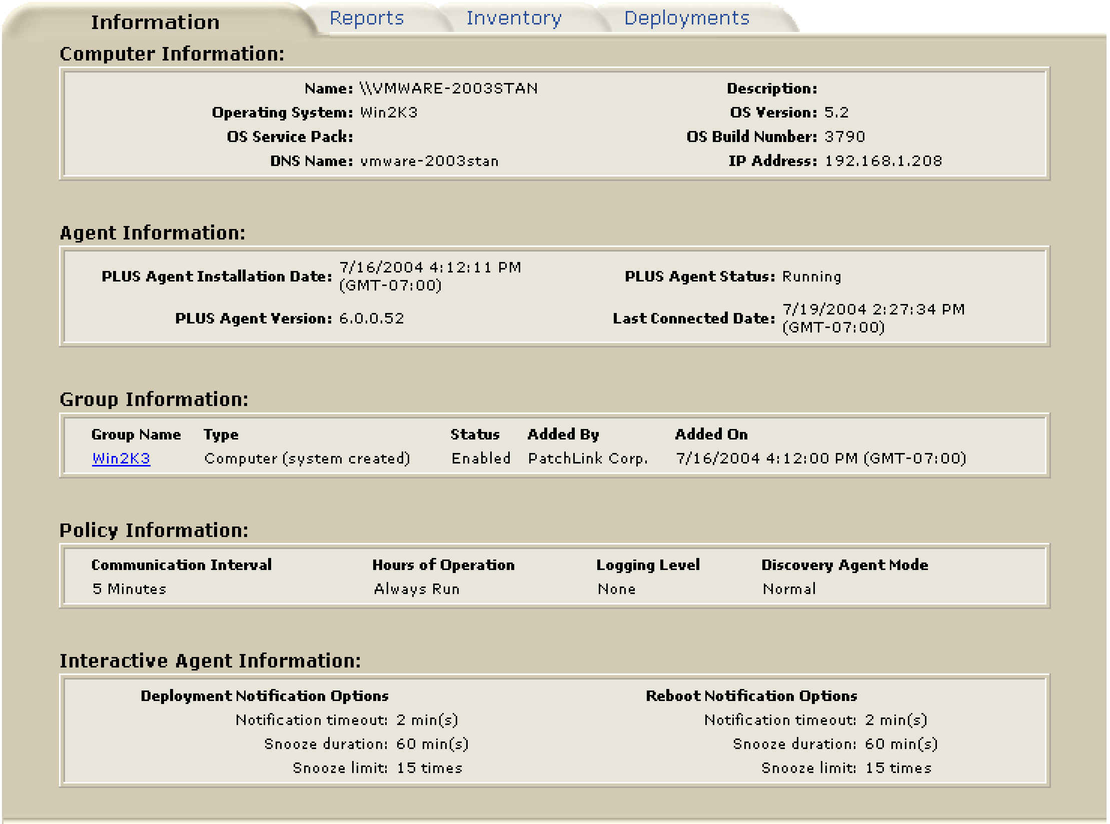
Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Computer Details

The Computer Details section of the Patch Management Server displays Server related and important information about a specific computer. Click on the actual Computer Name link under the Computer Name column. This will bring you to the details page.

- Selecting Reports Tab will display the Vulnerability Report Analysis for the computer.
- Selecting Inventory Tab will display the Inventory for the computer.
- Selecting Deployments Tab will display the deployments for the computer.

The Reports, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer. See Section 5; Vulnerability Reports, Section 6; Inventory, and Section 7; Packages for more detailed information.



Computer Information:

Name: \\VMWARE-2003STAN
Operating System: Win2K3
OS Service Pack:
DNS Name: vmware-2003stan
Description:
OS Version: 5.2
OS Build Number: 3790
IP Address: 192.168.1.208

Agent Information:

PLUS Agent Installation Date: 7/16/2004 4:12:11 PM (GMT-07:00)
PLUS Agent Status: Running
PLUS Agent Version: 6.0.0.52
Last Connected Date: 7/19/2004 2:27:34 PM (GMT-07:00)

Group Information:

Group Name	Type	Status	Added By	Added On
Win2K3	Computer (system created)	Enabled	PatchLink Corp.	7/16/2004 4:12:00 PM (GMT-07:00)

Policy Information:

Communication Interval	Hours of Operation	Logging Level	Discovery Agent Mode
5 Minutes	Always Run	None	Normal

Interactive Agent Information:

Deployment Notification Options
Notification timeout: 2 min(s)
Snooze duration: 60 min(s)
Snooze limit: 15 times

Reboot Notification Options
Notification timeout: 2 min(s)
Snooze duration: 60 min(s)
Snooze limit: 15 times

If information is not applicable to a specific section, the section will simply not be present on the details page.

Computer Information

- Name: This displays the name of the computer

- Operating System: This displays the abbreviated operating system platform name of the computer.
- OS Service Pack: This displays the service pack level of the computer
- DNS Name: This displays the DNS name of the computer.
- Description: This displays the description of the computer.
- OS Version: This displays the operating system version number of the computer.
- OS Build Number: This displays the operating system build number of the computer.
- IP Address: This displays the IP Address of the computer.

Agent Information

- Patch Management Server Agent Installation Date: The date the agent was installed and registered against the Patch Management Server.
- Patch Management Server Agent Version: This displays the version of the agent.
- Patch Management Server Agent Status: This displays the status of the agent.
- Last Connected Date: The date the agent last contacted the Patch Management Server.

Group Information

- Group Name: This displays the name of the group the computer is a member of.
- Type: This displays the type of the group.
- Status: This displays the status of the group.
- Added By: This displays the User who added the computer to the group.
- Added On: This displays the date the computer was added to the group.

Policy Information

- Communication Level: This displays how often the agent communicates with the Patch Management Server.
- Hours of Operation: This displays the hours of operation in which the agent will communicate with the Patch Management Server.
- Logging Level: The logging level determines how much data the agent will log while it performs its tasks.

Page Functions

Reports Tab

Selecting this tab will display the Vulnerability Report Analysis for the computer.

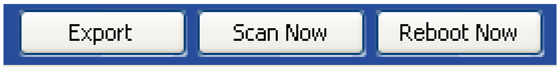
Inventory Tab

Selecting this tab will display the Inventory for the computer.

Deployments Tab

Selecting this tab will display the deployments for the computer.

Action Menu



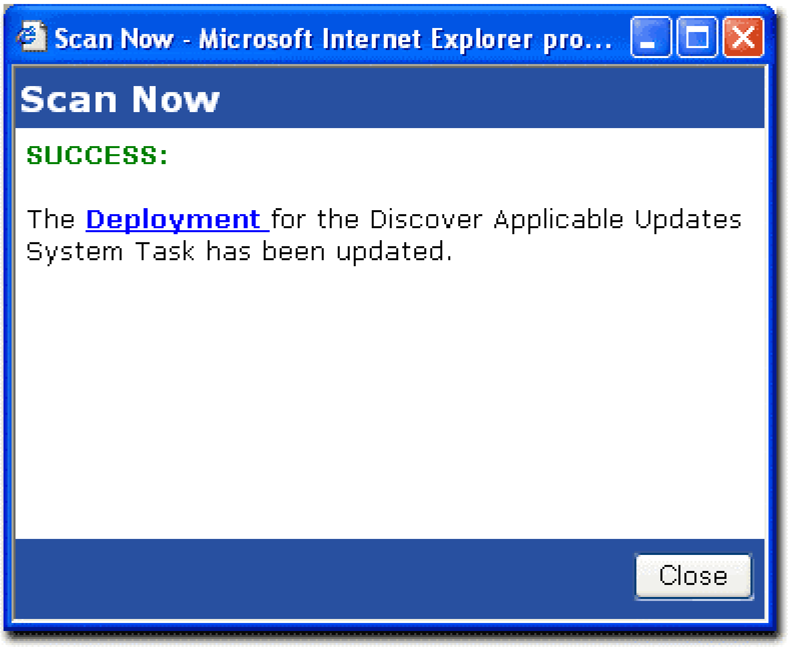
Export

Export the computer information to a comma-separated value (CSV) file.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected computers.

The Patch Management Server will reschedule the computer and initialize a screen stating its success and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.



Scan Now

SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

Upon clicking the Close button on the screen, the Computers page will be refreshed and initialized. Previously selected deployment options are maintained.

Computer Details Security

The Computer Information section of the Patch Management Server requires the View Computers access right. If a user does not have the correct access, the access denied error message is displayed.

To export the computer information to a comma-separated value (CSV) file requires the Export Computer Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

To be able to view the vulnerability reports results for the computer requires the View Reports access right. If a user does not have the correct access, the Reports tab is disabled.

To be able to view the computer inventory section requires the View OS Inventories access right. If a user does not have the correct access, the Inventory tab is disabled.

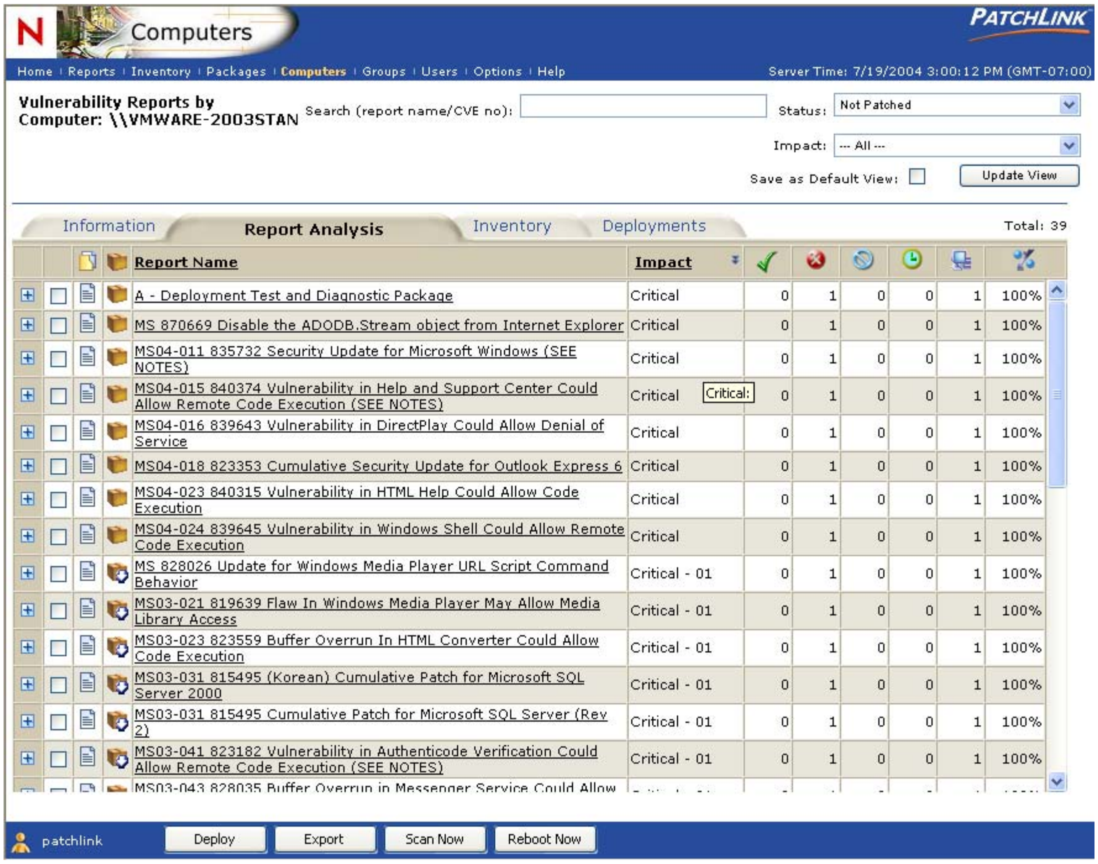
To be able to view the computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Detection Reports by Computer

A Vulnerability Report encompasses any vulnerability, how to detect it, and its associated patch or patches. The detection portion of it, also called a Vulnerability Report, contains the necessary signatures and fingerprints on which to properly determine if the vulnerability is patched or not patched.

Click on the actual **Reports Tab** in the Computer Details screen.



Server Time: 7/19/2004 3:00:12 PM (GMT-07:00)

Vulnerability Reports by Computer: \\VMWARE-2003STAN

Search (report name/CVE no):

Status: Not Patched

Impact: --- All ---

Save as Default View: □

Total: 39

Report Name	Impact	✓	✗	⊘	◷	🖥	%
A - Deployment Test and Diagnostic Package	Critical	0	1	0	0	1	100%
MS 870669 Disable the ADODB.Stream object from Internet Explorer	Critical	0	1	0	0	1	100%
MS04-011 835732 Security Update for Microsoft Windows (SEE NOTES)	Critical	0	1	0	0	1	100%
MS04-015 840374 Vulnerability in Help and Support Center Could Allow Remote Code Execution (SEE NOTES)	Critical	0	1	0	0	1	100%
MS04-016 839643 Vulnerability in DirectPlay Could Allow Denial of Service	Critical	0	1	0	0	1	100%
MS04-018 823353 Cumulative Security Update for Outlook Express 6	Critical	0	1	0	0	1	100%
MS04-023 840315 Vulnerability in HTML Help Could Allow Code Execution	Critical	0	1	0	0	1	100%
MS04-024 839645 Vulnerability in Windows Shell Could Allow Remote Code Execution	Critical	0	1	0	0	1	100%
MS 828026 Update for Windows Media Player URL Script Command Behavior	Critical - 01	0	1	0	0	1	100%
MS03-021 819639 Flaw In Windows Media Player May Allow Media Library Access	Critical - 01	0	1	0	0	1	100%
MS03-023 823559 Buffer Overrun In HTML Converter Could Allow Code Execution	Critical - 01	0	1	0	0	1	100%
MS03-031 815495 (Korean) Cumulative Patch for Microsoft SQL Server 2000	Critical - 01	0	1	0	0	1	100%
MS03-031 815495 Cumulative Patch for Microsoft SQL Server (Rev 2)	Critical - 01	0	1	0	0	1	100%
MS03-041 823182 Vulnerability in Authenticode Verification Could Allow Remote Code Execution (SEE NOTES)	Critical - 01	0	1	0	0	1	100%
MS03-043 828035 Buffer Overrun in Messenger Service Could Allow							

patchlink

Vulnerability Report Analysis

This section displays the analysis results of the vulnerability reports during the discovery and analysis process on the computer. The report analysis gives a simple top-down view of the computer in each status.

The Reports, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer. See Section 5; Vulnerability Reports, Section 6; Inventory, and Section 7; Packages for more detailed information.

Page Functions

Information Tab

Selecting this tab will display additional Computer Information.

Inventory Tab

Selecting this tab will display the Inventory for the computer.

Deployments Tab

Selecting this tab will display the deployments that the computer has been assigned to.

Action Menu

Deploy

This creates a deployment for the selected vulnerability report. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

Export

Export the vulnerability report analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.

Computer Vulnerability Security

The Computer Reports section of the Patch Management Server requires the View Reports Page access right. If a user does not have the correct access the access denied error message is displayed.

To be able to change the filter from detected vulnerability reports to disabled or all requires the Change Report Filter access right. If a user does not have the correct access, the filter will not have any options to choose from.

To be able to view the associated distribution packages for a given vulnerability report requires the View Packages access right. If a user does not have the correct access, the link on the package status image is disabled.

To be able to create a deployment based on the report analysis requires the Deploy Reports access right. If a user does not have the correct access, the Deploy button is disabled.

To export all of the vulnerability report analysis's to a comma-separated value (CSV) file requires the Export Report Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

To be able to view the computer inventory section requires the View OS Inventories access right. If a user does not have the correct access, the Inventory tab is disabled.

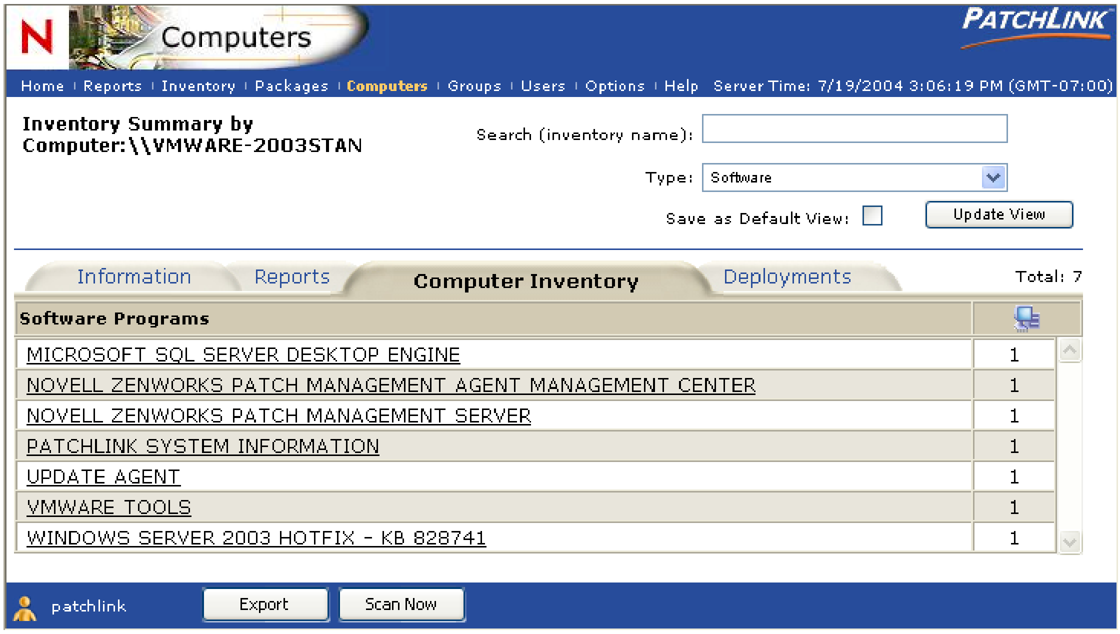
To be able to view the computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Computer Inventory Summary

The following inventories are gathered while in the discovery and analysis process: Operating Systems, Installed Software, Hardware and their device drivers, and Services. The Filter changes the display between the different inventories. When displaying the Inventory based on a single computer, the Software inventory is the initial inventory displayed.

The Reports, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer. See Section 5; Vulnerability Reports, Section 6; Inventory, and Section 7; Packages for more detailed information.



Server Time: 7/19/2004 3:06:19 PM (GMT-07:00)

Inventory Summary by Computer:\\VMWARE-2003STAN

Search (inventory name):

Type: Software

Save as Default View: □

Total: 7

Software Programs	
MICROSOFT SQL SERVER DESKTOP ENGINE	1
NOVELL ZENWORKS PATCH MANAGEMENT AGENT MANAGEMENT CENTER	1
NOVELL ZENWORKS PATCH MANAGEMENT SERVER	1
PATCHLINK SYSTEM INFORMATION	1
UPDATE AGENT	1
VMWARE TOOLS	1
WINDOWS SERVER 2003 HOTFIX - KB 828741	1

Page Functions

Information Tab

Selecting this tab will display additional Computer Information.

Reports Tab

Selecting this tab will display the results of the Discovery and Analysis process for the Vulnerability Reports.

Deployments Tab

Selecting this tab will display the deployments that the computer has been assigned to.

Action Menu

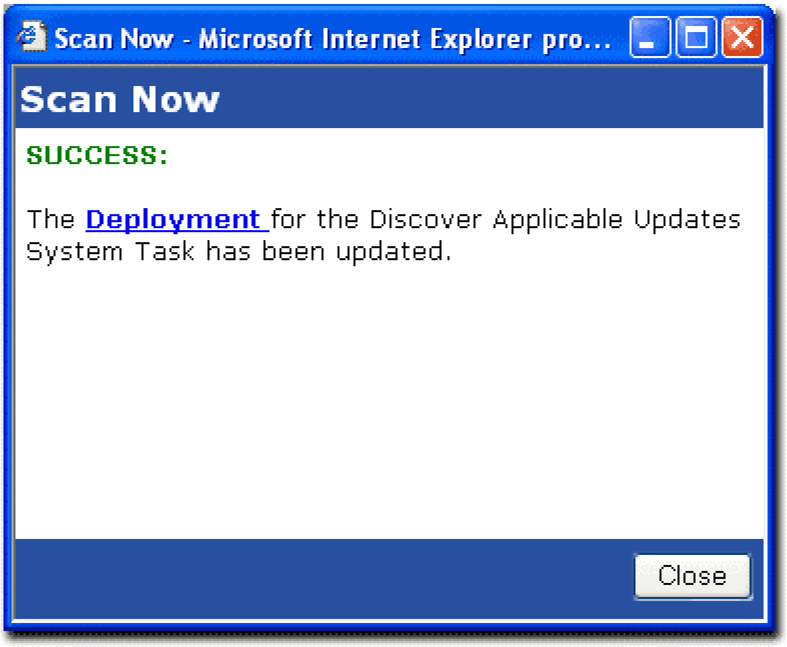
Export

Export the vulnerability report analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates System Task** deployment for immediate execution to all selected computers.

The Patch Management Server will reschedule the computer and initialize a screen stating its success and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.



SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

Upon clicking the Close button on the screen, the Computers page will be refreshed and initialized. Previously selected deployment options are maintained.

Computer Inventory Security

The Computer Inventory section of the Patch Management Server requires the View OS Inventories access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the Software inventory requires the View Software Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Hardware inventory requires the View Hardware Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Services inventory requires the View Services Inventories access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the list of computers on which an inventory belongs to requires the View Computers access right. If a user does not have the correct access, the hyperlink on the inventory item is disabled.

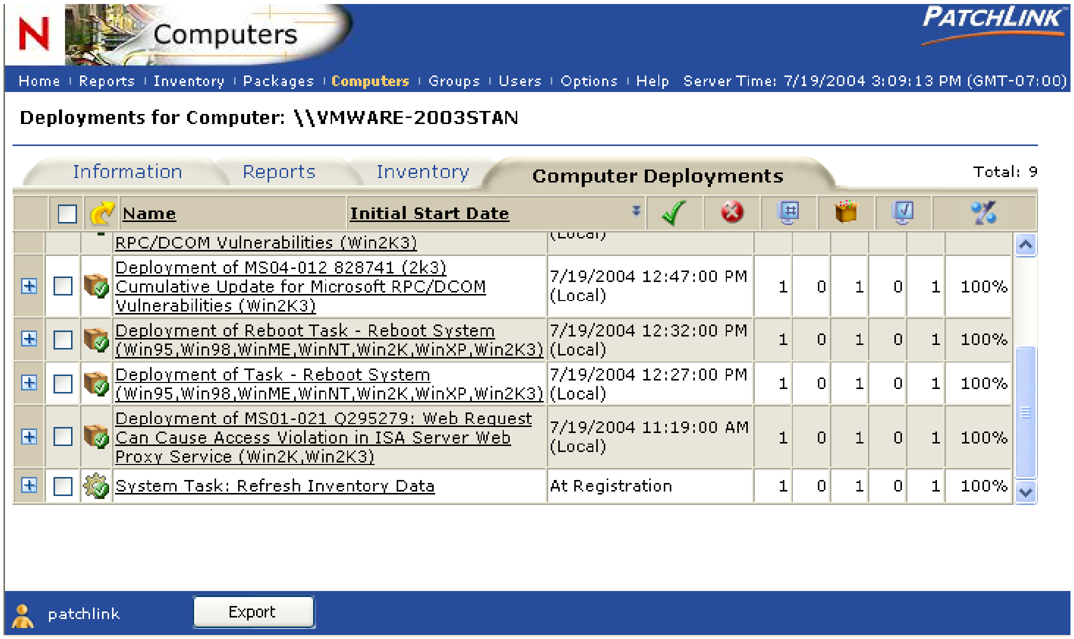
To export the inventory to a comma-separated value (CSV) file requires the Export Inventory Data access right. If a user does not have the correct access, the Export button is disabled.

To be able to view the vulnerability reports results for the computer requires the View Reports access right. If a user does not have the correct access, the Reports tab is disabled.

To be able to view the computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Computer Deployments

The Computer Deployments section displays all of the deployments that the computer has been assigned to.


N
Computers
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Information
Reports
Inventory
Computer Deployments
patchlink
Export

Server Time: 7/19/2004 3:09:13 PM (GMT-07:00)

Deployments for Computer: \\VMWARE-2003STAN

Total: 9

	□		Name	Initial Start Date	✓	✗				%
			RPC/DCOM Vulnerabilities (Win2K3)	(Local)						
⊞	□		Deployment of MS04-012 828741 (2k3) Cumulative Update for Microsoft RPC/DCOM Vulnerabilities (Win2K3)	7/19/2004 12:47:00 PM (Local)	1	0	1	0	1	100%
⊞	□		Deployment of Reboot Task - Reboot System (Win95,Win98,WinME,WinNT,Win2K,WinXP,Win2K3)	7/19/2004 12:32:00 PM (Local)	1	0	1	0	1	100%
⊞	□		Deployment of Task - Reboot System (Win95,Win98,WinME,WinNT,Win2K,WinXP,Win2K3)	7/19/2004 12:27:00 PM (Local)	1	0	1	0	1	100%
⊞	□		Deployment of MS01-021 Q295279: Web Request Can Cause Access Violation in ISA Server Web Proxy Service (Win2K,Win2K3)	7/19/2004 11:19:00 AM (Local)	1	0	1	0	1	100%
⊞	□		System Task: Refresh Inventory Data	At Registration	1	0	1	0	1	100%

The Reports, Inventory, and Deployments tabs serve as a quick link to those related inquiries for a specific computer. See Section 5; Vulnerability Reports, Section 6; Inventory, and Section 7; Packages for more detailed information.

Action Menu

Export

Export

Export the vulnerability report analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.

Page Functions

Information Tab

Selecting this tab will display additional Computer Information.

Reports Tab

Selecting this tab will display the results of the Discovery and Analysis process for the Vulnerability Reports.

Inventory Tab

Selecting this tab will display the Inventory for the computer.

Computer Deployments Security

The computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to view the vulnerability reports results for the computer requires the View Reports access right. If a user does not have the correct access, the Reports tab is disabled.

To be able to view the computer inventory section requires the View OS Inventories access right. If a user does not have the correct access, the Inventory tab is disabled.

To be able to view the computer deployments section requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

To be able to export the computer deployment data requires the Export Deployment Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

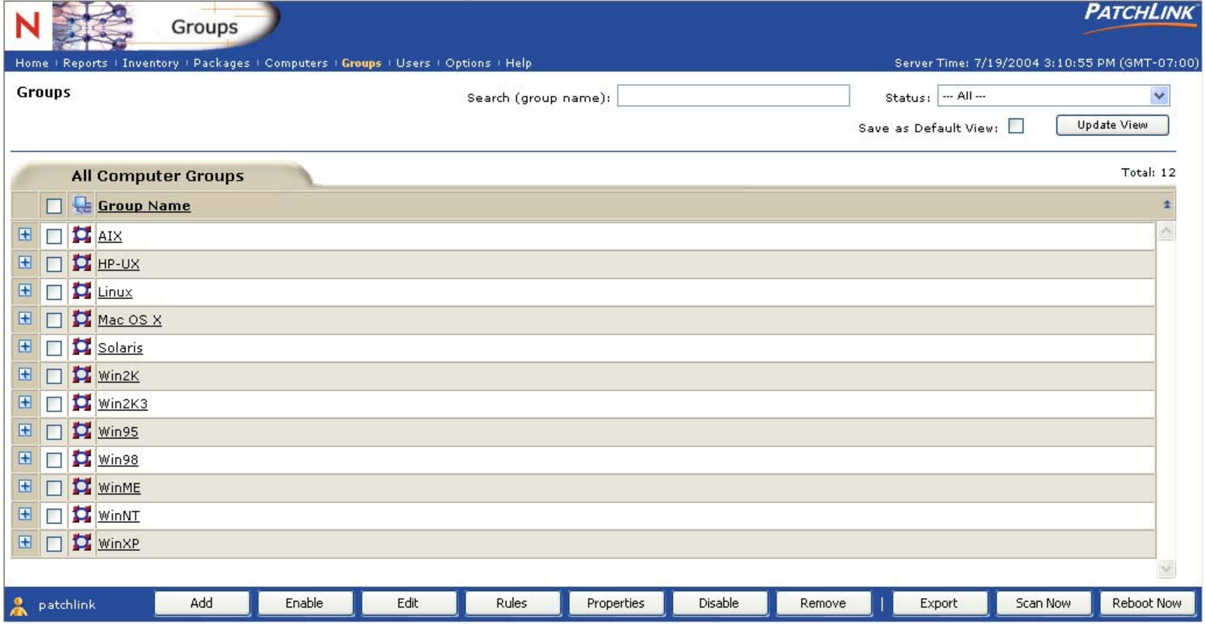
11. Groups

Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |

A group is a collection of computers for the purpose of making deployments on a “groupwise” basis.

The purpose is based upon user specification to provide an easier way to manage the entire group rather than managing each computer one at a time.

Clicking on the group name will display the group information and properties page. This is the same thing as selecting the group and clicking on the Properties button.


N
Groups
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help

Server Time: 7/19/2004 3:10:55 PM (GMT-07:00)

Groups

Search (group name):

Status: --- All ---

Save as Default View: □

All Computer Groups

Total: 12

	□	Group Name
⊞	□	AIX
⊞	□	HP-UX
⊞	□	Linux
⊞	□	Mac OS X
⊞	□	Solaris
⊞	□	Win2K
⊞	□	Win2K3
⊞	□	Win95
⊞	□	Win98
⊞	□	WinME
⊞	□	WinNT
⊞	□	WinXP

patchlink

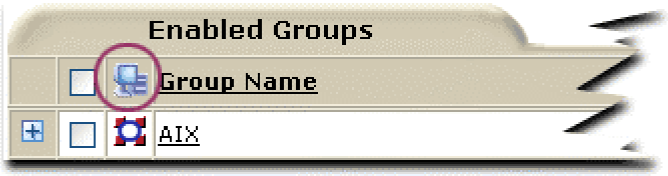
With a group you can:

- Deploy a distribution package (from an associated Vulnerability or local distribution package) to all computers of the group. When deploying from the Vulnerability Report’s section, the only computers which will receive the distribution package are the ones that are applicable to the vulnerability report.
- Define a set of policies which determine the behavior of the agents installed on those computers.
- Define a baseline of Vulnerability Reports or local distribution packages which are declared as mandatory. This ensures that these baseline items must be installed or detected as patched; else the deployments for those items will be auto-generated for immediate execution.
- View the results of the Vulnerability Report Analysis for the entire membership of the group.

- View the results of the detected Inventory for the entire membership of the group.
- Reschedule the Discovery and Analysis process (Discover Applicable Updates System Task) to verify the Inventory and Report data is current.

Group Status

This displays the various groups that have been pre-generated by the Patch Management Server or user-defined by the local administrator. Each group entry displays the name of the group plus the status and type of the group.



Status	Description
▣	This is an enabled system group. One system group is formed automatically corresponding to each operating system in the network.
▢	This is a disabled system group. One system group is formed automatically corresponding to each operating system in the network. Reports are prevented from running on computers in this group.
◉	This is a enabled system group. These are the groups which are manually created by the administrator. Either one agent or multiple agents belonging to multiple operating systems can be added to a group.
○	This is a disabled system group. These are the groups which are manually created by the administrator. Either one agent or multiple agents belonging to multiple operating systems can be added to a group. Reports are prevented from running on computers in this group.

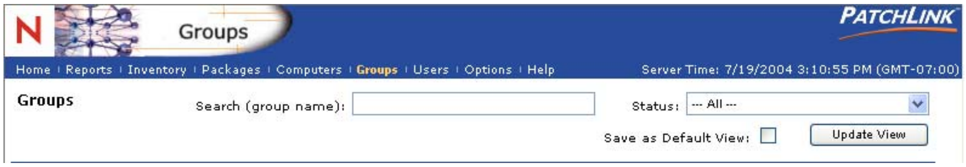
Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟,⊞) is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Groups page header.



Groups

PATCHLINK

Home | Reports | Inventory | Packages | Computers | **Groups** | Users | Options | Help

Server Time: 7/19/2004 3:10:55 PM (GMT-07:00)

Groups

Search (group name):

Status: --- All ---

Save as Default View: □

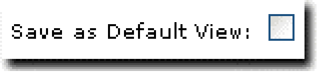
Update View

- Search

  Search (group name):

  You may search Groups for more granular results by entering the group name text into the **Search** field and clicking on the Update View Update View button.

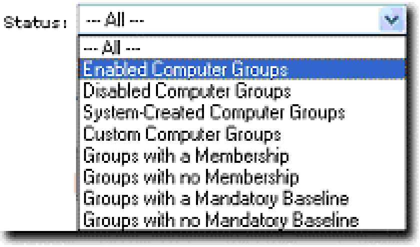
  This will return the Group(s) having the name of the entered text.   You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

  Save as Default View: □

- Status

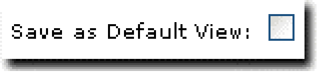
  Filter by Status using the dropdown menu and click on the Update View Update View button.

  Status: --- All ---

  --- All ---
  Enabled Computer Groups
  Disabled Computer Groups
  System-Created Computer Groups
  Custom Computer Groups
  Groups with a Membership
  Groups with no Membership
  Groups with a Mandatory Baseline
  Groups with no Mandatory Baseline

  This will return the Group(s) having the selected status.   You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

  Save as Default View: □

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

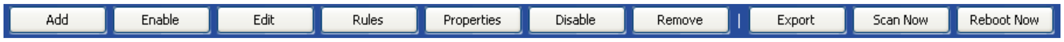
Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Add

Clicking this button will bring up the Group Property page allowing new groups to be created See Section 12; Add a Group Wizard for more information.

Edit

By clicking on the button, a edit group wizard comes up in which u can enter all the information about the already existing group. See Section 12; Add a Group Wizard for more information.

Rules

Clicking the Rules button allows the User the ability to create and populate a group based on a few minimal parameters. Group Name, Group Description, and a comma-delimited list of computer names (Windows computers must be prefixed with \\) may be entered.

Properties

Selecting a group and clicking on this button will display the group information and properties page.

Disable

This disables all group-based functionality for the group members.

Enable

This enabled all of the group-based functionality for the group members.

Remove

This will delete all selected disabled groups.

Export

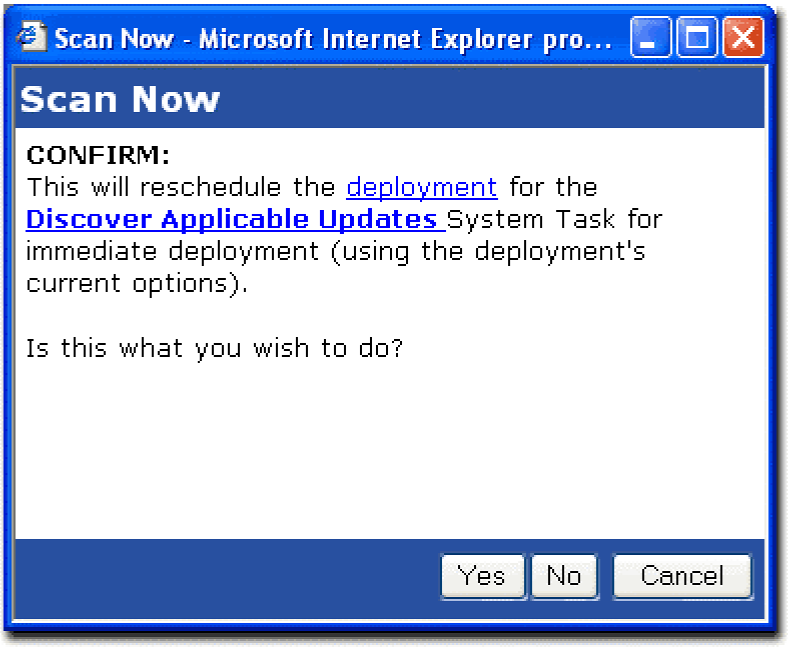
Export the group data to a comma-separated value (CSV) file. The amount and order of the data is based on what the Group List view is filtered and sorted on.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected groups.
To initialize (choose) all groups, click on the Scan Now button without selecting any groups **or** select a group (or Groups) by clicking in the checkbox and click the **Scan**

Now button.

If you choose to not select any groups, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the members for all of the groups.

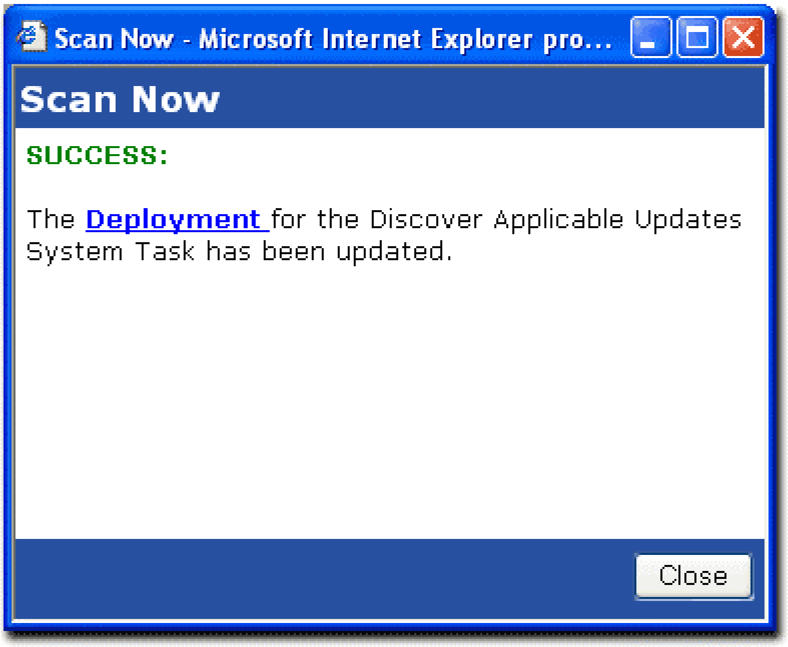


Scan Now

CONFIRM:
This will reschedule the deployment for the Discover Applicable Updates System Task for immediate deployment (using the deployment's current options).

Is this what you wish to do?

To reschedule the **Discover Applicable Updates**, select Yes.



Scan Now

SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

The Patch Management Server will reschedule the selected group(s)'s membership (or all groups' memberships) ,initialize a pop-up screen stating its success, and provide a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the screen, the Groups page will be refreshed and initialized. Previously selected deployment options are maintained.

Groups Security

The Groups section of the Patch Management Server requires the View Groups access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to create, edit, enable, disable, and remove groups requires the Manage Groups access right. If a user does not have the correct access, the Add, Edit, Rules, Enable, Disable and Remove buttons are disabled.

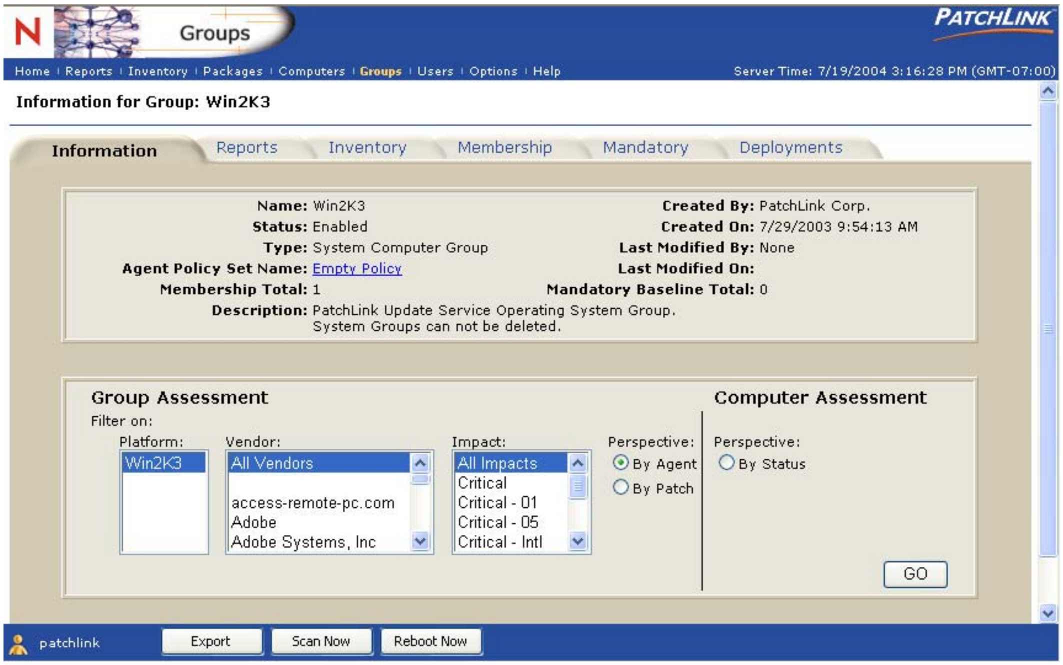
To export all of the group data to a comma-separated value (CSV) file requires the Export Group Data access right. If a user does not have the correct access, the Export button is disabled.

To reschedule the discovery and analysis process (Discover Applicable Updates System Task) for all members of the selected groups requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Group Information

The group information and properties section of the Patch Management Server displays group related information, properties, and assessment graphs for viewing various statuses concerning the group's membership. Click on the actual group name link. The information tab of the Computer Information page (default) appears. (Win XP, All vendors, All Impacts, By Agent is used as an example)



Server Time: 7/19/2004 3:16:28 PM (GMT-07:00)

Information for Group: Win2K3

Name: Win2K3
Status: Enabled
Type: System Computer Group
Agent Policy Set Name: Empty Policy
Membership Total: 1
Description: PatchLink Update Service Operating System Group. System Groups can not be deleted.
Created By: PatchLink Corp.
Created On: 7/29/2003 9:54:13 AM
Last Modified By: None
Last Modified On:
Mandatory Baseline Total: 0

Group Assessment
Filter on:
Platform: Win2K3
Vendor: All Vendors, access-remote-pc.com, Adobe, Adobe Systems, Inc
Impact: All Impacts, Critical, Critical - 01, Critical - 05, Critical - Intl
Perspective: ● By Agent ○ By Patch

Computer Assessment
Perspective: ○ By Status

Information

- Name: This displays the name of the group.
- Status: This displays the current status of the group.
- Type: This displays the type of the group with respective to how it was created.
- Agent Policy Set Name: This displays the assigned Agent Policy Set name and link to view the agent policy set information.
- Membership Total: This displays the total number of computers which are a member of the group.
- Created By: This displays the user who created the group.
- Created On: This displays when the group was created.
- Last Modified By: This displays the user who last modified the group.
- Last Modified On: This displays when the group was last modified.
- Mandatory Baseline Total: This displays the total number of patches which create the baseline for the group.
- Description: This displays the group's description.

Group Assessment

There are three basic graphs that can display status information about the group's membership. Selecting any one of the three options and clicking the **Go** button will initialize a graphical representation pie chart screen illustrating the assessment.

Group Patch Status by Agent

This displays the how many agents are in each of the following patch statuses:

- Fully Patches: the computer requires no additional patches at this time.

- Partially Patched: the computer is not fully patched, but has some patches are installed.
- Not Patched: The computer contains is not patched at all.
- Detecting: In process of running the Discovery and Analysis Process
- Pending: The initial Discovery and Analysis process has not started so there is no data on which to determine the status.

Additionally there are three filters that can define down to obtain more precise status information. The filters are:

- Platform
- Vendor
- Vulnerability Report Impact

Group Patch Status by Patch

This displays the how many applicable patches are in each of the following patch statuses:

- Fully Patches: the computer requires no additional patches at this time.
- Partially Patched: the computer is not fully patched, but has some patches are installed.
- Not Patched: The computer contains is not patched at all.
- Detecting: In process of running the Discovery and Analysis Process
- Non-applicable: The number of computers which have no Vulnerability Reports applicable to them.

Additionally there are three filters that can define down to obtain more precise status information. The filters are:

- Platform
- Vendor
- Vulnerability Report Impact

Agent Status

This displays the number of computers in each of the various agent states. The various states are:

- Sleeping: these computers are outside their defined hours of operation.
- Offline: these computers haven't contacted the Patch Management Server in over two communication intervals (15 minutes minimum for intervals smaller than 10 minutes).
- Running: these computers are currently running the Discovery and Analysis process and they do not correspond to a registered Deployment agent.
- Idle: these computers are active yet not performing any deployments.
- Working: these computers are working on some deployments.
- Disabled: these computers are disabled and will be given no work to do.

Lock Information

If a User has locked a group's reports, software, hardware or services, then information about the lock is displayed here.

Lock Type

This displays what type of group lock was done. The four various types are:

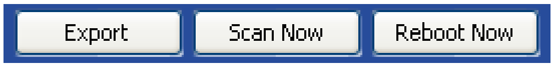
- Group Vulnerability Report Locks
- Group Inventory Software Locks
- Group Inventory Hardware Locks
- Group Services Hardware Locks

Total Locked

This displays the total number of items which were locked.

- Last Locked By: This displays who locked the group.
- Last Locked On: This displays when the group was locked.
- Lock Notes: This displays any notes that were added when the group was locked.

Action Menu

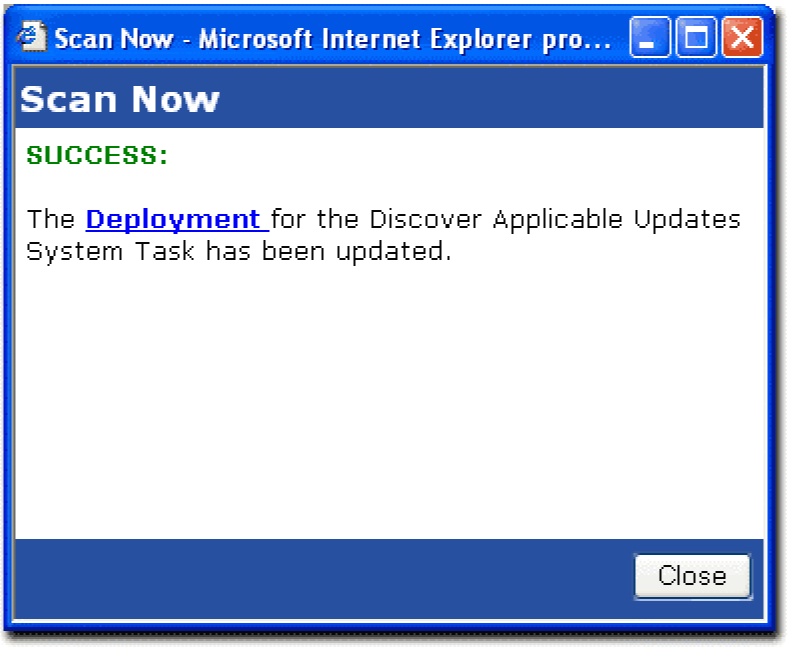


Export

Export the group information to a comma-separated value (CSV) file.

Scan Now

Initializes a screen that allows you to reschedule the deployment of the Discover Applicable Updates System Task for immediate execution to all enabled group members. Previously selected deployment options are maintained.



SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

The Patch Management Server will reschedule the computer and initialize a screen stating its success and provides a **Deployment** link to initialize a new window with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on screen, the Groups page will be refreshed and initialized. Previously selected deployment options are maintained.

Security

The Group Information and Properties section requires the View Groups access right. If a user does not have the correct access, the access denied error message is displayed.

To export all of the group information data to the comma-separated value (CSV) file requires the Export Group Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

The Reports tab requires the View Report access right. If a user does not have the correct access, the Reports tab is disabled.

The Inventory tab requires the View Software Inventory access right. If a user does not have the correct access, the Inventory tab is disabled.

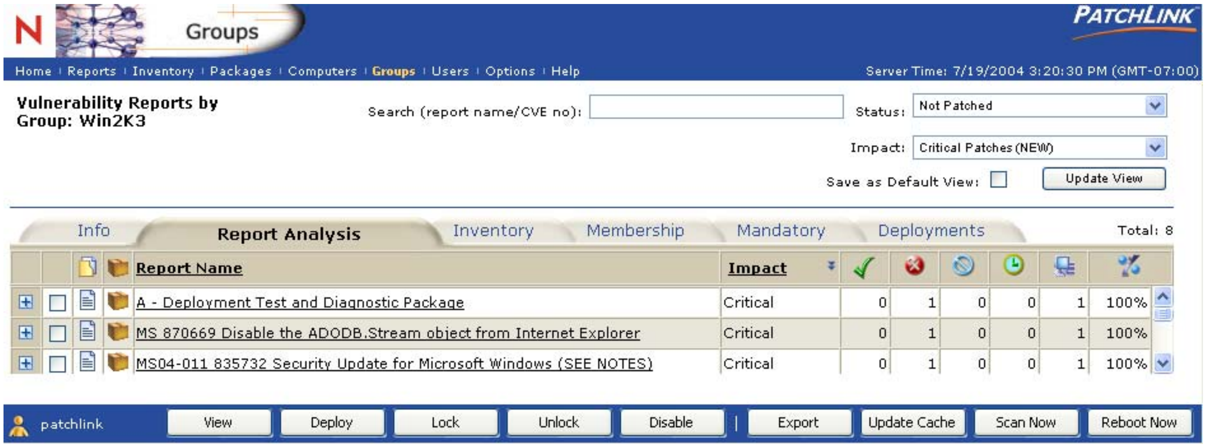
The Membership tab requires the View Computers access right. If a user does not have the correct access, the Membership tab is disabled.

The Deployments tab requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Vulnerability Reports by Group

A Vulnerability Report encompasses any vulnerability and how to detect it and its associated patch or patches. The detection portion of it, also called a Vulnerability Report, which contains the necessary signatures and fingerprints on which to properly determine if the vulnerability is patched or not patched.



Server Time: 7/19/2004 3:20:30 PM (GMT-07:00)

Vulnerability Reports by Group: Win2K3

Search (report name/CVE no):

Status: Not Patched

Impact: Critical Patches (NEW)

Save as Default View: □

Update View

Total: 8

				Report Name	Impact	✓	✗	⊘	🕒	🖥	%
⊞	□			A - Deployment Test and Diagnostic Package	Critical	0	1	0	0	1	100%
⊞	□			MS 870669 Disable the ADODB.Stream object from Internet Explorer	Critical	0	1	0	0	1	100%
⊞	□			MS04-011 835732 Security Update for Microsoft Windows (SEE NOTES)	Critical	0	1	0	0	1	100%

Vulnerability Report Analysis

This section gives the analysis of running those vulnerability reports against the group computer members. The report analysis gives a simple top-down view on how many computers are in each status. The various statuses are detailed below.

See Section 5; Vulnerability Reports, for more information.

Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟, ⊞) is only available for Microsoft Internet Explorer at this time.

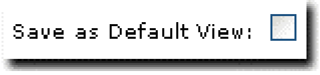
Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Groups Report Analysis page header.

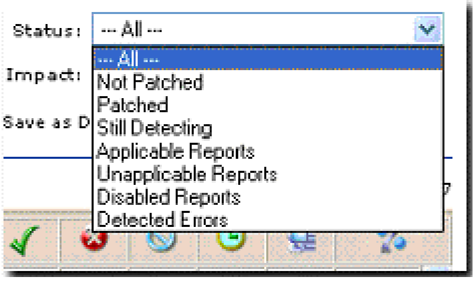
- **Search**

You may search reports for more granular results by entering the report name (CVE; Common Vulnerabilities and Exposures) text into the **Search** field and clicking on the Update View Update View button.

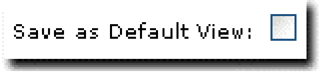
This will return the report(s) having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- **Status**
  Filter by Report Statuses using the dropdown menu and click on the Update View Update View button.

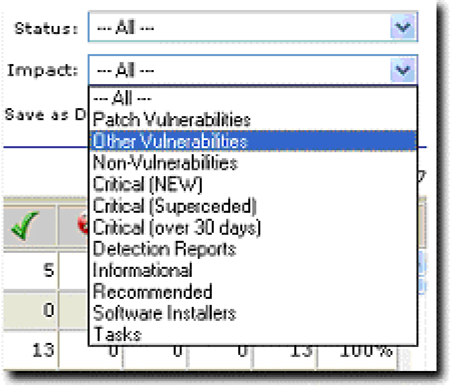


  This will return the report(s) having the selected status. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

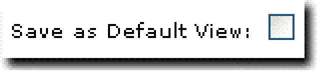


- **Impact**
  Filter by Report Impact levels using the dropdown menu and click on the Update View Update View button.

  This is extremely useful when you want to find or display only the Reports that, for example, are Critical (NEW).



This will return the report(s) having the selected impact. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

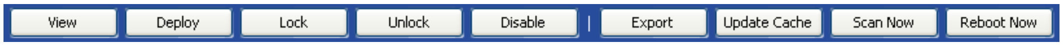
Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



View

To display additional information about the report for this group computer, select a report and click on the View button. This performs the same function as clicking on the name of the report.

Deploy

Deploy the selected detection reports associated update packages. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

Lock

Locks report(s) for this group and its computer members.

Unlock

Unlocks report(s) for this group and its computer members

Enable

To enable selected disabled computers, click on the Enable button.

Disable

To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.

Export

Export the vulnerability report analysis to a comma-separated value (CSV) file. The amount and order of the data is based on what the analysis view is filtered and sorted on.

Update Cache

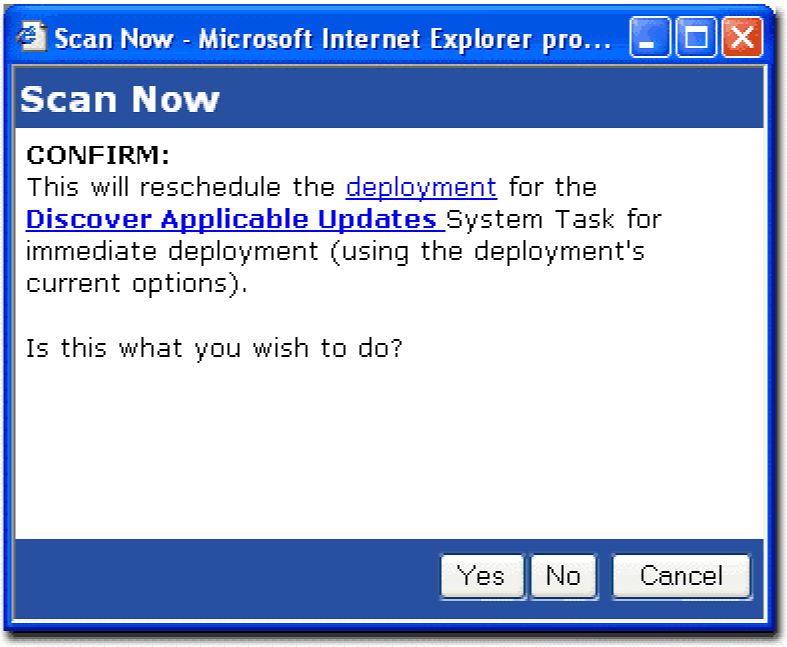
Deploys all of the **Discover Applicable Updates System Task** to all computers (or selected computers).

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to all selected groups.

To initialize (choose) all groups, click on the Scan Now button without selecting any groups and click the **Scan Now** button.

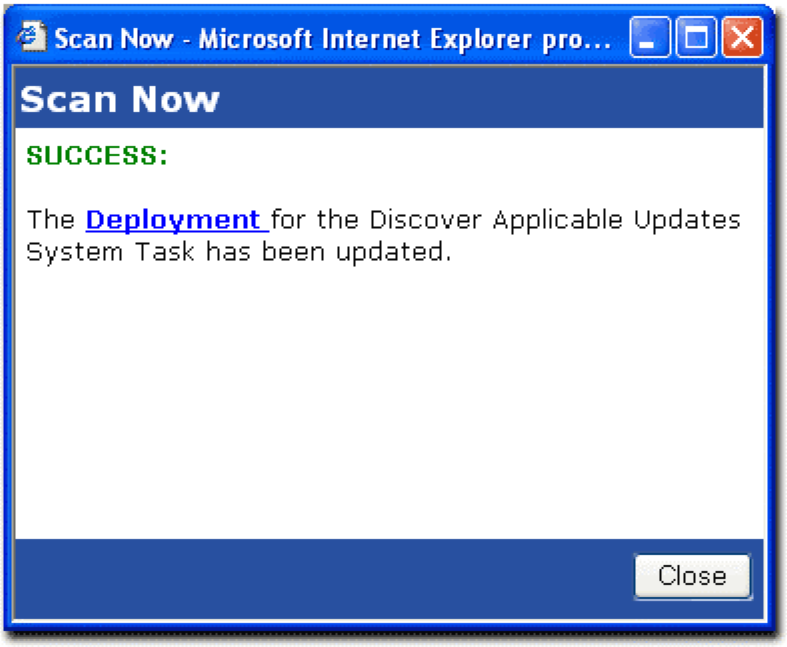
If you choose not to select any groups, the screen will ask you if you wish to **confirm** the reschedule the **Discover Applicable Updates System Task** for all of the groups.



CONFIRM:
This will reschedule the deployment for the Discover Applicable Updates System Task for immediate deployment (using the deployment's current options).

Is this what you wish to do?

To reschedule the **Discover Applicable Updates**, select Yes.



Scan Now

SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

The Patch Management Server will reschedule the selected groups(s)'s membership (or all groups' memberships), initialize screen stating its success and provide a **Deployment** link to initialize a new screen with the results of the Discover Applicable Updates Deployment.

Upon clicking the **Close** button on the screen, the Groups page will be refreshed and initialized.

Previously selected deployment options are maintained.

Group Vulnerability Security

The Reports section of the Patch Management Server requires the View Reports Page access right. If a user does not have the correct access the access denied error message is displayed.

To be able to view the detailed report analysis requires the View Report Details access right. If a user does not have the correct access, the hyperlink will not be shown and the View button is disabled.

To be able to change the filter from detected vulnerability reports to disabled or all requires the Change Report Filter access right. If a user does not have the correct access, the filter will not have any options to choose from.

To be able to view the associated distribution packages for a given vulnerability report requires the View Packages access right. If a user does not have the correct access, the link on the package status image is disabled.

To be able to create a deployment based on the report analysis requires the Deploy Reports access right. If a user does not have the correct access, the Deploy button is disabled.

To be able to enable or disable vulnerability reports from being available by the discovery and analysis process requires the Manage Reports access right. If a user does not have the correct access, the Enable and Disable buttons are disabled.

To be able to lock or unlock the results of the selected vulnerability reports analysis for the group's membership requires the Manage Group Report Locks access right. If a user does not have the correct access, the Lock and Unlock buttons are disabled.

To export all of the vulnerability report analysis's to a comma-separated value (CSV) file requires the Export Report Data access right. If a user does not have the correct access, the Export button is disabled.

To restart the discovery and analysis process for all of the computers registered to the Patch Management Server requires the Manage System Tasks access right. If a user does not have the correct access, the Scan Now button is disabled.

To cache the associated distribution of the selected vulnerability reports requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

The Inventory tab requires the View Software Inventory access right. If a user does not have the correct access, the Inventory tab is disabled.

The Membership tab requires the View Computers access right. If a user does not have the correct access, the Membership tab is disabled.

The Deployments tab requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

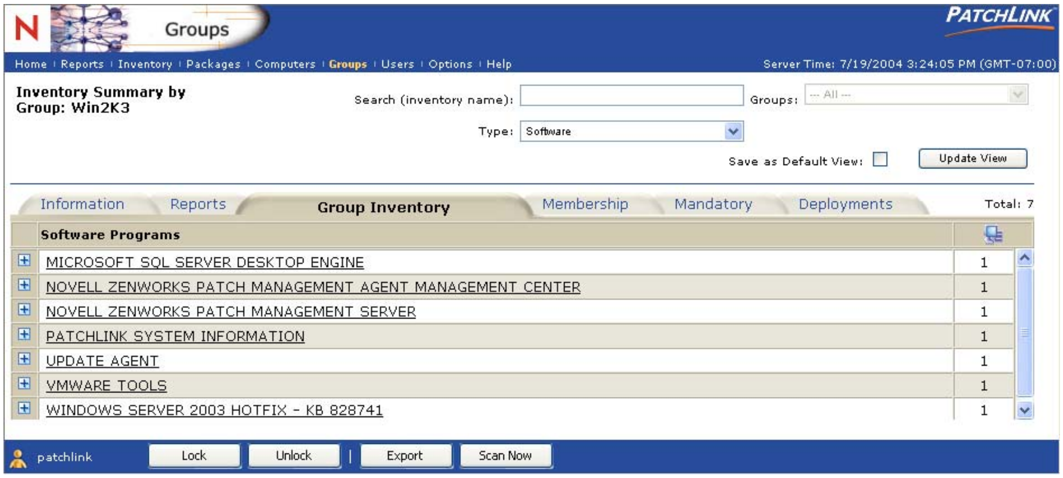
Group Inventory Summary

This view will display the software, hardware, operating systems and services that were detected on the computers in the group. When displaying the Inventory based on a single computer, the Software inventory is the initial inventory displayed.

This view is the same as the Inventory Summary view with the following differences:

1. Only displays the inventory based upon the member computers of the selected group.
2. The Scan Now button will only reschedule the **Discover Applicable Updates System Task** for the selected group's membership.

See Section 6; Inventory, for more detailed information.



Groups
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help

Server Time: 7/19/2004 3:24:05 PM (GMT-07:00)

Inventory Summary by Group: Win2K3

Search (inventory name):
Groups: --- All ---
Type: Software
Save as Default View: □
Update View

Information | Reports | Group Inventory | Membership | Mandatory | Deployments

Total: 7

	Software Programs	
⊞	MICROSOFT SQL SERVER DESKTOP ENGINE	1
⊞	NOVELL ZENWORKS PATCH MANAGEMENT AGENT MANAGEMENT CENTER	1
⊞	NOVELL ZENWORKS PATCH MANAGEMENT SERVER	1
⊞	PATCHLINK SYSTEM INFORMATION	1
⊞	UPDATE AGENT	1
⊞	VMWARE TOOLS	1
⊞	WINDOWS SERVER 2003 HOTFIX - KB 828741	1

Software Programs

This displays the name of the software application.

Lock Status

If the software is locked for the group this image indicates if the software application is in compliance or not.

Number of Instances

The number of times this software application was detected.

Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟, ⊞) is only available for Microsoft Internet Explorer at this time.

Advanced Page Search, Filtering, and View Saving

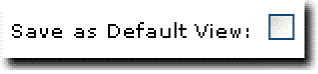
The advanced page search, filtering dropdown menus, and saving functions appear in the Group Inventory page header.

- Search

Search (inventory name):

You may search inventory for more granular results by entering the inventory name text into the **Search** field and clicking on the Update View Update View button.

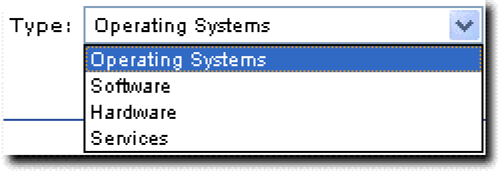
This will return the inventory having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Save as Default View: ☐

- Type

  Filter by Type using the pull down menu and click on the Update View Update View button.



Type: Operating Systems

Operating Systems
Software
Hardware
Services

This allows you to search for Operating Systems, Software, Hardware and Services.

- Operating Systems View

  Displays the full operating system platform names and the number of instances, or times this operating system was detected.

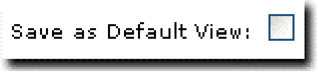
- Software View

  Displays the installed software applications and the number of instances, or times this software application was detected.

  Software Programs
  This displays the name of the software application. Click the ⊞ for a software application to display the list of computers for that application. Click on the ⊟ to close this list.

  Number of Instances
  The number of times this software application was detected.

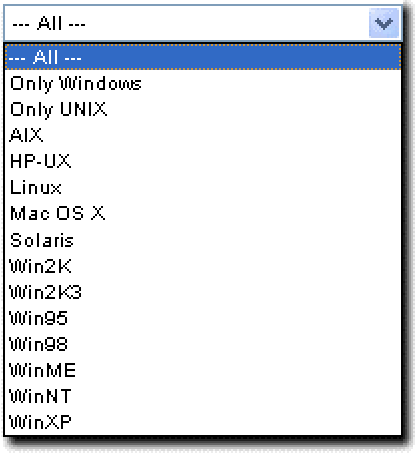
  You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



Save as Default View: ☐

- Groups

  Filter by Group using the pull down menu and click on the Update View Update View button.

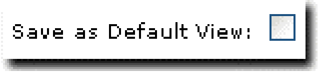


This allows the user to search on any user defined or server defined groups that exist.

  - Operating Systems
    Displays the selected or filtered operating system.

  - Number of Instances
    This displays the number of times this operating system platform has been detected. For displaying the Operating System Inventory for a single computer, this is always one.

    You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- Hardware View
  Displays the client Hardware devices.

  - Hardware Device Class
    Hardware is separated into device classes such as disk drives, processors, network adapters, etc. Click the ⊞ to display the list of devices for each class, or click on the ⊞ to display them all (for a long list of devices this may take a few moments to generate). Click the ⊟ to close this list.

  - Device
    A device is a specific piece of hardware, such as a “Microsoft USB IntelliMouse Optical”. Click the ⊞ for a device to display the list of computers for that device. Click the ⊟ to close this list.

  - Number of Instances
    An Instance is a specifically detected device or installed driver. A computer may contain multiple instances of a installed device or driver. For example, a computer may contain a video graphics adapter that contains multiple video sources and destinations in which each source or

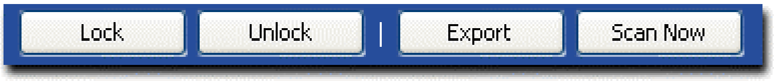
destination is discovered as multiple instances of the same device or driver.

- Services View
  Displays the detected services that may or may not be running.
  - Service Name
    This displays the name of the service.
  - Number of Instances
    The number of times this service was detected.

Mouse Overers

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Action Menu



Lock

Clicking on the lock button will lock the selected inventory for all computers members of the group. When the inventory changes for one of the computer members the inventory item is highlighted as being out of compliance and an e-mail notification is sent to the group notification list of the occurrence.

Unlock

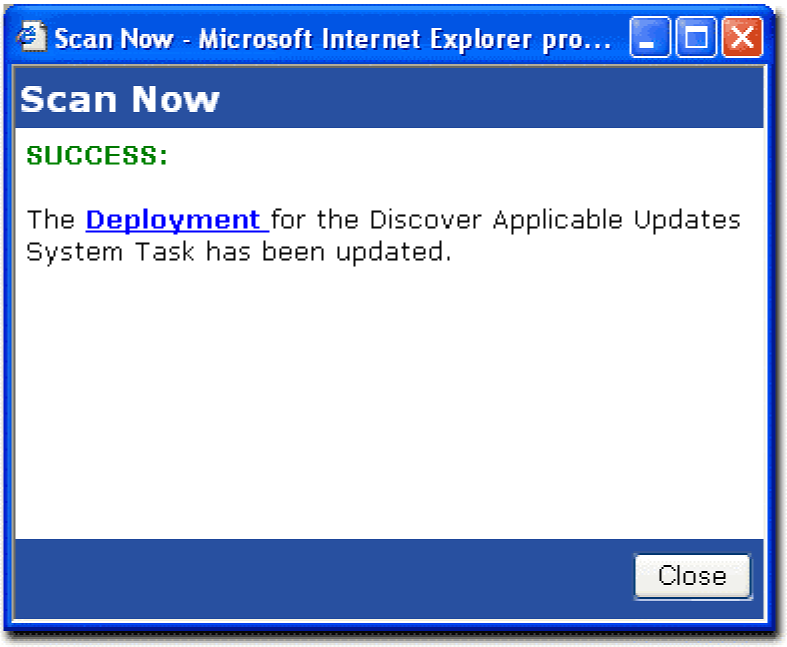
Clicking on the unlock button will clear the lock.

Export

Clicking on the Information tab will display the Group Information and Properties page.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates System Task** deployment for immediate execution to the selected groups.



Scan Now

SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

The Patch Management Server will reschedule the computer and initialize a screen stating its success and provides a **Deployment** link to initialize a screen with the results of the Discover Applicable Updates Deployment.

Upon clicking the Close button on the screen, the Groups page will be refreshed. Previously selected deployment options are maintained.

Group Inventory Security

The Group Inventory section of the Patch Management Server requires the View Software Inventory access right. If a user does not have the correct access, the filter will not have this option available and the inventory display will default to the inventory the user has access to view or the access denied error message is displayed.

To be able to view the Operating Systems Inventory requires the View Inventory OS access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Hardware Inventory requires the View Hardware Inventory access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Services Inventory requires the View Services Inventory access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the list of computers on which an inventory belongs to requires the View Computers access right. If a user does not have the correct access, the hyperlink and ⊞, ⊟ *more information images are disabled.*

To export the inventory to a comma-separated value (CSV) file requires the Export Inventory Data access right. If a user does not have the correct access, the Export button is disabled.

The Reports tab requires the View Report access right. If a user does not have the correct access, the Reports tab is disabled.

The Membership tab requires the View Computers access right. If a user does not have the correct access, the Membership tab is disabled.

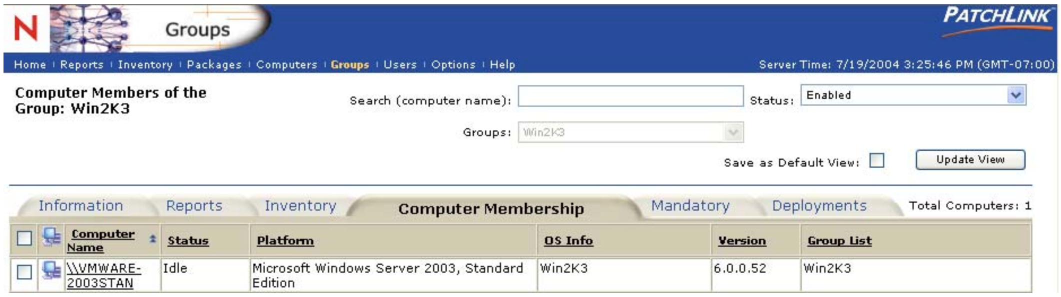
The Deployments tab requires the View Deployment Status access right. If a user does not have the correct access, the Deployments tab is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Group Membership

The Group Membership section of the Patch Management Server displays all computers which are members of the group. Clicking on a computer name will allow you to display a computer's specific information.

This view is almost identical to the computers section of the Patch Management Server. See [Section 10; Computers] for more information.



Server Time: 7/19/2004 3:25:46 PM (GMT-07:00)

Computer Members of the Group: Win2K3

Search (computer name):

Status: Enabled

Groups: Win2K3

Save as Default View: □

Total Computers: 1

□	Computer Name	Status	Platform	OS Info	Version	Group List
□	\\VMWARE-2003STAN	Idle	Microsoft Windows Server 2003, Standard Edition	Win2K3	6.0.0.52	Win2K3

Computer Name

This displays the name of the computer. Click on the computer name to display specific information about the computer.

Status

This displays the status of the computer.

Platform

This displays the operating system platform the computer is running.

OS Info

This displays additional information about the operating system the computer is running.

Version

This displays the version of the agent running on the computer.

Group List

This displays the list of groups that the computer is a member of.

Agent Status

Status	Description
	This is an idle deployment agent.
	This deployment agent is idle and has deployments in its work queue.
	The agent is sleeping as it is outside its hours of operation.
	The agent is sleeping as it is outside its hours of operation and has deployments in its work queue.
	This agent is currently working on a deployment.
	This is an enabled detection agent that does not correspond to a registered deployment agent [2].
	The agent is considered to be offline as it has not contacted the Patch Management Server in more than two intervals (minimum of 15 minutes).
	The agent is considered to be offline as it has not contacted the Patch Management Server in more than two intervals (minimum of 15 minutes) and has deployments in its work queue.
	This agent has been disabled.

Additional information about the status of the agent is displayed once your mouse hovers over the image.

Page Functions

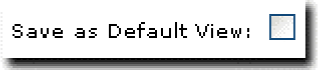
Advanced Page Search, Filtering, and View Saving

The advanced page search, filtering dropdown menus, and saving functions appear in the Computers page header.

- Search

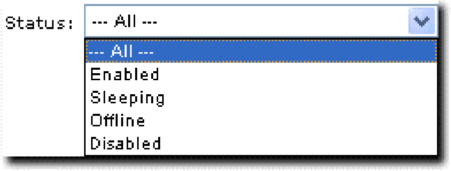
You may search computers for more granular results by entering the computer name text into the **Search** field and clicking on the Update View button.

This will return the computer having the name of the entered text. You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.



- Status

  Filter by status using the dropdown menu and click on the Update View Update View button.

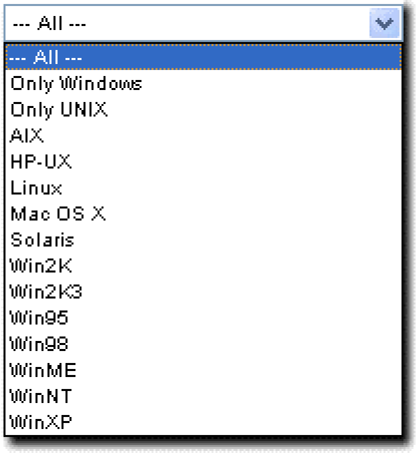


This allows the user to search on enabled, sleeping, offline, and disabled systems that exist.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

- Groups

  Filter by group using the dropdown menu and click on the Update View Update View button.



This allows the user to search on any user defined or server defined groups that exist.

You may then click the **Save as Default View** button to save your filtered view as your default view for the next time the page is visited.

Sort

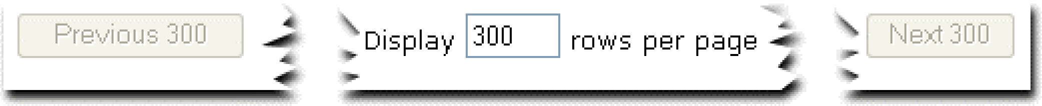
The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Display

Depending on the amount of items available for display and what page you are viewing determines the display function located at the bottom of enabled pages above the Action Menu.

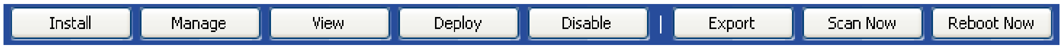


- Next: To display the next page of computers, click on the next button. If the last computer is displayed, the next button is disabled.
- Previous: To display the previous page of computers, click on the previous button. If the first computer is being displayed, the previous button is disabled.
- Computers per Page: The computer list initially displays up to 100 computers per page. To change the number of computers to display per page, enter a new number in to the Computers per Page input field. To display all computers enter a zero in the input field.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Install

Click on the Install button to display the list of agent installers that can be used to register computers to the Patch Management Server.

The agent installer screen contains links to all of the agent installations and additional information on Operating Systems, Requirements, and Installation Notes.

See Item 11.4.; Install, for more information.

Manage

Manage the group's computer membership. Initializes the Group Property page. See Section 12; Add a Group Wizard for more information.

View

To display additional information about the computer, select a computer and click on the View button. This performs the same function as clicking on the name of the computer.

Enable

To enable selected disabled computers, click on the Enable button.

Deploy

To deploy a package to specified computers within the computer membership, simply click the Deploy button, select the package, the computers, and the deployment options.

See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

Disable

To disable selected enabled computers, click on the Disable button. Disabled computers do not take up an agent license.

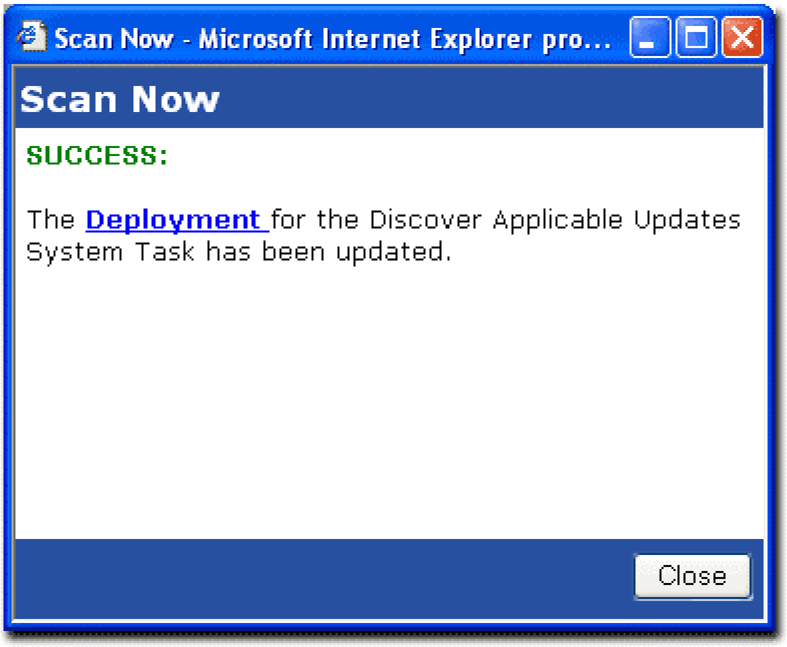
Export

Exports the group membership information to a comma-separated value (CSV) file.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to the selected group.

The Patch Management Server will reschedule the computer and initialize a screen stating its success and provides a **Deployment** link to initialize a screen with the results of the Discover Applicable Updates Deployment.



SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

Upon clicking the Close button on the screen, the Groups page will be refreshed. Previously selected deployment options are maintained.

Group Membership Security

The Group Membership section of the Patch Management Server requires the View Group Membership access right. If a user does not have the correct access, the filter will not have this option available and the inventory display will default to the inventory the user has access to view or the access denied error message is displayed.

To be able to view the Enabled Group Membership requires the View Enabled Group Membership access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the Disabled Group Membership requires the View Disabled Group Membership access right. If a user does not have the correct access, the filter will not have this option available.

To be able to view the All Group Membership requires the View All Group Membership access right. If a user does not have the correct access, the filter will not have this option available.

To be able to utilize the Scan Now capability requires the Scan Now access right.

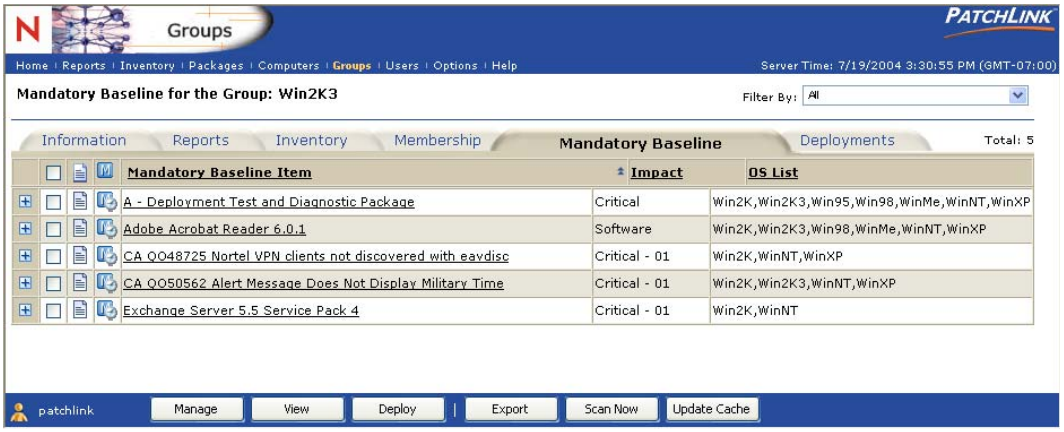
To be able to install, manage, view, deploy or disable group memberships requires the Manage Group Membership access right. If a user does not have the correct access, the Install, Manage, View, Deploy and Disable buttons are disabled.

To export the inventory to a comma-separated value (CSV) file requires the Export Group Membership Data access right. If a user does not have the correct access, the Export button is disabled.

Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Groups Mandatory Baseline

Mandatory Baselines are the mandatory packages (defined by the user) for a computer group that will be delivered to all members.



Server Time: 7/19/2004 3:30:55 PM (GMT-07:00)

Mandatory Baseline for the Group: Win2K3

Filter By: All

Total: 5

Mandatory Baseline Item	Impact	OS List
A - Deployment Test and Diagnostic Package	Critical	Win2K,Win2K3,Win95,Win98,WinMe,WinNT,WinXP
Adobe Acrobat Reader 6.0.1	Software	Win2K,Win2K3,Win98,WinMe,WinNT,WinXP
CA QO48725 Nortel VPN clients not discovered with eavdisc	Critical - 01	Win2K,WinNT,WinXP
CA QO50562 Alert Message Does Not Display Military Time	Critical - 01	Win2K,Win2K3,WinNT,WinXP
Exchange Server 5.5 Service Pack 4	Critical - 01	Win2K,WinNT

Notes:

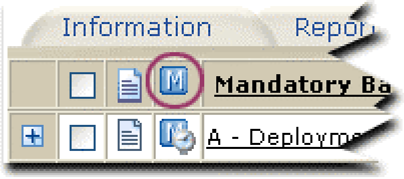
- Any non-system report with one or more associated packages can be associated with a given computer group as a Mandatory patch.
- Mandatory report based patches shall be applied to every computer in the computer group which is of a compatible operating system type to the report.
- Mandatory report based patches shall be applied to a given computer only when the report for that given computer shows a failure condition showing that the patch is not already installed on the computer.

The Group Summary shows three views of currently existing groups on the Patch Management Server. Select the desired **Filter by:** item from the upper right drop down menu to view the results. The views are:

- **Vulnerability Reports:** Show only the vulnerability reports
- **Distribution Packages:** Show only the distribution packages
- **All reports:** Show all the mandatory baseline of the Groups that exist on the Patch Management Server.

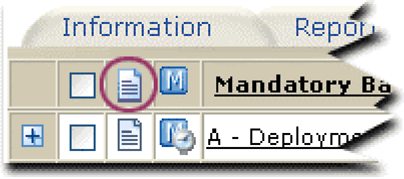
Status

There are two status columns for the Mandatory Baseline page. The first will display one of the following icons giving information about the patch itself:



Status	Description
📄	This is a current vulnerability report
📄	This is a new vulnerability report
📄	This is a disabled vulnerability report.
✉	This is a distribution package.

The second column will display information about the group with respect to the patch using one of the following icons:



Status	Description
🔍	At least one member of this group is either Detecting, Obtaining the Package, Waiting On Detection, or in a Deployment Not Started state. (None of the members have errors).
M	At least one member of this group is Deploying this patch. (None of the members have errors, nor are they Detecting).
M	All of the members of this group are Disabled for this patch.
M ✓	All of the members of this group are either Not Applicable or In Compliance for this patch. (Some can also be disabled).
M ✗	At least one member of this group is out of compliance. This indicates that an error has occurred. More specific information about the type of error will appear in the mouse over text.

- Mandatory Baseline Item:

  Name of the Item
- Impact:

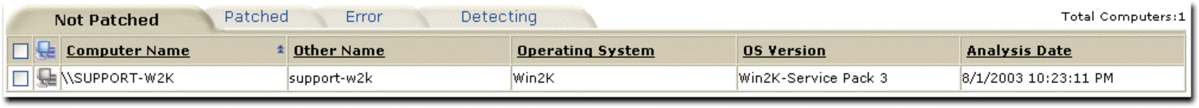
  If applicable, Impact of the Vulnerability Report
- OS List:

  List of applicable Operating Systems

Select

To select a Mandatory Baseline you can:

- Click anywhere within the mandatory baseline entry line (be careful: *mandatory baseline item name* are links to view other information (see below).
- Click the checkbox for that mandatory baseline item and click the **View** button.
- Click the checkbox in the header section to select all of the mandatory baseline items.



Total Computers:1

□	Computer Name	Other Name	Operating System	OS Version	Analysis Date
□	\\SUPPORT-W2K	support-w2k	Win2K	Win2K-Service Pack 3	8/1/2003 10:23:11 PM

This view is similar to the Reports Section. See Item 5.7 Vulnerability Report Analysis Details for more details

At the View Mandatory deployment stage, you can select computers and schedule a deployment to them. Also, at this stage you get the complete statistics for the computers whose Detection Agents have run the detected report.

These computers are divided in 9 categories:

- Compliance
- Detecting
- Disabled
- Deploying
- Not Applicable
- Obtaining Package
- Deployment Not Started
- Waiting On Detection
- Error: {specific error message}

These are two error categories:

- Detection Errors
- Deployment Errors
- Item Type

Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟, ⊞) is only available for Microsoft Internet Explorer at this time.

Filter by

Filter your results selecting the desired item from the **Filter by** drop down menu in the upper right hand corner.

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

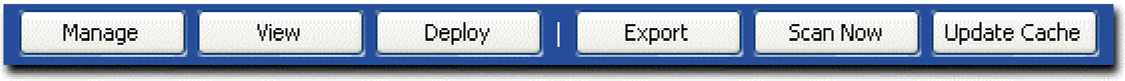
Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Manage

Initializes the Group Property Page to manage the baseline of the Group. .See Section 12; Add a Group Wizard for more information.

View

Views the Vulnerability Report analysis for the Group

Deploy

Deploys the selected package to the specified Computer. See Section 9; Deploying Packages: Schedule Deployment Wizard for more information.

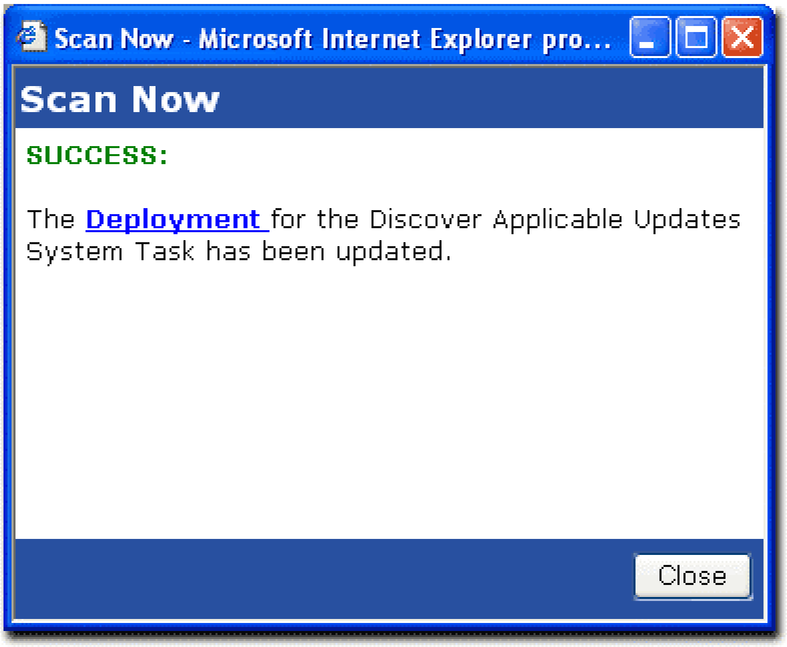
Export

Exports the group mandatory baseline information to a comma-separated value (CSV) file.

Scan Now

Initializes a screen that allows you to reschedule the **Discover Applicable Updates** System Task deployment for immediate execution to the selected computer.

The Patch Management Server will reschedule the computer and initialize a screen stating its success and provides a **Deployment** link to initialize a screen with the results of the Discover Applicable Updates Deployment.



Scan Now

SUCCESS:

The Deployment for the Discover Applicable Updates System Task has been updated.

Upon clicking the Close button on the screen, the Groups page will be refreshed and initialized. Previously selected deployment options are maintained.

Update Cache

Initiates the process to cache (or re-cache) for the selected distribution packages. If no distribution packages are selected this will re-cache all of the previously cached distribution packages.

Group Mandatory Baseline Security

The Group Membership section of the Patch Management Server requires the View Group Mandatory access right. If a user does not have the correct access, the filter will not have this option available and the inventory display will default to the inventory the user has access to view or the access denied error message is displayed.

To be able to view the Group Mandatory Baseline requires the View Enabled Group Membership access right. If a user does not have the correct access, the filter will not have this option available.

To be able to manage, view, deploy or disable group memberships requires the Manage Group Membership access right. If a user does not have the correct access, the Manage, View, Deploy and Disable buttons are disabled.

To be able to utilize the Scan Now capability requires the Scan Now access right

To cache the associated distribution of the selected vulnerability reports requires the Cache Packages access right. If a user does not have the correct access, the Update Cache button is disabled.

To export the inventory to a comma-separated value (CSV) file requires the Export Group Membership Data access right. If a user does not have the correct access, the Export button is disabled.

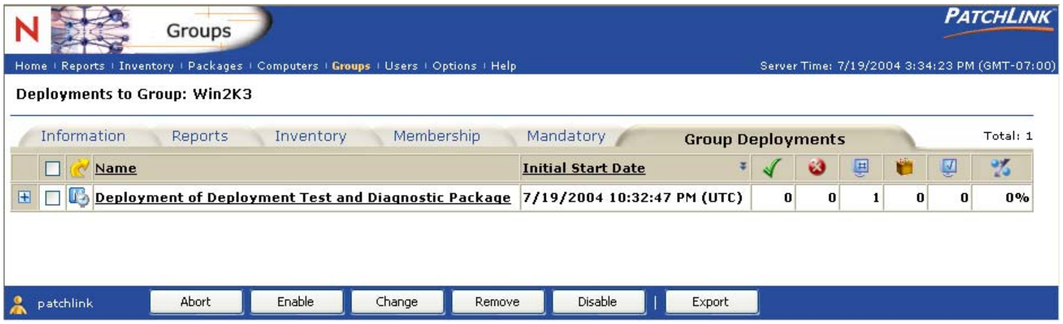
Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

Group Deployments

This view displays the deployments that the selected group has been assigned to.

Note:
This view does not display the individual deployments each member has been assigned to, only the deployments that the group, as an entity, have been assigned to.

This view is the same as the Deployment Summary view, but displays all deployments that the selected group has been assigned to.



Deployments to Group: Win2K3

	□	Name	Initial Start Date	✓	✗				
⊞	□	Deployment of Deployment Test and Diagnostic Package	7/19/2004 10:32:47 PM (UTC)	0	0	1	0	0	0%

Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟, ⊞) is only available for Microsoft Internet Explorer at this time.

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

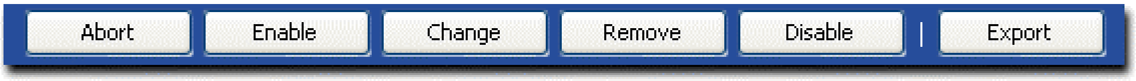
Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Abort

Allows the user to abort the deployment for the group.

Enable

Allows the user to enable the selected disabled deployments.

Change

Allows the user to change the selected deployment.

Remove

Allows the user to change the selected disabled deployment(s).

Disable

Allows the user to disable the selected deployments.

Export

Exports the group deployment(s) information to a comma-separated value (CSV) file.

Group Deployments Security

To be able to change, disable, enable, abort or remove a deployment(s) requires the Manage Deployments access right. If a user does not have the correct access, the Change, Disable, Enable, Abort and Remove buttons are disabled.

To export the inventory to a comma-separated value (CSV) file requires the Export Group Membership Data access right. If a user does not have the correct access, the Export button is disabled.

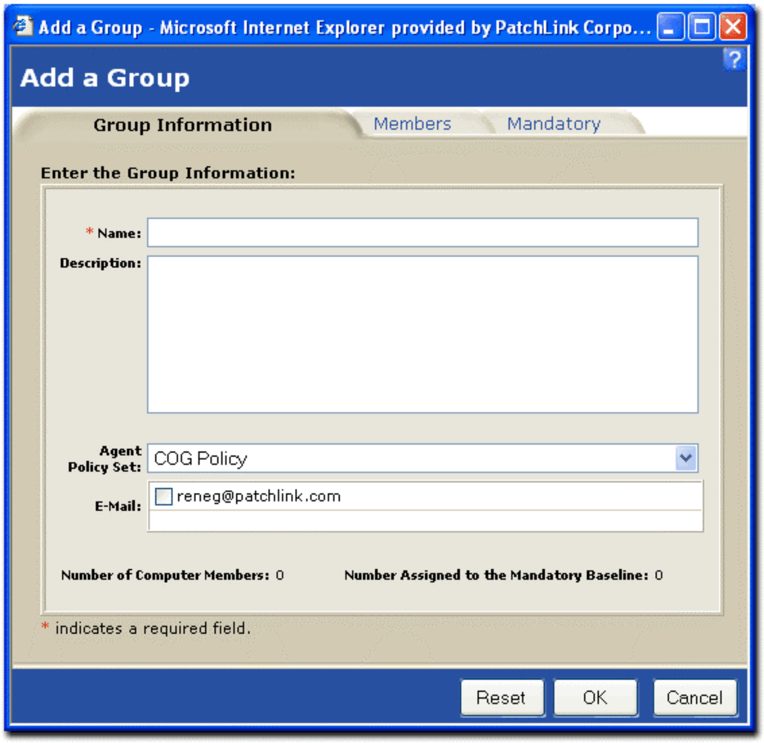
Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security

12. Add a Group Wizard

Plus has the ability to add groups. From the **Groups** homepage, click on the **Add** button on the Action Menu.

Group Property Screen - Info

The **Group Information** Screen section of the Patch Management Server allows the ZENworks® Patch Management User the ability to create a group, System-defined groups cannot be changed. The **Group Information** tab of the property page contains the base information and it is this tab in which a group's information is loaded and saved.


Add a Group - Microsoft Internet Explorer provided by PatchLink Corpo...
Add a Group
Group Information
Members
Mandatory
Reset
OK
Cancel

Enter the Group Information:

* Name:

Description:

Agent Policy Set: COG Policy

E-Mail: □ reneg@patchlink.com

Number of Computer Members: 0

Number Assigned to the Mandatory Baseline: 0

* indicates a required field.

- Group Name

  The name of the group to be created. This field is required for groups to be created.
- Description

  Notes or information describing the group.
- Agent Policy Set

  The desired Agent Policy Set to use for the computers who are members of the group. When a computer's policies are calculated, the Patch Management Server determines the superset of all Agent Policy Sets for the groups the computer is a member of. Thus, if one policy set says the agent has a 60 minute interval and another says the computer has a 30 minute interval, the resulting policy set is 30 minutes.

Set the Agent Policy Set to the Empty Policy if this group is to have to effect on the policy calculations.

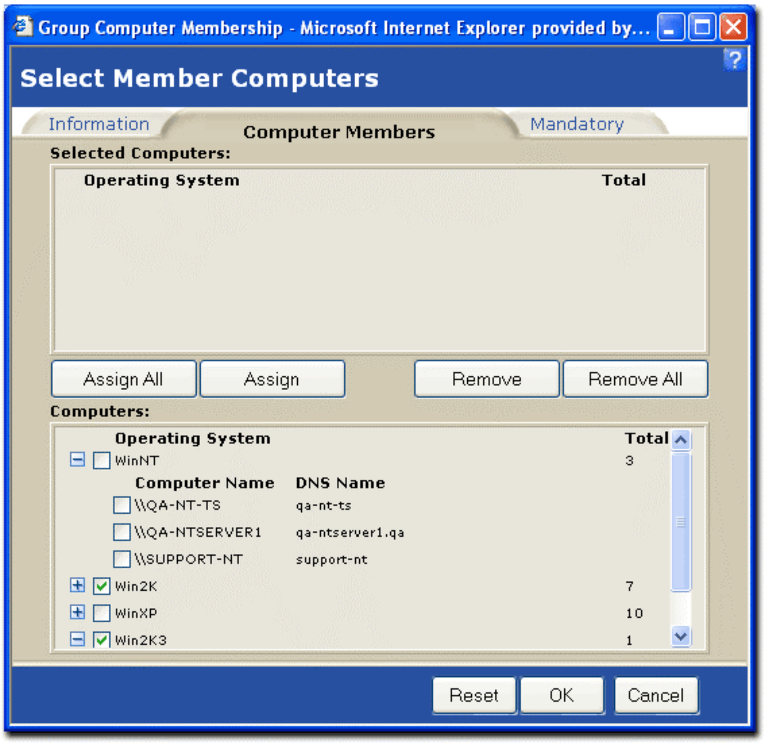
- E-Mail
  Select any users who have been added to the E-Mail Notification list on the Patch Management Server The selected users will be sent group-based notifications.
- Number of Computer Members
  The total number of computers that are in the selected group.
- Number of Computers assigned to the Mandatory Baseline
  The total number of computers who are currently assigned to the group.

Screen Functions

- Reset
  Resets the page back to its initial state**.**
- OK
  Initiates the process to save the group. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- Cancel
  Cancels the add process and closes the group property page window.

Group Property Screen - Members

The Computer Members Group Property Page section of the Patch Management Server allows the ZENworks® Patch Management User the ability to create a group. System-defined groups cannot be changed. The **Computer Members** tab of the property page contains a list of all computers which have been assigned as members of the group and the list of computers which are not a member of the group.



Selected Computers:

Operating System	Total

Computers:

Operating System		Total
⊟ □ WinNT		3
Computer Name	DNS Name	
□ \\QA-NT-TS	qa-nt-ts	
□ \\QA-NTSERVER1	qa-ntserver1.qa	
□ \\SUPPORT-NT	support-nt	
⊞ ☑ Win2K		7
⊞ □ WinXP		10
⊟ ☑ Win2K3		1

Selected Computers

- Operating System

  The operating system platform name. Click the ⊞ to display the list of computers for that operating system. Click ⊟ to close the list.
- Computer Name
  The name of the computer.
- DNS Name
  The DNS name assigned to the computer
- Total Selected per OS
  The total number of computers that have been selected for the operating system platform.

Available Computers

- Operating System

  The operating system platform name. Click the ⊞ to display the list of computers for that operating system. Click ⊟ to close the list.

- Computer Name

  The name of the computer.
- DNS Name
  The DNS name assigned to the computer

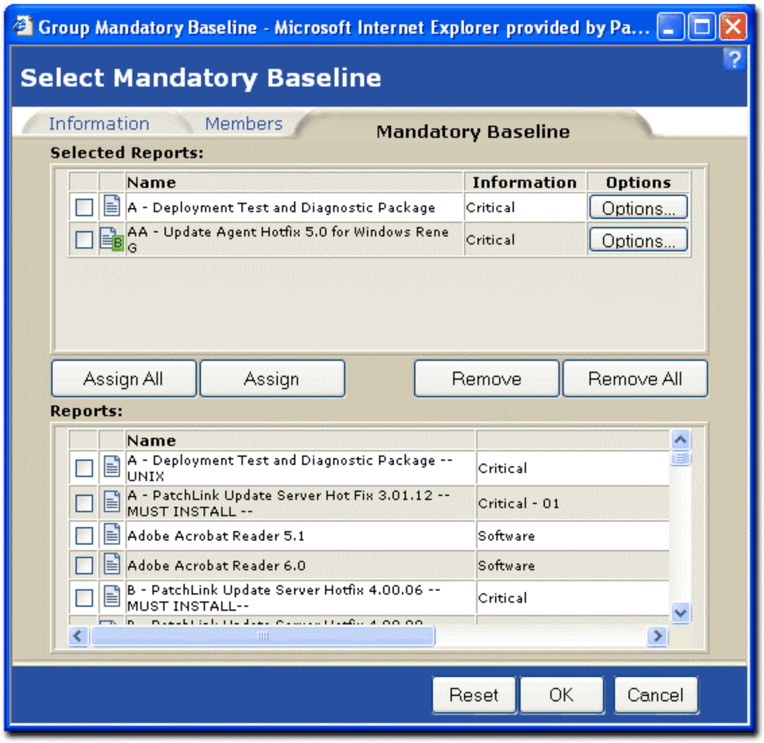
- Total Selected per OS
  The total number of computers that have not been selected for the operating system platform.

Screen Functions

- Assign All
  Assigns all available computers to the group.
- Assign
  Assigns all available computers to the group.
- Remove
  Removes the selected computers from the group.
- Remove All
  Removes all selected computers from the group.
- Cancel
  Cancels the add process and closes the group property page window.
- Reset
  Resets the page back to its initial state.
- OK
  Initiates the process to save the group (or the group's changes). If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- Cancel
  Cancels the add process and closes the group property page window.

Group Property Screen –Mandatory Baseline

The Group Property Page section of the Patch Management Server allows the User the ability to create a group, system-defined groups cannot be changed. The **Mandatory Baseline** tab of the property page contains the lists of selected and available Vulnerability Reports and Locally-created Distribution Packages for the group's baseline.



Group Mandatory Baseline - Microsoft Internet Explorer provided by Pa...
Select Mandatory Baseline
Information
Members
Mandatory Baseline
Assign All
Assign
Remove
Remove All
Reset
OK
Cancel

Selected Reports:

	Name	Information	Options
□	A - Deployment Test and Diagnostic Package	Critical	Options...
□	AA - Update Agent Hotfix 5.0 for Windows Rene G	Critical	Options...

Reports:

	Name	
□	A - Deployment Test and Diagnostic Package -- UNIX	Critical
□	A - PatchLink Update Server Hot Fix 3.01.12 -- MUST INSTALL --	Critical - 01
□	Adobe Acrobat Reader 5.1	Software
□	Adobe Acrobat Reader 6.0	Software
□	B - PatchLink Update Server Hotfix 4.00.06 -- MUST INSTALL--	Critical

Selected Baseline Items

- Baseline Item Name
  The name of the report or package.
- Baseline Item Type
  This is either a Vulnerability Report or a Distribution Package.
- Information
  This contains information about the operating systems for the package or the impact for a report.
- Options
  Click the Options button to display a screen with the deployment options and information about the item.

Available Computers

- Baseline Item Name
  The name of the report or package.
- Baseline Item Type
  This is either a Vulnerability Report or a Distribution Package.
- Information
  This contains information about the operating systems for the package or the impact for a report.

Screen Functions

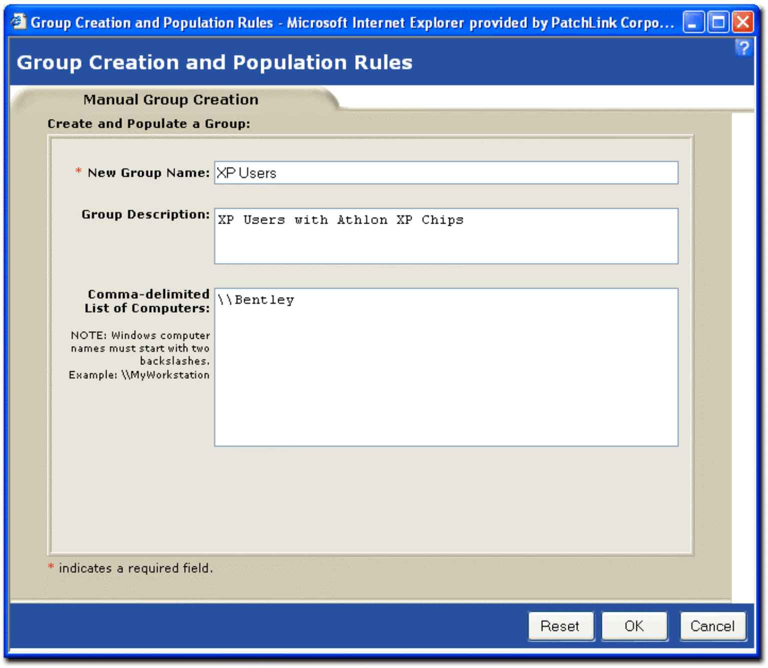
- Assign All
  Assigns all available reports and packages to the group.
- Assign
  Assigns all available reports and packages to the group.
- Remove
  Removes the selected reports and packages from the group.
- Remove All
  Removes all selected reports and packages from the group.
- Reset
  Resets the page back to its initial state.
- OK
  Initiates the process to save the group (or the group's changes). If a Mandatory Baseline item has been added which requires a license to agree prior to the saving of the group, a license agreement page will be displayed. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- Cancel
  Cancels the add process and closes the group property page window.
- Options
  Displays a window with the deployment options for the item.

Edit

Selecting a group and clicking on this button will bring up the Group Property screen with this group's information allowing the group to be changed. See Section 13; Edit a Group Wizard for more information.

Rules

Clicking this button will bring up the Manual Group Creation and Population Rules property page.


Group Creation and Population Rules - Microsoft Internet Explorer provided by PatchLink Corpo...

Group Creation and Population Rules

Manual Group Creation

Create and Populate a Group:

* New Group Name: XP Users

Group Description: XP Users with Athlon XP Chips

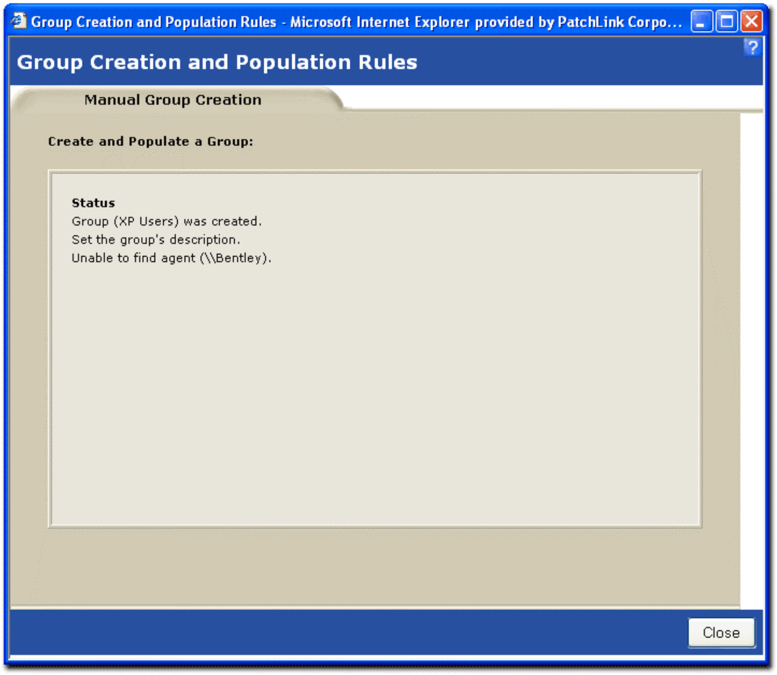
Comma-delimited List of Computers: \\Bentley

NOTE: Windows computer names must start with two backslashes. Example: \\MyWorkstation

* indicates a required field.

Define a new group by filling in a new group's name and description. The group will be auto-populated by adding in a comma-separated list of computer names.

Clicking the OK button initializes the Manual Group Creation status screen.


Group Creation and Population Rules - Microsoft Internet Explorer provided by PatchLink Corpo...

Group Creation and Population Rules

Manual Group Creation

Create and Populate a Group:

Status
Group (XP Users) was created.
Set the group's description.
Unable to find agent (\\Bentley).

Upon clicking the Close button of the Manual Group Creation status screen, the **Groups Homepage** is automatically refreshed showing the newly created computer group.

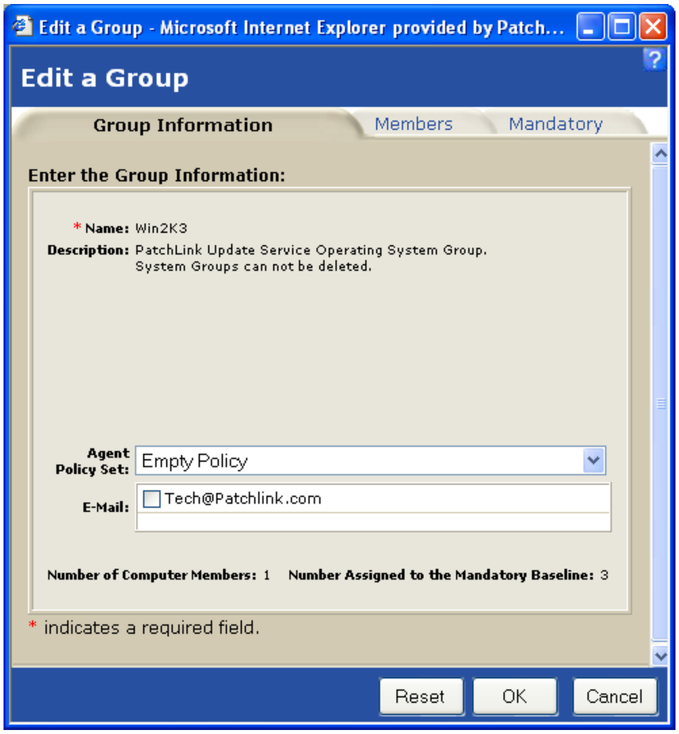
13. Edit a Group Wizard

Plus has the ability to edit groups. To Edit a group, you must first create one. See Section 12; Add a Group Wizard for more information.

From the **Groups** homepage, select the group that you wish to edit by clicking in the checkbox next to the item and click on the **Edit** button on the Action Menu.

Group Property Screen - Info

The **Group Information** Screen section of the Patch Management Server allows the User the ability to edit a group. System-defined groups cannot be changed. The first tab of the property page contains the base information and it is this tab in which a group's information is loaded and saved.


Edit a Group - Microsoft Internet Explorer provided by Patch...
Edit a Group
Group Information
Members
Mandatory
Reset
OK
Cancel

Enter the Group Information:

* Name: Win2K3

Description: PatchLink Update Service Operating System Group. System Groups can not be deleted.

Agent Policy Set: Empty Policy

E-Mail: □ Tech@Patchlink.com

Number of Computer Members: 1   Number Assigned to the Mandatory Baseline: 3

* indicates a required field.

- Group Name

  The name of the group selected to be edited.
- Description

  Previously entered notes or information describing the group.
- Agent Policy Set

  The desired Agent Policy Set to use for the computers who are members of the group. When a computer's policies are calculated, the Patch Management Server determines the superset of all Agent Policy Sets for the groups the computer is a member of. Thus, if one policy set says the agent has a 60 minute interval and another says the computer has a 30 minute interval, the resulting policy set is 30 minutes.

Set the Agent Policy Set to the Empty Policy if this group is to have to effect on the policy calculations.

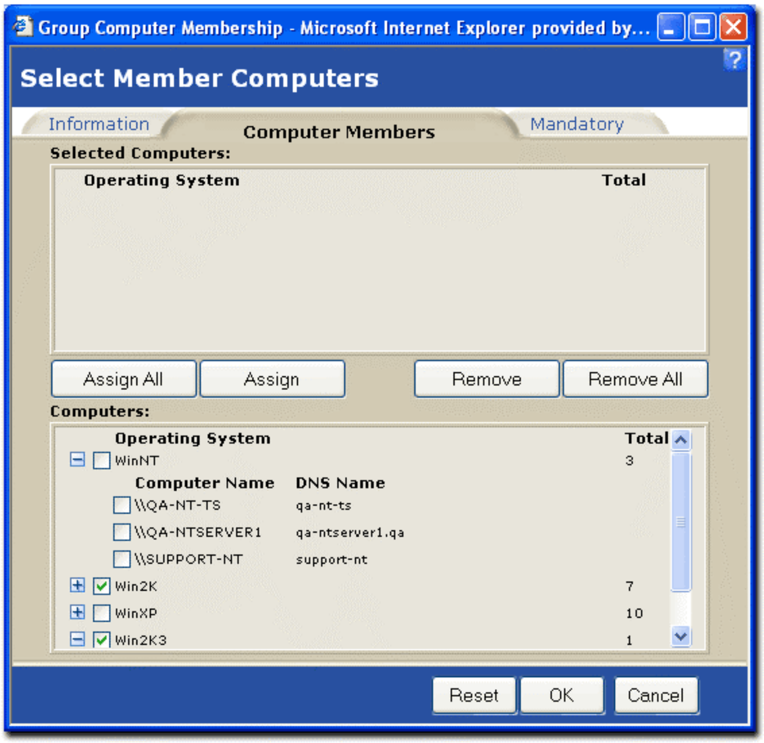
- E-Mail
  Select any users who have been added to the E-Mail Notification list on the Patch Management Server. The selected users will be sent group-based notifications.
- Number of Computer Members
  The total number of computers that are in the selected group.
- Number of Computers assigned to the Mandatory Baseline
  The total number of computers who are currently assigned to the group.

Screen Functions

- Reset
  Resets the page back to its initial state.
- OK
  Initiates the process to save the group's changes. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- Cancel
  Cancels the edit process and closes the group property page window.

Group Property Screen - Members

The Computer Members Group Property Page section of the Patch Management Server allows the User the ability to edit a group. System-defined groups cannot be changed. The **Computer Members** tab of the property page contains a list of all computers which have been assigned as members of the group and the list of computers which are not a member of the group.



Selected Computers:

Operating System	Total

Computers:

Operating System		Total
⊟ □ WinNT		3
Computer Name	DNS Name	
□ \\QA-NT-TS	qa-nt-ts	
□ \\QA-NTSERVER1	qa-ntserver1.qa	
□ \\SUPPORT-NT	support-nt	
⊞ ☑ Win2K		7
⊞ □ WinXP		10
⊟ ☑ Win2K3		1

Selected Computers

- Operating System

  The operating system platform name. Click the ⊞ to display the list of computers for that operating system. Click ⊟ to close the list.
- Computer Name
  The name of the computer.
- DNS Name
  The DNS name assigned to the computer
- Total Selected per OS
  The total number of computers that have been selected for the operating system platform.

Available Computers

- Operating System

  The operating system platform name. Click the ⊞ to display the list of computers for that operating system. Click ⊟ to close the list.
- Computer Name

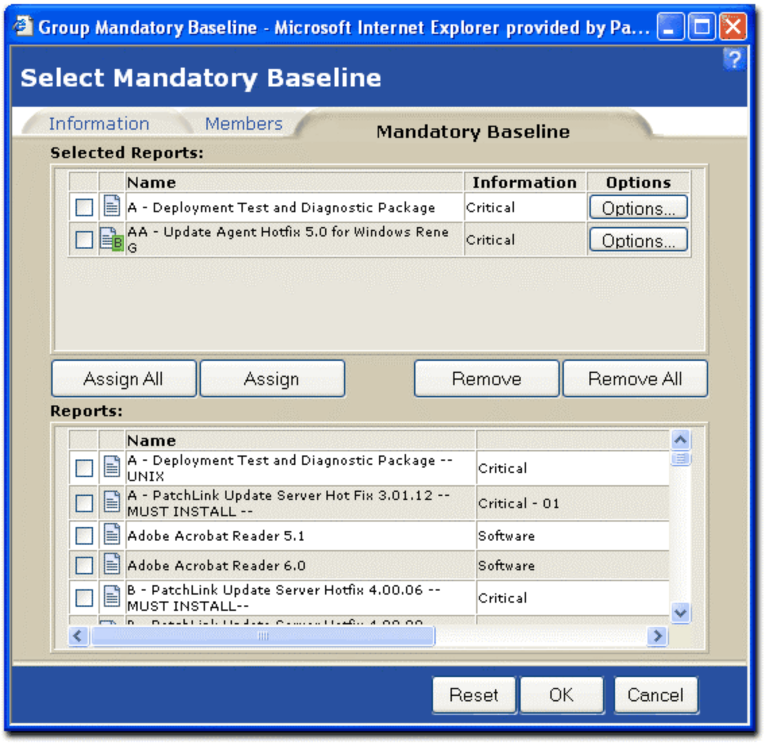
  The name of the computer.
- DNS Name
  The DNS name assigned to the computer
- Total Selected per OS
  The total number of computers that have not been selected for the operating system platform.

Screen Functions

- Assign All
  Assigns all available computers to the group.
- Assign
  Assigns all available computers to the group.
- Remove
  Removes the selected computers from the group.
- Remove All
  Removes all selected computers from the group.
- Cancel
  Cancels the edit process and closes the group property page window.
- Reset
  Resets the page back to its initial state.
- OK
  Initiates the process to save the group (or the group's changes). If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- Cancel
  Cancels the edit process and closes the group property page window.

Group Property Screen –Mandatory Baseline

The Group Property Page section of the Patch Management Server allows the User the ability to edit a group, system-defined groups cannot be changed. The **Mandatory Baseline** tab of the property page contains the lists of selected and available Vulnerability Reports and Locally-created Distribution Packages for the group's baseline.


Group Mandatory Baseline - Microsoft Internet Explorer provided by Pa...
Select Mandatory Baseline
Information
Members
Mandatory Baseline
Assign All
Assign
Remove
Remove All
Reset
OK
Cancel

Selected Reports:

		Name	Information	Options
□		A - Deployment Test and Diagnostic Package	Critical	Options...
□		AA - Update Agent Hotfix 5.0 for Windows Rene G	Critical	Options...

Reports:

		Name	
□		A - Deployment Test and Diagnostic Package -- UNIX	Critical
□		A - PatchLink Update Server Hot Fix 3.01.12 -- MUST INSTALL --	Critical - 01
□		Adobe Acrobat Reader 5.1	Software
□		Adobe Acrobat Reader 6.0	Software
□		B - PatchLink Update Server Hotfix 4.00.06 -- MUST INSTALL--	Critical

Selected Baseline Items

- Baseline Item Name
  The name of the report or package.
- Baseline Item Type
  This is either a Vulnerability Report or a Distribution Package.
- Information
  This contains information about the operating systems for the package or the impact for a report.
- Click the Options button to display a screen with the deployment options and information about the item.

Available Computers

- Baseline Item Name
  The name of the report or package.
- Baseline Item Type
  This is either a Vulnerability Report or a Distribution Package.
- Information
  This contains information about the operating systems for the package or the impact for a report.

Screen Functions

- Assign All
  Assigns all available reports and packages to the group.

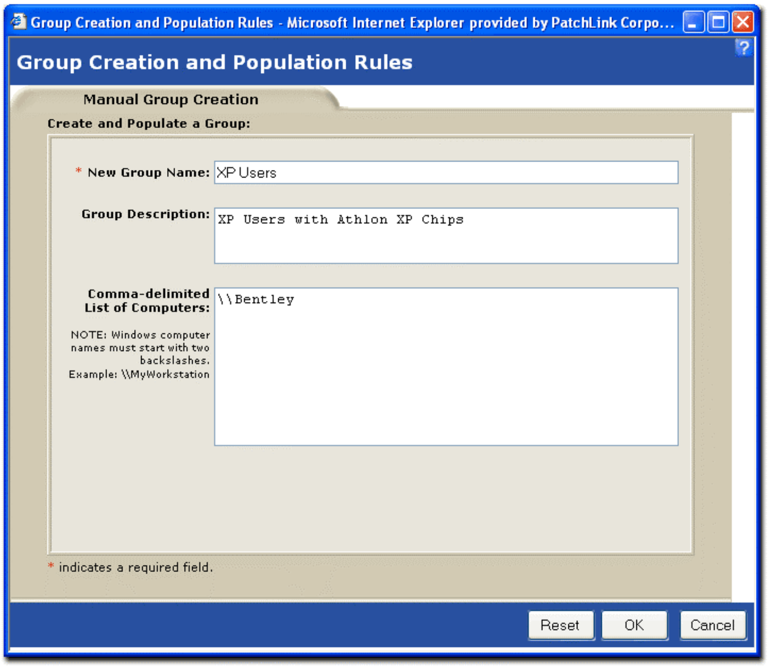
- Assign
  Assigns all available reports and packages to the group.
- Remove
  Removes the selected reports and packages from the group.
- Remove All
  Removes all selected reports and packages from the group.
- Reset
  Resets the page back to its initial state.
- OK
  Initiates the process to save the group (or the group's changes). If a Mandatory Baseline item has been edited which requires a license to agree prior to the saving of the group, a license agreement page will be displayed. If an error occurs during the save process the window will display the error. If no errors occur then the window will be closed.
- Cancel
  Cancels the edit process and closes the group property page window.
- Options.
  Displays a window with the deployment options for the item.

Edit

Selecting a group and clicking on this button will bring up the Group Property page with this group’s information allowing the group to be changed.

Rules

Clicking this button will bring up the Manual Group Creation and Population Rules property page.



Group Creation and Population Rules - Microsoft Internet Explorer provided by PatchLink Corpo...
Group Creation and Population Rules
Manual Group Creation
Reset
OK
Cancel

Create and Populate a Group:

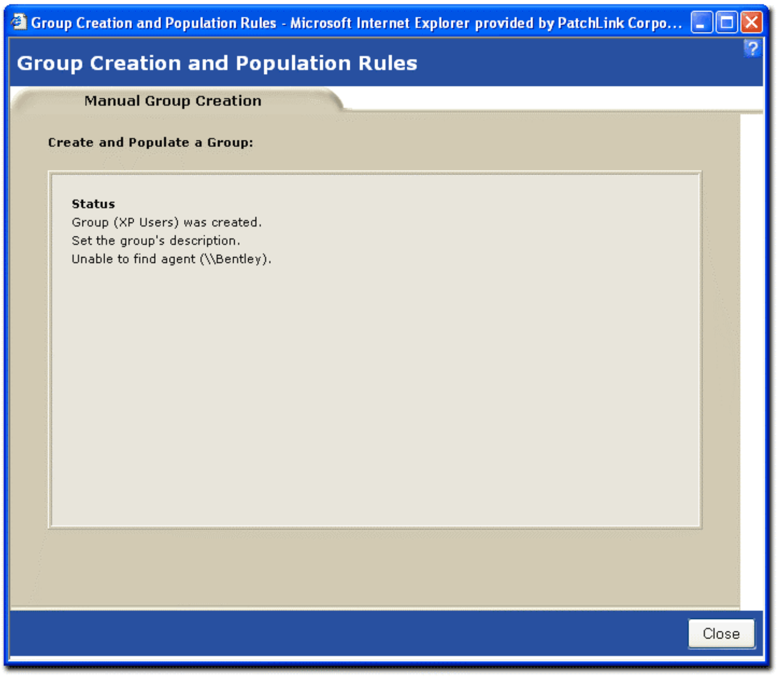
* New Group Name:	XP Users
Group Description:	XP Users with Athlon XP Chips
Comma-delimited List of Computers:	\\Bentley

NOTE: Windows computer names must start with two backslashes. Example: \\MyWorkstation

* indicates a required field.

Define a new group by filling in a new group's name and description. The group will be auto-populated by adding in a comma-separated list of computer names.

Clicking the OK button initializes the Manual Group Creation status screen.


Group Creation and Population Rules - Microsoft Internet Explorer provided by PatchLink Corpo...
Group Creation and Population Rules
Manual Group Creation
Create and Populate a Group:
Close

Status
Group (XP Users) was created.
Set the group's description.
Unable to find agent (\\Bentley).

Upon clicking the Close button of the Manual Group Creation status screen, the **Groups Homepage** is automatically refreshed showing the newly created computer group.

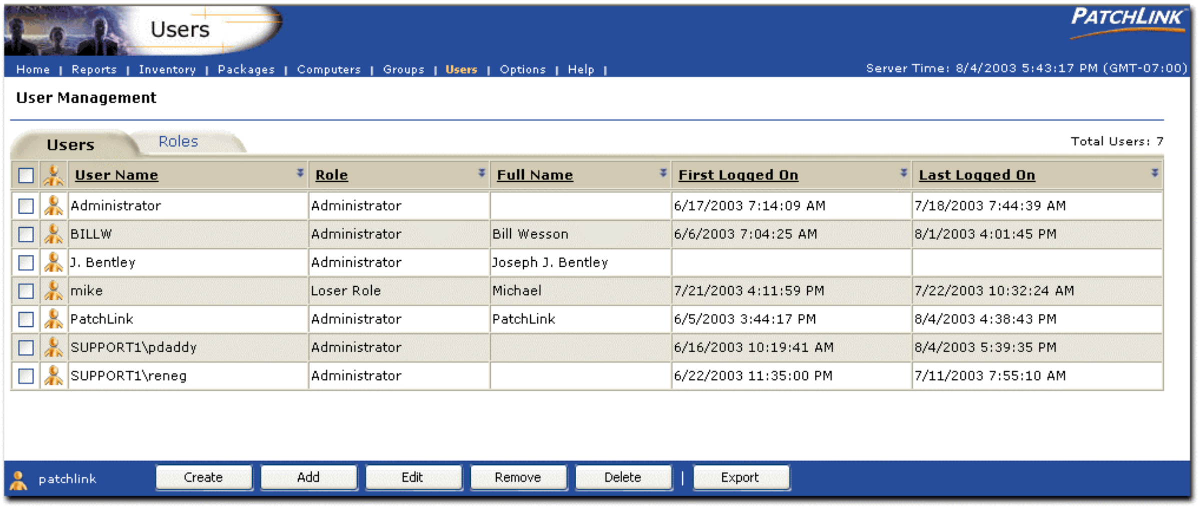
14. Users

Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |

The User Management section of the Patch Management Server allows the Patch Management Administrator the ability to manage who has access to log in to the Server and once they are logged in, what sections and functions they can access, and what computers and groups they can perform those functions on.

ZENworks® Patch Management Server Users

This displays the users who have the ability to log in to Patch Management Server and what User Role each user has.


Users
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |
Users
Roles
patchlink
Create
Add
Edit
Remove
Delete
Export

Server Time: 8/4/2003 5:43:17 PM (GMT-07:00)

User Management

Total Users: 7

□	User Name	Role	Full Name	First Logged On	Last Logged On
□	Administrator	Administrator		6/17/2003 7:14:09 AM	7/18/2003 7:44:39 AM
□	BILLW	Administrator	Bill Wesson	6/6/2003 7:04:25 AM	8/1/2003 4:01:45 PM
□	J. Bentley	Administrator	Joseph J. Bentley		
□	mike	Loser Role	Michael	7/21/2003 4:11:59 PM	7/22/2003 10:32:24 AM
□	PatchLink	Administrator	PatchLink	6/5/2003 3:44:17 PM	8/4/2003 4:38:43 PM
□	SUPPORT1\pdaddy	Administrator		6/16/2003 10:19:41 AM	8/4/2003 5:39:35 PM
□	SUPPORT1\reneg	Administrator		6/22/2003 11:35:00 PM	7/11/2003 7:55:10 AM

User Information

Username

The name a user uses to log in to the Patch Management Server.

Role

What user role the user is assigned.

Full Name

The user's full name.

First Logged On

When the user first logged on to the Patch Management Server.

Last Logged On

When the user last logged on to the Patch Management Server.

Page Functions

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

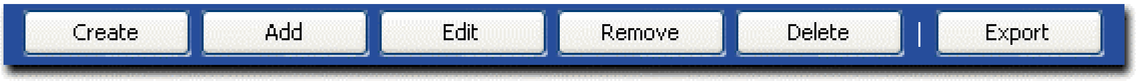
Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Create

Allows a Patch Management Administrator to create new local machine users and add them as users who have access to log on to the Patch Management Server. See Section 15; Create a User for more information.

Add

Allows a Patch Management Administrator to give an existing Windows user access to log on to the Patch Management Server. See Section 16; Add a User for more information.

Edit

The Edit a User Wizard allows Patch Management Administrator the ability to edit a user's information and change their user role, if needed. This page of the wizard gives an overview of the wizard's function. See Section 17; Edit a User for more information.

Remove

Allows a Patch Management Administrator to remove a Windows User from being able to log on to the Patch Management Server. This does not delete the Windows user.

Delete

Allows a Patch Management Administrator to remove a Windows User from being able to log on to the Patch Management Server and then delete the user from the local machine.

Export

Exports the lists of uses and their information to a comma-separated value (CSV) file.

User Management Security

The user management section of the Patch Management Server requires the View User Management access right. If a user does not have the correct access the access denied error message is displayed.

To be able to Create, Add, Edit, Remove, or Delete users within the User Management section of the Patch Management Server requires the Manage Users access right. If a user does not have the correct access, the Create, Add, Edit, Remove and Delete buttons are disabled.

To be able to export the user data to a comma-separated value (CSV) file requires the Export User Data access right. If a user does not have the correct access, the Export button is disabled.

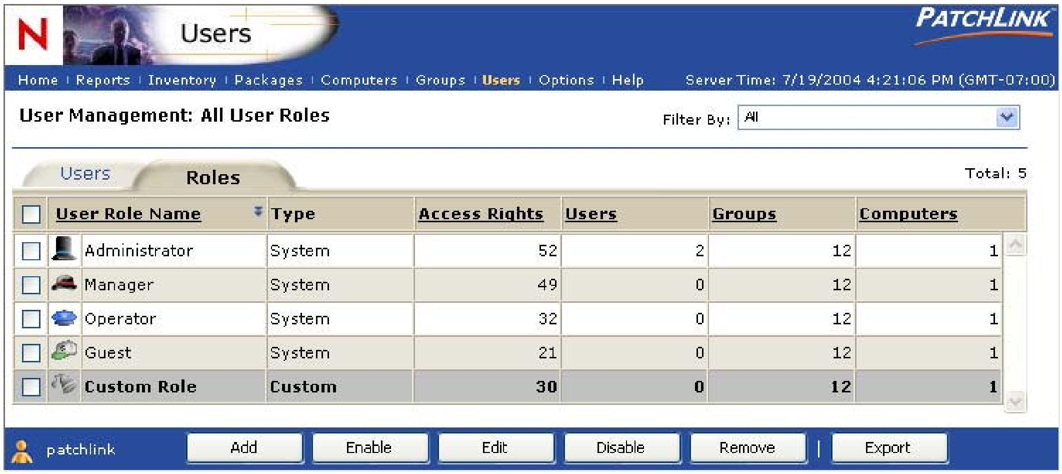
Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

User (Security) Roles

A User Role defines what a user can see, what they can do, and what they can perform those actions on. If a user is able to log in to the Patch Management Server but does not have any access they will not be able to view any pages, perform any functions on any groups or computers. This will literally see nothing, nor be able to do nothing. At any given time, there must be at least one user who has the Administrator User Role.

Every page, feature, function and individual action of the Patch Management Server is constrained to a series of Access Rights. Based on what Access Rights a role has defines what pages and functionality or actions the users who are assigned that role have.

By default there are four system-defined User Roles: Administrator, Manager, Operator and Guest. The Patch Management Server Administrator can assign these roles to Server users or use them as templates to create new User Roles. By default all groups and computers are added to these user roles when they are created or registered. The various roles are:


Users
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Users
Roles
patchlink
Add
Enable
Edit
Disable
Remove
Export

Server Time: 7/19/2004 4:21:06 PM (GMT-07:00)

User Management: All User Roles

Filter By: All

Total: 5

□	User Role Name	Type	Access Rights	Users	Groups	Computers
□	Administrator	System	52	2	12	1
□	Manager	System	49	0	12	1
□	Operator	System	32	0	12	1
□	Guest	System	21	0	12	1
□	**Custom Role**	**Custom**	**30**	**0**	**12**	**1**

User Roles

Administrator

Any user who is assigned this User Role is considered a Super-User, as they have full access to everything. Users of this role are the only users who can delegate newly installed computers to other user roles.

Manager

The Manager User role can manage every section of the Patch Management Server other than the Advanced Configuration Options and User Management.

Operator

The Operator user role can perform all routine operations (deploy, detect, export).

Guest

The Guest user role can access all of the pages but perform no functionality on what they see.

Custom

The custom user role is a role that is defined by a Patch Management Administrator. The Patch Management Administrator defines access rights, groups and computers that these roles have access to.

Disabled Custom

This customer user role has been disabled. Any users who are assigned this role do not have will not have any access to any of the Patch Management Server sections, functions, computers or groups.

User Role List

User Role Name

The name of the user role.

Type

System or Custom, based on who created the role.

Access Rights

The number of access rights assigned to the user role.

Users

The number of users assigned this user role.

Groups

The number of groups assigned to the user role.

Computers

The number of computers assigned to the user role.

Page Functions

Filter by

Filter your results selecting the desired item from the **Filter by** drop down menu in the upper right hand corner.

Sort

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

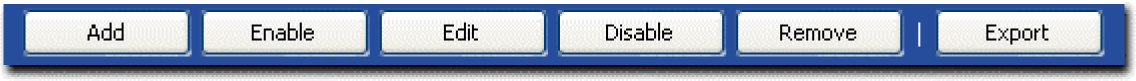
Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Checkboxes

Checkboxes are used to either select a single item or a group of items to initialize them for a certain function or selection. Checkboxes appear throughout the Patch Management Server and are **not** visible in Netscape.

Action Menu



Add

The Role Property pages allow the Patch Management Administrator to create or edit a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use this page to specify basic role information. See Section 18; Add a Role Wizard for more information.

Enable

Allows a Patch Management Administrator to enable an existing (non-system) user role.

Edit

Allows a Patch Management Administrator to change an existing (non-system) user role.
See Section 19; Edit a Role for more information.

Disable

Allows a Patch Management Administrator to disable an existing (non-system) user role.

Remove

Allows a Patch Management Administrator to delete an existing (non-system) disabled user role.

Export

Exports the lists of user roles and their information to a comma-separated value (CSV) file.

User Roles Security

The user roles section of the Patch Management Server requires the View User Management access right. If a user does not have the correct access, the access denied error message is displayed.

To be able to Add, Edit, or Remove user roles within the User Role section of the Patch Management Server requires the Manage Users access right. If a user does not have the correct access, the Add, Edit, and Remove buttons are disabled.

To be able to export the user role data to a comma-separated value (CSV) file requires the Export User Data access right. If a user does not have the correct access, the Export button is disabled.

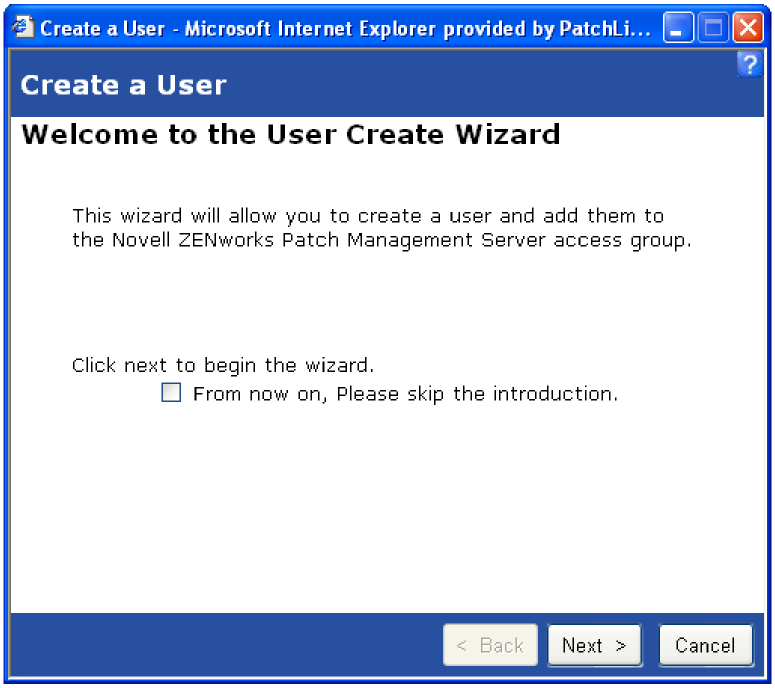
Contact your Patch Management Administrator for more information on ZENworks® Patch Management Security.

15. Create a User Wizard

The **Create a User** Wizard allows Patch Management Administrator the ability to create local Windows users and give them access to the Patch Management Server. Enter basic information required to create the user.

Welcome

From the **Users** homepage, Users Tab, click on the **Create** button on the Action Menu. The Welcome Screen appears.



Create a User - Microsoft Internet Explorer provided by PatchLi...
?
< Back
Next >
Cancel

Create a User

Welcome to the User Create Wizard

This wizard will allow you to create a user and add them to the Novell ZENworks Patch Management Server access group.

Click next to begin the wizard.

□ From now on, Please skip the introduction.

Screen Functions

Skip

The **Skip the Introduction** checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Create a User Wizard is initialized.

Back

The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.

Next

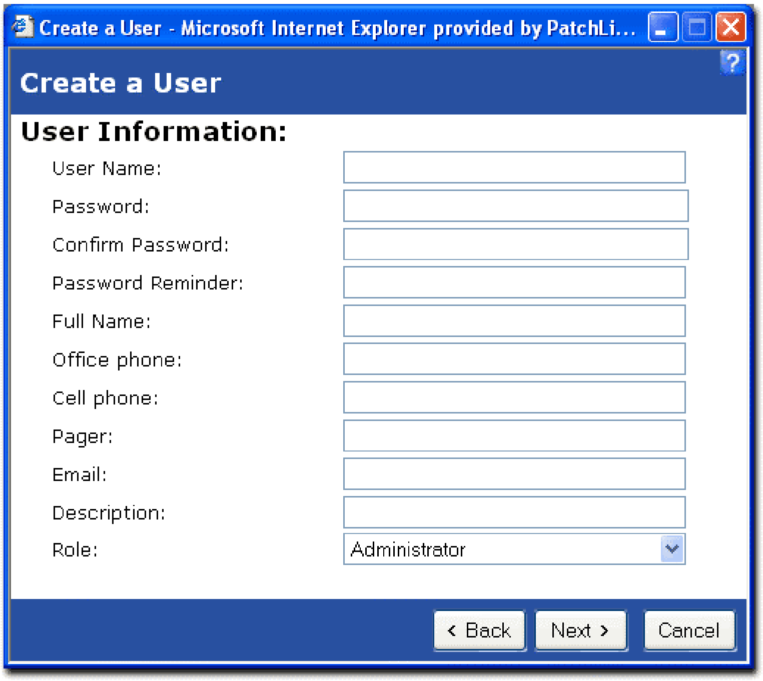
The **Next** button initializes the wizard’s next screen.

Cancel

The **Cancel** button closes the wizard.

User Information

Enter User Information into the appropriate fields and select their **Role** from the dropdown menu. A User Role defines what a user can see, what they can do, and what they can perform those actions on. If a user is able to log in to the Patch Management Server, but does not have any access, they will not be able to view any pages, perform any actions or functions on any groups or computers. This is literally see nothing, nor be able to do nothing. At any given time, there must be at least one user who is assigned to the Administrator User Role.



Create a User - Microsoft Internet Explorer provided by PatchLi...

Create a User

User Information:

User Name:

Password:

Confirm Password:

Password Reminder:

Full Name:

Office phone:

Cell phone:

Pager:

Email:

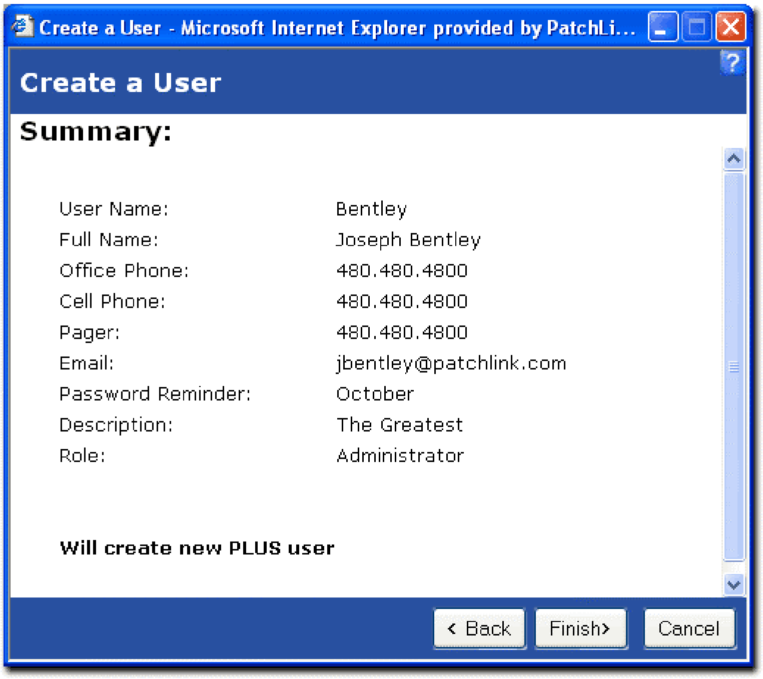
Description:

Role: Administrator

After entering in all User information, click the **Next** button to verify a summary of the data before the user is created.

Summary

Verify the accuracy of all entered User information. Click the **Back** button to initialize the previous User Information screen and edit user information. Click the **Next** button to initialize the creation of the user and to view the Status screen.


Create a User - Microsoft Internet Explorer provided by PatchLi...
?

Create a User

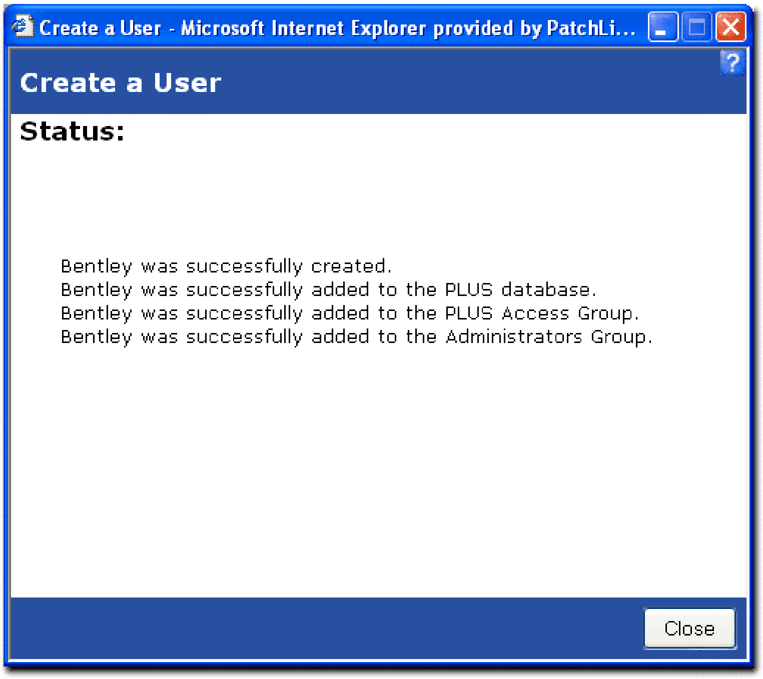
Summary:

User Name:	Bentley
Full Name:	Joseph Bentley
Office Phone:	480.480.4800
Cell Phone:	480.480.4800
Pager:	480.480.4800
Email:	jbentley@patchlink.com
Password Reminder:	October
Description:	The Greatest
Role:	Administrator

Will create new PLUS user

Status

The user was created and added to the Patch Management Server Access Group.


Create a User - Microsoft Internet Explorer provided by PatchLi...
Create a User
?
Status:
Close

```
Bentley was successfully created.
Bentley was successfully added to the PLUS database.
Bentley was successfully added to the PLUS Access Group.
Bentley was successfully added to the Administrators Group.
```

If the user was given access to a user role which has the Manage Users Access Right, they will also be added to the Windows Administrators group on the local Patch Management Server computer.

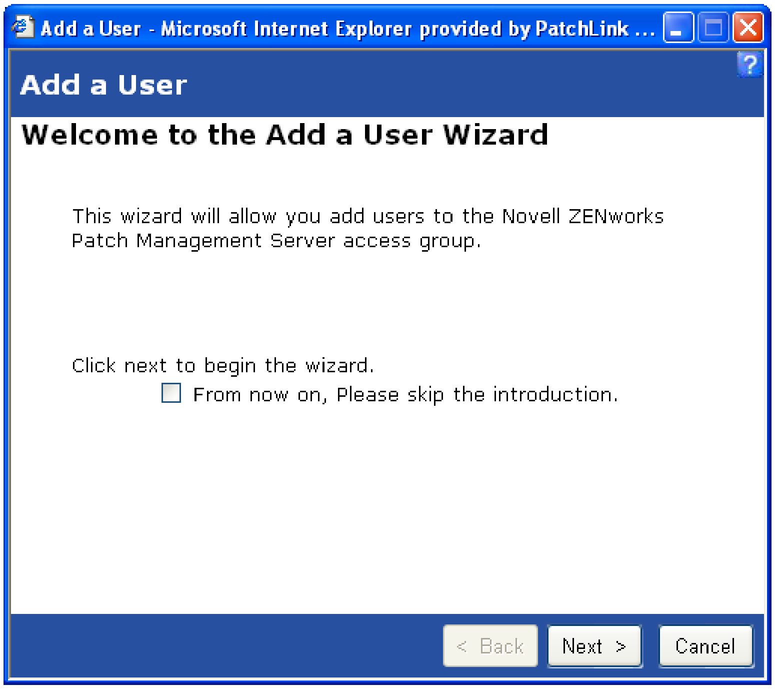
Upon Closure of the Status window, the newly created user will appear on the Users homepage after it is refreshed.

16. Add a User Wizard

The **Add a User** Wizard allows a Patch Management Administrator to give an existing Windows user access to log on to the Patch Management Server.

Welcome

From the **Users** homepage, Users Tab, click on the **Add** button on the Action Menu. The Welcome Screen appears.



Add a User - Microsoft Internet Explorer provided by PatchLink ...
Add a User

Welcome to the Add a User Wizard

This wizard will allow you add users to the Novell ZENworks Patch Management Server access group.

Click next to begin the wizard.

□ From now on, Please skip the introduction.

Screen Functions

Skip

The **Skip the Introduction** checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Add a User Wizard is initialized.

Back

The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.

Next

The **Next** button initializes the wizard's next screen.

Cancel

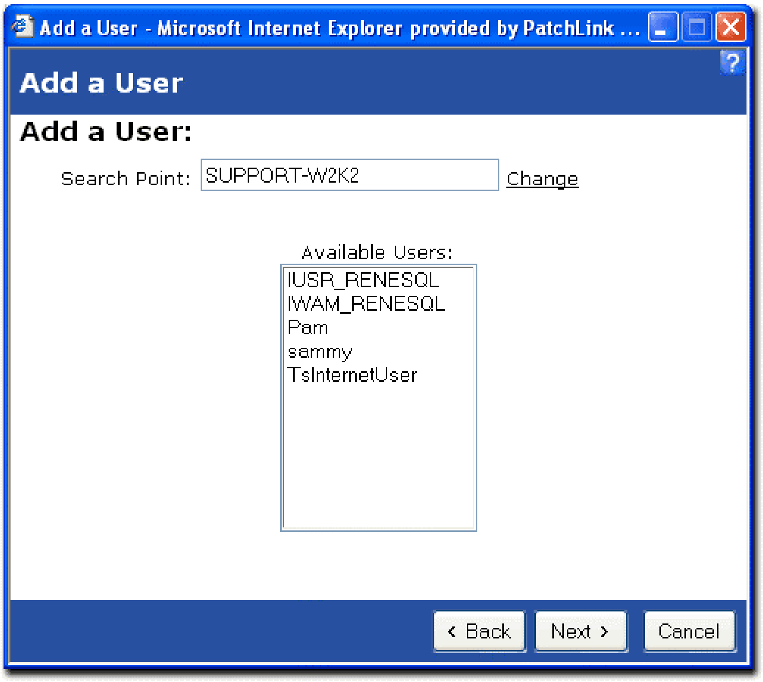
The **Cancel** button closes the wizard.

Click the **Next** button to enter User Information.

Add

Displayed are a list of users that are available (from your Created Users) to be added to the Patch Management Server Access Group.

Note: The Microsoft IIS Web server software does not support the entering of user names or passwords in languages (Korean, Kanji, etc.) that require Unicode characters. Since the Patch Management Server software uses Microsoft IIS as it's Web server, end-users cannot enter usernames and passwords in Unicode to log on to the Patch Management Server website.



Search Point: SUPPORT-W2K2

Available Users:
IUSR_RENESQL
IWAM_RENESQL
Pam
sammy
TsInternetUser

Search Point: Change

The default location to check for users is the name of the computer where the Patch Management Server is installed. To change this, enter in the new search location in to the Search Point field and click on the Change hyperlink.

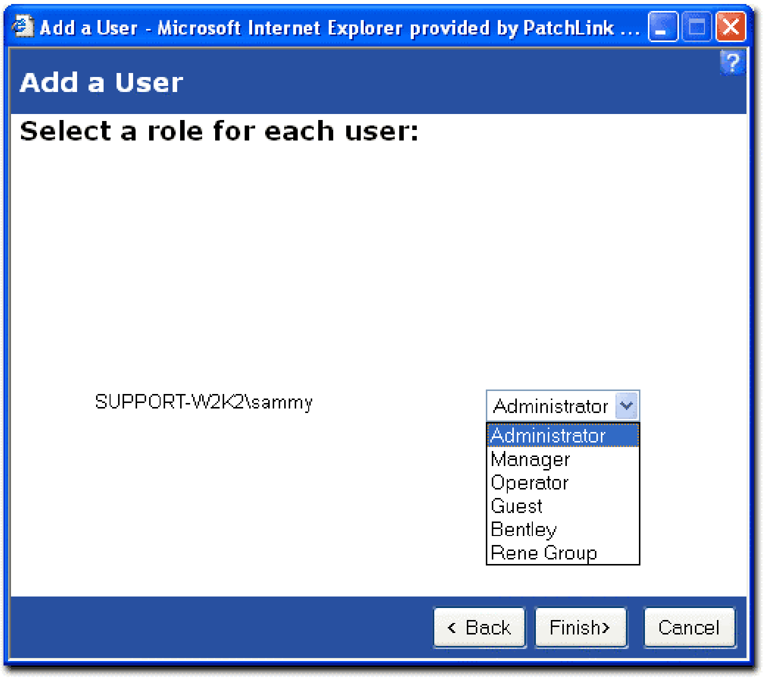
Available Users: Select

To select a user simply click on the user's name. To select multiple users, hold the **Ctrl** (control) key down and click on the user names.

Click the **Next** button to initialize the **Roles** screen.

Select a Role

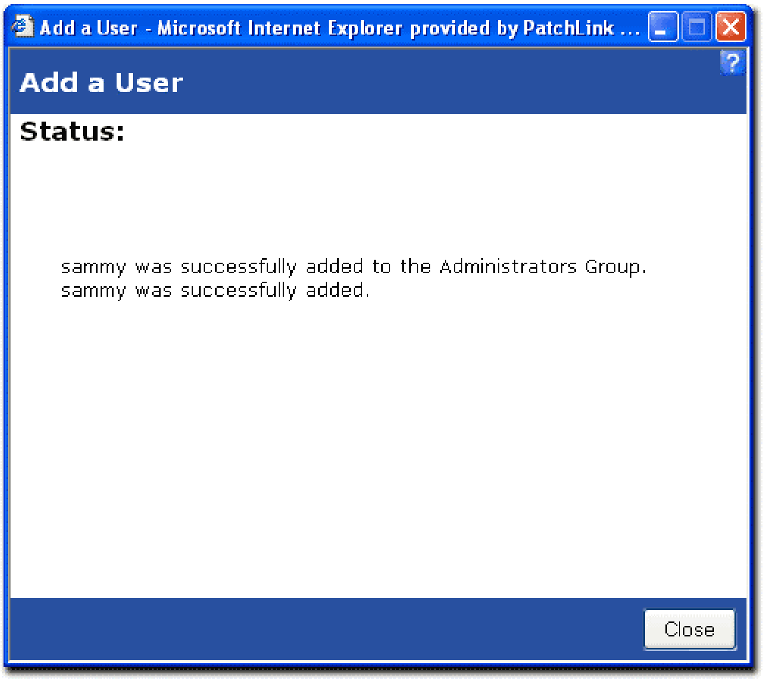
This screen displays the available user roles to choose. The selected role will be assigned to the user.



Select a User Role and click the **Finish** button.

Status

The status screen appears verifying the addition.


Add a User - Microsoft Internet Explorer provided by PatchLink ...
Add a User
?
Close

Status:

sammy was successfully added to the Administrators Group.
sammy was successfully added.

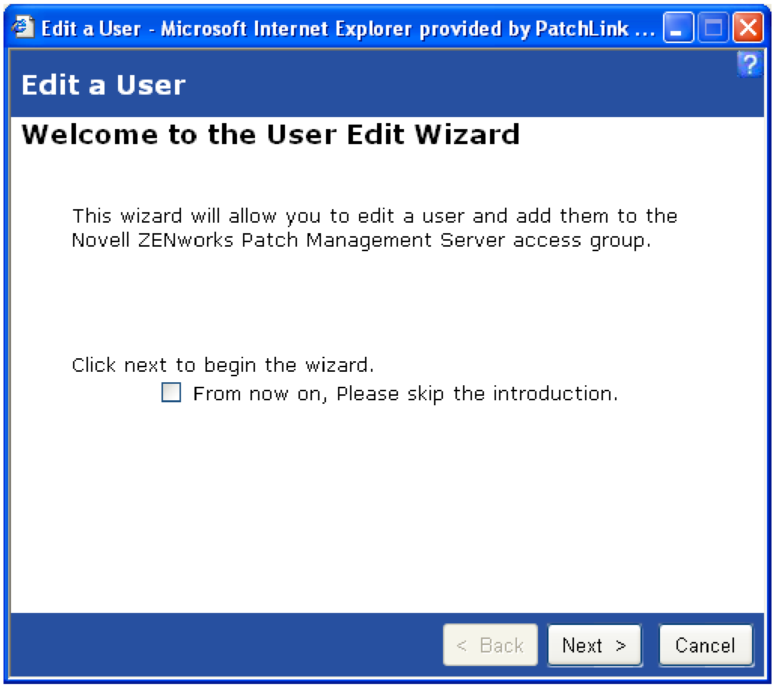
Upon clicking on the Close button, the User screen is automatically refreshed with the User addition.

17. Edit a User Wizard

The **Edit a User Wizard** allows Patch Management Administrator the ability to edit a user's information and change their user role, if needed.

Welcome

From the **Users** homepage, Users Tab, select a User that you wish to edit by clicking in the checkbox next to the item and click on the **Edit** button on the Action Menu. The Welcome Screen appears.


Edit a User - Microsoft Internet Explorer provided by PatchLink ...
?
< Back
Next >
Cancel

Edit a User

Welcome to the User Edit Wizard

This wizard will allow you to edit a user and add them to the Novell ZENworks Patch Management Server access group.

Click next to begin the wizard.

□ From now on, Please skip the introduction.

Screen Functions

Skip

The **Skip the Introduction** checkbox will determine if the Introduction page will be displayed each time the wizard is accessed. Click in the checkbox to prevent the Welcome screen from appearing the next time the Edit a User Wizard is initialized.

Back

The **Back** button is disabled since this is the first page of the wizard. In subsequent screens, the **Back** button will initialize the previous screen.

Next

The **Next** button initializes the wizard's next screen.

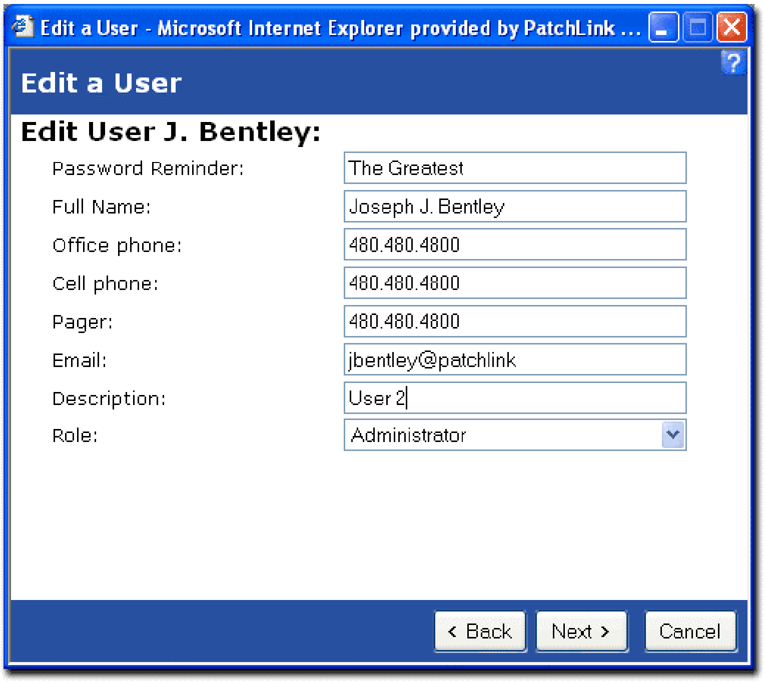
Cancel

The **Cancel** button closes the wizard.

Click the Next button to initialize the **Edit User** screen.

Edit Information

Displayed are the fields in which you entered information when you created a user.



Edit a User - Microsoft Internet Explorer provided by PatchLink ...
?
Edit a User

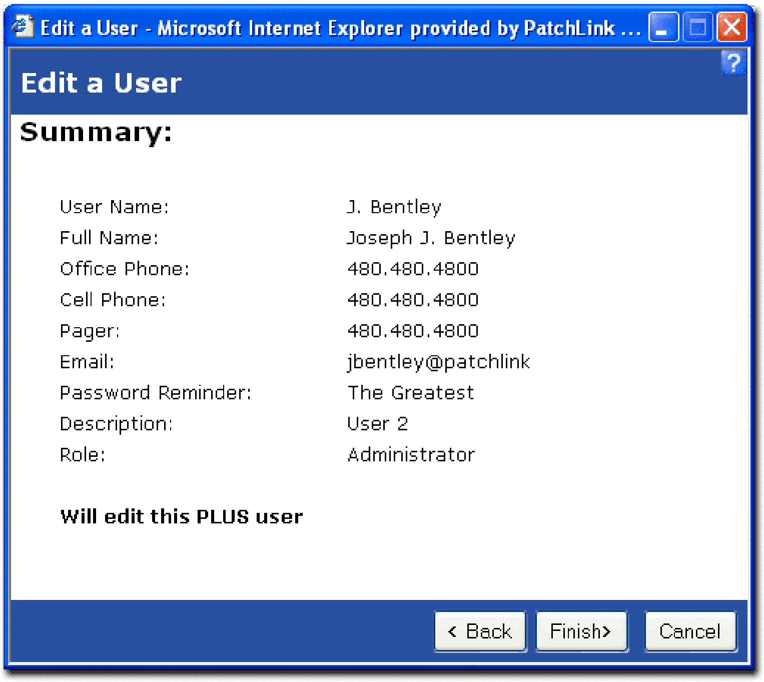
Edit User J. Bentley:

Password Reminder:	The Greatest
Full Name:	Joseph J. Bentley
Office phone:	480.480.4800
Cell phone:	480.480.4800
Pager:	480.480.4800
Email:	jbentley@patchlink
Description:	User 2
Role:	Administrator

Edit information and click the **Next** button.

Summary

Verify the accuracy of all entered User information. Click the **Back** button to initialize the previous Edit User Information screen and edit user information. Click the **Next** button to initialize the edit of the user and to view the Status screen.


Edit a User - Microsoft Internet Explorer provided by PatchLink ...
?
< Back
Finish>
Cancel

Edit a User

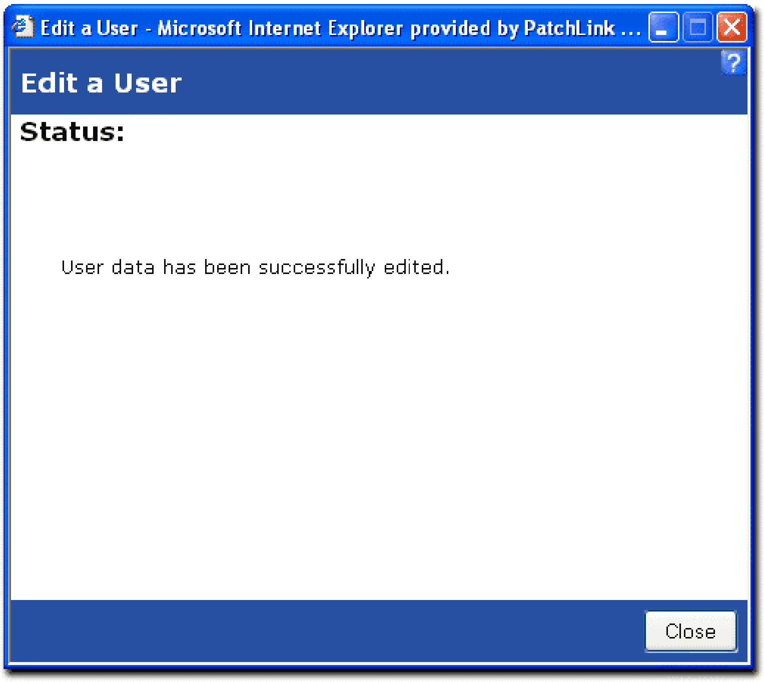
Summary:

User Name:	J. Bentley
Full Name:	Joseph J. Bentley
Office Phone:	480.480.4800
Cell Phone:	480.480.4800
Pager:	480.480.4800
Email:	jbentley@patchlink
Password Reminder:	The Greatest
Description:	User 2
Role:	Administrator

Will edit this PLUS user

Status

The status screen appears verifying the edit.


Edit a User - Microsoft Internet Explorer provided by PatchLink ...
?
Close

Edit a User

Status:

User data has been successfully edited.

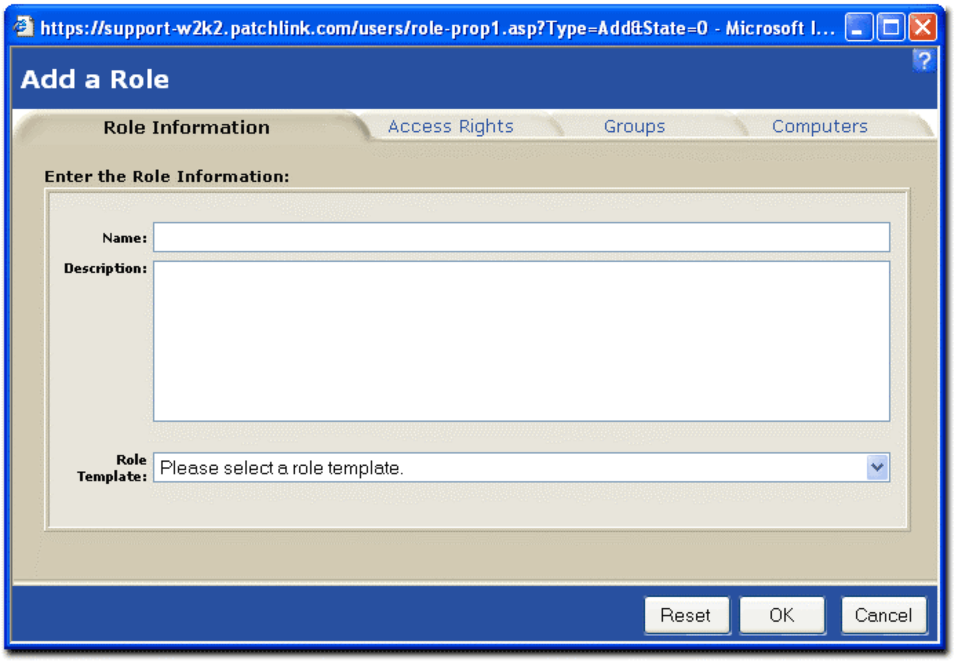
Upon Closure of the Status window, the newly edited user information will appear on the Users homepage item after it is refreshed and viewed.

18. Add a Role Wizard

The Role Property pages allow the Patch Management Administrator to create a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Role Information** screen to specify basic role information.

Add a Role

From the Users homepage, Roles Tab, Click on the Add button on the Action Menu to initialize the **Add a Role** wizard.


https://support-w2k2.patchlink.com/users/role-prop1.asp?Type=Add&State=0 - Microsoft I...
Add a Role
Role Information
Access Rights
Groups
Computers
Enter the Role Information:
Name:
Description:
Role Template:
Please select a role template.
Reset
OK
Cancel

Role Information

- Name

  Enter the name of the user role to be created or that of the role being edited.
- Description

  Enter the description of the user role.
- Role Template

  When creating a role, use this to select a pre-existing system role to use as starting point for further customization. When editing a role, this will initially display "custom" to indicate that the role is not a system role. As in creating a role, use this control to set your role to one of the system templates as a starting point for further editing.

Screen Functions

- Access Rights Tab

  Select this tab to specify this role's access rights to various Patch Management Server functionalities.
- Groups Tab

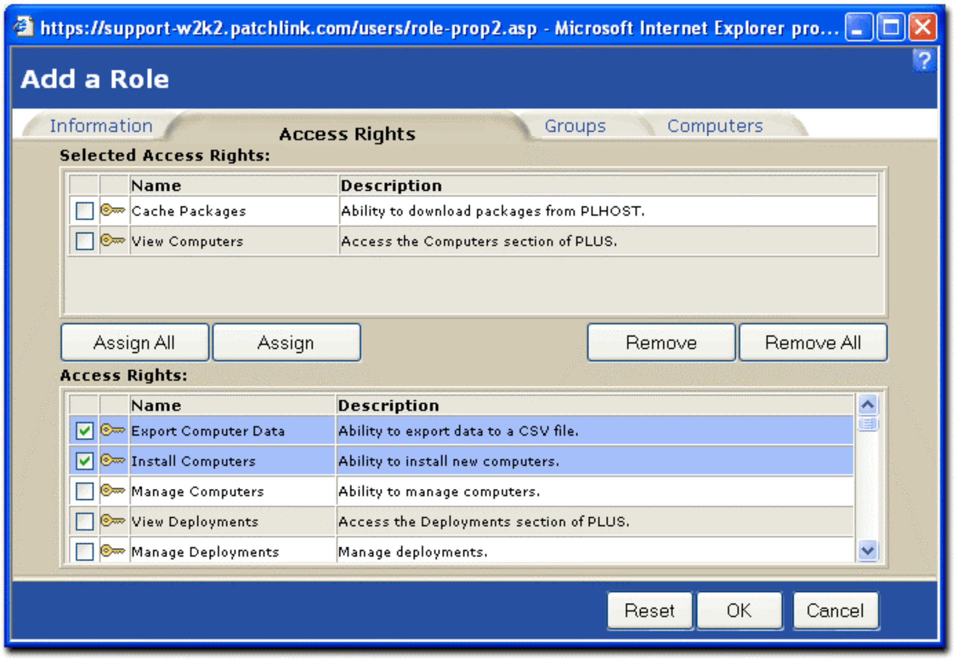
  Select this tab to specify the groups of computers that this role may access.
- Computers Tab

  Select this tab to specify individual computers that this role may access.

Select the Access Rights Tab to initialize the Access Rights screen and assign rights.

Access Rights

The Role Property screens allow the Patch Management Administrator to create a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Access Rights** to specify the access rights to Patch Management Server functionalities assigned to this user role.



Selected Access Rights:

	Name	Description
□	Cache Packages	Ability to download packages from PLHOST.
□	View Computers	Access the Computers section of PLUS.

Access Rights:

	Name	Description
☑	Export Computer Data	Ability to export data to a CSV file.
☑	Install Computers	Ability to install new computers.
□	Manage Computers	Ability to manage computers.
□	View Deployments	Access the Deployments section of PLUS.
□	Manage Deployments	Manage deployments.

Access Rights Information

- Selected Access Rights

  Select or Edit from the list of access rights that have been assigned to this user role.
- Access Rights

  A list of all the access rights that can be assigned to a user role. Scroll through and click in the checkbox next to the desired right(s) to initialize and click the **Assign** button. The system populates the **Selected Access Rights** window with your selections. Use the **Assign All** button to populate the **Selected Access Rights** with ALL rights from the **Access Rights** window.

Screen Functions

- Assign All

  Click to assign all available access rights to the user role.
- Assign

  After selecting any number of the access rights listed in the "Access Rights" (lower) pane, click here to assign these rights to the user role.
- Remove

  After selecting any number of the access rights listed in the "Selected Access Rights" (upper) pane, click here to remove these rights from the user role.
- Remove All

  Click to remove from the role all of the assigned access rights.
- Information Tab

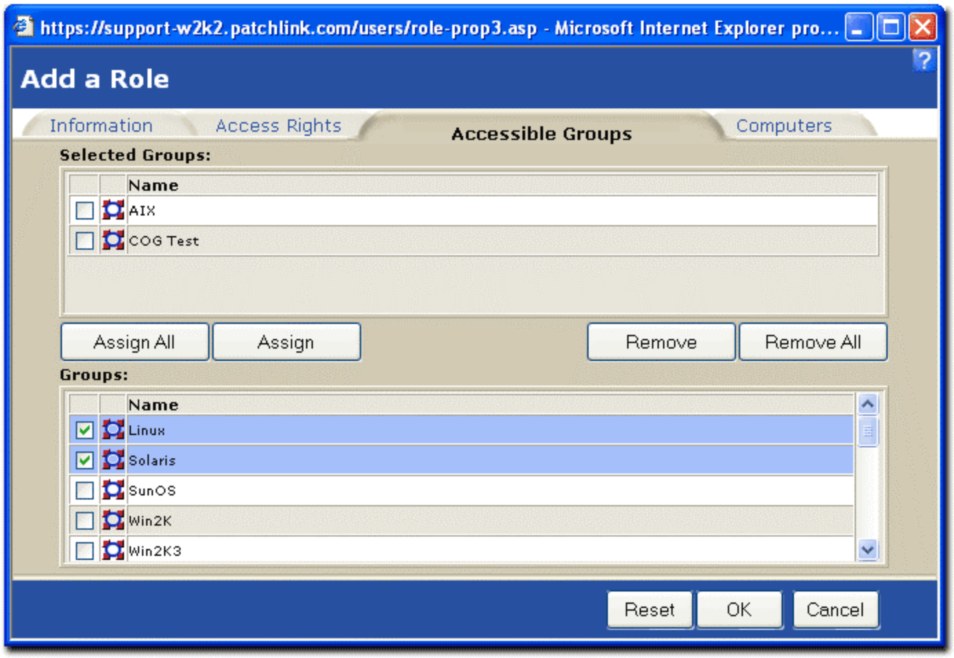
  Select this tab to specify this role's basic information.
- Groups Tab

  Select this tab to specify the groups of computers that this role may access.
- Computers Tab

  Select this tab to specify individual computers that this role may access.

Accessible Groups

The Role Property screens allow the Patch Management Administrator to create a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Accessible Groups** screen to specify the groups of computers that this user role may access.



Add a Role

Selected Groups:

□		Name
□		AIX
□		COG Test

Groups:

□		Name
☑		Linux
☑		Solaris
□		SunOS
□		Win2K
□		Win2K3

Accessible Groups Information

- Selected Groups

  A list of the groups of computers that have been assigned to this user role.
- Groups

  A list of all the groups of computers that can be assigned to this user role.

  Scroll through and click in the checkbox next to the desired group(s) to initialize and click the **Assign** button. The system populates the **Selected Groups** window with your selections. Use the **Assign All** button to populate the **Selected Groups** with ALL groups from the **Groups** window.

Screen Functions

- Assign All

  Click to assign all available groups to the user role.
- Assign

  After selecting any number of the groups listed in the "Groups" (lower) pane, click here to assign these groups to the user role.
- Remove

  After selecting any number of the groups listed in the "Selected Groups" (upper) pane, click here to remove these groups from the user role.
- Remove All

  Click here to remove from the role all of the assigned groups.
- Information Tab

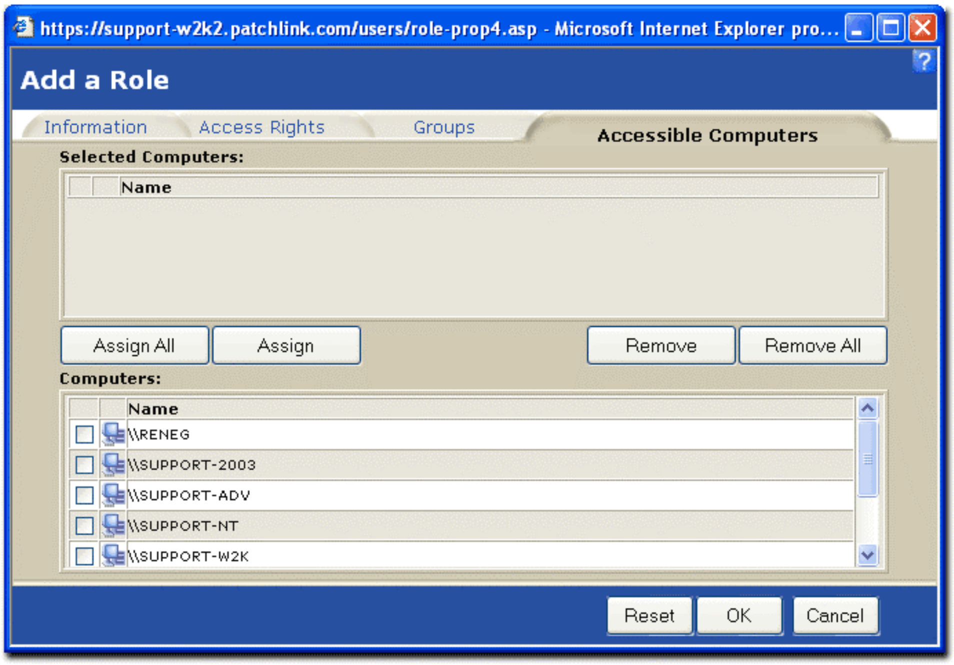
  Select this tab to specify this role's basic information.
- Access Rights Tab

  Select this tab to specify this role's access rights to Patch Management Server functionalities.
- Computers Tab

  Select this tab to specify individual computers that this role may access.

Accessible Computers

The Role Property screens allow the Patch Management Administrator to create or edit a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Accessible Computers** to specify the individual computers that this user role may access.



https://support-w2k2.patchlink.com/users/role-prop4.asp - Microsoft Internet Explorer pro...

Add a Role

Selected Computers:

	Name

Computers:

	Name
□	\\RENEG
□	\\SUPPORT-2003
□	\\SUPPORT-ADV
□	\\SUPPORT-NT
□	\\SUPPORT-W2K

Accessible Computers Information

- Selected Computers

  A list of all the computers that have been assigned to this user role.
- Computers

  A list of all the computers that can be assigned to this user role.

  Scroll through and click in the checkbox next to the desired computer(s) to initialize and click the **Assign** button. The system populates the **Selected Computers** window with your selections. Use the **Assign All** button to populate the **Selected Computers** with ALL computers from the **Computers** window.

Screen Functions

- Assign All

  Click to assign all available computers to the user role.
- Assign

  After selecting any number of the computers listed in the "Computers" (lower) pane, click here to assign these computers to the user role.
- Remove

  After selecting any number of the computers listed in the "Selected Computers" (upper) pane, click here to remove these computers from the user role.
- Remove All

  Click here to remove from the role all of the assigned computers.
- Information Tab

  Select this tab to specify this role's basic information.
- Access Rights Tab

Select this tab to specify this role's access rights to Patch Management Server functionalities.

- Groups Tab

  Select this tab to specify the groups of computers that this role may access.

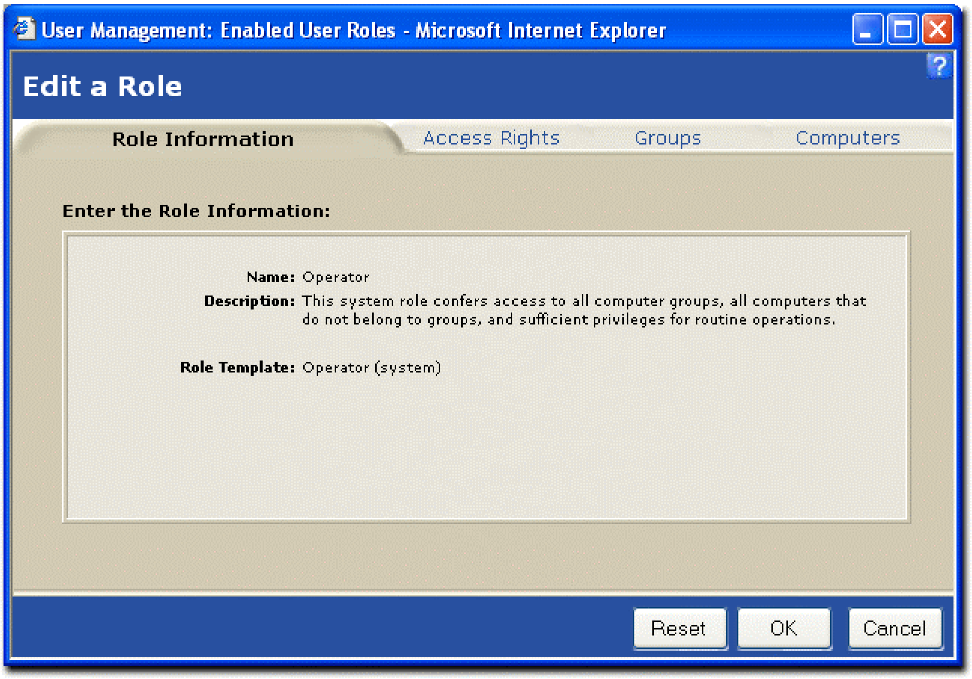
Upon closure of the Add a Role Wizard, the homepage will be refreshed with the newly entered Role.

19. Edit a Role Wizard

The Role Property screens allow the Patch Management Administrator to edit a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use this screen to view basic role information.

Edit a Role

From the Users homepage, click the Roles tab and select the Role you wish to edit by clicking in the checkbox next to it and clicking on the **Edit** button on the Action Menu. This initializes the **Edit a Role** wizard. To edit a role, you must first add one. See Section 19; Add a Role Wizard for more information.



Enter the Role Information:

Name: Operator

Description: This system role confers access to all computer groups, all computers that do not belong to groups, and sufficient privileges for routine operations.

Role Template: Operator (system)

Role Information

- Contains the Name, Description, and Role Template information about the specific role that you chose to Edit.

Screen Functions

- Access Rights Tab

  Select this tab to specify this role's access rights to various Patch Management Server functionalities.
- Groups Tab

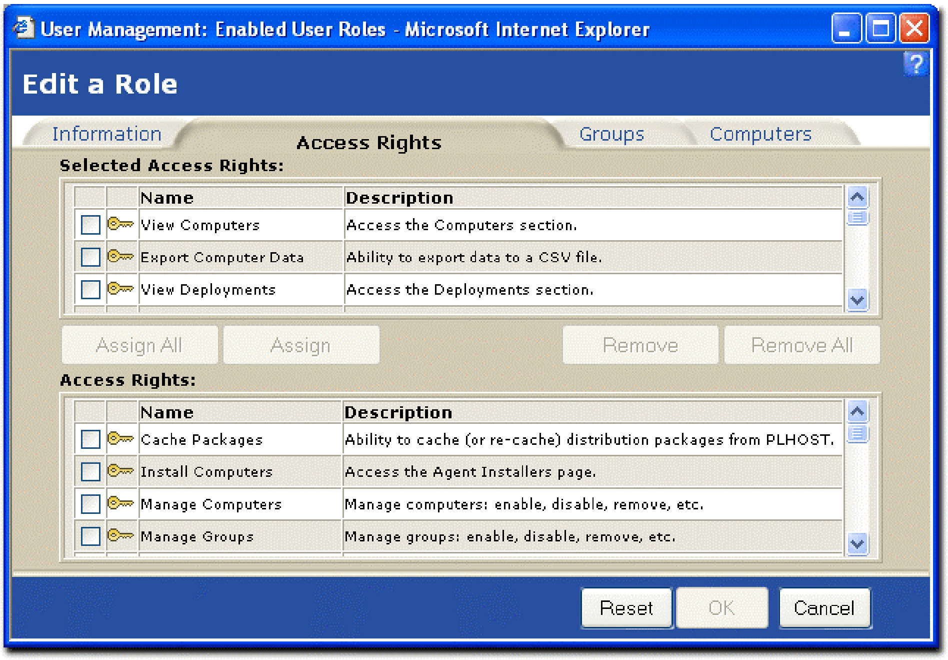
  Select this tab to specify the groups of computers that this role may access.
- Computers Tab

  Select this tab to specify individual computers that this role may access.

Select the Access Rights Tab to initialize the Access Rights screen and assign rights.

Access Rights

The Role Property screens allow the Patch Management Administrator to edit a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Access Rights** screen to specify the access rights to Patch Management Server functionalities assigned to this user role.



Selected Access Rights:

	Name	Description
□	View Computers	Access the Computers section.
□	Export Computer Data	Ability to export data to a CSV file.
□	View Deployments	Access the Deployments section.

Access Rights:

	Name	Description
□	Cache Packages	Ability to cache (or re-cache) distribution packages from PLHOST.
□	Install Computers	Access the Agent Installers page.
□	Manage Computers	Manage computers: enable, disable, remove, etc.
□	Manage Groups	Manage groups: enable, disable, remove, etc.

Access Rights Information

- Selected Access Rights

  Edit the list of access rights that have been assigned to this user role.

- Access Rights

  A list of all the access rights that can be assigned to a user role. Scroll through and click in the checkbox next to the desired right(s) to initialize and click the **Assign** button. The system populates the **Selected Access Rights** window with your selections. Use the **Assign All** button to populate the **Selected Access Rights** with ALL rights from the **Access Rights** window.

Screen Functions

- Assign All

  Click to assign all available access rights to the user role.

- Assign

  After selecting any number of the access rights listed in the "Access Rights" (lower) pane, click here to assign these rights to the user role.

- Remove

After selecting any number of the access rights listed in the "Selected Access Rights" (upper) pane, click here to remove these rights from the user role.

- Remove All

  Click to remove from the role all of the assigned access rights.
- Information Tab

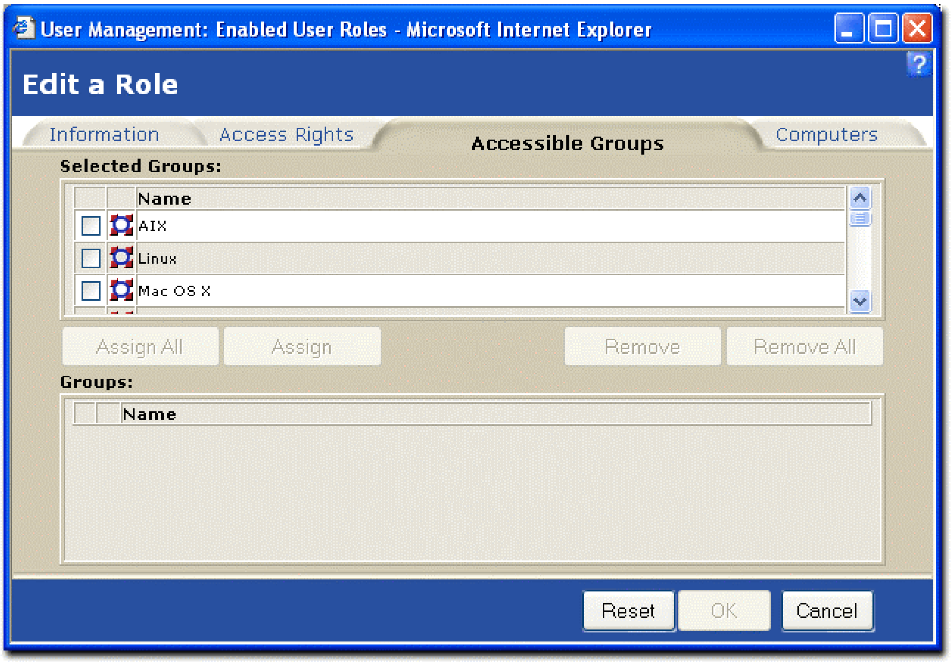
  Select this tab to specify this role's basic information.
- Groups Tab

  Select this tab to specify the groups of computers that this role may access.
- Computers Tab

  Select this tab to specify individual computers that this role may access.

Accessible Groups

The Role Property screens allow the Patch Management Administrator to edit a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Accessible Groups** screen to specify the groups of computers that this user role may access.



Selected Groups:

	Name
□	AIX
□	Linux
□	Mac OS X

Groups:

	Name

Accessible Groups Information

- Selected Groups

  A list of the groups of computers that have been assigned to this user role.
- Groups

  A list of all the groups of computers that can be assigned to this user role.

Scroll through and click in the checkbox next to the desired group(s) to initialize and click the **Assign** button. The system populates the **Selected Groups** window with your selections. Use the **Assign All** button to populate the **Selected Groups** with ALL groups from the **Groups** window.

Screen Functions

- Assign All

  Click to assign all available groups to the user role.
- Assign

  After selecting any number of the groups listed in the "Groups" (lower) pane, click here to assign these groups to the user role.
- Remove

  After selecting any number of the groups listed in the "Selected Groups" (upper) pane, click here to remove these groups from the user role.
- Remove All

  Click here to remove from the role all of the assigned groups.
- Information Tab

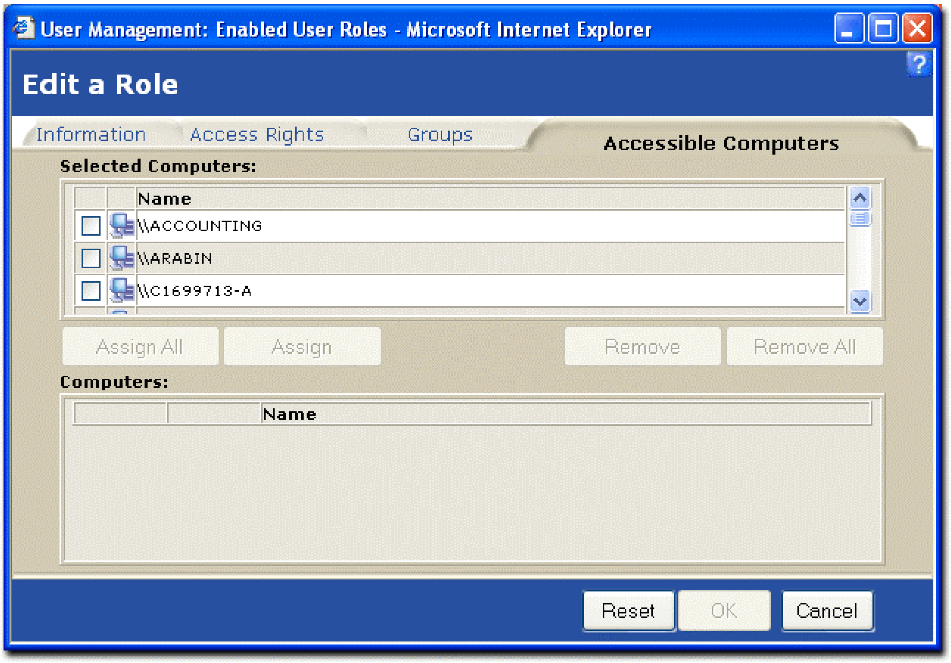
  Select this tab to specify this role's basic information.
- Access Rights Tab

  Select this tab to specify this role's access rights to Patch Management Server functionalities.
- Computers Tab

  Select this tab to specify individual computers that this role may access.

Accessible Computers

The Role Property screens allow the Patch Management Administrator to edit a user role. The role can be assigned access rights to various Patch Management Server functions, permission to access particular groups of computers, and permission to access individual computers. Use the **Accessible Computers** screen to specify the individual computers that this user role may access.



Selected Computers:

	Name
□	\\ACCOUNTING
□	\\ARABIN
□	\\C1699713-A

Computers:

	Name

Accessible Computers Information

- Selected Computers

  A list of all the computers that have been assigned to this user role.
- Computers

  A list of all the computers that can be assigned to this user role.

  Scroll through and click in the checkbox next to the desired computer(s) to initialize and click the **Assign** button. The system populates the **Selected Computers** window with your selections. Use the **Assign All** button to populate the **Selected Computers** with ALL computers from the **Computers** window.

Screen Functions

- Assign All

  Click to assign all available computers to the user role.
- Assign

  After selecting any number of the computers listed in the "Computers" (lower) pane, click here to assign these computers to the user role.
- Remove

  After selecting any number of the computers listed in the "Selected Computers" (upper) pane, click here to remove these computers from the user role.
- Remove All

  Click here to remove from the role all of the assigned computers.

- Information Tab

  Select this tab to specify this role's basic information.
- Access Rights Tab

  Select this tab to specify this role's access rights to Patch Management Server functionalities.
- Groups Tab

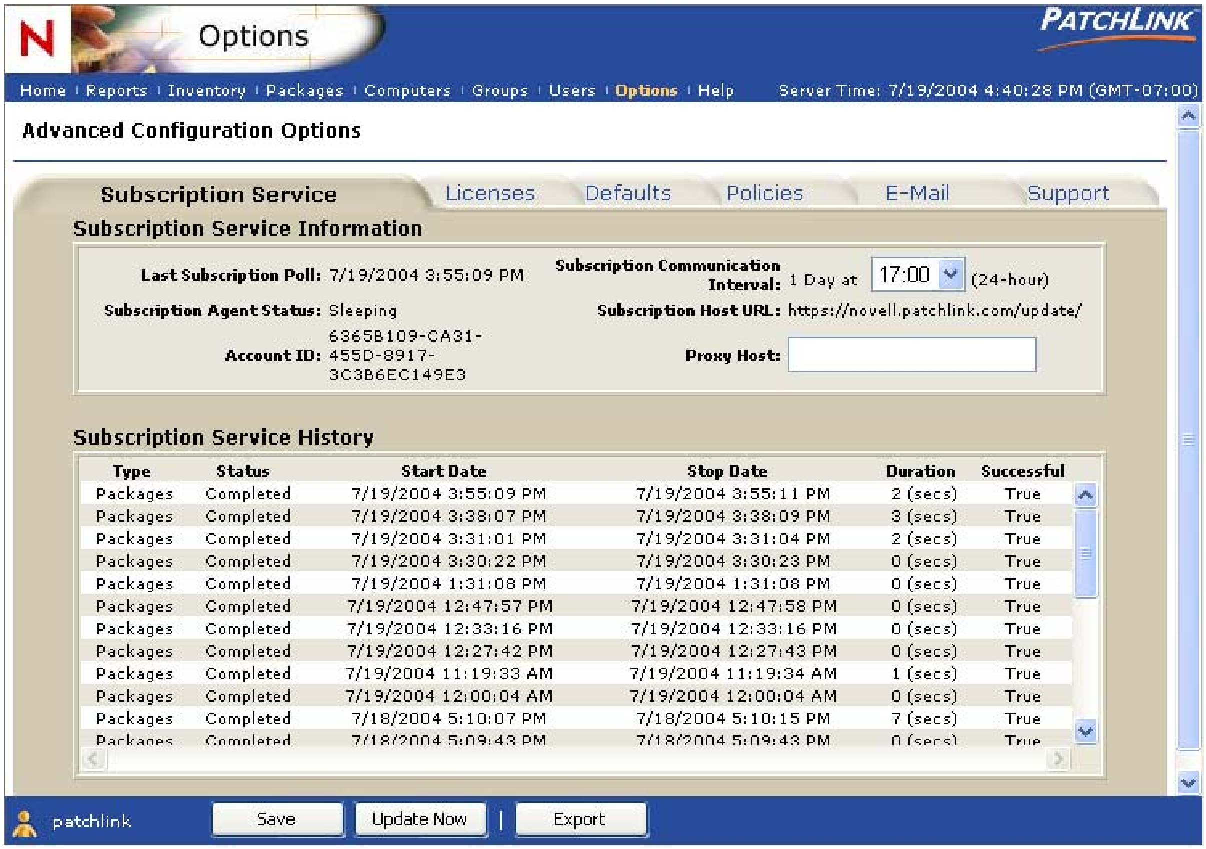
  Select this tab to specify the groups of computers that this role may access.

Upon closure of the Edit a Role Wizard, the homepage will be refreshed with the newly edited Role.

20. Options

Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |

The Advanced Configuration Options page displays six main option and configuration views on which the Patch Management Server relies on. They are: Subscription Service, Subscription Licenses, Patch Management Server Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.



Server Time: 7/19/2004 4:40:28 PM (GMT-07:00)

Advanced Configuration Options

Subscription Service Information

Last Subscription Poll: 7/19/2004 3:55:09 PM

Subscription Communication Interval: 1 Day at 17:00 (24-hour)

Subscription Agent Status: Sleeping

Subscription Host URL: https://novell.patchlink.com/update/

Account ID: 6365B109-CA31-455D-8917-3C3B6EC149E3

Proxy Host:

Subscription Service History

Type	Status	Start Date	Stop Date	Duration	Successful
Packages	Completed	7/19/2004 3:55:09 PM	7/19/2004 3:55:11 PM	2 (secs)	True
Packages	Completed	7/19/2004 3:38:07 PM	7/19/2004 3:38:09 PM	3 (secs)	True
Packages	Completed	7/19/2004 3:31:01 PM	7/19/2004 3:31:04 PM	2 (secs)	True
Packages	Completed	7/19/2004 3:30:22 PM	7/19/2004 3:30:23 PM	0 (secs)	True
Packages	Completed	7/19/2004 1:31:08 PM	7/19/2004 1:31:08 PM	0 (secs)	True
Packages	Completed	7/19/2004 12:47:57 PM	7/19/2004 12:47:58 PM	0 (secs)	True
Packages	Completed	7/19/2004 12:33:16 PM	7/19/2004 12:33:16 PM	0 (secs)	True
Packages	Completed	7/19/2004 12:27:42 PM	7/19/2004 12:27:43 PM	0 (secs)	True
Packages	Completed	7/19/2004 11:19:33 AM	7/19/2004 11:19:34 AM	1 (secs)	True
Packages	Completed	7/19/2004 12:00:04 AM	7/19/2004 12:00:04 AM	0 (secs)	True
Packages	Completed	7/18/2004 5:10:07 PM	7/18/2004 5:10:15 PM	7 (secs)	True
Packages	Completed	7/18/2004 5:09:43 PM	7/18/2004 5:09:43 PM	0 (secs)	True

Subscription Service Information

Subscription Service Information

- Last Subscription Poll

  The date and time of when the subscription agent last contacted the host site for new updates.
- Subscription Agent Status

  The current status of the subscription agent.td>
- Account ID

The identification number of your account with the host site. It is created when the Patch Management Server first registers itself with the host site.

- Subscription Communication Interval

  The amount of time (number of minutes, hours or days) the subscription agent will wait between contacting the host site. Select the desired time from the drop down menu and select the Save button on the Action Menu to validate the change.
- Subscription Host URL
- The URL (or web address) of the host site.
- Proxy Host
- The proxy host information the subscription agent uses, if it is going through a proxy. Enter the desired proxy information and select the Save button on the Action Menu to validate the change.

Subscription Service History

This is a history of the tasks the subscription agent has done or is doing. It tells:

- Type
- The *Type* of the agent task.
- Status
- The *Status* of an agent task.
- Start Date
- The *Start Date* is when the task started.
- Stop Date
- The *Stop Date* is when the task was completed.
- Duration
- The *Duration* is how long the task took.
- Successful

  Successful is whether or not the task completed successfully or ended in failure.

Page Functions

Licenses Tab

Licenses tab allows a User to display the Subscription Licenses tab of the Options section. This is where information on agent licenses are displayed.

Defaults Tab

Defaults tab allows a User to display the Patch Management Server Defaults tab of the Options section. This is where default settings for the Patch Management Server and default agent policies are located.

Policies Tab

Policies tab allows a User to display the Agent Policy Sets tab of the Options section. This is where agent policies can be grouped together in to a define policy set, which can be assigned to groups.

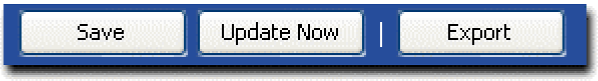
E-Mail Tab

E-Mail tab allows a User to display the E-Mail Notification tab of the Options section. This is where e-mail addresses are saved including what Patch Management Server notifications each entry will receive.

Support Tab

Support tab allows a User to display the Support Information tab of the Options section. This is where basic support information about the Patch Management Server is displayed.

Action Menu



Save

Allows the User the ability to save the changes to either the Subscription Communication Interval or Proxy Host.

Update Now

Allows the Patch Management Administrator the ability to initiate Replication to keep the Patch Management Server up to date with the latest Vulnerability Reports, Distribution Packages, and Subscription Licenses.

Export

Allows the User the ability to export the Subscription Data to a comma-separated value (CSV) file.

Subscription Service Security

The Subscription Service tab of the Options section requires the View Options: Subscription Access Right. If a user does not have the correct access, the display will automatically redirect the user over to an Options tab that they do have access to. If the user does not have access to any Options tabs, they will receive an access denied error message.

Save requires the Manage Options Security Access Right. If a user does not have the correct access, the button is disabled.

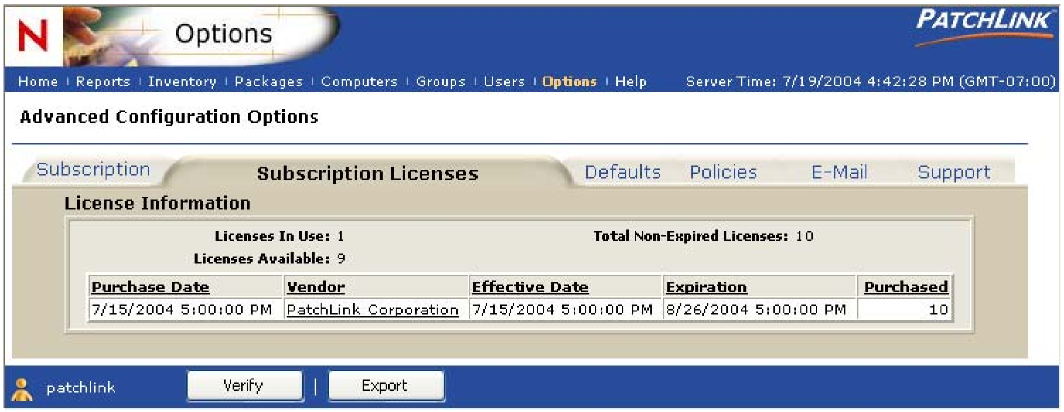
Update Now requires the Manage Options Security Access Right. If a user does not have the correct access, the button is disabled.

Export requires the Export Subscription Data Security Access Right. If a user does not have the correct access, the button is disabled.

Subscription Licenses

The Advanced Configuration Options page displays six main option and configuration views on which the Patch Management Server relies. They are: Subscription Service, Subscription

Licenses, Patch Management Server Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.



Server Time: 7/19/2004 4:42:28 PM (GMT-07:00)

Advanced Configuration Options

License Information

Licenses In Use: 1
Total Non-Expired Licenses: 10
Licenses Available: 9

Purchase Date	Vendor	Effective Date	Expiration	Purchased
7/15/2004 5:00:00 PM	PatchLink Corporation	7/15/2004 5:00:00 PM	8/26/2004 5:00:00 PM	10

License Information

- Licenses In Use

  The number of licenses the Patch Management Server has in use by registered agents.
- Licenses Available

  The total number of licenses that are left available.
- Total Non-Expired Licenses

  The total number of licenses the Patch Management Server that are not expired.

Each time you purchase a license, a license group entry is created that represents that purchase. The list of License Groups are displayed, and for each License Group is shown:

- Purchase Date

  The date the license group was purchased.
- Vendor

  Tells who the license group was purchased from. The name is also a web link, so by clicking on it, you will be taken to their homepage.
- Effective Date

  The date the license group becomes effective.
- Expiration

  The date the license group expires.
- Purchased

  The amount of licenses purchased.

Page Functions

Subscription Tab

Subscriptions tab allows a User to display the Patch Management Server Subscription information. This is where the Subscription Communication Interval and the Proxy host information can be entered and saved.

Defaults Tab

Defaults tab allows a User to display the Patch Management Server Defaults tab of the Options section. This is where default settings for the Patch Management Server and default agent policies are located.

Policies Tab

Policies tab allows a User to display the Agent Policy Sets tab of the Options section. This is where agent policies can be grouped together in to a define policy set, which can be assigned to groups.

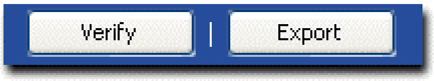
E-Mail Tab

E-Mail tab allows a User to display the E-Mail Notification tab of the Options section. This is where e-mail addresses are saved including what Patch Management Server notifications each entry will receive.

Support Tab

Support tab allows a User to display the Support Information tab of the Options section. This is where basic support information for the Patch Management Server is displayed.

Action Menu



Verify

Allows the Patch Management Administrator the ability to initiate License Replication to keep the Patch Management Server up to date with the latest Subscription Licenses.

Export

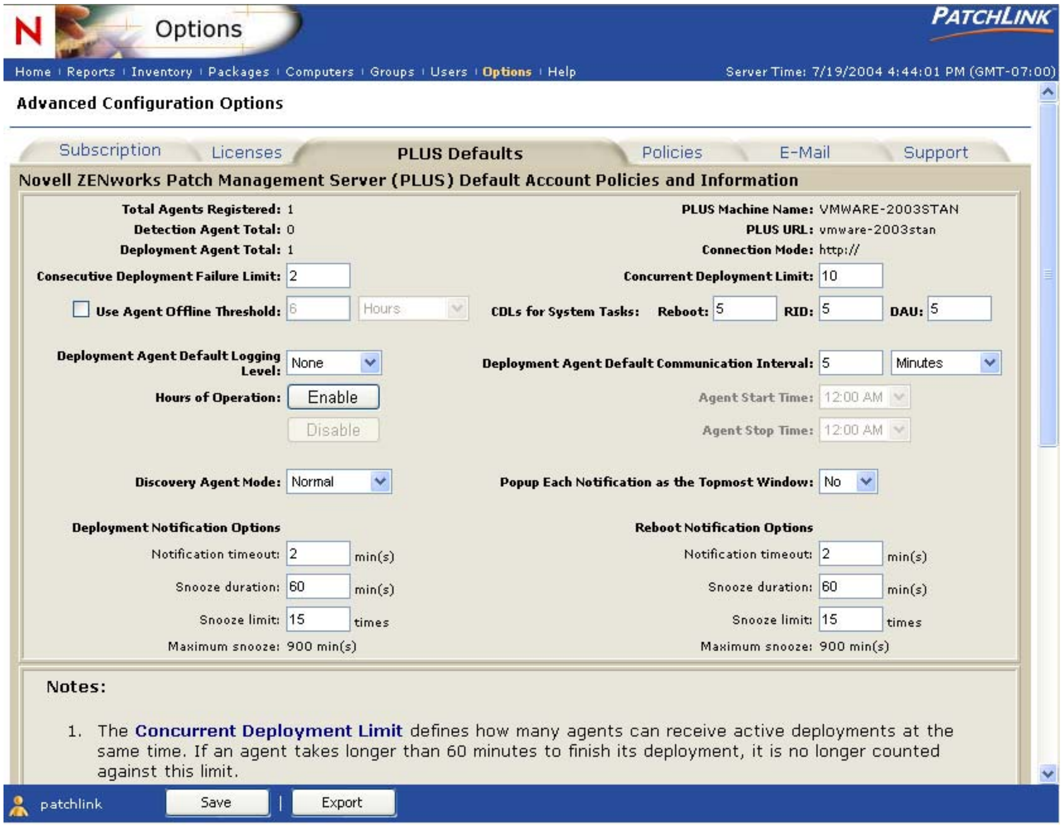
Allows the User the ability to export the License Data to a comma-separated value (CSV) file.

Subscription License Security

The License tab of the Options section requires the View Options: Licenses Security Access Right. If a user does not have the correct access, hyperlink is disabled.
Export requires the Export Subscription Data Security Access Right. If a user does not have the correct access, the button is disabled.

Patch Management Server Defaults

The Advanced Configuration Options page displays six main option and configuration views on which the Patch Management Server relies. These are Subscription Service, Subscription Licenses, Patch Management Server Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.


Options
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Server Time: 7/19/2004 4:44:01 PM (GMT-07:00)
Subscription
Licenses
PLUS Defaults
Policies
E-Mail
Support
Enable
Disable
patchlink
Save
Export

Advanced Configuration Options

Novell ZENworks Patch Management Server (PLUS) Default Account Policies and Information

Total Agents Registered: 1
Detection Agent Total: 0
Deployment Agent Total: 1
Consecutive Deployment Failure Limit: 2
□ Use Agent Offline Threshold: 6 Hours
Deployment Agent Default Logging Level: None
Hours of Operation:
Discovery Agent Mode: Normal

PLUS Machine Name: VMWARE-2003STAN
PLUS URL: vmware-2003stan
Connection Mode: http://
Concurrent Deployment Limit: 10
CDLs for System Tasks: Reboot: 5 RID: 5 DAU: 5
Deployment Agent Default Communication Interval: 5 Minutes
Agent Start Time: 12:00 AM
Agent Stop Time: 12:00 AM
Popup Each Notification as the Topmost Window: No

Deployment Notification Options
Notification timeout: 2 min(s)
Snooze duration: 60 min(s)
Snooze limit: 15 times
Maximum snooze: 900 min(s)

Reboot Notification Options
Notification timeout: 2 min(s)
Snooze duration: 60 min(s)
Snooze limit: 15 times
Maximum snooze: 900 min(s)

Notes:

1. The **Concurrent Deployment Limit** defines how many agents can receive active deployments at the same time. If an agent takes longer than 60 minutes to finish its deployment, it is no longer counted against this limit.

Patch Management Server Default Account Policies and Information

- Total Agents Registered

  The total number of agents registered to the Patch Management Server Detection.
- Detection Agent Total

  The total number of detection agents registered to the Patch Management Server.
- Deployment Agent Total

  The total number of deployment agents registered to the Patch Management Server.
- Patch Management Server Machine Name

  The name of the computer on which the Patch Management Server is installed.
- Patch Management Server URL

  The URL of the Patch Management Server.
- Connection Mode

  The connection mode in which the Patch Management Server is acting. It is either *HTTP://* which is insecure mode, or *HTTPS://*, which is secure mode.

- Concurrent Deployment Limit

  The *concurrent deployment limit* defines how many agents can receive active deployments at the same time. If an agent takes longer than 60 minutes to finish its deployment, it is no longer counted against this limit. The purpose of this limit is to throttle the number of deployments given to agents across the entire Patch Management Server.
  An example of this is the case of multiple deployments being created to run at the same time. Though each may have its own sequential limit of how many agents may perform the deployment at any one time, all of the deployments are running at the same time and this may cause the performance of the server to decrease.
- Deployment Agent Default Logging Level

  The level at which the agent is logging messages about its actions. The various levels are: None, Basic Information, Detailed, Debug.
- Deployment Agent Default Communication Interval

  The amount of time (number of minutes, hours or days) is the length of time the client agent will wait between contacting the Patch Management Server.
- Hours of Operation
  Clicking on the Enable button will enable the *Agent Timer.* Start and Stop times can be assigned for the agent to poll the Patch Management Server.

  Clicking on the disable button will disable the *Agent Timer.* The agent will no longer have a start and a stop time. It will start communicating with the Patch Management Server as soon as it is assigned this policy and will continue till the policy or the agent is removed.
- Agent Stop Time
  The time at which the agent will stop contacting the Patch Management Server.
- Agent Start Time
  The time at which the agent will start contacting the Patch Management Server.

Page Functions

Subscription Tab

Allows a User to display the Subscription Service tab of the Options section. This is where information on Service Replication (Reports, Packages, and Licenses) are displayed.

Licenses Tab

Allows a User to display the Subscription Licenses tab of the Options section. This is where information on agent licenses are displayed.

Policies Tab

Allows a User to display the Agent Policy Sets tab of the Options section. This is where agent policies can be grouped together in to a define policy set, which can be assigned to groups.

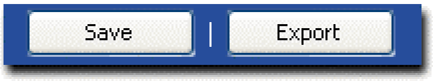
E-Mail Tab

Allows a User to display the E-Mail Notification tab of the Options section. This is where e-mail addresses are saved including what Patch Management Server notifications each entry will receive.

Support Tab

Allows a User to display the Support Information tab of the Options section. This is where basic support information about the Patch Management Server is displayed.

Action Menu



Save

Allows the Patch Management Administrator the ability to save License Replication the changes to the Patch Management Server and Agent Defaults.

Export

Allows the User the ability to export the License Data to a comma-separated value (CSV) file.

Patch Management Server Defaults Security

The Defaults tab of the Options section requires the View Options:Defaults Security Access Right. If a user does not have the correct access, hyperlink is disabled.

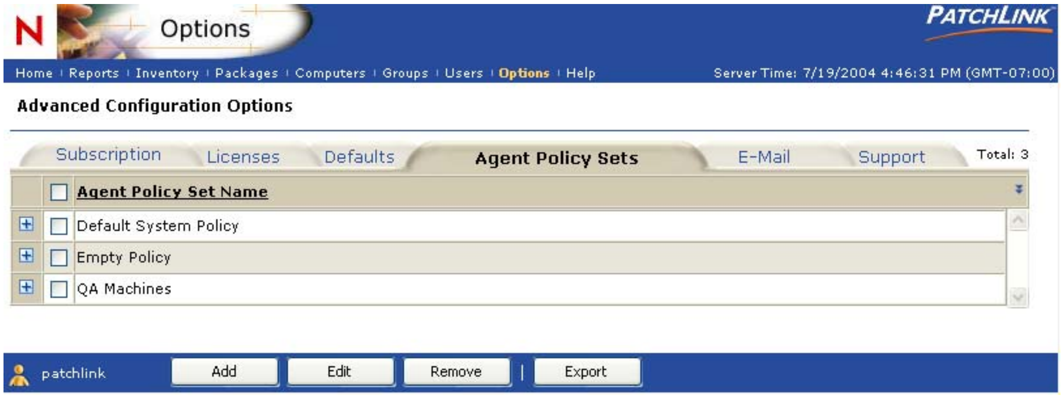
Save requires the Manage Options Security Access Right. If a user does not have the correct access, the button is disabled.

Export requires the Export Subscription Data Security Access Right. If a user does not have the correct access, the button is disabled.

Agent Policy Sets

The Advanced Configuration Options page displays six main option and configuration views on which Patch Management Server relies. They are: Subscription Service, Subscription Licenses, Patch Management Server Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.

A set of constraints that govern the agent features of communication interval, logging level, and the agent start and stop times. An agent policy is associated with a group and is applied to all the members of that group. For every newly created group, the system creates a default agent policy. Click the ⊞ to view additional information and statistics about the policy.



Server Time: 7/19/2004 4:46:31 PM (GMT-07:00)

Advanced Configuration Options

Total: 3

□ Agent Policy Set Name
□ Default System Policy
□ Empty Policy
□ QA Machines

Agent Policy Set Name

- Policy Name

  The name of the policy. There are two types of policies: System and User
- Policy Type

  This indicates whether the policy was created by a user or by the system
- Trace Level

  The logging level that is chosen at the time of Policy generation.
- Operation Start Time

  The time at which the agent will start communicating with the Patch Management Server.
- Operation Stop Time

  The time at which the agent will stop communicating with the Patch Management Server.
- Description

  The description that is entered at the time of Policy generation.

- Created On

  The date and time the policy was created
- Created By

  The user who created the policy
- Last Modified On

  The date and time the policy was last modified
- Last Modified By

  The user who last modified the policy
- Communication Interval

  The amount of time (number of minutes, hours or days)the client agent will wait between contacting the Patch Management Server.

Page Functions

Display and Hide

Click the ⊞ to display additional information and statistics about the represented item. Click the ⊟ to hide this information from view. The information is refreshed each time it is displayed. The information expansion functionality (⊟,⊞) is only available for Microsoft Internet Explorer at this time.

Sort ⇊

The sort function enables views by Ascending (default) or Descending order by clicking on a sort enabled column heading or the sort icon.

Mouse Overs

Additional information may be displayed by hovering your mouse pointer over an enabled icon or link.

Subscription Tab

Allows a User to display the Subscription Service tab of the Options section. This is where information on Service Replication (Reports, Packages, and Licenses) are displayed.

Licenses Tab

Allows a User to display the Subscription Licenses tab of the Options section. This is where information on agent licenses are displayed.

Defaults Tab

Allows a User to display the Patch Management Server Defaults tab of the Options section. This is where default settings for the Server and default agent policies are located.

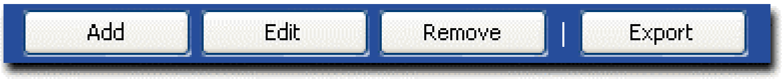
E-Mail Tab

Allows a User to display the E-Mail Notification tab of the Options section. This is where e-mail addresses are saved including which Patch Management Server notifications each entry will receive.

Support Tab

Allows a User to display the Support Information tab of the Options section. This is where basic support information for the Patch Management Server is displayed.

Action Menu



Add

Allows the Patch Management Administrator the ability to create a new Agent Policy Set using the Agent Policy Set Property Page. See Section 22; Add a Policy Wizard for more information.

Edit

Allows the Patch Management Administrator the ability to edit a selected Agent Policy Set using the Agent Policy Set Property Page. See Section 23; Edit a Policy Wizard for more information.

Remove

Allows the Patch Management Administrator the ability to delete a selected Agent Policy Set.

Export

Allows the User the ability to export the Subscription Data to a comma-separated value (CSV) file.

Agent Policy Sets Security

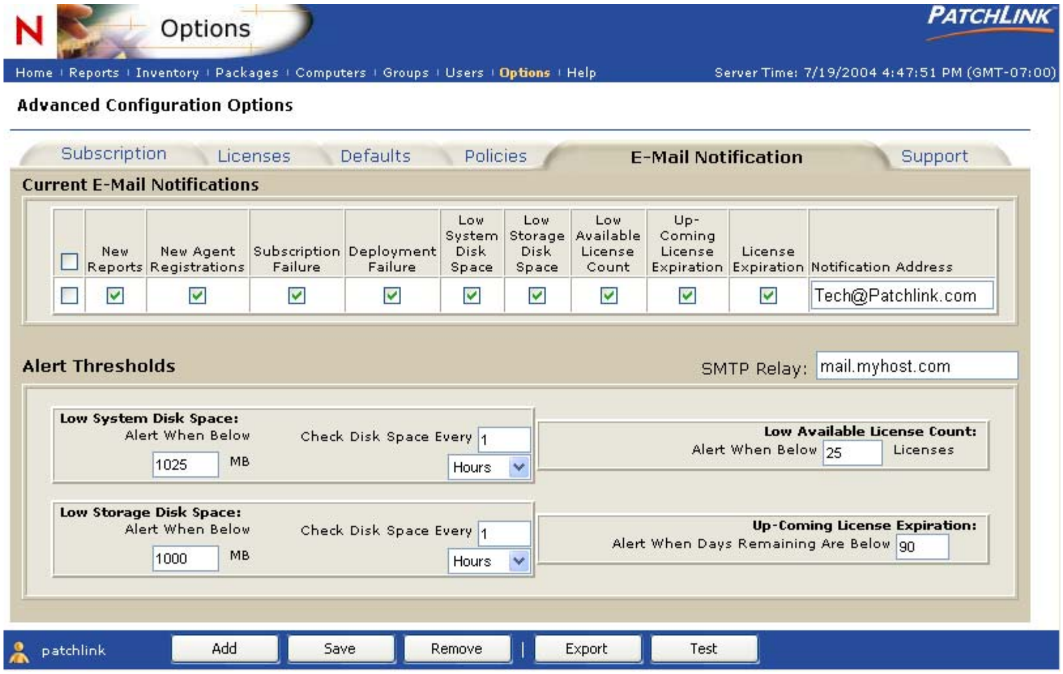
The Policies tab of the Options section requires the View Options: Policies Security Access Right. If a user does not have the correct access, hyperlink is disabled.

Export requires the Export Subscription Data Security Access Right. If a user does not have the correct access, the button is disabled.

Advanced E-Mail Notifications

The Advanced Configuration Options page displays six main option and configuration views on which Patch Management Server relies. They are: Subscription Service, Subscription Licenses, Patch Management Server Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.

Set up the Patch Management Server to alert you via email when certain thresholds are reached.


Options
PATCHLINK
Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help
Server Time: 7/19/2004 4:47:51 PM (GMT-07:00)
Subscription
Licenses
Defaults
Policies
E-Mail Notification
Support
patchlink
Add
Save
Remove
Export
Test

Advanced Configuration Options

Current E-Mail Notifications

☐	New Reports	New Agent Registrations	Subscription Failure	Deployment Failure	Low System Disk Space	Low Storage Disk Space	Low Available License Count	Up-Coming License Expiration	License Expiration	Notification Address
☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	Tech@Patchlink.com

Alert Thresholds

SMTP Relay: mail.myhost.com

Low System Disk Space:
Alert When Below 1025 MB
Check Disk Space Every 1 Hours

Low Storage Disk Space:
Alert When Below 1000 MB
Check Disk Space Every 1 Hours

Low Available License Count:
Alert When Below 25 Licenses

Up-Coming License Expiration:
Alert When Days Remaining Are Below 90

Current E-Mail Notifications

- New Reports

  By selecting this notification, you will be sent an e-mail notification each time new reports are downloaded via the subscription agent from the host site.

- New Agent Registrations

  By selecting this notification, you will be sent an e-mail notification each time a new agent registers up to the Patch Management Server.

- Subscription Failure

  By selecting this notification, you will be sent an e-mail notification each time the subscription agent task fails.

- Deployment Failure

  By selecting this notification, you will be sent an e-mail notification each time a client agent fails at deploying a package.

- License Expiration

  By selecting this notification, you will be sent an e-mail notification whenever a license group expires.

- Notification Address

  The e-mail addresses that will be notified when any of the following events occur.

Alert Thresholds

- Low System Disk Space

  By selecting this notification, you will be sent an e-mail notification whenever the disk space on the system volume goes under this value (in megabytes). Besides an input field to be able to change this value (under the Alert Thresholds section) there is another field which is the Check Disk Space Interval. This value is the amount of time (number of minutes, hours or days) that the Patch Management Server will wait between checking the system disk space.

- Low Storage Disk Space

  By selecting this notification, you will be sent an e-mail notification whenever the disk space on the storage volume goes under this value (in megabytes). Besides an input field to be able to change this value (under the Alert Thresholds section) there is another field which is the Check Disk Space Interval. This value is the amount of time (number of minutes, hours or days) that the Patch Management Server will wait between checking the storage disk space.

- Low Available License Count

  By selecting this notification, you will be sent an e-mail notification whenever the license count gets below this value. This value can be changed by changing it in the Alert Thresholds section.

- Up-Coming License Expiration

  By selecting this notification, you will be sent an e-mail notification whenever a license group is about to expire within this value (in Days). This value can be changed by changing it in the Alert Threshold section.

Page Functions

Subscription Tab

Allows a User to display the Subscription Service tab of the Options section. This is where information on Service Replication (Reports, Packages, and Licenses) are displayed.

Licenses Tab

Allows a User to display the Subscription Licenses tab of the Options section. This is where information on agent licenses are displayed.

Defaults Tab

Allows a User to display the Patch Management Server Defaults tab of the Options section. This is where default settings for the Patch Management Server and default agent policies are located.

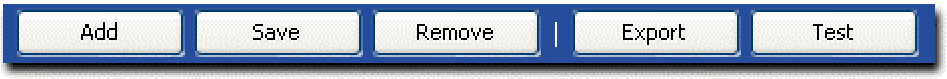
Policies Tab

Allows a User to display the Agent Policy Sets tab of the Options section. This is where agent policies can be grouped together in to a define policy set, which can be assigned to groups.

Support Tab

Allows a User to display the Support Information tab of the Options section. This is where basic support information for the Patch Management Server is displayed.

Action Menu



Add

Allows the Patch Management Administrator the ability to add a new e-mail notification entry.

Save

Allows the Patch Management Administrator the ability to save the e-mail notification changes as well as the changes notification alert thresholds.

Remove

Allows the Patch Management Administrator the ability to remove selected e-mail notification entries.

Export

Allows the User the ability to export the Subscription Data to a comma-separated value (CSV) file.

Test

Allows the Patch Management Administrator the ability to send a e-mail to a selected e-mail address to verify that e-mails are getting through.

Advanced E-mail Notifications Security

The E-Mail tab of the Options section requires the View Options: E-Mail Security Access Right. If a user does not have the correct access, hyperlink is disabled.

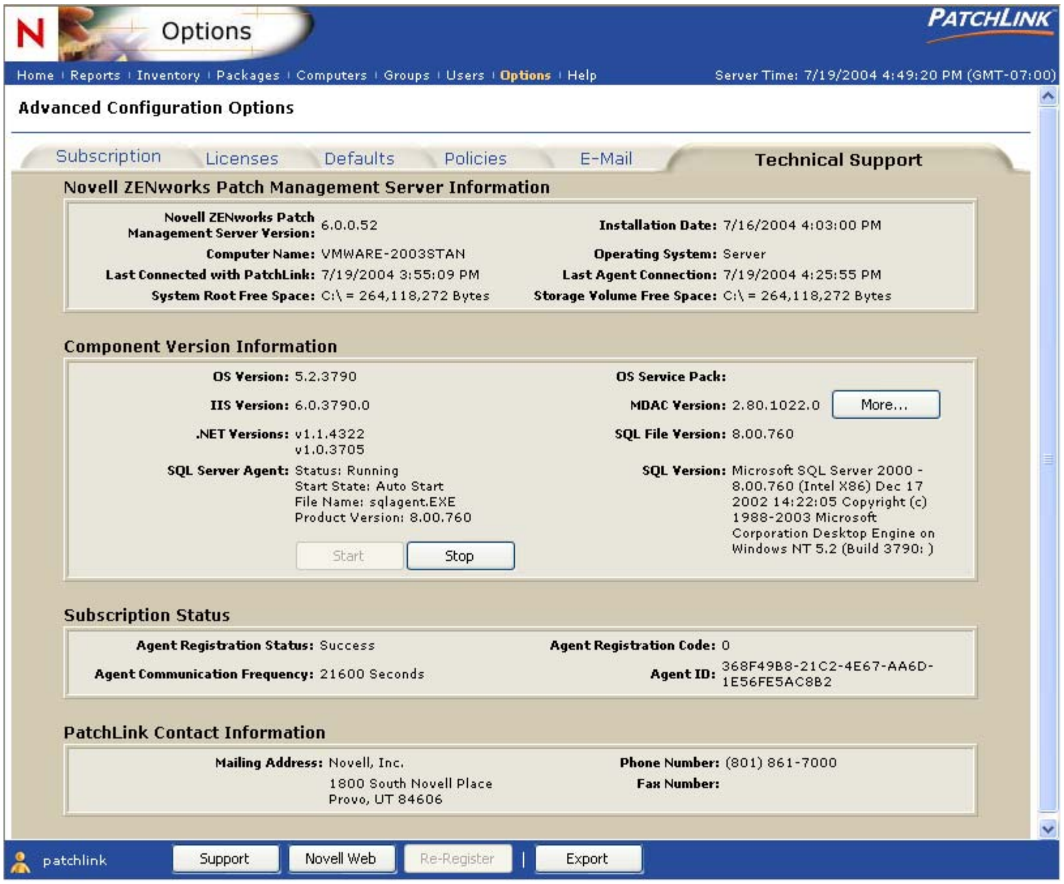
Save requires the Manage Options Security Access Right. If a user does not have the correct access, the button is disabled.

Export requires the Export Subscription Data Security Access Right. If a user does not have the correct access, the button is disabled.

Technical Support

The Advanced Configuration Options page displays six main option and configuration views on which the Patch Management Server relies. They are: Subscription Service, Subscription Licenses, Patch Management Server Defaults, Agent Policy Sets, E-Mail Notifications, and Support Information.

View Technical Information about the Patch Management Server



Server Time: 7/19/2004 4:49:20 PM (GMT-07:00)

Advanced Configuration Options

Novell ZENworks Patch Management Server Information

Novell ZENworks Patch Management Server Version:	6.0.0.52	Installation Date:	7/16/2004 4:03:00 PM
Computer Name:	VMWARE-2003STAN	Operating System:	Server
Last Connected with PatchLink:	7/19/2004 3:55:09 PM	Last Agent Connection:	7/19/2004 4:25:55 PM
System Root Free Space:	C:\ = 264,118,272 Bytes	Storage Volume Free Space:	C:\ = 264,118,272 Bytes

Component Version Information

OS Version:	5.2.3790	OS Service Pack:	
IIS Version:	6.0.3790.0	MDAC Version:	2.80.1022.0
.NET Versions:	v1.1.4322 v1.0.3705	SQL File Version:	8.00.760
SQL Server Agent:	Status: Running Start State: Auto Start File Name: sqlagent.EXE Product Version: 8.00.760	SQL Version:	Microsoft SQL Server 2000 - 8.00.760 (Intel X86) Dec 17 2002 14:22:05 Copyright (c) 1988-2003 Microsoft Corporation Desktop Engine on Windows NT 5.2 (Build 3790:)

Subscription Status

Agent Registration Status:	Success	Agent Registration Code:	0
Agent Communication Frequency:	21600 Seconds	Agent ID:	368F49B8-21C2-4E67-AA6D-1E56FE5AC8B2

PatchLink Contact Information

Mailing Address:	Novell, Inc. 1800 South Novell Place Provo, UT 84606	Phone Number:	(801) 861-7000
		Fax Number:	

Patch Management Server Information

- Novell® ZENworks® Patch Management Server Version

  The version number of the Patch Management Server.
- Computer Name

  The name of the computer on which the Patch Management Server was installed.
- Last Connected with PatchLink

  The last date and time that the subscription agent connected up with the host site.
- System Root Free Space

The amount of free disk space for the system volume.

- Installation Date

  The date Patch Management Server was installed.

- Operating System

  The operating system that Patch Management Server is running on.

- Last Agent Connection

  The last date and time any agent has connected up with the Patch Management Server.

- Storage Volume Free Space

  The amount of free disk space for the storage volume.

Component Version Information

- OS Version

  The extra operating system information.

- IIS Version

  The version number of the IIS web server.

- .NET Version

  The version number of the .NET Framework(s) installed on the server

- SQL Server Agent: Clicking the Start / Stop button will start or stop the SQL Server Agent.

  Displays the following:
  - The current status
  - The start up state
  - SQL Agent Filename
  - Product Version number
  - File Version number

- OS Service Pack

  The service pack information about the operating system.

- MDAC Version

  The version number of MDAC. Click on the MDAC to view all of the MDAC component version numbers.

- SQL File Version

  The version number of the SQL Server File: SQLServer.exe.

- SQL Version

  The SQL Server version information.

Subscription Status

- Agent Registration Status

  The status of the registration process for the subscription agent against the host site.

- Agent Registration Code

  The status code number for the registration status message.

- Agent Communication Frequency

  The amount of time (number of minutes, hours or days) is the length of time the subscription agent will wait between contacting the host site.

- Agent ID

  The ID number given to the subscription agent upon registration by the host site.

Novell® Contact Information

- Mailing Address
- Phone Number
- Fax Number

Page Functions

Subscription Tab

Allows a User to display the Subscription Service tab of the Options section. This is where information on Service Replication (Reports, Packages, and Licenses) are displayed.

Licenses Tab

Allows a User to display the Subscription Licenses tab of the Options section. This is where information on agent licenses are displayed.

Defaults Tab

Allows a User to display the Patch Management Server Defaults tab of the Options section. This is where default settings for the Patch Management Server and default agent policies are located.

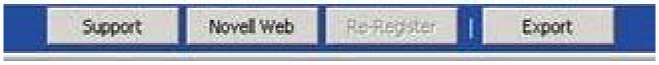
Policies Tab

Allows a User to display the Agent Policy Sets tab of the Options section. This is where agent policies can be grouped together in to a define policy set, which can be assigned to groups.

E-Mail Tab

Allows a User to display the E-Mail Notification tab of the Options section. This is where e-mail addresses are saved including which Patch Management Server notifications each entry will receive.

Action Menu



Support

Provides Novell® Support contact information.

Novell Web

Allows the User to instantly bring up the Novell Support Web site.

Re-Register

Allows the Patch Management Administrator the ability to initiate the process to register (or re-register) the Patch Management Server Subscription Agent against the Subscription Host Server. This button is only available when the Subscription Agent has not successfully registered against the Subscription Host Server.

Export

Allows the User the ability to export the Subscription Data to a comma-separated value (CSV) file.

Technical Support Security

The Support tab of the Options section requires the View Options: Support Info Security Access Right. If a user does not have the correct access, hyperlink is disabled.

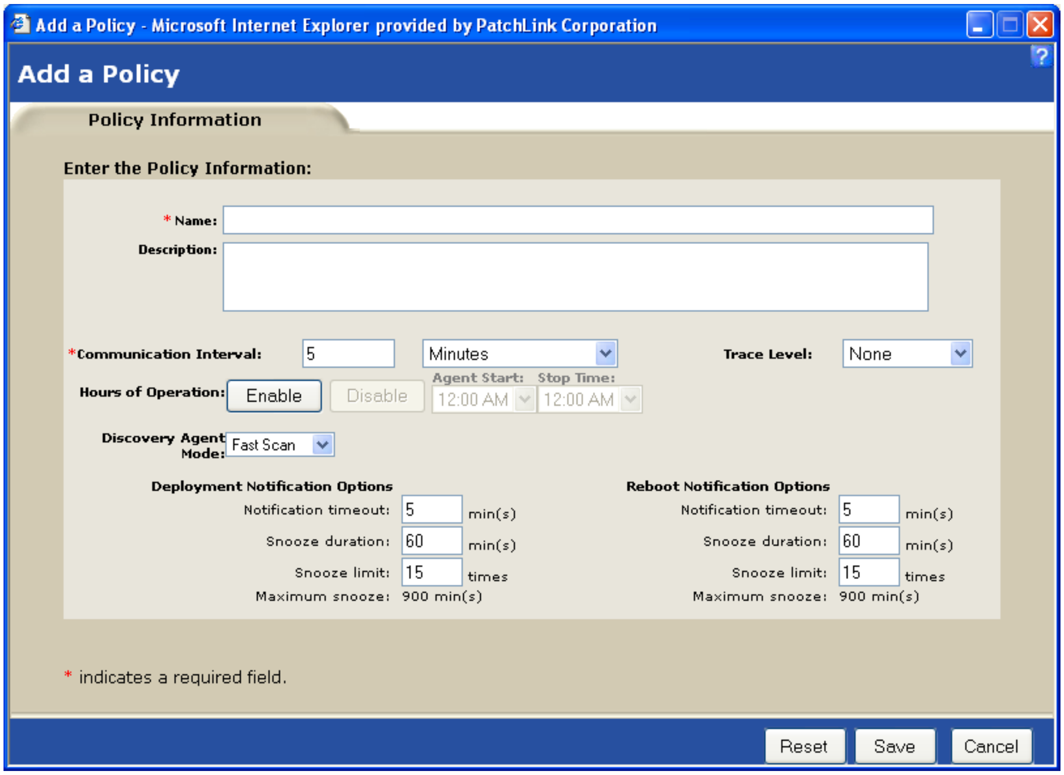
Export requires the Export Subscription Data Security Access Right. If a user does not have the correct access, the button is disabled.

21. Add a Policy Wizard

This wizard allows you to create and add a policy to the Patch Management Server. You can specify the policy attributes by entering data in the fields of the wizard.

Go to the **Options** homepage and select the **Agent Policy Sets** tab. Click on the **Add** button to add a on the Action Menu. This will initialize the **Add a Policy** Wizard.

Policy Information


Add a Policy - Microsoft Internet Explorer provided by PatchLink Corporation
Add a Policy
Policy Information
Reset
Save
Cancel

Enter the Policy Information:

* Name:

Description:

*Communication Interval: 5 Minutes

Trace Level: None

Hours of Operation: Enable Disable Agent Start: 12:00 AM Stop Time: 12:00 AM

Discovery Agent Mode: Fast Scan

Deployment Notification Options

Notification timeout: 5 min(s)

Snooze duration: 60 min(s)

Snooze limit: 15 times

Maximum snooze: 900 min(s)

Reboot Notification Options

Notification timeout: 5 min(s)

Snooze duration: 60 min(s)

Snooze limit: 15 times

Maximum snooze: 900 min(s)

* indicates a required field.

Name

Input a Name for your Policy (required)

Description

Add a Description of your Policy (optional)

- Enter in the desired Communication interval: The amount of time (number of minutes, hours or days) is the length of time the client agent will wait between contacting the Patch Management Server.
- Enter in the desired Logging Level: The level at which the agent is logging messages about its actions. The various levels are:

  - None
  - Basic Information
  - Detailed

- Debug

Hours of Operation

Clicking on the Enable button will enable the Agent Timer. Start and Stop times can be assigned for the agent to poll the Patch Management Server.

Clicking on the   button will disable the Agent Timer. The agent will no longer have a start and a stop time. It will start communicating with the Patch Management Server as soon as it is assigned this policy and will continue till the policy or the agent is removed.

Agent Stop Time: The time at which the agent will stop contacting the Patch Management Server.

Agent Start Time: The time at which the agent will start contacting the Patch Management Server.

Page Functions

Save

Saves the field values that you manually entered

Cancel

Exits the wizard and does not save any changes to the field values.

Reset

Resets the field values to their original state

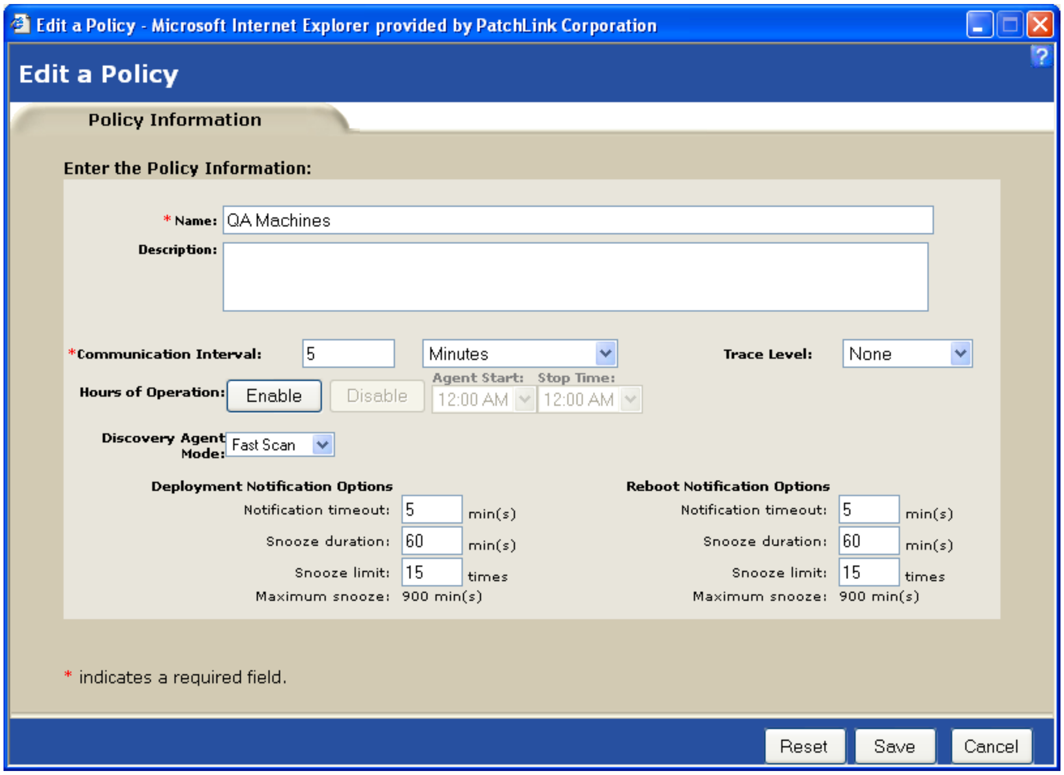
Upon refreshing the Options homepage, the Policy will is added and appears under the Agent Policy Set Name

22. Edit a Policy Wizard

This wizard allows you to change the attributes of an existing policy set. You can edit and specify the policy attributes by entering data in the fields of the wizard.

Go to the **Options** homepage, select the **Agent Policy Sets** tab, and select the policy that you wish to edit by clicking in the checkbox next to that specific policy. Click on the Edit button on the Action Menu. This will initialize the **Edit a Policy** Wizard.

Policy Information



Edit a Policy - Microsoft Internet Explorer provided by PatchLink Corporation

Edit a Policy

Policy Information

Enter the Policy Information:

* Name: QA Machines

Description:

*Communication Interval: 5 Minutes

Trace Level: None

Hours of Operation: Enable Disable

Agent Start: 12:00 AM Stop Time: 12:00 AM

Discovery Agent Mode: Fast Scan

Deployment Notification Options

Notification timeout: 5 min(s)

Snooze duration: 60 min(s)

Snooze limit: 15 times

Maximum snooze: 900 min(s)

Reboot Notification Options

Notification timeout: 5 min(s)

Snooze duration: 60 min(s)

Snooze limit: 15 times

Maximum snooze: 900 min(s)

* indicates a required field.

Name

Edit the Name for your Policy

Description

Edit the Description of your Policy

- Enter in the desired Communication interval: The amount of time (number of minutes, hours or days) is the length of time the client agent will wait between contacting the Patch Management Server.
- Enter in the desired Logging Level: The level at which the agent is logging messages about its actions. The various levels are:

  - None
  - Basic Information
  - Detailed

- Debug

Hours of Operation

Clicking on the Enable button will enable the Agent Timer. Start and Stop times can be assigned for the agent to poll the Patch Management Server.

Clicking on the   button will disable the Agent Timer. The agent will no longer have a start and a stop time. It will start communicating with the Patch Management Server as soon as it is assigned this policy and will continue till the policy or the agent is removed.

Agent Stop Time: The time at which the agent will stop contacting the Patch Management Server.

Agent Start Time: The time at which the agent will start contacting the Patch Management Server.

Page Functions

Save

Saves the field values that you manually entered.

Cancel

Exits the wizard and does not save any changes to the field values.

Reset

Resets the field values to their original state.

Upon refreshing the Options homepage, the edited Policy will is added and appears under the Agent Policy Set Name.

23. Hardening the Patch Management Server

Steps that can be taken to harden a Patch Management Server

There are a few steps that can be taken to harden a Patch Management Server that is to be put on the public Internet. You can opt to implement some or all of these suggestions, and these are of course just guidelines:

INSTALL YOUR SERVER WITH SSL:

Purchase a valid certificate from Verisign, Entrust, Thawte etc for your IIS web server, and use it with the Patch Management Server. This process just involves installing your .CER certificate file before rebooting after the main filecopy phase of the installation. The advantage is that with an SSL certificate installed, all agent communication and all administration is now fully encrypted - and so there is no way to spoof or snoop communications on the wire.

TURN OFF NON-CRITICAL SERVICES:

Microsoft Windows2000 ships with all the features turned on. There are a number of services you may wish to turn off (eg: RPC, Remote Registry, etc) to reduce the risk of hacker attacks. This type of lockdown is not encouraged - we would suggest using port blocking or a firewall instead – however, if you are careful this can be an effective approach.

The following are *required* services to run ZENworks® Patch Management:

- wwwpublishing
- IIS Admin Service
- Mssqlserver
- Sqlserver agent
- PatchLink Update

REMOVE YOUR SERVER FROM THE DOMAIN:

You probably don't have your machine in a corporate domain if it is out on the Internet! For safety’s sake you should have as few people being able to login to the server as possible - just use local accounts.

USE SECURE PASSWORDS:

Worm attacks frequently try to log in with weak / commonly used passwords (letmein, no password, etc) so please don't use them. For an Internet secure password we would recommend DOD standard 12 characters with alpha, numeric, punctuation and mixed case characters all being represented in your password.

TURN OFF WINDOWS NETWORKING:

Click on My Network Places, Select "Properties" from its popup menu, Choose the "Local Area Connection", Select "Properties" from its popup menu. This will show you the "Local Area Connection Properties" ... the properties of your main network card (there may be multiple network cards in your server). Go ahead and select "File and Printer Sharing for Microsoft Networks" and push the "Uninstall" button to remove MS file & print network service. NOTE: do NOT uninstall the "Client for Microsoft Networks" as it is required by MS

SQL Server and MS Internet Information Server.

LOCK OFF ALL BUT THE REQUIRED TCP/IP PORTS:

Within "Local Area Connection Properties" window, select "Internet Protocol

TCP/IP" and push the "Properties" button. On the Properties dialog, push the "Advanced..." button, then click the "Options" tab, select "TCP/IP filtering" and push the "Properties" button. You are now able to set specific port filters for your computer, so that you can 'firewall' off all but the ports that you need:

=> Check the "Enable TCP/IP Filtering" checkbox
=> Select the "Permit Only" TCP Ports button
- Add port number 443
- Add port number 80 (not needed if you followed step 1)
- No other ports are required, though you may want to allow DNS out, maybe TS or VNC
=> Select the "Permit Only" UDP Ports button
- No UDP ports are required, leave this section blank

Once you save these settings and reboot your server, your machine will now be fully isolated from TCP/IP access except through HTTP/HTTPS. If you lock out everything except port 80/ port443, you will also have to add an entry to your HOSTS file in the \winnt\system32\drivers\etc directory so that your server can get to novell.patchlink.com/update/ to pick up its patch subscription:

204.138.167.5 novell.patchlink.com
216.205.112.66 storage12.patchlink.com

PUT YOUR UPDATE SERVER BEHIND A FIREWALL:

Since the Patch Management Server software pulls its patch updates from the subscription servers, there is no need to allow access from the Internet to the Patch Management Server. Be sure to allow access to both subscription servers through your firewall from the internal network to the Internet on the following ports:

```
https://novell.patchlink.com   204.138.167.5     Port 443
https://storage12.patchlink.com      216.205.112.66    Port 443
```

This is normally an easier alternative to (6), however if your company does not have a hardware or software firewall, you can use method (6) to get the same level of network isolation.

APPLY THE MSDE SQL PATCHES:

Apply these patches so you don't get the SLAMMER worm on your server, apply the most recent applicable patches for IIS, SQL, and the Operating System.

24. Patch Management Server Reference

Patch Management Server Security

There are multiple layers to security for the ZENworks® Patch Management Server:

- Web Site Authentication
- Web Site Encryption via SLL
- User (Security) Roles

Web Site Authentication

Internet Information Services (IIS) controls authentication in to the Patch Management Server web site, which means the operating system itself is validating users and their passwords when they log in to the site. Control of who has access and who does not, at this level, is controlled by a local user group.

Web Site Encryption via SSL

SSL provides an encrypted wrapper around all web communication to and from the product. Since all communication is over the web, this means by installing the Patch Management Server in to SSL mode and then adding an SSL certificate to the Patch Management Server web site will provide a wall around customer's data, away from prying eyes.

User (Security) Roles

Every feature, page and action throughout the Patch Management Server has been assigned to a series of Access Rights. Combining these access rights together form a user role. Roles also contain a list of groups and computers (which do not belong to the list of groups). Put this all together and the Patch Management Server now contains a mechanism in which regardless of how you authenticated in to the Patch Management Server web application, what you can do is defined solely by your Patch Management Administrator. If a user does not have a User Role, or it is disabled, and their access immediately is denied to everything.

Error Pages

The Patch Management Server provides four distinct error pages. These pages are:

Insufficient Browser Capabilities

This page is displayed whenever a user visits the Patch Management Server with a browser incapable of properly processing the site. The minimum browser requirements are provided on this page, along with links to download the latest versions of popular browsers.

Requested Page Not Found

This page is displayed whenever a user attempts to navigate to an address that does not exist on the Patch Management Server. Links are provided to common sections of the Patch Management Server to assist the user in returning to the site.

Login Failure

This page is displayed whenever a user fails to provide valid credentials for access to the Patch Management Server.

System Component Version Conflict

This page is display whenever a system component version conflict is detected. The system components of the Patch Management Server are checked every time a user logs into the site. If a conflict is detected, this page is displayed providing the component(s) that failed to meet the required version. The Patch Management Server also attempts to notify the system administrator via email of the conflict.

25. Programmer's Reference

Programmer's reference gives you some samples and examples of the coding necessary to perform advanced functions on the Patch Management Server.

PLCCAgent Script Object

The Agent scripting host contains the imbedded object *PLCCAgent*. This object provides quick functions to the Windows Registry, Agent Environment, and Output.

PLCCAgent GetOSVersion Method

The **GetOSVersion** function obtains information about the version of the operating system that is currently running.

Syntax

object.**GetOSVersion** (str*OS*, iMajor, iMinor, iBuild, strServicePack)

Parameters

Parameter	Description
object	**PLCCAgent** object.
strOS	Win95, Win98, WinME, WinNT, Win2K, WinXP
iMajor	Major version (NT 4.0 Major = 4)
iMinor	Minor Version
iBuild	Build Number
strServicePack	Service Pack Number

Example

PLCCAgent.GetOSVersion szOS, iMajor, iMinor, iBuild, szPS

PLCCAgent GetPolicy Method

Description

The **GetPolicy** function obtains the value for an agent policy.

Syntax

object.**GetPolicy** (str*Name*, strValue)

Parameters

Parameter	Description
object	**PLCCAgent** object.

strName	“Interval”, “IntervalType”,”TraceLevel”
strValue	Returned value of a policy

PLCCAgent InitiateSystemShutdown Method

Description

Used to restart machine.

Syntax

object.**InitiateSystemShutdown**

Parameters

Parameter	Description
object	**PLCCAgent** object.

Remarks

Causes the machine to restart. See Window SDK API **ExitWindowsEx**

PLCCAgent PollHost Method

Description

The ***PollHost*** function tells the agent to poll the host as soon as this package containing this script completes.

Syntax

object.***PollHost*** ()

Parameters

Parameter	Description
object	**PLCCAgent** object.

PLCCAgent RegCloseKey Method

Syntax

object.***RegCloseKey***(hKey)

Parameters

Parameter	Description
object	**PLCCAgent** object.

hKey	Handle to open key

Return

Returns non zero value if successful.

Example

```
If PLCCAgent.RegOpenKey( 0, “HKLM\Software\Microsoft\Windows\CurrentVersion",
hKey ) then
  ‘ Key opened successfully
  PLCCAgent.CloseKey( hKey )
End if
```

PLCCAgent RegEnumKey Method

Description

The ***RegEnumKey*** function enumerates subkeys of the specified open registry key. The function retrieves the name of one subkey each time it is called.

Syntax

object. ***RegEnumKey*** (hKey, strEnumKey, iIndex)

Parameters

Parameter	Description
object	**PLCCAgent** object.
hKey	Handle to an open registry key.
strEnumKey	A variable that receives the name of the subkey in string form. This function copies only the name of the subkey, not the full key hierarchy.
iIndex	Specifies the index of the subkey to retrieve. This value should be zero for the first call to the ***RegEnumKey*** function and then incremented for subsequent calls

Return

Returns non zero value if successful.

Remarks

To enumerate subkeys, an application should initially call the ***RegEnumKey*** function with the *iIndex* parameter set to zero. The application should then increment the *iIndex* parameter and call the ***RegEnumKey*** function until there are no more subkeys (until the function returns 0). While an application is using the **RegEnumKey** function, it should not make calls to any registry functions that might change the key being queried.

Example

```
If PLCCAgent.RegOpenKey( 0, “HKLM\Software\Microsoft\Windows\CurrentVersion",
hKey ) then
   iKeyIndex = 0 ‘ Must start with 0
   do while PLCCAgent.RegEnumKey( hKey, szKey, iKeyIndex )
     PLCCAgent.Write "Key = “ & szKey & vbcrlf
     iKeyIndex = iKeyIndex + 1 'Next Key
   loop
  PLCCAgent.CloseKey( hKey )
 End If
```

PLCCAgent RegEnumValue Method

Description

The ***RegEnumValue*** function enumerates the values for the specified open registry key. The function copies one indexed value name and data block for the key each time it is called.

Syntax

object.***RegEnumValue***(hKey, strEnumValue, iIndex)

Parameters

Parameter	Description
object	**PLCCAgent** object.
hKey	Handle to an open registry key.
strEnumValue	A variable that receives the value name in string form.
iIndex	Specifies the index of the value to retrieve. This value should be zero for the first call to the ***RegEnumValue*** function and then incremented for subsequent calls

Return

Returns non zero value if successful.

Remarks

To enumerate *values*, an application should initially call the ***RegEnumValue*** function with the *iIndex* parameter set to zero. The application must increment the *iIndex* parameter and call the ***RegEnumValue*** function until there are no more *values* (until the function returns 0).

Example

```
' Read all Values from a Key and output them to the Host
If PLCCAgent.RegOpenKey( 0, “HKLM\Software\Microsoft\Windows\CurrentVersion",
hKey ) then
  iKeyValue = 0 ‘ Must start with 0
  do while PLCCAgent.RegEnumValue( hKey, szValue, iValueIndex )
    PLCCAgent.Write "Value = “ & szValue &vbcrlf;
    iKeyValue = iKeyValue + 1 'Next Value
  loop
  PLCCAgent.CloseKey(hKey )
End if
```

PLCCAgent RegOpenKey Method

Description

Returns the registry value named by *strName*.

Syntax

object. ***RegOpenKey***(hRootKey, strKey, strValue)

Parameters

Parameter	Description
object	**PLCCAgent** object.
hRootKey	Handle to previous open key (0=none)
strKey	Key name to open.
hRetKey	Return Handle to open key.

Return

Returns non zero value if successful.

Remarks

If *hRootKey* is 0, *StrName* must begin with one of following root key names . Otherwise, this key must be a subkey of the key identified by the *hRootKey* parameter. The ***RegOpenKey*** function uses the default security access mask to open a key.

Root Key Name	Description
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE
HKCR	HKEY_CLASSES_ROOT

Example

```
If PLCCAgent.RegOpenKey( 0, “HKLM\Software\Microsoft\Windows\CurrentVersion",
hKey ) then
  ‘ Key opened successfully
End if
```

PLCCAgent RegQueryValue Method

PLCCAgent RegRead Method

Description

Returns the registry value named by *strName*.

Syntax

object.***RegRead***(strName, strValue,iType)

Parameters

Parameter	Description
object	**PLCCAgent** object.
strName	Value name to read.
strValue	Data read from registry.
iType	An Integer variable that receives a code indicating the type of data stored in the specified value. 1 = REG_SZ, 2 = REG_EXPAND_SZ, 4 = REG_DWORD

Remarks

StrName must begin with one of following root key names:

Root Key Name	Description
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE
HKCR	HKEY_CLASSES_ROOT

The ***RegRead*** method supports only REG_SZ, REG_EXPAND_SZ, REG_DWORD and REG_BINARY data types. If the registry has other data types, ***RegRead*** returns 0.

Example

The following example reads a value from the registry:

```
Dim Value
if ( PLCCAgent.ReadReg (
“HKLM\Software\Microsoft\Windows\CurrentVersion\ProductId", Value, Type ) then
PLCCAgent.Write “The Product is “ & Value & vbcrlf
endif
```

PLCCAgent RegSetValue Method

Description

The ***RegSetValue*** function sets the data and type of a specified value under a registry key.

Syntax

object.***RegSetValue***

Parameters

Parameter	Description
object	**PLCCAgent** object.
hKey	Handle to an open registry key.
strSubKey	A string containing the name of the value to set.
Type	A code indicating how the data is to be stored. 1 = REG_SZ, 2 = REG_EXPAND_SZ, 4 = REG_DWORD < /FONT >
Value	Variable that contains the data to set in the registry. If an Integer variable is a VarType of vbInteger and the Type is set to 1 (REG_SZ) then the value will be converted to a decimal string and stored as a REG_SZ. The same holds true for a string stored as an Integer.

Return

Returns non zero value if successful.

Remarks

All variables in VBScript/JScript are Variant in nature(meaning the variable could represent any type from integers, strings, to arrays); therefore, conversion of data types could yield undesirable results. If storing an Integer (REG_DWORD) try passing an Integer variable.

Example

```
If PLCCAgent.RegOpenKey( 0, “HKLM\Software\Microsoft\Windows\CurrentVersion",
hKey ) then
 Value = “This is a string”
 Type = 1 ' 1 = String or REG_SZ
 PLCCAgent.RegSetValue( hKey, “Test”, Value, Type )
 PLCCAgent.CloseKey( hKey )
End if
```

PLCCAgent SetReturnCode Method

Description

The ***SetReturnCode*** function is use to alter the package status. If during a PreScript or PostScript execution the script decides that this package has not accomplished its task, it may set a return code and a description of what went wrong.
If set return code is used in the pre-script the package files will not be downloaded and the error returned to the host.

Syntax

object.***SetReturnCode*** (*iRc, strRCDescription*)

Parameters

Parameter	Description
object	**PLCCAgent** object.
iRC	A return code. Range must be from 1-255
strRCDescription	A string description of the return code

Example

PLCCAgent.SetReturnCode 1,"This install didn't work!"

PLCCAgent Write Method

Description

Used to return data to the Host Server.

Syntax

object.***Write***(output)

Parameters

Parameter	Description
object	**PLCCAgent** object.
output	String data to be sent to Host

Remarks

Output can be vbString, vbInteger, or vbLong. vbInteger and vbLong are converted to string prior to send.
The agent supports two different scripts, Pre-Script and Postscript. Therefore two output streams will be received by the Host for each script.

Note: There is currently no user interface provided at the host to view the contents of this stream. A future version may provide a user and/or programmatic interface to this stream.

Example

PLCCAgent.Write "Hello World" & vbcrlf

26. Glossary

Terms, definitions and definitions for terminology used throughout the Patch Management Server.

Agent

A software routine that resides in the background and waits to perform an action when a specified event occurs.

Agent Policies

An agent's behavior is defined by its policies. The three main policies are:

- Hours of Operation
- Communication Interval
- Logging Level

Though the policies can be overridden locally on the computer via the Novell® Patch Management Control Panel Applet, they will be reset whenever the policies are changed by the Patch Management Administrator on the Patch Management Server.

ATL Controls

ATL (Active Template Library, formerly called ActiveX Template Library) is a Microsoft program library (set of prepackaged program routines) for use when creating Active Server Page (ASP) code and other ActiveX program components with C++ (including Visual C++) that runs in a browser to enhance the user experience.

Authentication

The act of verifying that a user has access to a system or function of a software application running on the web server.

Authenticode

Authenticode is a technology based on industry standards that provides a method for developers to digitally sign their code (.EXE, .CAB, .OCX, and .CLASS files). When code is signed, the company signing the code vouches that the code is safe and free of viruses, and takes responsibility for the code.

Browser

Application software that allows the user to access and view documents on the Internet or World Wide Web.

Code Signing

The process of digitally signing programs for verification purposes.

Control Panel Applet

ZENworks® Patch Management provides an applet found in the Control Panel, labeled Novell® Patch Management, that allows easy interaction with the Patch Management Agents. The Action menu in applicable sections allows this interaction. See the Action Menu in each section for applicability.

Client

In relation to Agent-to-Client language, a client is used in reference to, and may also be, a computer, node, server, or system.

Cross Platform

Open interfaces now allow some programs to run on different platforms (operating systems) or to interoperate with different platforms through mediating programs.

Deployment Agent

This Deployment Agent is a service running on the computer that performs two primary tasks: 1) communicates with the Patch Management Server and gathers its updated agent policies and deployments to perform and 2) executes those deployments then sends the results back to the Patch Management Server. Since this service is required to run all the time, its behavior is defined by agent policies set by the Patch Management Administrator on the Patch Management Server.

Detection Agent

The Detection Agent is executed either by a user manually from the computer or automatically by the deployment agent when the Discover Applicable Updates System Task is the next deployment for the agent to perform. It is this process in which the discovery and vulnerability analysis is performed on the computer. The Detection Agent will communicate with the Patch Management Server to send up its system information and inventory and based on the system information, the Patch Management Server begins to send down the vulnerability reports which are determined to be applicable to the computer. The Detection Agent will continue this process until there is no vulnerability reports left to do.

DHCP

Dynamic Host Configuration Protocol is a protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network.

Discovery Agent

Provides both hardware and software information about a computer on which the Patch Management Agent has been installed. There is no requirement to install the discovery agent, as it will be automatically deployed as needed by the Patch Management Server.

DNS Names

The domain name system (DNS) is the way that Internet domain names are located and translated into IP (Internet Protocol) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Firewall

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks.

FTP

File Transfer Protocol, a standard protocol, is the simplest way to exchange files between computers on the Internet. (IETF/W3C RFC959)

Host Name

The server computer name that typically is the DNS name (e.g., novell.patchlink.com).

HTTP

The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. (IETF/W3C RFC2616)

HTTPS

HTTPS Secure Hypertext Transfer Protocol is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned via HTTP over SSL by the Web server.

IIS

Internet Information Server is a group of Internet servers (Web or HTTP, FTP, and Gopher) and other capabilities for Microsoft's Windows NT Server operating system.

IP

Internet Protocol is the network transmission standard for Internet communication.

LDAP

Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet.

MSDE

Microsoft Data Engine is an enabling technology that provides local data storage and is completely compatible with the Microsoft SQL Server(tm) version 7.0 code base. This technology transforms Access from a simple file-server database application into an extremely powerful and highly scalable client-server solution for any size organization.

OSD

Open Software Distribution is an Extensible Markup Language (XML) grammar. It creates a standard way to describe software components -- their versions, their underlying structure and their relationships to other components. This is the standard for using the Internet for automatic software updates.

Password

A unique code entered with the User Name to access a computer on a network or a particular function of a software application.

Patch Management Administrator

Any user who is assigned any of the Patch Management Server access rights which control the functionality of the Patch Management Server or its deployments is considered a Patch Management Administrator. This is not to be confused with the PatchLink Super-User, who is assigned the Administrator user role.

PatchLink Super-User

Any number of users can be assigned the Administrator user role and thus can be called a PatchLink Super-User.

User

Any user who has access to authenticate in to the Patch Management Server is considered a User.

Subscription Host Server

The Patch Management Server obtains its subscription of patches from these central repositories where vulnerability reports and their associated patches are located.

Patch Management Server

The Patch Management Server allows users to be able to determine what vulnerabilities are not patched on their networks.

Port Number

A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server.

Proxy Server

In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Server

A computer that provides file sharing and various other servers between many users and computers on a network.

SQL Server

A trademark for a Microsoft database server that utilizes SQL. SQL Server is a popular database management system for Windows NT environments.

SSL

Secure Sockets Layer is a program layer created by Netscape for managing the security of message transmissions in a network.

TCP/IP

Transmission Control Protocol/Internet Protocol is the basic communication language or protocol of the Internet.

UDP

User Datagram Protocol is a communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP).

Patch Management Agent Software

Software that is installed on computers which enable ZENworks® Patch Management to distribute files and software onto those computers.

User Name

A unique name for access purposes assigned to a user of a computer on a network.

User Role

A user role contains a chosen set of Patch Management access rights and computers and/or groups on which those access rights may pertain to. There are four system user role templates a Patch Management Administrator may use to create custom user roles that fit in a more precise manner with the security policies of an organization. When a user role is assigned to a User, that user now has access to view certain pages, perform certain functions on the assigned computers and/or groups.

Verisign Certificate

VeriSign, Inc, provides Internet-based trust services needed by websites, enterprises and individuals to conduct secure communications and electronic commerce on-line. A VeriSign certificate is issued after a person's or company's identity is verified and enables them to digitally sign programs that run in a browser, or to prove authenticity of a given web site address.

Vulnerability

A breach from the original design, concept or intended behavior of a computer's hardware or software which leaves the computer, or any piece of it, in an exposed state. Malicious users can use this to force other unattended actions to be performed. Vulnerabilities are often caused by defects or bugs, though this is not always the case. Many times the very configuration may result in unexpected exposures. Even out of date documentation may be labeled as a vulnerability as un-informing a user of how to perform actions in the preferred manner may result in systems being widely exposed.

Vulnerability Report

A series of signatures designed to determine a computer is applicable to the vulnerability. Once a computer has been determined that it is applicable to a given vulnerability, the report's fingerprints determine the patch status of the computer.

Vulnerability Report Analysis

The results for a given (or all) vulnerability report(s).

Web Server

A program that publishes content using the HTTP protocol so that it can be viewed using any type of compliant browser from any location on the connected Intranet or Internet.

X.500

An acronym for CCITT Directory Services Protocol that is an industry standard for directory information contents.

XML

eXtensible Markup Language is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

27. Revisions

Version	Revision Date	Change Description	Author
1.0	07/19/04	Initial document	J. Burkett
1.1			