Workstation Management

IV

Much of the functionality of the Workstation Management component of Novell® ZENworks® Desktop Management depends on the preliminary administrative work you do in ConsoleOne® as you import user workstations into the directory and set up the policies that can be associated with User and Workstation objects.

Before you can manage your network's workstations, you must understand Workstation Management and set up policies. After deploying Workstation Management, you can perform periodic maintenance operations, such generating reports of effective policies and policy package associations, copying policy packages from one container in the directory to another container, and more.

Refer to the following sections for further information:

Understanding Workstation Management

<div style="text-align: right">10</div>

The following sections help you to understand and plan a full deployment of the Workstation Management component of Novell® ZENworks® 7 Desktop Management on your network:

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

10.1 Workstation Management Components and Features

Workstation Management helps you reduce the overall cost and complexity of configuring and maintaining workstation desktops in your network. Desktop Management policies provide you with automatic management of server, user, and workstation configurations, processes, and behaviors. You set up these policies using ConsoleOne®, which means that you do not need to visit each workstation in your site to configure user and workstation settings.

Using Workstation Management, you can:

- Enable roaming profiles and set default desktop preferences for users
- Use extensible policies (for Windows 98) and Group policies (for Windows 2000/XP) to control any application function that is configured in the Windows registry
- Set parameters such as remote control and remote view for remotely managing users' workstations
- Set parameters for imaging workstations
- Configure users created on Windows 2000/XP workstations after they have authenticated to the directory
- Set parameters to specify what inventory information to collect
- Set parameters to automatically import new workstations into the tree and to remove workstations when they are no longer is use
- Set user parameters for printing using the Novell iPrint client, which lets users print to any iPrint printer, regardless of the printer's physical location
- Configure users' Terminal Server connections

The following sections provide basic information on Workstation Management components and features:

10.1.1 Components

Workstation Management has the following components:

- "Workstation Resident Modules" on page 142
- "ConsoleOne Snap-Ins" on page 142

Workstation Resident Modules

The workstation resident modules authenticate the user to the workstation (Windows 2000/XP only) and network, and transfer configuration information to and from the directory. Under Windows 2000/XP, Workstation Management runs with administrative privileges that allow it to dynamically create and delete user accounts, provided it can communicate with the directory.

ConsoleOne Snap-Ins

The ConsoleOne snap-ins are Java files that are used to create, view, and configure the various Workstation Management directory objects through ConsoleOne. For more information about ConsoleOne, see the ConsoleOne Documentation Web site (http://www.novell.com/documentation).

10.1.2 Features

Workstation Management features let you store and configure Windows 98/2000/XP desktop policies in the directory and push them to the client. The client workstation can be thought of as an extension of the user.

Workstation Management has the following features:

- "Multiple Platform Support" on page 142
- "Windows 2000/XP Support" on page 143
- "Workstation Profile Management" on page 143
- "Scheduled Actions" on page 143
- "Server and Client Policies" on page 143
- "Directory Storage for Extensible Policies" on page 143
- "ZENworks Desktop Management Reports" on page 143

Multiple Platform Support

Workstation Management software allows all user account and desktop information for Windows 98/2000/XP to be centrally managed within the directory using ConsoleOne as the single administrative utility.

Configuration information is stored in policy package objects. For example, there are policy package objects containing policies for Windows 98, Windows 2000, Windows XP, and Microsoft Terminal Servers that can be downloaded to the workstations.

For more information about Desktop Management support for the Windows NT* platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

Windows 2000/XP Support

For Windows 2000/XP environments, Workstation Management also eliminates the need for domains or for a large number of user accounts to reside in the local Security Access Manager (SAM) of each workstation.

The Windows Group policy is an extension of extensible policies for Windows 2000/XP and Active Directory.

Workstation Management stores user information, desktop configuration, OS configuration, and workstation information in the directory. For 2000/XP users, this means that when a user's directory account is associated with this configuration information, the user can access the network using any 2000/XP workstation configured with Workstation Management.

If the user does not have an account on the workstation at the time of login, Workstation Management can automatically create an account according to the associated user information. After the user is attached to the network, associated policies are downloaded to the workstation to provide a consistent desktop on each workstation used.

Workstation Profile Management

You can create and manage mandatory user profiles, and you can control user interface options, such as the command console and display control attributes. After you have set these attributes, users cannot modify these settings unless they are given the appropriate rights.

Scheduled Actions

This feature lets you schedule actions to occur at a specific time, such as during the evening when the workstation is not in use. These actions can be done without requiring users to be logged in to the network from the workstation. As long as the workstation is powered on, Workstation Management can authenticate the workstation to the directory and perform the action.

Server and Client Policies

Desktop Management uses policies for hands-off management of server and client processes. Policies can be set for automating workstation import and removal, managing users and workstations, and providing workstation inventory information.

Directory Storage for Extensible Policies

Workstation Management lets you create extensible policies using ConsoleOne instead of the Microsoft POLEDIT utility. This approach to creating policies provides three specific benefits:

- It eliminates the requirement that you copy the policy file to the `sys:\public` directory of each server on the network, thus reducing your initial setup workload.
- Because the policy is stored in the directory, you only need to make changes once.
- Any change you make to a policy is automatically replicated across the network in a multiple-partition network, thus providing automatic fault tolerance.

ZENworks Desktop Management Reports

Desktop Management provides predefined reports for effective policies and policy package associations. The scope of both reports is for a selected container and, optionally, its subcontainers.

The Effective Policies report provides the following information:

Version
Tree
Container
Object DN
Platform
Effective Policy DN

The Package Associations report provides the following information:

Tree
Container
Package DN
Association

The report results are displayed in Notepad and are automatically saved as text files on the workstation where you are running ConsoleOne. For further information, see Chapter 16, "Generating Policy Reports," on page 217.

10.2 ZENworks Database

The ZENworks database is used for logging report information for Desktop Management. Therefore, to run reports on Workstation Management, you need a configured Database object with an associated ZENworks Database policy.

If you selected to install the Sybase* database management system during installation of Desktop Management, you should configure and enable the ZENworks Database policy to identify the location of the database object, which knows the location of the database file (mgmtdb.db).

If you are using a Sybase database, the Database object is created during installation if you selected the Inventory option. The Database object then contains default values.

If you are using an Oracle* or Microsoft SQL database, you need to create and configure the Database object and the database.

For more information on configuring the Database object for both Sybase and Oracle, as well as information on configuring the ZENworks Database policy, see Section 13.6, "ZENworks Database Policy," on page 169.

10.3 ZENworks Desktop Management Policies and Policy Packages

To fully deploy the Workstation Management component of Desktop Management, you must configure, enable, and associate the necessary policies and policy packages in ConsoleOne.

A policy is a set of rules that defines how workstations, users, and servers can be configured and controlled, including application availability and access, file access, and the appearance and contents of individual desktops. Policies are contained within policy packages, where they are also administered and customized.

A policy package is a Novell eDirectory™ object containing one or more individual policies. A policy package groups policies according to function, making it easier to administer them. It also provides the means for the administrator to change policy settings and to determine how they affect other eDirectory objects.

Review the following sections for an understanding of Desktop Management policies and policy packages:

- "Policy Packages" on page 145
- "ZENworks Desktop Management Policies" on page 145
- "Plural Policies" on page 146
- "Enabling Policies" on page 146
- "Policy Scheduling" on page 147
- "Policy Package Associations" on page 147
- "Search Policy" on page 148
- "Effective Policies" on page 148
- "Extensible Policies" on page 149

10.3.1 Policy Packages

Desktop Management policies are grouped into policy packages for ease of administration. You create and manage policy packages using ConsoleOne.

The property page for each policy package contains one or more platform-specific tabs that list one or more policies specific to that platform and package. These pages each identify an operating platform, such as General, NetWare, Windows (9x/NT/2000/XP), or Windows Terminal Server (2000/XP). Any policy that you enable on a General page applies to all platforms indicated by the other pages. However, any policy configurations you set on a specific platform page override similar settings on the General page.

The Desktop Management policy packages are:

Container Package
Server Package
Service Location Package
User Package
Workstation Package

The Container Package and Service Location Package are identical to the policy packages used in ZENworks Server Management. The Server Package also exists in ZENworks Server Management; however, in ZENworks Desktop Management it contains different polices. The User Package and Workstation Package are unique to Desktop Management. For more information, see Chapter 11, "Creating Policy Packages," on page 151.

10.3.2 ZENworks Desktop Management Policies

A policy is a set of rules that defines how workstations, users, and servers can be configured and controlled, including application availability and access, file access, and the appearance and contents of individual desktops. Policies are contained within policy packages, where they are also

administered and customized. Desktop Management policies provide you with automated management of server, user, and workstation configurations, processes, and behaviors. For example, you could set up a user policy that determines how a certain user's desktop looks, regardless of the machine that users logs in from. Or, you could set up a workstation policy that determines how a certain machine's desktop looks, regardless of which user logs in.

You can use policies to define the following:

- Parameters for importing workstation objects to the tree
- How far in the tree to search for effective policies
- Parameters for collecting hardware and software inventory
- Parameters for remotely controlling a workstation
- Event and action scheduling

Each policy's properties contains one or more tabs where you can specify settings or configurations related to User, Workstation, Group, or container objects, depending on the type of policy. For more information, see Chapter 11, "Creating Policy Packages," on page 151.

10.3.3 Plural Policies

Plural policies allow you to have multiple instances of the same policy type within the same policy package or as effective policy. Desktop Management has one plural policy in both the User and Workstation Policy packages with the default name of Scheduled Action.

Because you can have several different actions that you might want to run on different schedules, when you add a Scheduled Action policy to the policy package you should name it to reflect the action being scheduled.

For Desktop Management, the Scheduled Action plural policy is available for all platforms in the User Package and Workstation Package. For more information about the Scheduled Action policy in the User Package, see Section 15.6, "Scheduled Action Policy (User and Workstation Packages)," on page 195.

10.3.4 Enabling Policies

As your Workstation Management needs change, you can enable, disable, or modify a policy using any of the three states for policy settings:

Table 10-1   *States for Policy Settings*

State	Description
Enabled	Activates the policy's settings; however, settings are not enforced unless the policy package is also associated with an object.
Disabled	Clears a policy. However, disabling a policy in ConsoleOne does not immediately clear its effect at the workstation. The workstation runs the policy with the cleared settings because the settings for each policy are saved in the workstation's registry.
Ignored	Does not guarantee the clearing or enabling of a policy, because it allows the workstation to continue with whichever policy setting it previously had.

When you create a policy package, its policies are disabled by default. After you enable a policy, some default settings are still in place.

A policy can be enabled when you:

- Create a policy package
- Modify a policy package

A policy can also be enabled anytime from within most of the lists where the policy is displayed.

10.3.5 Policy Scheduling

Some policies can be scheduled to run at a certain time. During creation, all policy packages are given a default run schedule. This means that all applicable policies in this package run according to the default schedule. However, you can change the entire policy package schedule, or you can set a policy within the package to run at a different time from the rest of the package.

If you enable a policy but fail to schedule it, it runs according to the schedule currently defined in the Default Package Schedule.

10.3.6 Policy Package Associations

When you have enabled a policy, you must then associate it to make it effective. Configuring, enabling, and scheduling a policy only sets it up. A policy is enforced through its association with a directory object, such as a Server, Container, User, Group, or Workstation object.

Because policy package associations flow down a tree like inherited rights flow in the directory, you can associate a policy package directly with an object. You can also associate a policy package indirectly, such as with the object's parent container.

When you view the associated policy packages for an object, Desktop Management starts at the object and searches up the tree in the following order for the associated policy packages to be displayed (unless the search order has been changed with a Search policy):

1. The object itself
2. Any Group where the object has membership
3. Any container above the object up to [Root]

Similar to assigning different rights for different users in the directory, you can set a general policy for most users and unique policies for unique users.

You must have the Write right to both the policy package and the object in order to associate one with the another.

You can associate a policy package with Server, Container, User, Group, or Workstation objects when you:

- Create or modify the policy package
- Create or modify the Server, Container, User, Group, or Workstation object
- Associate a policy package with a group or container where the User or Workstation objects have membership

IMPORTANT: Do not associate the policy packages with Alias objects. Alias objects are not supported.

10.3.7 Search Policy

The Search policy is used to prevent tree-walking. Unless specified differently in a Search policy, when Desktop Management starts searching for an object's associated policy packages, it starts at the object and works its way up the tree. If Desktop Management does not have any Search policies defined, it walks the tree until it finds the root object. This can cause unnecessary network traffic. Therefore, plan to use Search policies wherever needed.

Unless otherwise specified in a Search policy, all enabled policies in a policy package that is associated directly with an object have precedence over contradicting policies in policy packages higher in the tree.

For more information about configuring the Search policy, see "Setting Up the Search Policy in the Container Package" on page 153.

10.3.8 Effective Policies

Effective policies for a directory object are those that have been configured, enabled, and associated with the object. Just as the effective rights in the directory flow down the tree, policy package associations also flow down the tree.

The following sections provide more information on effective policies:

- "How Effective Policies Are Determined" on page 148
- "How Package Associations Are Resolved to Determine Effective Policies" on page 148

### How Effective Policies Are Determined

When Desktop Management calculates the effective policies for an object, it starts with all policy packages assigned to that object. It then looks up the tree for policy packages associated to Group objects and then for policy packages associated to Containers (assuming that the search order starts at the leaf object and goes up towards the root of the tree).

How Package Associations Are Resolved to Determine Effective Policies

Because Desktop Management policies provide management-by-exception through policy package associations, a lower package association overrides an upper package association. In other words, a package associated to a User object overrides any similar settings in a package associated to the user's container object.

The following illustrates policy package associations:

Figure 10-1   *Directory Tree Showing Policy Package Associations*

My World
  The Network
    My_Tree
      Novell
        Users (User Package 1 is associated with this Organizational Unit)
          Admin (User Package 2 is associated with this User)
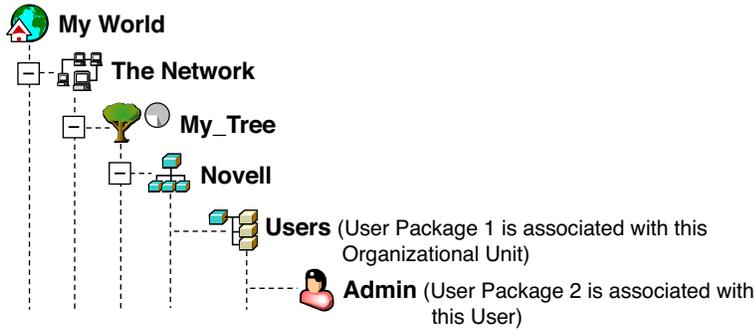
Suppose that in this illustration, User Package 1 contains three enabled policies: Windows Desktop Preferences, Inventory, and Remote Control. User Package 2 contains one enabled policy: Windows Desktop Preferences. For the User object, the Windows Desktop Preferences policy settings in User Package 2 overrides the similar policy settings in User Package 1.

The effective policies for the user are the Windows Desktop Preferences policy in Policy Package 2 and the Inventory and Remote Control policies in Policy Package 1. The *Associations* tab for this User object lists the one policy in User Package 2 that has been enabled. The two enabled policies in User Package 1 are also listed on the User object's *Associations* tab. In other words, effective policies are the sum of all enabled policies in all policy packages associated directly or indirectly to an object.

Extensible Policies

For any Windows-compatible software program, an extensible policy allows you to control any application function that is configured in the Windows registry. Desktop Management lets you easily customize and deploy extensible policies across your network to accommodate your specific business practices.

Extensible policies are not supported on Windows XP. You should use Windows Group policies to configure policies for Windows XP systems. Additionally, we recommend that you use Windows Group policies instead of extensible policies for Windows 2000 or newer. You should continue using extensible policies for the Windows 9.*x* platforms.

For more information, see Section 15.2.1, "Understanding Extensible Policies," on page 181.

Creating Policy Packages

11

For Novell® ZENworks® 7 Desktop Management to function properly, you must create the policy packages so that you can configure, enable, schedule, and associate your planned policies.

Many of the Desktop Management policies are available only if you select the *Workstation Management* installation option. For installation steps, refer to "Installing the ZENworks Desktop Management Server" in the "Novell ZENworks 7 Desktop Management Installation Guide".

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

A policy package is a Novell eDirectory™ object containing one or more individual policies. A policy package groups policies according to function, making it easier to administer them. It also provides the means for the administrator to change policy settings and to determine how they affect other eDirectory objects.

You should create an Organizational Unit (OU) to hold the policy packages. Consider the following when determining where to place this OU:

- If you have partitions in your tree
- The 256-character limit in eDirectory for the full distinguished name
- The Search policy that is used to determine the search order and the search level ceiling for the policy package

To minimize tree walking, it is best to create this policy package OU at the root of the partition that contains the objects with which the policy package is associated and to configure the Search policy to stop searching at the container in which the policy package is located. In doing so, the following benefits are realized:

- Tree walking is minimized with the root of the partition and the Search policy being used
- Placing the OU at the partition's root maximizes the number of characters that are available for naming plural policies

To create an OU and then a policy package:

1 In ConsoleOne®, right-click the container where you want the container for the policy packages placed, click *New*, then click *Organizational Unit*.

2 Give the container a short name, then click *OK*.

Because you can have ZENworks Desktop Management, ZENworks Handheld Management, and ZENworks Server Management policies in the same tree, make sure you use a name that distinguishes your Desktop Management policies container, for example, Desktop Policies.

3 Right-click the new container that will hold your policy packages, click *New*, then click *Policy Package*.

4 Select one of the following policy packages:

> *Container Package*
> *Server Package*
> *Service Location Package*
> *User Package*
> *Workstation Package*

To see a list of policies that are contained in each policy package, select the desired policy package in the *Policy Packages* list on the left side to display the available policies in the *Policies* list on the right.

5 Click *Next*, give the package a short name, click *Nex*t, click *Create Another Policy Package* (unless this is the last one being created), then click *Finish*.

Short package name suggestions include:

> Container
> Server
> Location
> User
> Workstation

6 Repeat Step 4 through Step 5 for each policy package to be created.

Setting Up the Search Policy in the Container Package

12

The Container Package contains only the Search policy. The Search policy is used to limit how far up the tree Desktop Management searches for the effective policies.

The Search policy provides the following benefits:

- Improved security
- The ability to reorder a search
- Better search performance by limiting the search levels traversed in Novell® eDirectory™ and by avoiding unnecessary LAN traffic

The Search policy locates policy packages that are associated with containers. To make a Search policy effective, you associate it with a container.

You can specify the number of levels above or below the location to begin the search:

Table 12-1 *Search Policy Levels*

Number	Description
0	Limits the search to the selected level.
1	Limits the search to one level above the selected level.
	For example, if you selected the server's parent container, this limits the search to one level above the parent level.
-1	Limits the search to one level below the selected level.
	For example, if you selected [Root], -1 would limit the search to one level below [Root].

Without a Search policy in effect, the default is to search from the parent container to [Root]. The search checks each container up the tree towards [Root] for policy packages associated with those containers.

The default Search policy recognizes the policy package associated with the User or Workstation object before it looks in any group or container where such an object resides.

The default search order, *Object > Group > Container > Root*, can be reordered and can include as few as one of the locations. For instance, you can exclude Group objects by setting the search order to *Object > Container > Root*.

You can avoid unnecessary LAN traffic by searching to an associated or selected container instead of [Root].

When you view the associated policy packages for an object, by default Desktop Management starts at the object and searches up the tree to [Root] for all policy packages associated with:

- The object

◆ Any Group where the object has membership

◆ Any of the object's parent containers

The Search policy is required to limit the range which is being used to find other policies. You set up Search policies at a container level. Set up as many Search policies as you need to help minimize network traffic.

To set up a Search policy:

1 In ConsoleOne®, right-click the Container Package, then click *Properties*.

If you have not yet created the Container Package, see "Creating Policy Packages" on page 151.

2 Select the check box under the *Enabled* column for the Search policy.

This both selects and enables the policy.

3 Click *Properties* to display the Search Level Page.
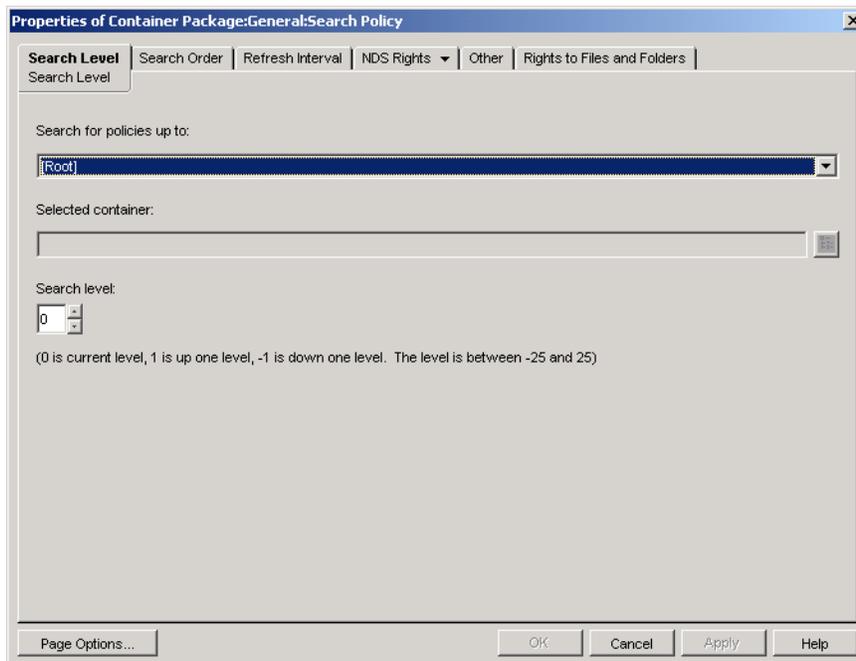
4 Using the drop-down list, select the level to search up to:

[Root]: Searches from the object to the root of the tree.

Object Container: Searches to the parent container of the Server, User, or Workstation object.

Associated Container: Searches to the associated container that this Search policy is associated with. The Associated Container level replaces Partition in earlier versions of ZENworks® for Desktops.

If you are upgrading from a previous version, and you use Partition in your Search policy, make sure that the Container Package is associated only to the partition root.

Selected Container: Searches from the object to the selected container.

5 (Conditional) If you chose Selected Container, browse for and select the container.

6 To determine the searching limits in either direction, specify a number in the Search Level box:

Number	Description
0	Limits the search to the selected level. This is the default setting.
1	Limits the search to one level above the selected level.
	For example, if you selected the server's parent container, this would limit the search to one level above the parent level.
-1	Limits the search to one level below the selected level.
	For example, if you selected [Root], -1 limits the search up to one level below [Root].

You can specify any number between -25 and 25, but using the default setting of 0 is a good administrative practice.

7 Click the *Search Order* tab.
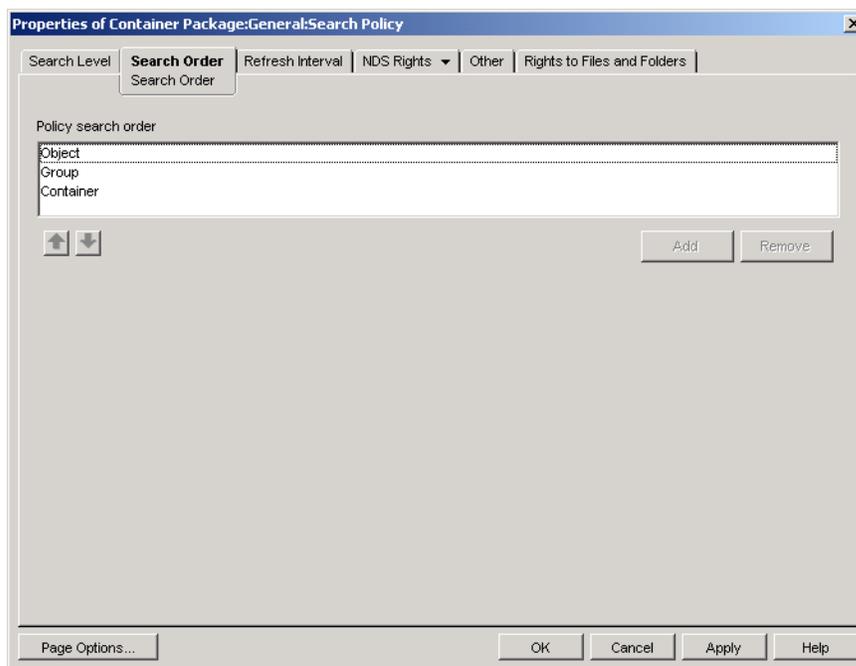
8 Specify the policy searching order using the arrow keys, the *Add* button, and the *Remove* button as necessary.

The default search order is *Object > Group > Container*.

9 Click the *Refresh Interval* tab.
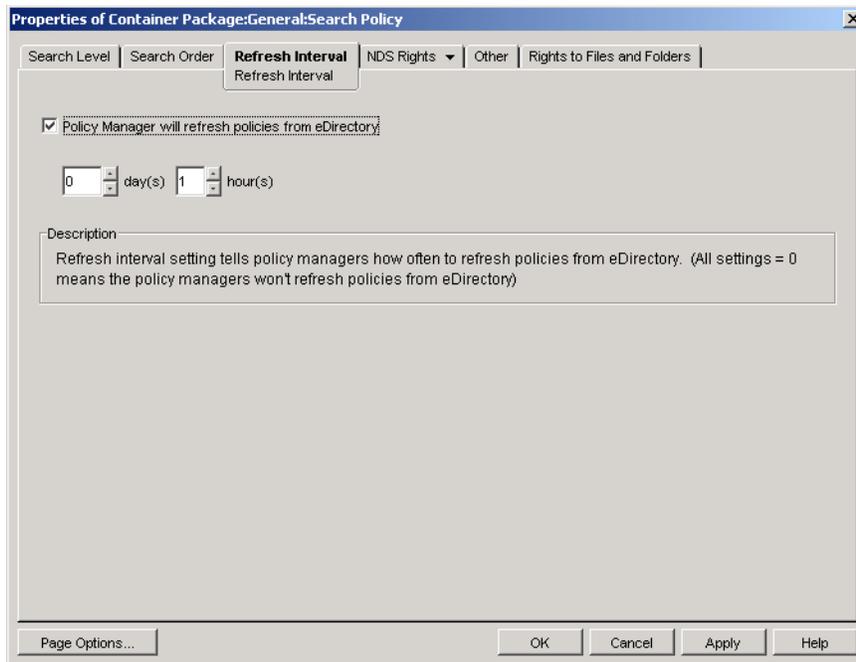
10 Specify the frequency for how often the server should refresh its policies.

By default, the *Policy Manager Will Refresh Policies from eDirectory* option is enabled and the refresh interval is set to one hour. If you set both time increments to zero (0), policies are never refreshed, even if you have the *Policy Manager Will Refresh Policies from eDirectory* option enabled.

11 Click *OK*.

12 Click the *Associations* tab, then click *Add*.

13 Browse for and select the container object for association to the Search policy.

14 Click *OK* when finished.

Setting Up Server Package Policies

<div style="text-align: right; font-size: large;">13</div>

The Server Package has six policies that are used for ZENworks® Desktop Management server functions. The policies you configure and enable are not in effect until you associate their policy package with a container or server object. For further information on configuring the available policies and associating them, see the following sections:

NOTE: The Distributed Server Package is not used by ZENworks Desktop Management. It is only used by Policy and Distribution Services in ZENworks Server Management.

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

13.1 Dictionary Update Policy

This policy allows you to specify where the source for the software dictionary list is located. A software dictionary contains a list of files that, when found on the drive, constitute a known software package. The software dictionary is stored on each individual workstation as it performs its scanning process for it to determine the software packages present on the workstation.

Occasionally, you might want to update the dictionary to include additional, internal software package files. This policy tells the workstation agents where to find the source and how often to update their individual dictionary files.

To configure the Dictionary Update policy:

1 In ConsoleOne®, right-click the *Server Package*, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the *General* tab.

2 Select *Dictionary Update Policy*, then click *Properties*.
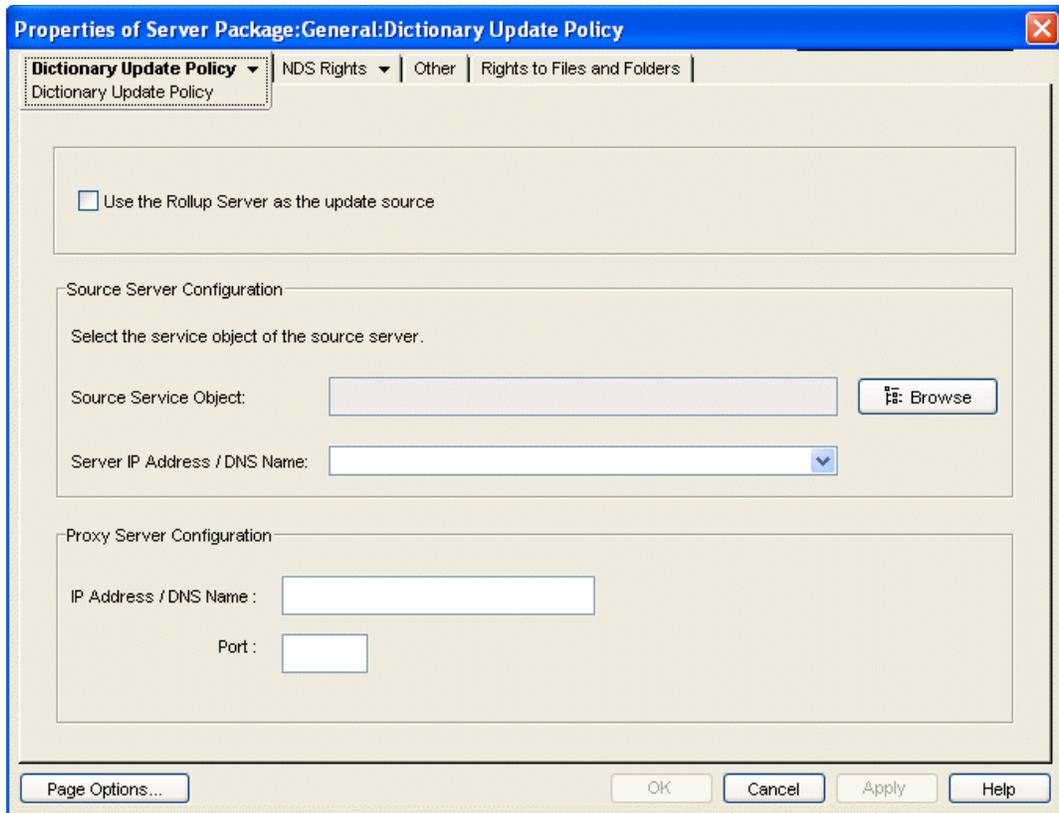
3 Fill in the fields:

Use the Rollup Server as the update source: Select this option if you want the Dictionary Update Service to use the Inventory server configured in the Roll-Up policy as the source for dictionary updates. If you do not select this option, the Dictionary Update Service will use the following settings.

NOTE: Do not select this option for a Standalone server. You must manually configure the following settings of the policy.

Source Server Configuration

  • **Source Service Object:** Browse to select the DN of the Inventory server, which provides the dictionary updates.

  • **Server IP Address / DNS Name:** Select the IP address or the DNS name of the Inventory server, which provides the dictionary updates.

Proxy Server Configuration: If the Inventory server, which provides the dictionary updates, is across a firewall, specify the IP address port number of the proxy server.

  • **IP Address / DNS Name:** Specify the IP address or the DNS name of the proxy server.

  • **Port:** Specify the port number of the proxy server.

Page Options: Click to specify your preferences for arranging the property pages for this type of object. These preferences are saved and used the next time you start Novell® ConsoleOne® on this computer.

4 Click the down-arrow on the *Dictionary Update Policy* tab and click *Dictionary Update Schedule*.
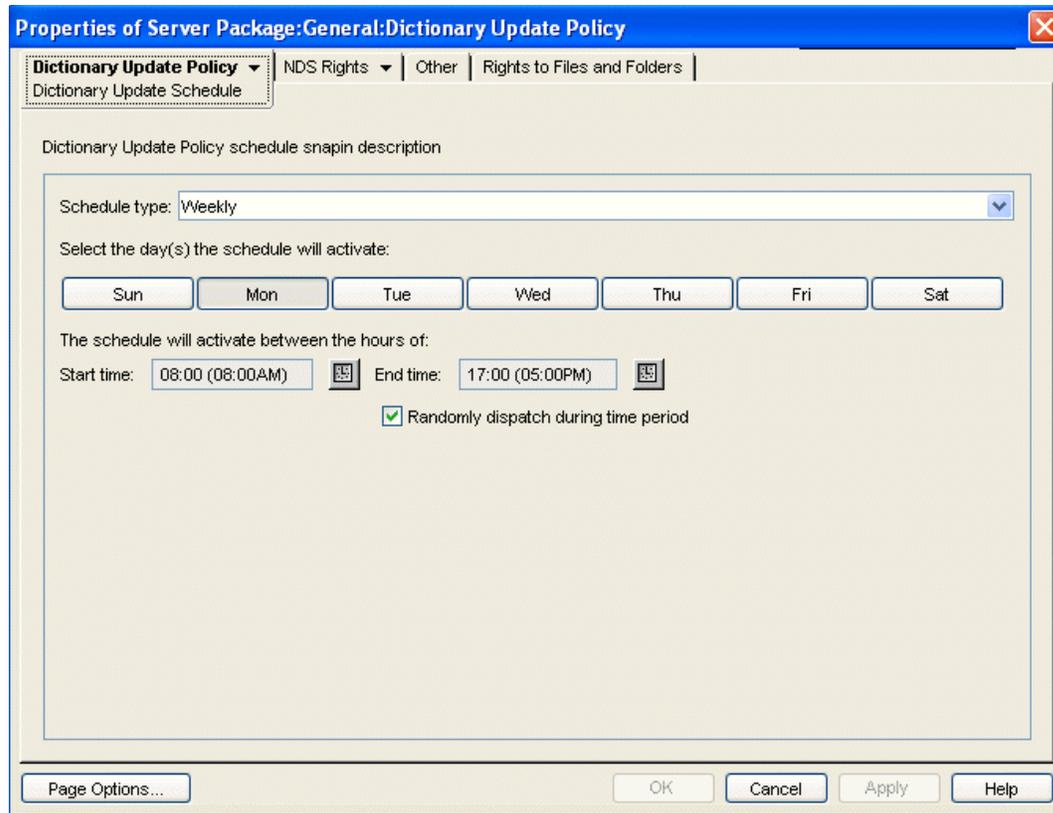
5 Select the schedule using the *Schedule Type* drop-down list:

Daily
Monthly
Yearly
Never

6 Select the days the schedule will activate.

7 Click *Apply*.

13.2 Imaging Server Policy

If you will be imaging workstations, configure and enable this policy. This policy sets rules that determine which images to put on workstations that are imaged by this policy. For more detailed information, see Chapter 58, "Setting Up Imaging Policies," on page 705.

13.3 Inventory Roll-Up Policy

If you want to track workstation inventory information, configure and enable the Inventory Roll-Up policy. For more detailed information on Inventory, see Part VIII, "Workstation Inventory," on page 881.

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the Inventory Roll-Up policy:

1 In ConsoleOne, right-click the Server Package, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the General page.

2 Select the check box under the *Enabled* column for the Inventory Roll-Up policy.

This both selects and enables the policy.

3 Click *Properties*.

4 Fill in the fields:

Destination Service Object: Browse to and select the DN of the next-level server for the selected Inventory server.

Server IP Address / DNS Name: Select the IP address or DNS name of the next-level Inventory server.

IP Address / DNS Name: If the Inventory server is outside of the firewall, specify the IP address or DNS name of the proxy server.

Port: If the Inventory server is outside of the firewall, specify the port number of the proxy server.

5 Click the down-arrow on the *Roll-Up Policy* tab, then click *Roll-Up Schedule*.
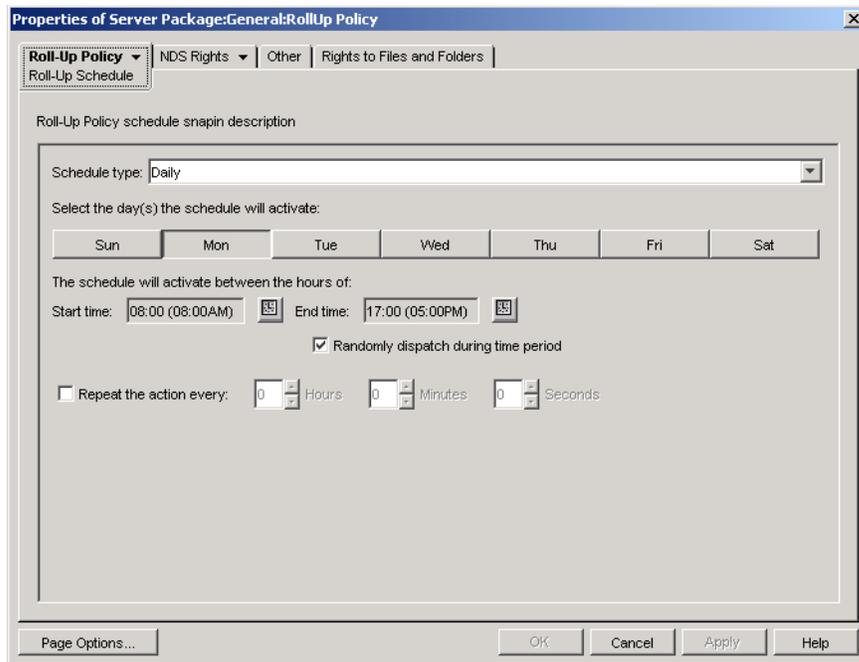
6 Select the schedule using the *Schedule Type* drop-down list:

Daily
Monthly
Yearly
Never

Click the *Help* button on the Roll-Up Schedule page for detailed information about each schedule type and its options.

7 Click *OK* to save the policy.

8 Repeat Step 1 through Step 7 for each platform where you want to set an Inventory Roll-Up policy.

9 When you have finished configuring all of the policies for this package, continue with the steps under Section 13.7, "Associating the Server Package," on page 172 to associate the policy package.

13.4 Workstation Import Policy

The Workstation Import policy sets parameters to control automatic workstation importing. It must be enabled for Automatic Workstation Import to function. For more detailed information, see Section 7.1, "Understanding Workstation Import and Registration," on page 127.

You can set rules on how Workstation objects are named and where they are created. You should decide if you want to create Workstation objects in their own containers or in the container where the User objects reside.

You might find it easiest to manage Workstation objects in a common container if your User objects are scattered among various containers in the tree.

You might also find it easiest to keep User and Workstation objects in the same container.

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the Workstation Import policy:

1 In ConsoleOne, right-click the Server Package, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the *General* tab.

**2** Select the check box under the *Enabled* column for the Workstation Import policy.

This both selects and enables the policy.

3 Click *Properties* to display the Containers page.
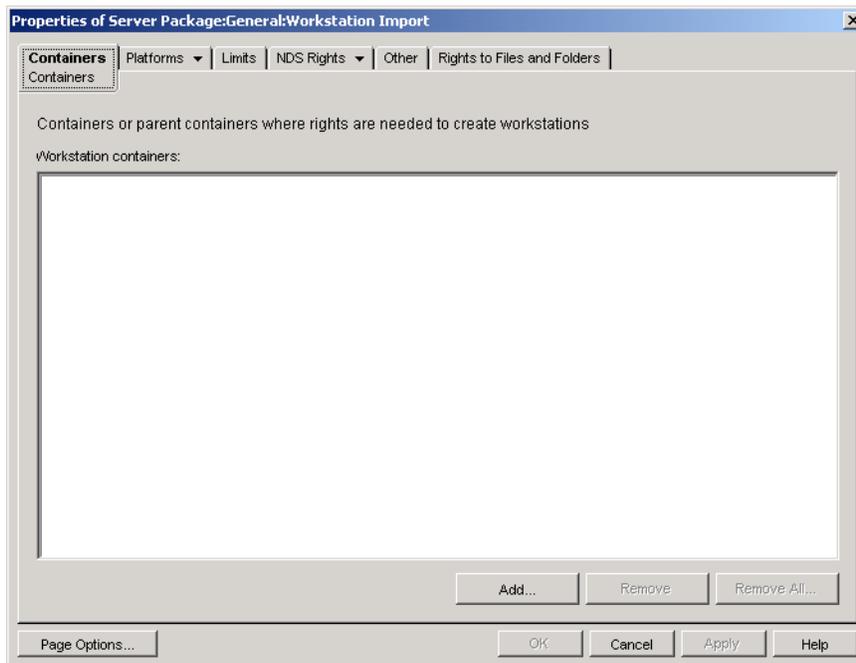
4 Click *Add*, select the eDirectory™ containers where rights are needed for creating Workstation objects, then click *OK*.

5 Click the *Limits* tab.
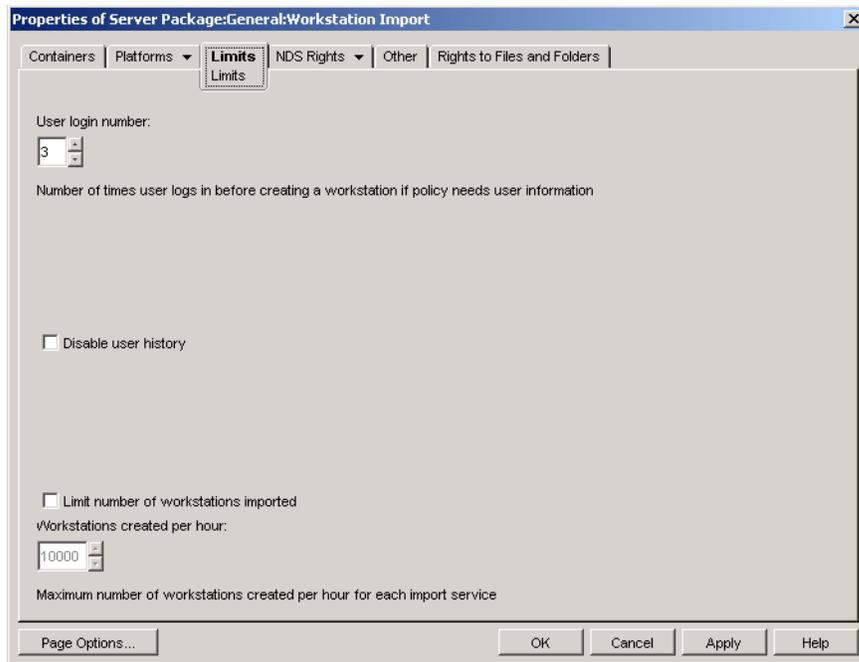
6 Fill in the fields:

User Login Number: If the Workstation Import policy requires user information, this number represents the number of times the user needs to log in before the user's Workstation object is created.

Disable User History: Each time a user logs in to a workstation, the Workstation object's User History page is updated so that an administrator can view a complete list of all users who have logged in to that workstation. If you do not want user history to be collected for workstations, you should enable this option.

This option lets you disable the collection of user history for all workstations imported after you enable this option. To disable user history collection on workstations that were imported before you enabled this option, right-click the appropriate Workstation object, click *Properties*, click the *User History* tab, then select the *Do Not Add to History* check box.

Limit Number of Workstations Imported: To help balance server workload, enable this option to limit how many workstations are imported. When you select this option, the *Workstations Created Per Hour* box is available.

Workstations Created Per Hour: Specify the limit for how many Workstation objects can be created per hour.

7 Click the *Platforms* tab, then click *General*, *WinNT*, *Win2000*, *WinXP*, or *Win9x*, as applicable.
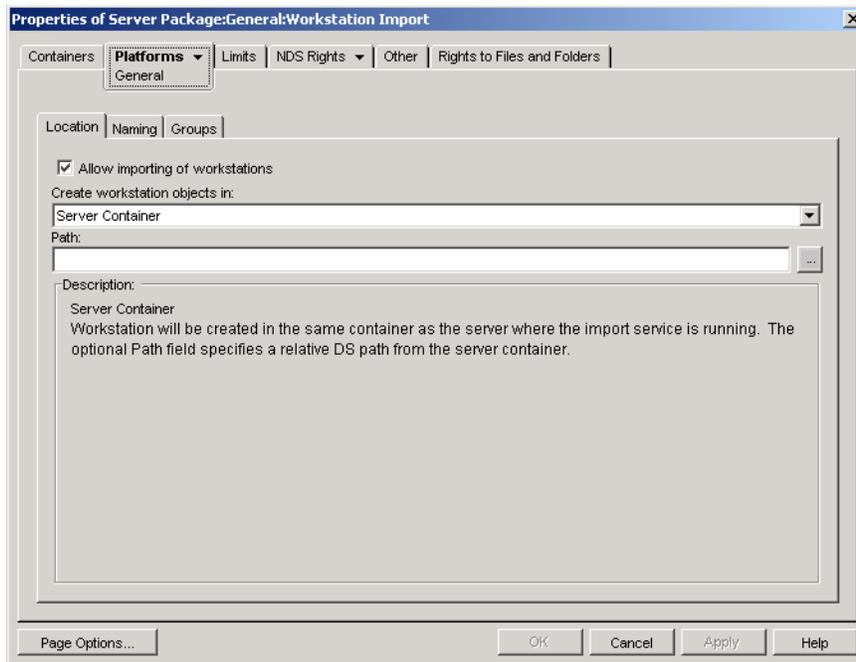
8 Fill in the fields:

Enable Platform Settings to Override General Settings: This check box appears only on the WinNT, Win2000, WinXP, and Win9x platform pages; it does not appear on the General page. Select this check box to override the settings on the General page with the setting you configure on one of the four specific platform pages.

Allow Importing of Workstations: Enable this option to allow registered workstations to be imported.

Create Workstation Objects In: Select an option from the drop-down list:

* **Selected Container:** The Workstation object is created in the container specified in the Path field. This is an absolute path.

* **Server Container:** The Workstation object is created in the same container as the server running the import service. You can specify a relative path from the server container.

* **User Container:** The Workstation object is created in the container where the User object resides for the logged-in user. You can specify a relative path from the user container.

* **Associated Object Container:** The Workstation object is created in the container that is associated with the Workstation Import policy. You can specify a relative path from the associated container.

Path: If you are using a relative path, specify a string. The number of periods you end the path with determines the number of relative levels. If you are using an absolute path, select the container.

9 Click the *Naming* tab.
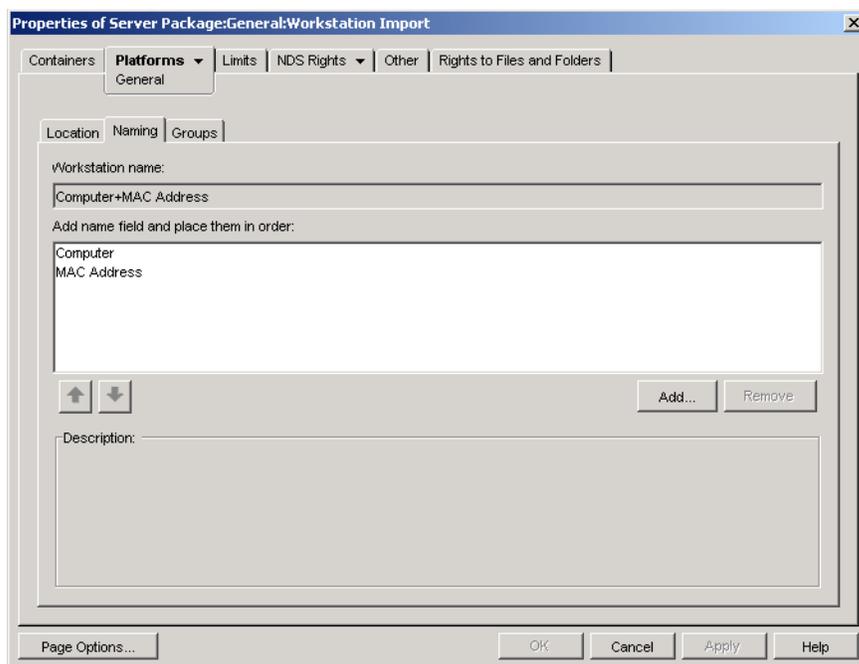
10 Fill in the fields:

Workstation Name: Displays the workstation naming convention currently defined in the *Add Name Fields and Place Them in Order* list. Whenever there is a potential name conflict (such as two Workstation objects in the same container named after the User object), the system appends a 3-digit number on the end of the name that you enter here.

Add Name Fields and Place Them in Order: You must have at least one option in this list. By default, *Computer + Network Address* is displayed in the list. Click *Add* to select from the following list of name fields. After creation of the Workstation object, this information is static and does not change.

Name Field	Description
Computer	The Windows computer name, usually as it was named during the Windows installation process.
MAC Address	The workstation's MAC address. This address is unique to the workstation's network card.
Container	The container where the User object resides.
<User Defined>	You can type your own information here. You must use characters that are valid in a DS object name. Do not use the following characters: ◆ Underscore (_) ◆ Asterisk (*) ◆ Less than symbol (<) ◆ Greater than symbol (>) ◆ Semicolon (;) ◆ Pound sign (#)
User	The name of the user that is logged in.

Name Field	Description
IP Address	The workstation's Internet Protocol (IP) address.
DNS	The Domain Name System name (the logical name related to the IP address).
Server	The workstation's preferred server.
OS	The workstation's operating system (Windows 98, Windows NT, Windows 2000, Windows XP).
CPU	The type of central processing unit in the workstation (386, 486, Pentium*, and so forth).

11 Click the *Groups* tab.
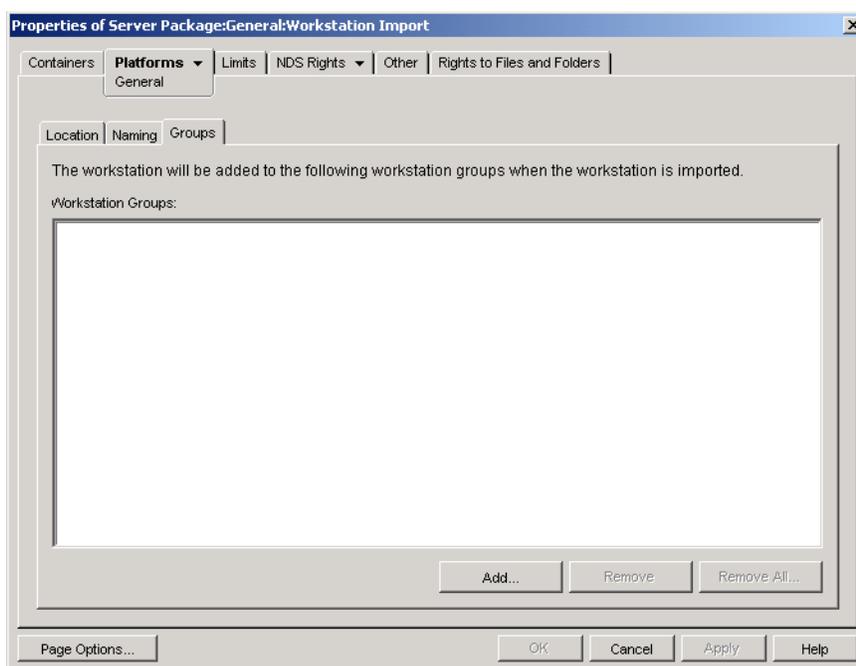
12 Click *Add*, then browse for and select the workstation groups you want this Workstation object to belong to when it is imported.

13 Click *OK* to save the policy.

14 Repeat Step 1 through Step 13 for each platform where you want to set a Workstation Import policy.

15 When you have finished configuring all of the policies for this package, continue with the steps under to associate the policy package.

13.5 Workstation Removal Policy

If you want Workstation objects to be automatically removed after they have not been used for a specified period of time, configure and enable the Workstation Removal policy. For more detailed

information on workstation removal, see Part III, "Automatic Workstation Import and Removal," on page 125.

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the Workstation Removal policy:

1 In ConsoleOne, right-click the Server Package, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the *General* tab.

2 Select the check box under the *Enabled* column for the Workstation Removal policy.

This both selects and enables the policy.

3 Click *Properties* to display the Containers page.
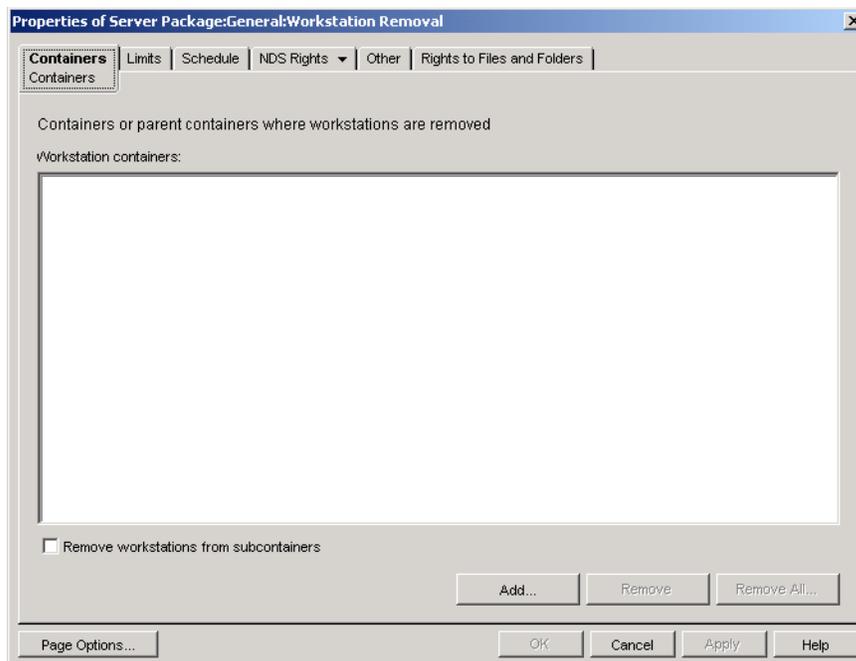
4 Click *Add*, select the containers where workstations to be removed reside, then click *OK*.

Select the *Remove Workstations From Subcontainers* check box, if desired.

5 Click the *Limits* tab.
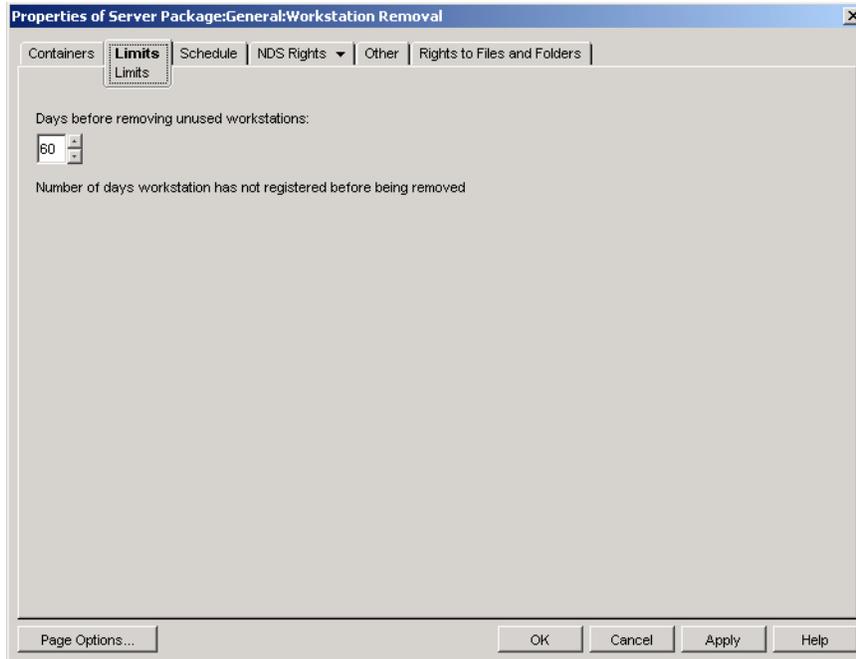
6 Specify the number of days a Workstation object should remain in the tree without registering before its object is removed.

7 Click the *Schedule* tab.
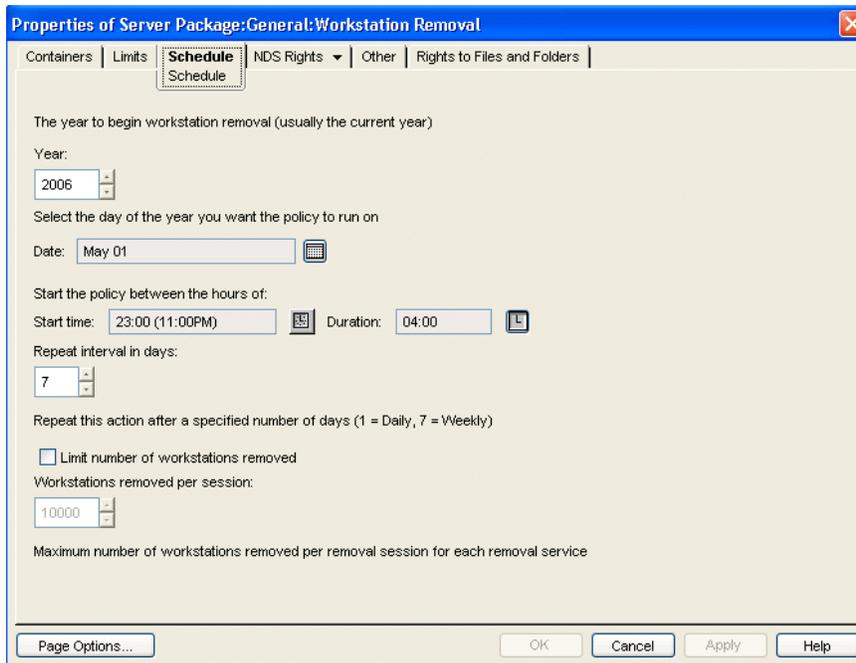
8 Fill in the fields:

Year: The year to begin workstation removal.

Date: The day of year that you want the policy to run on.

Start Time: The beginning time of when the policy can run.

Duration: Length of the time window.

Repeat Interval In Days: Beginning from the starting date, Workstation object removal is performed at this interval.

Limit Number of Workstations Removed: To help balance server workload, enable this option to limit how many workstations are removed in a session. When you select this option, the *Workstation Removed Per Session* option becomes available.

Workstations Removed Per Session: Specify a number to set the limit for how many Workstation objects can be removed per session.

9 Click *OK* to save the policy.

10 Repeat Step 1 through Step 9 for each platform where you want to set a Workstation Removal policy.

11 When you have finished configuring all of the policies for this package, continue with the steps under Section 13.7, "Associating the Server Package," on page 172 to associate the policy package.

13.6 ZENworks Database Policy

This policy identifies the location of the ZENworks Database object. If you selected to install the ZENworks database, you should configure and enable this policy.

NOTE: In previous versions of ZENworks for Desktops, you configured and enabled the ZENworks Database policy using the Service Location Package. In ZENworks for Desktops 4.*x* and later, you can also configure and enable this policy in the Server Package.

The ZENworks Database policy in the Server Package lets you configure only the Inventory database. The ZENworks Database policy in the Service Location Package lets you configure both the Inventory database and the Application Management databases.

If backward compatibility with an existing ZENworks Database policy for ZENworks for Desktops 3.*x* is important, you might want to configure this policy in the Service Location Package. However, there is improved manageability if you configure this policy in the Server Package. Configuring the ZENworks Database policy in the Server Package allows you to associate the policy with individual servers rather than with containers.

Sybase: If you are using a Sybase database, the Database object might have been installed with default property values, depending on whether you selected to install Desktop Management Inventory. In either case, follow the applicable steps under "Configuring the ZENworks Database Object for Sybase" on page 170, then continue with "Setting Up the ZENworks Database Policy" on page 171.

Oracle: If you are using an Oracle database, you need to create the Database object and enter the required property values. In this case, follow the steps under "Configuring the ZENworks Database Object for Oracle" on page 170, then continue with "Setting Up the ZENworks Database Policy" on page 171.

13.6.1 Configuring the ZENworks Database Object for Sybase

While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

1 In ConsoleOne, right-click the Database object, then click *Properties*.

The *ZENworks Database* tab should be displayed.

2 Fill in the applicable fields, keeping the user name and password pairs together:

Database (Read-Write) User Name: Secures read and write access to the database file.

Database (Read-Write) Password: Secures read and write access to the database file.

Database (Read Only) User Name: Secures only read access to the database file.

Database (Read Only) Password: Secures only read access to the database file.

Database (Write Only) User Name: Secures only write access to the database file.

Database (Write Only) Password: Secures only write access to the database file.

3 To change any default JDBC* driver type information, click the *JDBC Driver Information* tab, then edit the fields:

Driver
Protocol
Subprotocol
SubName
Port
Flag
Database Service Name

4 If you will use an ODBC driver for the database file, click the *ODBC Driver Information* tab, then fill in the fields:

Driver Filename
Data Source Name
Connection Parameters

5 Click *OK* to save the database property changes.

Continue with .

13.6.2 Configuring the ZENworks Database Object for Oracle

While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

1 In ConsoleOne, right-click the container where the Database object is to be created, click *New*, click *Object*, click *ZENworks Database*, then click *OK*.

2 Specify a name for the Database object, click *Define Additional Properties*, then click *OK*.

The *ZENworks Database* tab should be displayed.

3 Select the DN of the server where the database files are to be stored.

4 (Optional) Specify the IP address of the server.

5 Fill in the applicable fields, keeping the user name and password pairs together:

Database (Read-Write) User Name: Secures read and write access to the database file.

Database (Read-Write) Password: Secures read and write access to the database file.

Database (Read Only) User Name: Secures only read access to the database file.

Database (Read Only) Password: Secures only read access to the database file.

Database (Write Only) User Name: Secures only write access to the database file.

Database (Write Only) Password: Secures only write access to the database file.

6 To specify the JDBC driver type, click the *JDBC Driver Information* tab, click the *Populate Fields With Default Values For An Oracle Database* button, then click *Populate Now*.

7 To change any default JDBC driver type information, edit the fields:

Driver
Protocol
SubProtocol
SubName
Port

8 If you will use an ODBC driver for the database file, click the *ODBC Driver Information* tab, then fill in the fields:

Driver Filename
Data Source Name
Connection Parameters

9 Click *OK* to save the database property changes.

Continue with .

13.6.3 Setting Up the ZENworks Database Policy

While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

1 In ConsoleOne, right-click the Server Package or the Service Location Package, then click *Properties*.

The *General* tab is displayed.

2 Select the check box under the *Enabled* column for the ZENworks Database policy.

This both selects and enables the policy.

3 Click *Properties*.

4 Select the database DN, then click *OK*.

5 When you have finished configuring all of the policies for this package, continue with the steps under to associate the policy package.

13.7 Associating the Server Package

The policies you configured and enabled are not in effect until you associate their policy package with a container or server object.

1 In ConsoleOne, right-click the Server Package, then click *Properties*.

2 Click the *Associations* tab > *Add*.

3 Browse for and select the container or server for associating the package, then click *OK*.

Setting Up Service Location Package Policies

14

The Service Location Package includes four policies on the General platform page. The policies you configure and enable are not in effect until you associate their policy package with a container object. For further information on configuring the available policies and associating them, see the following sections:

14.1 SMTP Host Policy

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the SMTP Host policy:

1 In ConsoleOne®, right-click the Service Location Package, then click *Properties*.

   The *General* tab is displayed.

2 Select the check box under the *Enabled* column for the SMTP Host policy.

   This both selects and enables the policy.

3 Click *Properties* to display the SMTP Host page.
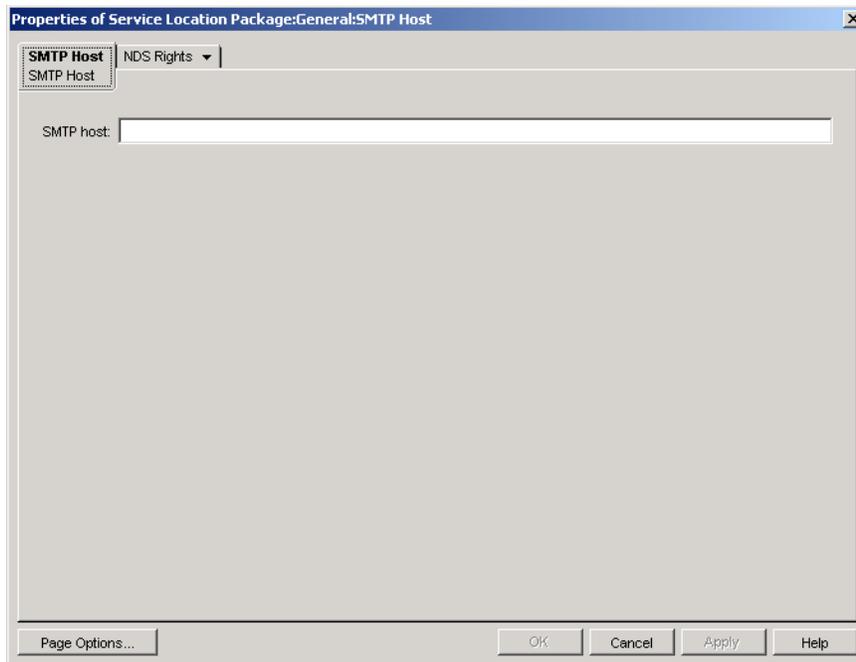
4 Specify the TCP/IP address or DNS name of the relay host server, then click *OK*.

5 When you have finished configuring all of the policies for this package, continue with the steps under Section 14.5, "Associating the Service Location Package," on page 176 to associate the policy package.

14.2 SNMP Trap Targets Policy

If you are using SNMP, you should configure and enable this policy. You use this policy to establish the targets (or locations) where you want SNMP traps sent. Each target must be a valid TCP/IP address or DNS name.

To set up the SNMP Trap Targets policy:

1 In ConsoleOne, right-click the Service Location Package, then click *Properties*.

The *General* tab is displayed.

2 Select the check box under the *Enabled* column for the SNMP Trap Targets policy.

This both selects and enables the policy.

3 Click *Properties*.

Properties of Service Location Package:General:SNMP Trap Targets

Snmp Trap Policy | NDS Rights ▾ | Other | Rights to Files and Folders
Snmp Trap Policy

SNMP trap targets:

Add...

Remove

Page Options...   OK   Cancel   Apply   Help
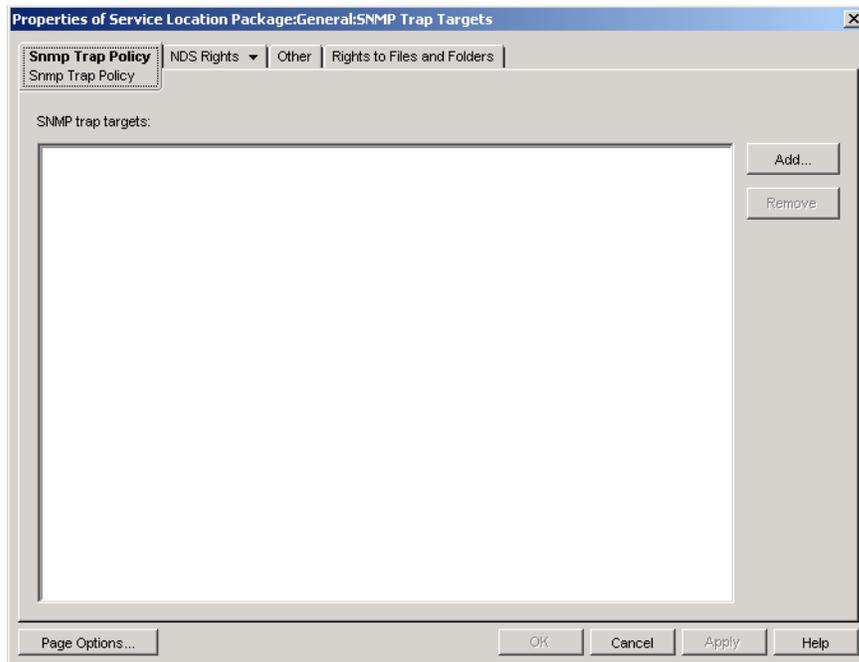
4 Click *Add*, enter a new target, then click *OK*.

5 Repeat Step 4 for each trap target you need.

6 Click *OK* to save the policy.

7 When you have finished configuring all of the policies for this package, continue with the steps under Section 14.5, "Associating the Service Location Package," on page 176 to associate the policy package.

14.3 XML Targets Policy

Extensible Markup Language (XML) is a flexible way to create common information formats and share both the format and the data on the Internet, intranets, and elsewhere. If you choose to export and view Application Management information in XML format via the Internet, you should configure and enable this policy. The XML Targets policy lets you assign the URL that you'll use to view this information.

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the XML Targets policy:

1 In ConsoleOne, right-click the Service Location Package, then click *Properties*.

The *General* tab is displayed.

2 Select the check box under the *Enabled* column for the XML Targets policy.

This both selects and enables the policy.

3 Click *Properties*.
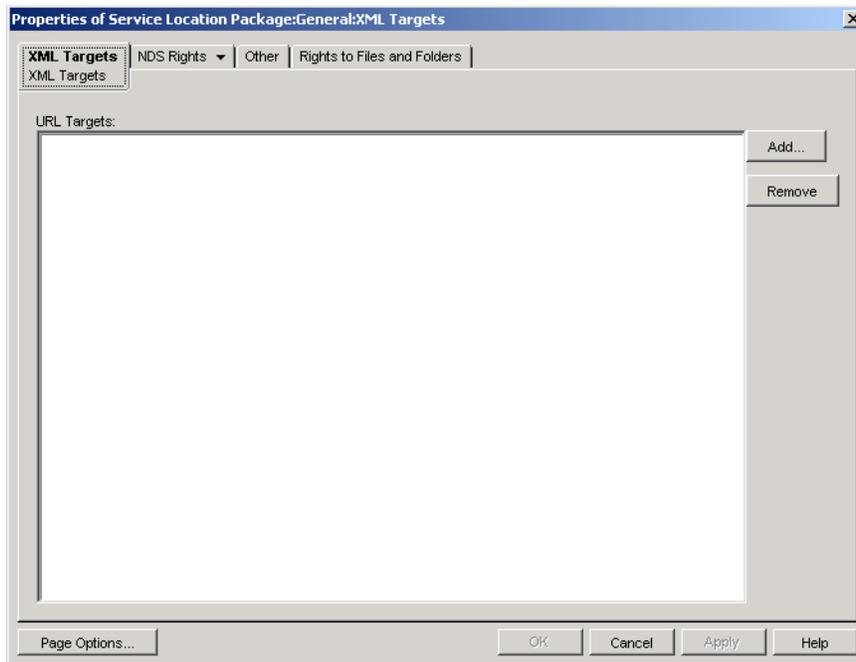
4 Click *Add*, type the URL, then click *OK*.

5 Click *OK* to save the policy.

6 When you have finished configuring all of the policies for this package, continue with the steps under Section 14.5, "Associating the Service Location Package," on page 176 to associate the policy package.

14.4 ZENworks Database Policy

In previous versions of ZENworks® for Desktops, you configured and enabled the ZENworks Database policy using the Service Location Package only. You can now also configure and enable this policy in the Server Package. For more information see, Section 13.6, "ZENworks Database Policy," on page 169.

14.5 Associating the Service Location Package

The policies you configured and enabled are not in effect until you associate their policy package with a container object.

1 In ConsoleOne, right-click the Service Location Package, then click *Properties*.

2 Click the *Associations* tab, then click *Add*.

3 Browse for and select the container for associating the package, then click *OK*.

Setting Up User and Workstation Package Policies

15

Review the following sections for information to help you set up and associate the User and Workstation Package policies:

NOTE: The information in this section also applies to ZENworks® 7 Desktop Management with Support Pack 1.

15.1 Platform Pages

Desktop Management provides policies that apply to various individual computer platforms, to a combination of platforms, and to a General platform, which lets you configure policies that apply to all platforms.

To display a platform page:

1 In ConsoleOne®, right-click the User Package or Workstation Package, then click *Properties*.

2 Click the down-arrow on the *Policies* tab, then select the desired platform.

Figure 15-1   *The User Package Properties Page*
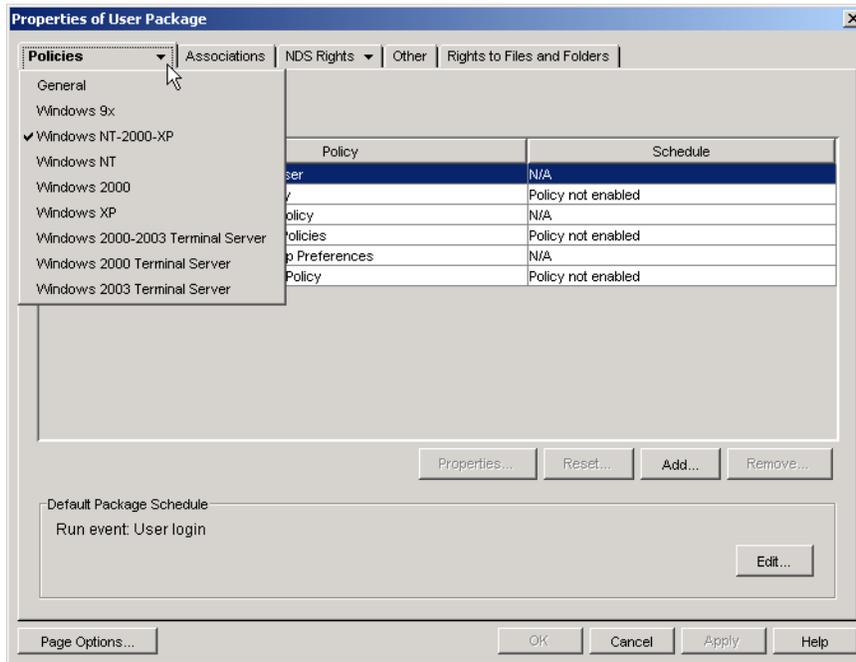
The following table lists each platform page, the package that contains each platform page, and a brief description:

Table 15-1   *Platform Pages and the Packages They Contain*

Platform Page	Package	Description
General	User and Workstation Packages	Lists the available policies for the General page.
		Policies set on this page apply to all platforms unless you configure the same policy on a specific platform page; policies set on a specific platform page override policies set on the General page.
Windows 9x	User and Workstation Packages	Lists the available policies for Windows 9.*x* machines.
		Although Microsoft no longer supports Windows 95, existing Windows 95/98 policies from a previous installation of ZENworks that are associated with Windows 95 machines or users will continue to function. Desktop Management does not allow you to create new policies for Windows 95 machines or users.

Platform Page	Package	Description
Windows NT-2000-XP	User and Workstation Packages	Lists the available policies for Windows NT/2000/XP machines.

Use this page if you do not want to treat Windows NT/2000/XP machines as separate platforms. You can also use this page to set policies for users and workstations that are using earlier versions of ZENworks for Desktops.

If you are using the Novell Client™ without the Desktop Management Agent, you must configure and enable policies on this page rather than on the individual platform pages listed below (Windows NT, Windows 2000, or Windows XP).

If you are upgrading from a previous version of ZENworks for Desktops, your existing policies are listed on this platform page. New platform pages that separate the Windows NT/2000/XP platforms into individual platform pages were new enhancements to ZENworks for Desktops 4. You can continue to manage your policies from a previous version of ZENworks for Desktops on this page or you can configure and enable new policies that apply to individual platforms by using one of the specific platform pages listed below.

For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*. |
| Windows NT | User and Workstation Packages | Lists the available policies for Windows NT machines[1].

For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*. |
| Windows 2000 | User and Workstation Packages | Lists the available policies for Windows 2000 machines[1]. |
| Windows XP | User and Workstation Packages | Lists the available policies for Windows XP machines[1]. |

Platform Page	Package	Description
Windows 2000-2003 Terminal Server	User Package only	Lists the available policies for Windows 2000 or Windows 2003 Terminal Servers[2].
		You should use this page if you want to set policies that apply to both platforms to make managing Terminal Servers easier. If you want to treat Windows 2000 and Windows 2003 Terminal Servers as separate platforms, use one of the specific platform pages.
Windows 2000 Terminal Server	User Package only	Lists the available policies for Windows 2000 Terminal Servers[2].
Windows 2003 Terminal Server	User Package only	Lists the available policies for Windows 2003 Terminal Servers[2].

[1] Policies enabled on this page are applied only on workstations that have been upgraded to ZENworks for Desktops 4 or newer. To set policies for workstations using earlier versions of ZENworks for Desktops, use the Windows NT-2000-XP page.

[2] Because earlier versions of ZENworks did not support Terminal Servers, policies enabled on this page are applied only on workstations that have been upgraded to ZENworks for Desktops 4 or newer.

You must be running the Desktop Management Agent to configure and enable policies for Terminal Servers.

Terminal Servers do not support the Scheduled Action and Remote Control policies.

15.2 Computer/User Extensible Policies (Workstation/User Packages)

For any Windows-compatible software program, an extensible policy allows you to control any application function that is configured in the Windows registry. Desktop Management lets you easily customize and deploy extensible policies across your network to accommodate your specific business practices.

NOTE: Computer Extensible policies are contained in the Workstation Package; User Extensible policies are contained in the User Package. The information in this section applies to both packages; however, there are differences between the two packages. When you set Computer Extensible policies in the Workstation Package, the policies apply to all users who log in to an associated workstation. When you set User Extensible policies in the User Package, the policies apply to all associated users regardless of the workstation they use.

The following sections contain additional information:

-
-

15.2.1 Understanding Extensible Policies

Desktop Management leverages Microsoft desktop enhancements by doing the following to provide extensible policies that are enabled in the directory:

- Moving the policy editor functionality into the directory
- Moving Windows registry information for applications into the directory
- Enabling the directory to point to extensible policy files

Review the following sections for more information:

- "How Extensible Policies Work" on page 181
- ".Adm Files" on page 181

How Extensible Policies Work

When you install a software application that is compatible with Windows, the application's installation program uses the Microsoft policy editor (`poledit.exe`) to read the application's `.adm` file and create a `.pol` file that updates the workstation's Windows registry. However, when you install an application on a workstation under the umbrella of Desktop Management, the Desktop Management policy editor (`wmpolsnp.exe`) is used to read the `.adm` file and make the necessary changes to the workstation's Windows registry.

The Microsoft policy editor lets you make changes to the policies created by the `.adm` files, but only per workstation. If an application is installed using the Application Management component of Desktop Management, the Desktop Management policy editor ensures that the application's directory-enabled policies are automatically applied across the network, rather than manually to one workstation at a time.

Extensible policies are not supported on Windows XP. You should use Windows Group policies to configure policies for Windows XP systems. Additionally, we recommend that you use Windows Group policies instead of extensible policies for Windows 2000 or newer. You should continue using extensible policies for the Windows 9.*x*/NT platforms.

Extensible policies are not cumulative. Unless specified differently in a Search policy, when Desktop Management starts searching for an object's associated policy packages, it starts at the object and works its way up the tree. Because extensible policies are not cumulative, Desktop Management walks the tree until it finds the first effective policy for the object and applies that policy's settings.

.Adm Files

Files with the `.adm` extension provide customizable attributes for users and workstations. You can add existing `.adm` files and configure their settings to create extensible policies. Depending on whether you are configuring User Extensible policies or Computer Extensible policies, the attributes you can customize will vary.

The `.adm` files are static templates for creating policies in the ZENworks database. When you edit a policy in Desktop Management, the changes are made in the database rather than in the `.adm` file. Even so, you should not delete an `.adm` file from a directory after it has been used in Desktop Management because it is needed to undo registry changes if you should remove the policy from Desktop Management.

When you have `.adm` files that you want to use, you should place them in a location where you can easily browse for them. You should save them on a server, because after the `.adm` file has been used to create a policy, it is not needed again until you modify the policy.

Because Desktop Management automatically displays any policies listed in the following location when you view an Extensible Policies page, we recommend that you use it:

```
sys:\public\mgmt\consoleone\1.2\bin\zen\adm files
```

This is the default location where `.adm` files shipped with Desktop Management are placed if you run ConsoleOne from the server. If you run ConsoleOne from a workstation, `.adm` files are placed in the `consoleone\1.2\bin\zen` directory on the workstation.

15.2.2 Configuring Extensible Policies

The Computer Extensible/User Extensible policies are not found on the General or Windows XP platform pages.

To set up the Computer Extensible or User Extensible policies:

1 In ConsoleOne, right-click the User Package or the Workstation Package, click *Properties*, then click the appropriate platform page.

For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2 Select the check box under the *Enabled* column for the Computer Extensible or User Extensible policies.

This both selects and enables the policy.

3 Click *Properties* to display the User Extensible/Computer Extensible Policies page.
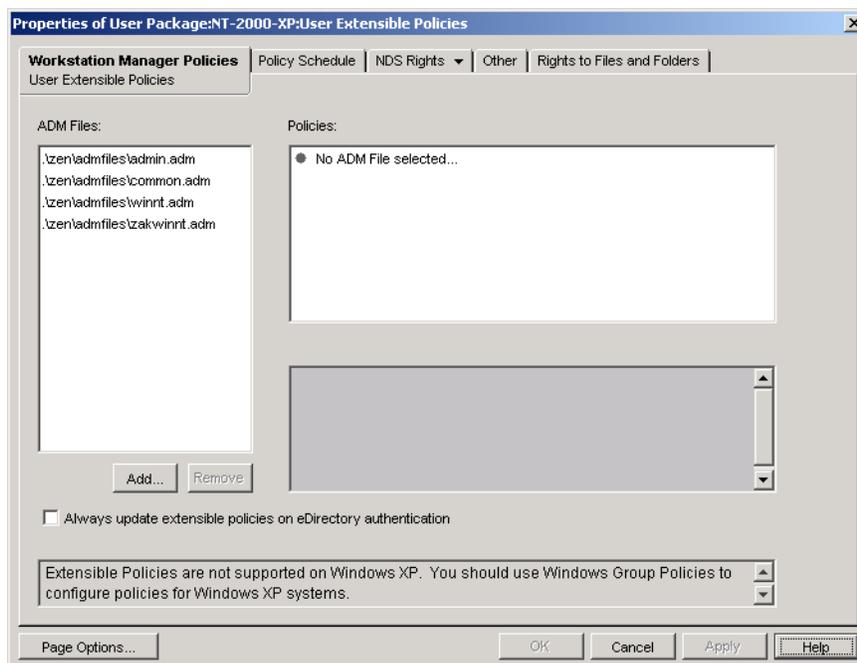
The User Extensible/Computer Extensible Policies page is divided into three areas.

- **ADM Files:** The *ADM Files* list box displays, by default, the four `.adm` files that are automatically pulled into ConsoleOne by the Desktop Management plug-in: `admin.adm`, `common.adm`, `winnt.adm`, and `zakwinnt.adm`. You can use the *Add* button to add `.adm` files for applications that you have installed using ZENworks Application Management to the list. You can use the *Remove* button to remove `.adm` files from the list. Do not manually delete an `.adm` file from its directory without first removing it in ConsoleOne from the *ADM Files* list. If you first delete the `.adm` file from the directory, registry changes that enable the policy are still in effect.

- **Policies:** When you select an `.adm` file in the *ADM Files* list box, its registry contents are displayed in the *Policies* list box. You can expand and traverse the policy tree to enable or disable each policy attribute.

- **Settings:** The policy-specific *Settings* box at the bottom right of the page displays other attribute options with check boxes that can be enabled or disabled. It can also provide fields for information entry or drop-down lists for selecting attribute options.

4 To edit the properties of a policy, click the policy in the *ADM Files* box, then browse and edit the policy settings in the *Policies* and *Settings* list boxes.

The check box states are as follows:

Check Box	State	Description
☑	Enabled	The attribute is enabled in the client. Any values you enter for it are applied.
☐	Disabled	The attribute is disabled in the client.
☐ or ☑	Ignored	The attribute is ignored (not changed in the client). If the attribute is already enabled in the client, it remains enabled. If it is already disabled in the client, it remains disabled.

5 (Optional) Select the *Always Update Extensible Policies on eDirectory Authentication* check box if you want extensible policies to be pushed when the user or workstation is authenticated.

6 Repeat Step 4 and Step 5 for each extensible policy to be added.

7 Click the *Policy Schedule* tab.
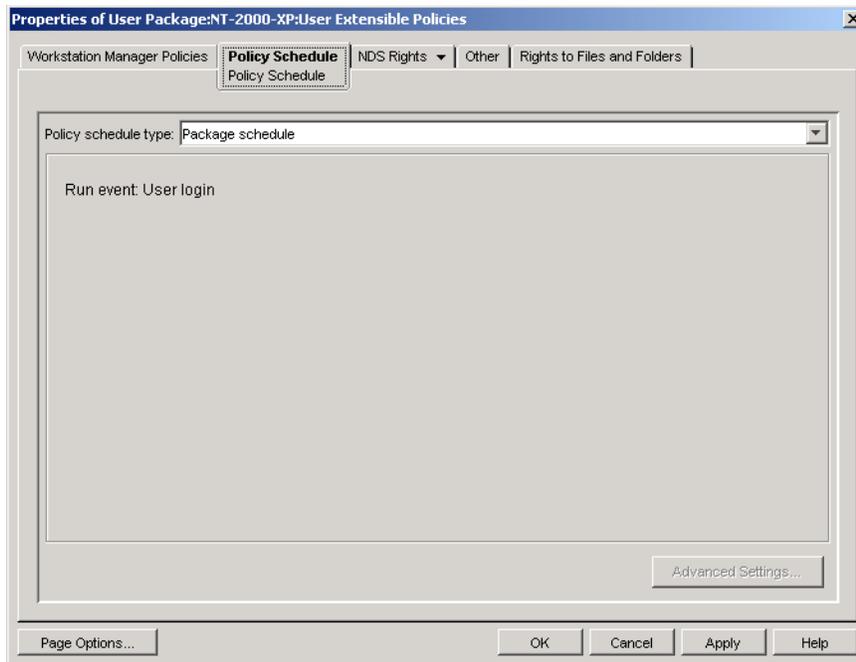
When you create an extensible policy, you must schedule it to run before it can take effect. Some hard-coded policies are run explicitly at login. Such policies are not scheduled.

8 Select a schedule type:

Package Schedule
Event
Daily
Weekly
Monthly
Yearly

Click the *Help* button on the *Schedule* tab for more information about each schedule.

For a Windows 98 User Extensible policy, even if you select *User Login* on the Policy Schedule page, the *Color Scheme* settings are not applied until the user logs out. When the user logs in again, the settings are correct. However, if you first create a user profile on the workstation under *Control Panel > Users*, the settings are applied when the user logs in the first time.

9 Click *Apply*.

Until you click Apply, policy changes are kept in a temporary location. Because of this, if two `.adm` files have the same check box item attribute (the same Windows registry entry), a change made in one `.adm` file is seen in the other.

10 Repeat Step 1 through Step 9 for each platform where you want to set a User Extensible/Computer Extensible policy.

11 When you have finished configuring all of the policies for this package, continue with the steps under Section 15.13, "Associating the User or Workstation Package," on page 216 to associate the policy package.

15.3 Dynamic Local User Policy (User Package)

A dynamic local user (DLU) is a User object that is temporarily or permanently created in the workstation's Security Access Manager (SAM) database.

A temporary user or account is known as a volatile user, and the duration is determined by the administrator. This type of account prevents the SAM from becoming too large.

If your environment has several users who log on to a shared workstation or Terminal Server, you can configure and enable the Dynamic Local User (DLU) policy. After you have configured and enabled this policy, Desktop Management dynamically creates user accounts on the local workstation or Terminal Server while the user is logging in to the system.

For Windows NT/2000/XP workstations and Windows 2000/2003 Terminal Servers, the Dynamic Local User policy lets you configure users created on Windows NT/2000/XP workstations and Windows 2000/2003 Terminal Servers after they have authenticated to the directory. After a user has been associated with a Configuration object, NetWare® Graphical Identification and Authentication (NWGINA) can retrieve information from the Configuration object to create a user account on the workstation.

If a user is not defined as a DLU and does not have an account on the workstation, the user's account cannot be created. Therefore, the user cannot log in to the workstation, unless there is a previous account, or the administrator manually creates the user's account on the workstation. If the user is not defined as a DLU, the user's credentials from the *Windows NT/2000/XP* tab of the login dialog box are used to authenticate to the workstation.

If the user is defined as a DLU, the user's credentials from the directory or from the User Package, depending on how the administrator sets it up, are used.

If you configure a DLU in a User Policy Package to administer user access to NT/2000/XP workstations or Windows 2000/2003 Terminal Servers, and if you use a credential set other than the NetWare credential set, the workstation user accounts created have a random, unknown password and are created as volatile user accounts. If volatile user caching is also enabled, the user accounts persist on the workstation for the duration of the cache life. However, these accounts are inaccessible because they have an unknown password.

If you use volatile user caching for users with non-NetWare credential sets, those user accounts are not accessible unless the users log in to the directory concurrently and have the *Manage Existing User Account* option set.

You can allow or restrict DLU login access to certain workstations by using the Login Restrictions page. Workstations and containers listed in the *Excluded Workstation* list cannot use DLU access; workstations listed or workstations that are part of containers listed in the *Included Workstations* list can use DLU access.

To properly manage group priorities, do not allow users associated with DLUs to be members of multiple groups.

To set up the Dynamic Local User policy:

1 In ConsoleOne, right-click the User Package, click *Properties*, then click the appropriate platform page.

For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2 Select the check box under the *Enabled* column for the Dynamic Local User policy.

This both selects and enables the policy.

3 Click *Properties*.
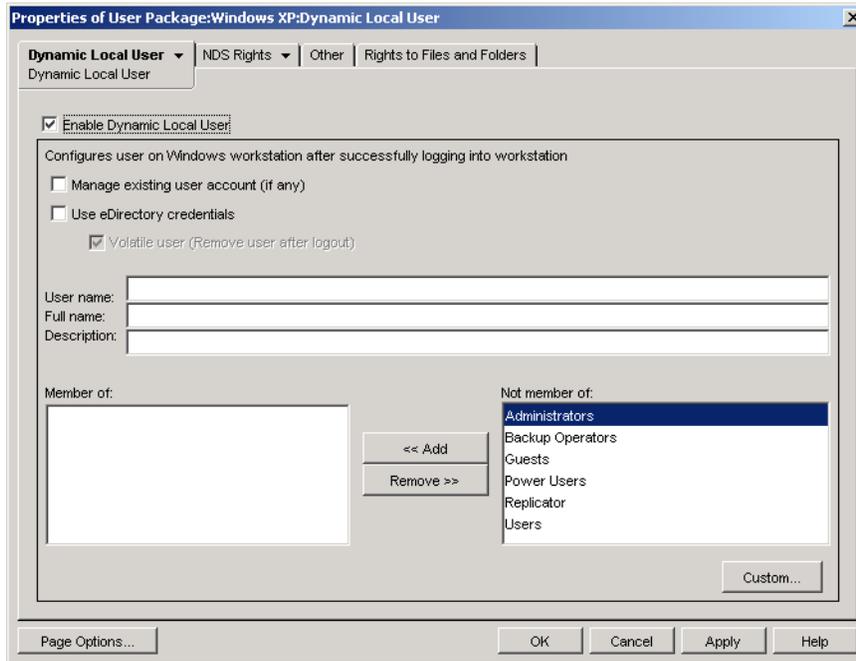
4 Fill in the fields:

Enable Dynamic Local User: Enables creation of a User object that resides either temporarily or permanently in the workstation's Security Access Manager (SAM) database.

NWGINA requires that you specify whether a local user is to be created.

If this check box is not selected, NWGINA does not create a user in the local SAM. Instead, NWGINA attempts to find an existing user with the credentials indicated in the NWGINA login interface.

If the *Enable Dynamic Local User* check box is selected, NWGINA gets the Username from the Configuration object and queries the local SAM to see if the Username already exists. If it does exist, NWGINA authenticates the user to the workstation or Terminal Server and access is granted. If the Username does not exist, NWGINA creates the user in the local workstation's or Terminal Server's SAM.

If password restriction policies are set on the local workstation or Terminal Server, Dynamic Local User is not used. The password that the DLU uses for the local account must meet local workstation password restrictions.

Manage Existing User Account (If Any): Allows management through the existing user account. Enable this option if the User object you want to manage already exists. Workstation group assignments specified by Workstation Management are implemented, including changing the account from nonvolatile to volatile when the user logs in to the account. The account is also removed from the workstation after the user logs out.

If this check box and the *Volatile User* check box are both selected, and the user has a permanent local account that uses the same credentials specified in eDirectory™, the permanent account is changed to a volatile (temporary) account. The account is managed, but is removed when the volatile user cache age is reached or the user logs out.

Any settings you change here overwrite the current account settings at the workstation or Terminal Server. If this option is not enabled, Workstation Management cannot manage the existing User object.

Use eDirectory Credentials: Enables logging in through the user's eDirectory credentials instead of NT/2000/XP credentials. When creating the user account, NWGINA can use either the same credential set used for eDirectory authentication or a predetermined credential set specified in the Configuration object. When using eDirectory credentials to create the workstation user account, NWGINA queries the user's eDirectory account for the login name, full name, and description. The password for the NT/2000/XP user account is the same as that for the eDirectory user account.

If eDirectory credentials are not used, the account is always volatile and is not accessible. F*ull Name* and *Description* can also be included to provide a complete user description.

If you don't use eDirectory credentials and the user account does not already exist (as indicated by the *Manage Existing User Accounts* check box), the user account is created as a volatile user account, which means that the user account is automatically deleted at logout. This is apparent because the *Volatile User* check box is automatically enabled if the *Use eDirectory Credentials* check box is not enabled.

Volatile User (Remove User After Logout): Specifies the use of a volatile user account for login. The user account that NWGINA creates on the local workstation can be either a volatile or a nonvolatile account.

Be aware that if you select both the *Volatile User (Remove User After Logout)* and *Manage Existing User Account (If Any)* check boxes, the volatile user account is removed when the user logs out, even if the account existed before the user logged in using DLU.

User Name: The NT/2000/XP user name. The user name (not including the context) must contain fewer than 20 characters for a dynamic local user to log in.

A user that is manually created via User Manager can't have a longer name.

Full Name: The user's full name.

Description: Enter any additional information that helps you to further identify this user account.

Member Of: Lists the groups where this user has membership. When NWGINA creates the workstation user, it can provide group membership to any user groups. The groups that the user is added to are listed in the *Members Of* list. The default configuration is for the user to be added to the Users group. Other groups can be added by selecting the group and clicking *Add*. Groups can be removed by selecting the group and clicking *Remove*.

Not Member Of: Lists available groups where this user has not been assigned as a member.

Custom: Opens the Custom Groups page, where you can add a new custom group, delete an existing custom group, and view or modify properties of an existing custom group. Click the *Help* button on the Custom Group Properties dialog box for more information about the available options.

5 (Optional) If you want to restrict DLU access to certain workstations, click the down-arrow on the *Dynamic Local User* tab > click *Login Restrictions*.
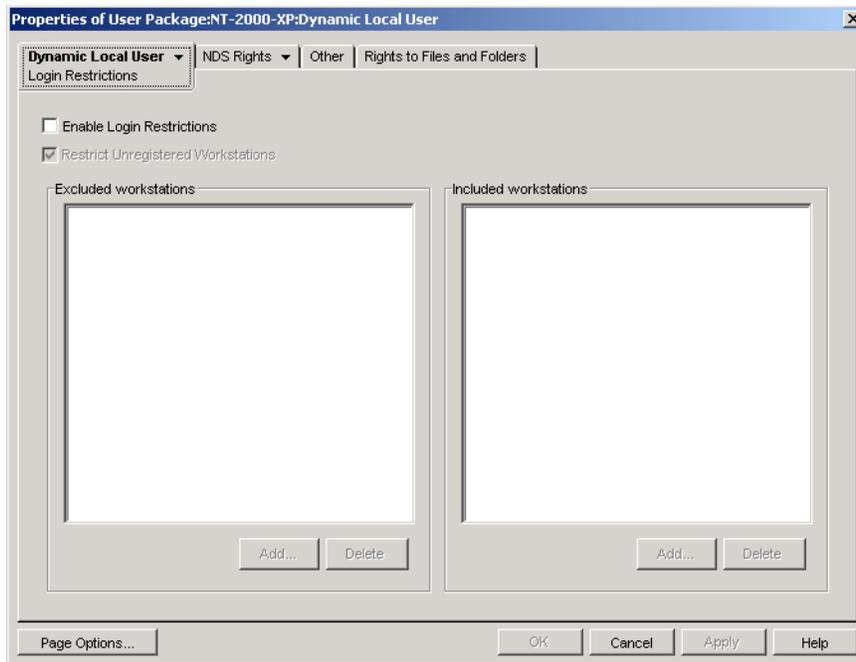
5a Select the *Enable Login Restrictions* check box to restrict DLU access to certain workstations.

When you select the *Enable Login Restrictions* check box, the *Add* and *Delete* buttons are available.

5b Select the *Restrict Unregistered Workstations* check box if you want to restrict DLU access to unregistered workstations

In previous releases of ZENworks for Desktops, workstations that had not registered in eDirectory could not be given DLU access because they could not be listed in the *Included Workstation* list. If you enable this option, all unregistered workstations cannot be granted DLU access (as in previous versions of ZENworks for Desktops). If you do not select the *Restrict Unregistered Workstations* check box, all unregistered workstations can be granted DLU access even if they do not appear in the *Included Workstations* list.

5c Use the *Add* and *Delete* buttons under the *Excluded Workstations* list box as appropriate.

The *Excluded Workstation* box lists the workstations and containers that you want to exclude DLU access to. Workstations listed or workstations that are part of containers listed in this box cannot use DLU access. You can make exceptions for individual workstations by listing them in the *Included Workstation* list. This allows DLU access to those workstations only, while excluding DLU access to the remaining workstations in the container.

5d Use the Add and *Delete* buttons under the *Included Workstations* list box as appropriate.

The *Included Workstations* box lists the workstations and containers that you want to allow DLU access to. Workstations listed or workstations that are part of containers listed in this box can use DLU access. You can make exceptions for individual workstations by listing them in the *Excluded Workstation* list. This excludes DLU access to those workstations only, while allowing DLU access to the remaining workstations in the container.

6 (Optional) Click the down-arrow on the *Dynamic Local User* tab > click *File Rights* if you want to manage DLU file system access on Windows NT/2000/XP workstations and Terminal Servers.
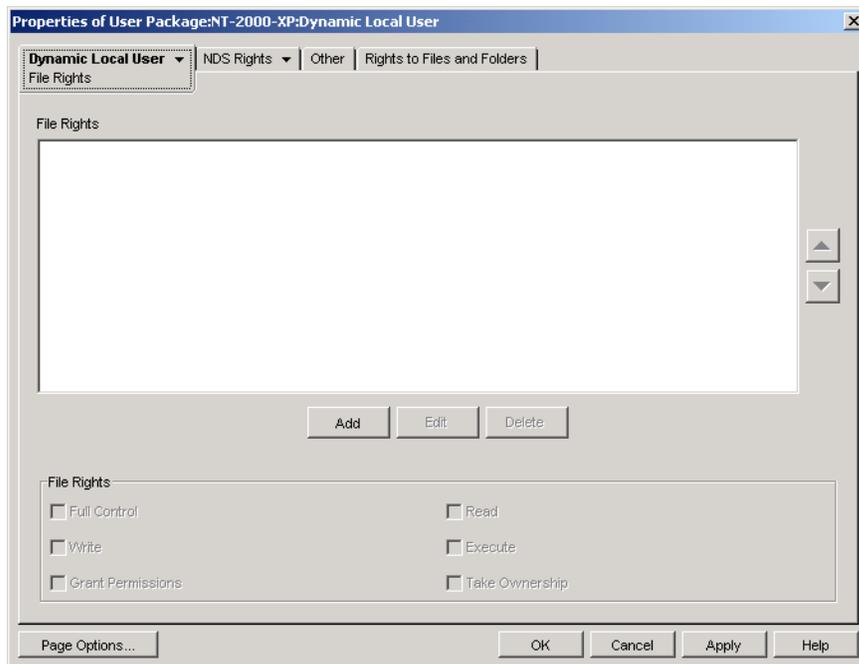
You can control access to entire directories or to individual files. For example, if the Dynamic Local User policy creates the user as a member of a group that does not give access to a directory required to run an application, you can use this page to explicitly grant the required directory rights. Or, if the user has Full Control rights to a directory, you can use this page to limit rights to any of the directory's files.

6a Use the *Add* button to modify the directories and files to which the user has been explicitly assigned file system rights.

You are prompted to enter or select the directory or file. The directory or file path must be from the perspective of the workstation or Terminal Server where the rights will be assigned. After you add a directory or file to the list, select the directory or file, then use the *File Rights* box to assign the appropriate file rights (Full Control, Read, Write, Execute, Grant Permissions, and Take Ownership).

The *File Rights* list displays the directories and files to which the user has been explicitly assigned file system rights. When you select a directory or file in the list, the assigned rights are shown in the *File Rights* box below the list. For an explanation of each of these rights (Full Control, Read, Write, Execute, Grant Permissions, and Take Ownership), refer to the Microsoft Windows operating system documentation.

6b Use the Arrow buttons on the right side of the *File Rights* list box to reposition the entries as appropriate.

Directory rights are assigned in the order the directories are listed, from top to bottom. Because of directory rights inheritance, if a directory and its subdirectory are listed, the subdirectory must be listed after its parent directory. This ensures that the subdirectory's explicitly assigned rights are not overridden by rights inherited from its parent directory.

File rights always take precedence over directory rights, regardless of their position in the list. For example, if you assign Full Control rights to the `c:\program files` directory and Read and Execute rights to the `c:\program files\sample.txt` file, the user is assigned Read and Execute rights to the file regardless of whether the file is listed before or after the directory.

It is possible to block the inheritance of rights on the NTFS files system, and under Windows XP, by default, the Windows directory does not allow rights to be inherited.

7 Click *OK* to save the policy.

8 Repeat Step 1 through Step 7 for each platform where you want to set a Dynamic Local User policy.

9 When you have finished configuring all of the policies for this package, continue with the steps under Section 15.13, "Associating the User or Workstation Package," on page 216 to associate the policy package.

15.4 Novell iPrint Policy (User and Workstation Packages)

The Novell® iPrint policy lets you configure a Novell iPrint client that can be placed on workstations. Using the Novell iPrint client, users can use the Internet to print to iPrint printers just like any other printer, regardless of the printer's physical location.

NOTE: The Novell iPrint policy is contained in both the User Package and in the Workstation Package. The information in this section applies to both packages; however, there are differences between the two packages. When you configure the Novell iPrint policy contained in the User Package, the policy applies to all associated users regardless of the workstation they use. When you configure the Novell iPrint policy contained in the Workstation Package, the policy applies to all users who log in to an associated workstation.

IMPORTANT: Unless you are running NetWare 6.5 SP2 or later, you must download the latest Novell iPrint utility file from TID 2968629 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2968629.htm). See Step 4 on page 192 for more information.

Novell iPrint ships with NetWare 6 (Support Pack 2 or newer) and Open Enterprise Server Linux, or it can be purchased separately. Novell iPrint also runs on NetWare 5.1 (Support Pack 5 or newer). The Novell iPrint policy in Desktop Management replaces all previous ZENworks printer policies. If you are upgrading from a previous version of ZENworks for Desktops and are running previous printer policies, Desktop Management supports them. For further information about iPrint, see the iPrint Product Web page (http://www.novell.com/products/netware/printing/index.html).

In order to use the Novell iPrint policy, be aware of the following:

- **NetWare/Open Enterprise Server Linux:** To use the iPrint client, you must have at least one NetWare or Open Enterprise Server Linux server in your system. If you choose to not use the iPrint client, you can still use your existing Microsoft printing setup outside of Desktop Management.

- **Desktop Management Agent:** You must also install the Desktop Management Agent on each workstation where you want to run the iPrint client; the policy does not run on a workstation that uses only the Novell Client.

- **Using the Novell iPrint Policy for the Windows NT/2000/XP Platforms Contained in the User Package:** If you configure the Novell iPrint policy as part of a User package to be pushed to Windows NT/2000/XP workstations, you must change the *AllowUserPrinters* value in the `iprint.ini file` (refer to Step 4 on page 192 for the default location of the `iprint.ini` file) from the default value of 0 to 1.

- **Using the Novell iPrint Policy in Conjunction with the Dynamic Local User or Windows Desktop Preferences Policies:** If you are managing user profiles using the Dynamic Local User or Windows Desktop Preferences policy, you must rename the native Microsoft Internet Print Provider (`inetpp.dll`) registry reference. Renaming this registry reference ensures that user profiles are properly closed or deleted when users log out. If user profiles remain open, when users log back in to workstations, the profile remains locked, causing multiple user accounts to be created.

  To prevent this situation, you should change the following registry value:

  `HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Print\Providers\Internet Print Provider\Name`

  from `inetpp.dll` to `inetpp.old`.

You can also use ZENworks Application Management to deliver the iPrint client to users' workstations. For more information, see Chapter 28, "Distribution: Simple Applications," on page 321. If you choose to distribute the iPrint client with a simple Application object, follow the instructions under Path to the Novell iPrint Client Install in Step 4 on page 192 to make sure that the iPrint client install file (`nipp-s.exe`) is in its own directory location on your server.

To set up the Novell iPrint policy:

1 In ConsoleOne, right-click the User Package or Workstation Package, click *Properties*, then click the appropriate platform page.

> **NOTE:** For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2 Select the check box under the *Enabled* column for the Novell iPrint policy.

This both selects and enables the policy.

3 Click *Properties* to display the Client Install page.
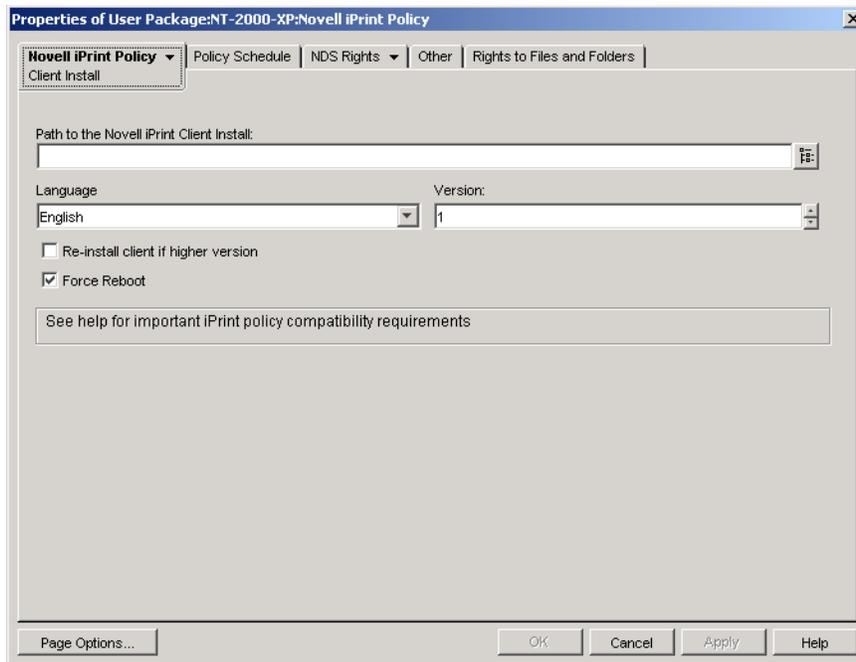
4 Fill in the fields:

Path to the Novell iPrint Client Install: Specify the path to the iPrint client install file (`nipp-s.exe`). This file must be the only file in its own directory location on your server. Make sure that users have rights to this directory.

Unless you are running NetWare 6.5 SP2 or later, you must download the latest Novell iPrint client install file from TID 2968629 in the Novell Knowledgebase (http://support.novell.com/search/kb_index.jsp?sourceidint=hdr_support_kb).

The downloadable iPrint client install file is a self-extracting utility that places the `nipp-s.exe` file and other files in the directory that it is executed in.

After the latest `nipp.exe` is extracted, copy the `nipp-s.exe` (on NetWare 6.5 SP 2 it is already extracted to `sys:\apache2\htdocs\ippdocs`) to an empty directory where users have rights. For example, create an iprint directory under `sys:\login` and then copy the file to `sys:\login\iprint\`.

Language: Select a language from the drop-down list. If you are using the latest Novell iPrint client install file, the language that is installed is detected automatically, based on the configuration of the workstation. The English language is the default. If you push the iPrint client to a workstation that is configured for a non-localized language (Japanese, for example), the English version of the iPrint client is installed.

Version: Specify a version number for this iPrint policy. The version number you provide in this field does not reflect the actual version of the iPrint client. If you want to force a new iPrint policy to workstations or users to upgrade the iPrint client, you should increment the version number (from 1 to 2, for example). This version number is stored in the Windows registry. If the version number stored in the registry is lower than the number in the *Version* field, the iPrint client is installed if the *Re-install client if higher version* check box is selected.

Re-install client if higher version: Select this check box to re-install the iPrint client if the iPrint client listed in the *Path to the Novell iPrint Client Install* is newer than that installed on the workstation.

Force Reboot: Enable this option to force a reboot on each workstation after the iPrint client has been installed. We recommend that you use the default setting (enabled) for this option. You should use the default setting if you are performing a silent install after working hours. Also, you should use the default setting to avoid possible errors if you should uninstall the iPrint client from a workstation or reinstall the iPrint client to a workstation.

5 Click the down-arrow on the *Novell iPrint Policy* tab > click *Settings*.
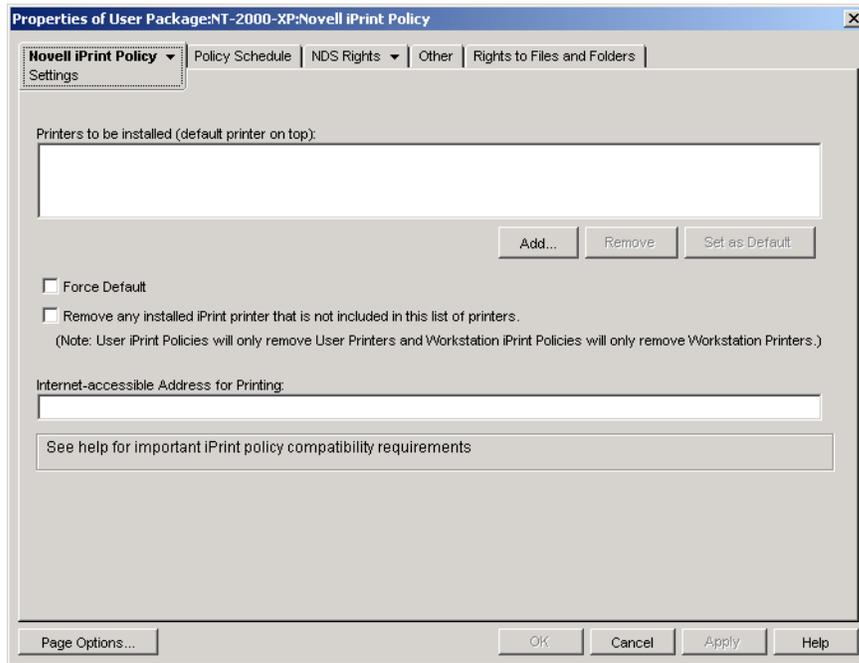
6 Click *Add* to browse to a printer to add to the *Printers to be installed* list box.

or

Select a printer to be removed from the *Printers to be installed* list box, then click *Remove*.

Depending on users' driver signing settings, user workstations might display a "This driver is not digitally signed" message when the printer is installed. If you do not want users to see this message and be forced to choose to install the driver, you can change this setting in the Control Panel of each workstation (*Start > Settings > Control Panel > System > Hardware > Driver Signing*) or you can change this setting using a Windows Group policy in Desktop Management.

7 To select a default printer, select a printer in the *Printers to be installed* list box, then click *Set as Default*.

The user can also select another printer to use as the default.

8 Select the *Force Default* check box to force the selection of the default printer.

If a user changes the default printer, the default printer that you choose is set as the default each time this policy is run, according to its schedule.

The *Force Default* printer setting can only be set when a user is logged in. This setting does not work when the policy is scheduled to run at system startup.

9 (Optional) Select the *Remove any installed iPrint printer that is not included in this list of printers* check box.

If you selected the *Re-install client if higher version* check box in step Step 4 on page 192, any iPrint printers that were pushed by a previous version of the Novell iPrint policy to the workstation are removed, unless they are listed in the *Printers to be installed* list box.

Consider the following platform-specific information about using the *Remove any installed iPrint printer that is not included in this list of printers* check box:

* **Windows NT/2000/XP and Windows 2000/2003 Terminal Servers Platforms Contained in the User Package:** For the Windows NT/2000/XP platforms and Windows 2000/2003 Terminal Servers, if you are configuring the Novell iPrint policy contained in the User Package, enabling this option removes only those iPrint printers that were pushed to the workstation or Terminal Server using the Novell iPrint policy in the User Package.

* **Windows NT/2000/XP Platforms Contained in the Workstation Package:** For the Windows NT/2000/XP platforms, if you are configuring the Novell iPrint policy contained in the Workstation Package, enabling this option removes only those iPrint printers that were pushed to the workstation using the Novell iPrint policy in the Workstation Package. Additionally, if you enable this option in the Novell iPrint policy contained in the Workstation Package, and if the user of that workstation is locked down, that user does not have sufficient rights for that iPrint printer to be removed.

* **Windows 9x Platform in the User or Workstation Package:** For the Windows 9*x* platform, if you are configuring the Novell iPrint policy contained in either the User Package or the Workstation Package, the printers are installed as workstation printers, regardless of which type of package they were installed from. Enabling this option removes any iPrint printers that were pushed to the workstation using the Novell iPrint policy in either package.

10 (Optional) If you have workstations that are physically located outside the firewall, use the *Internet accessible Address for Printing* field to specify the proxy, firewall, or Network Address Translation (NAT) address followed by a colon (:) and the port number.

If you have workstations outside the firewall and they use Novell iPrint printers, you must open port 631. If you have workstations outside the firewall and they use secure printers that are not Novell iPrint printers, you must open port 443 (the standard port number for secure printers coming through a firewall).

If workstations are not located outside of the firewall, you should leave this field empty.

If you are using NetWare 6.5 and have workstations outside of the firewall, you must have a server proxy set up in order to use the Novell iPrint policy.

11 (Optional) Click the Policy Schedule page to schedule the Novell iPrint policy.

If you configure the Novell iPrint policy as part of a Workstation Package and schedule the package to run at system startup, the iPrint policy runs; however, printers cannot be pushed at system startup. For printers to be pushed to the workstation, a user must be logged in to the workstation. This is not an issue if you configure the Novell iPrint policy as part of a User Package because you cannot schedule User Package policies to run at system startup.

If you normally schedule Workstation Packages to run at system startup, you should create a schedule for the iPrint policy to run at user login or some other time when the user is logged in to the workstation. If you schedule an iPrint policy in a Workstation Package to run at user login, make sure that the *Impersonation* remains at the default: *System Impersonation* (*Advanced Settings > Impersonation*). If you set the policy to run at user login and interactive user, the policy fails to run.

12 Click *OK* to save the policy.

13 Repeat Step 1 through Step 12 for each platform where you want to set a Novell iPrint policy.

14 When you have finished configuring all of the policies for this package, continue with the steps under to associate the policy package.

NOTE: On Windows 98, the iPrint client installation applies to all user profiles on the workstation. If you set up different user profiles on a Windows 98 workstation before installing the iPrint client, *Novell iPrint Client* appears on the default user's Start Menu rather than on the logged-in user's Start Menu. For this reason, if you want to uninstall the iPrint client from a Windows 98 workstation using the *Novell iPrint Client Uninstall* option on the Start Menu, you need to log in as the default user. On Windows NT/2000/XP workstations, after installation of the iPrint client, *Novell iPrint Client* appears on the logged in user's Start menu.

15.5 Remote Control Policy (User and Workstation Packages)

Sets parameters for remote management sessions. This policy is available on each of the platform pages. For more detailed information, see .

15.6 Scheduled Action Policy (User and Workstation Packages)

The Scheduled Action policy sets up schedules for specific actions that you specify. As many as 15 items can be placed in an action.

NOTE: The Scheduled Action policy is contained in both the User Package and in the Workstation Package. The information in this section applies to both packages; however, there are differences between the two packages. When you configure the Scheduled Action policy contained in the User Package, the policy applies to all associated users regardless of the workstation they use. When you configure the Scheduled Action policy contained in the Workstation Package, the policy applies to all users who log in to an associated workstation.

Because scheduled actions do not apply to Terminal Server sessions, the Add button has been disabled on the Windows 2000-2003 Terminal Server, Windows 2000 Terminal Server, and Windows 2003 Terminal Server platform pages. Only those policies that are run before the Terminal Server's desktop is started apply to Terminal Server sessions.

The Scheduled Action policy is a plural policy, meaning it can be added many times to the policy package. Plural policies allow you to have multiple instances of the same policy type within the same policy package.

Because you can have several different actions that you might want to run on different schedules, when you add a Scheduled Action policy to the policy package you should name it to reflect the action being scheduled.

The Scheduled Action policy is available for each of the platform pages.

To set up the Scheduled Action policy:

1 In ConsoleOne, right-click the User Package or Workstation Package, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the General page.

For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2 To add the Scheduled Action policy, click *Add*, give the policy a descriptive name, then click *OK*.

3 Select the check box under the *Enabled* column for the newly created Scheduled Action policy.

This both selects and enables the policy.

4 Click *Properties* to display the Actions page.
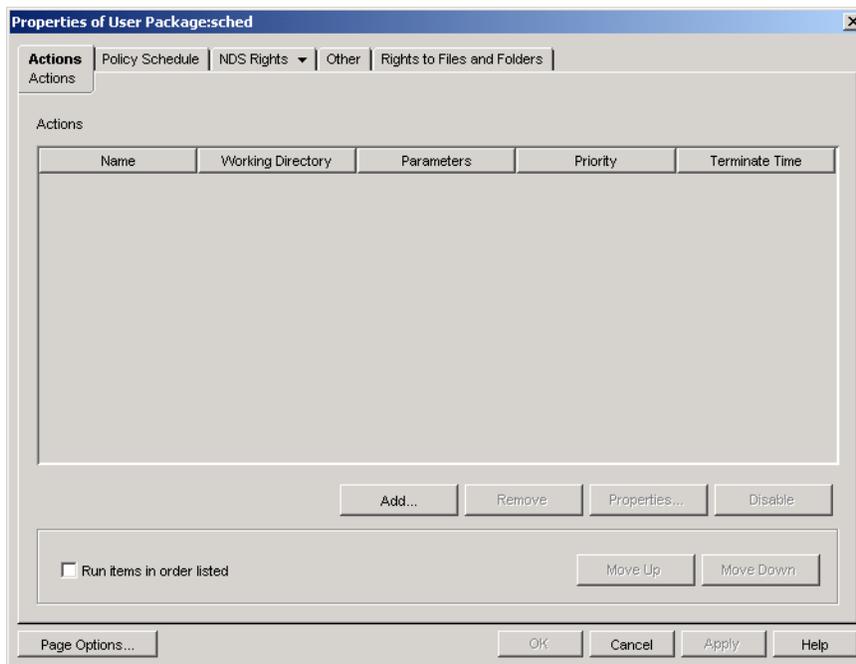
5 Click *Add*.

6 Fill in the fields:

Name: The name of the action item.

Working Directory: This is usually the path where the executable file for this action is located. It can be a different path if the program requires it.

Parameters: The parameters to pass to the action item. For more information, see the documentation associated with the executable file specified in the *Working Directory* field.

Priority: The importance assigned to this action in relation to the user's access to the workstation.

Terminate Time: The length of time this action can run before the system stops it. The assumption is that if it takes longer than a specified time to run, there might be a problem associated with running this action and the action should be terminated.

7 Click *OK*.

8 Select the *Run items in order listed* check box if you want the items to run in the order they display in the list. You can reorder the list with the *Move Up* and *Move Down* buttons.

9 Click the *Policy Schedule* tab.
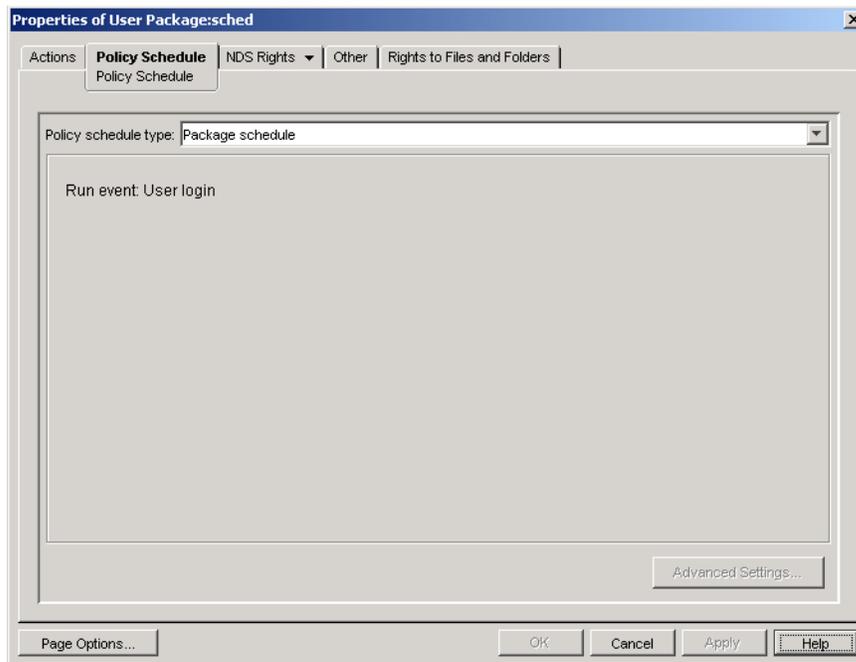
10 Select a schedule type:

Package schedule
Event
Daily
Weekly
Monthly
Yearly

Click the *Help* button on the Schedule tab for more information about each schedule.

If you select the *Event* schedule type and then select *User Logout* or *System Shutdown*, some actions cannot occur before the user is logged out or the system shuts down. If actions that are scheduled at user logout or system shutdown do not function as expected, try changing the schedule to another event.

11 Click *OK* to save the policy.

12 Repeat Step 1 through Step 11 for each platform where you want to set a Scheduled Action policy.

13 When you have finished configuring all of the policies for this package, continue with the steps under Section 15.13, "Associating the User or Workstation Package," on page 216 to associate the policy package.

15.7 User Extensible Policies (User Package)

For information about User Extensible policies, see Section 15.2, "Computer/User Extensible Policies (Workstation/User Packages)," on page 180.

15.8 Windows Desktop Preferences Policy (User Package)

Allows you to enable roaming profiles and apply desktop settings.

When a user logs on to a Windows 2000/XP workstation for the first time, Windows creates a user profile: a data file associated with that user containing information that defines customized desktop environments, which include individual display settings, network and printer connections, and other specified settings. The user profile maintains the desktop settings for each user's work environment on the local computer.

According to information on the Microsoft Web site about user profiles (http://www.microsoft.com/windows/windows2000/en/advanced/help/sag_UPconcepts_1.htm), there are three types of user profiles:

- **Local user profile:** A local user profile is created the first time a user logs on to a computer and is stored on a computer's local hard disk. Any changes made to the local user profile are specific to the computer where the user made the changes.

- **Roaming user profile:** A roaming user profile is created by the system administrator and is stored on a server. This profile is available every time a user logs on to any computer on the network. Changes made to the user's roaming user profile are updated on the server. For more information on creating a roaming profile in ZENworks, see Section 15.8.1, "Setting Up the Windows Desktop Preferences Policy in ConsoleOne," on page 198.

  Normally, a user profile works on just one workstation or Terminal Server, but a roaming profile follows the user regardless of where the user logs in, so each network workstation or Terminal Server where the user logs in always has the same appearance. If the applications are stored on the network, the user also has access to the same applications.

- **Mandatory user profile:** A mandatory user profile is a roaming profile that can be used to specify particular settings for individuals or an entire group of users. Only system administrators can make changes to mandatory user profiles.

You can enable a roaming profile or a mandatory profile and specify where the profile is to be stored. How changes to that profile are handled depends on the profile type.

This section includes information you can use to set up Windows user profiles (called *Windows Desktop Preferences* in ZENworks) to manage the user's desktop settings:

- Section 15.8.1, "Setting Up the Windows Desktop Preferences Policy in ConsoleOne," on page 198
- Section 15.8.2, "Accommodating Roaming Profiles on a Slow Network," on page 200
- Section 15.8.3, "Setting Up a Mandatory User Profile," on page 201

15.8.1 Setting Up the Windows Desktop Preferences Policy in ConsoleOne

To set up the Windows Desktop Preferences policy:

1 In ConsoleOne, right-click the User Package, click *Properties*, then click the appropriate platform page.

For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2 Select the check box under the *Enabled* column for the Windows Desktop Preferences policy.

This both selects and enables the policy.

3 Click *Properties* to display the Roaming Profiles page.
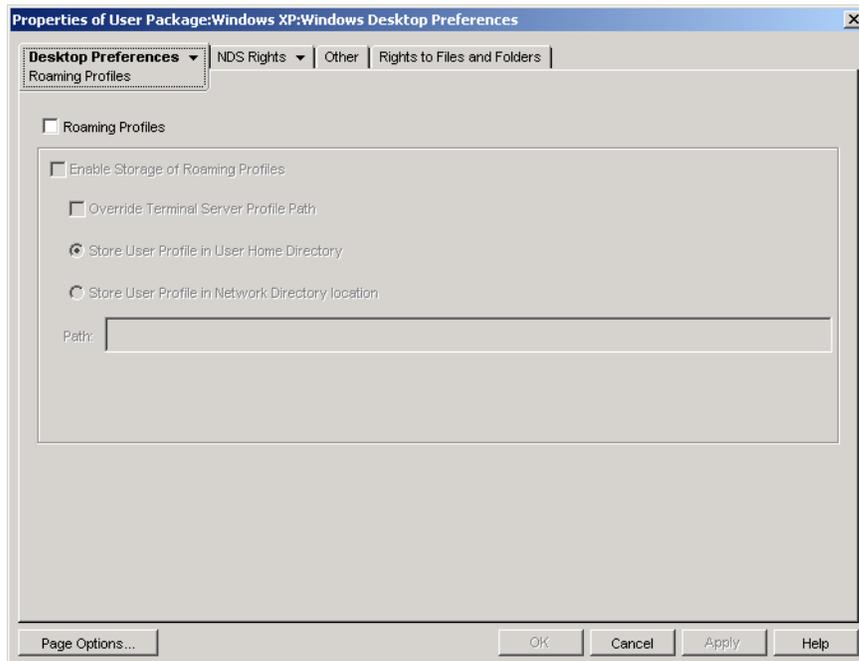
4 To enable roaming profiles, set the desired parameters in the following fields:

Roaming Profiles: Select this check box to enable roaming profiles. When you enable this check box, the other options on this page become available.

Enable Storage of Roaming Profiles: Select this check box to enable the storage of roaming profiles. This option allows profiles to be stored on a network server where they can be accessed from any workstation. Choose from the following options to specify how you want roaming profiles managed:

- **Override Terminal Server Profile Path:** If the user is accessing a Terminal Server that has its own profile, enable this option to override the Terminal Server's profile and use the roaming profile stored in the user's home directory or the profile stored in the network directory location specified in the Path field.

- **Store User Profile in User's Home Directory:** Stores the roaming profile on the network in the user's home directory. This allows the user to utilize the same desktop environment on all workstations throughout the network. Any changes made to the user's environment on one workstation are saved to the profile stored in the user's home directory on the network. The environment specified in the profile is then available on any workstation where the user subsequently logs in.

- **Store User Profile in Network Directory Location:** Stores the user profile in a network directory. When you choose this option, the user profile is stored on the network and users who have their roaming profiles pointed to this location share this profile. Any changes that users make to the profile are saved in the network directory location.

◆ **Path:** Specify the UNC path to the user's profile.

IMPORTANT: If roaming profiles are to be stored on a NetWare file system, either the Novell Client is required or CIFS needs to be installed on the NetWare server; CIFS lets workstations access the NetWare file system without needing the Novell Client.

You can store roaming profiles on a Windows server if the workstations are not running the Novell Client but are running the Microsoft SMB client.

---

5 Click the down-arrow on the *Desktop Preferences* tab, then click *Settings*.
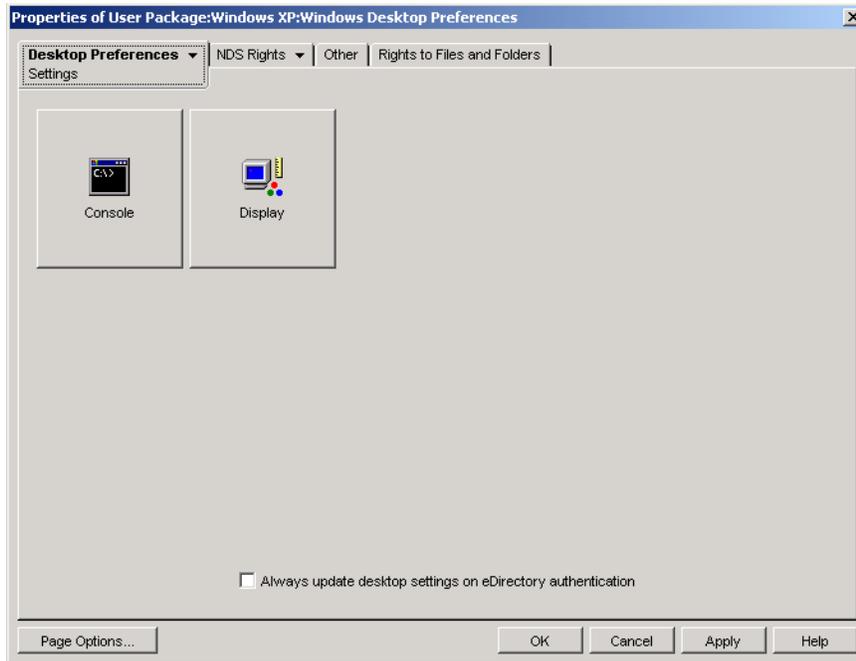
6 Click either the *Console* or *Display* button to display a dialog box that shows the options available for each feature.

This page displays icons matching the equivalent desktop features in Windows 98 or Windows NT/2000/XP.

See your Microsoft Windows documentation for help on these features and their options.

7 (Optional) Select the *Always update desktop settings on eDirectory authentication* check box.

8 Click *OK* to save the policy.

9 Repeat Step 1 through Step 8 for each platform where you want to set desktop preferences.

10 When you have finished configuring all of the policies for this package, continue with the steps under Section 15.13, "Associating the User or Workstation Package," on page 216 to associate the policy package.

15.8.2 Accommodating Roaming Profiles on a Slow Network

In ZENworks for Desktops 4.*x*, if a slow link was detected that would require significant time to download a roaming profile, you could set registry keys to automatically download the roaming profile, use the locally stored profile, or display an instructional dialog box to let the user choose to either continue the download or to use the locally stored profile. This functionality is no longer

supported in ZENworks 7 Desktop Management. All roaming profile processing is now handled by Microsoft code.

This functionality is provided by the Microsoft native support for slow link detection. The Microsoft Group Policy Editor should now be used to configure slow link detection.

15.8.3 Setting Up a Mandatory User Profile

You can create a default mandatory user profile appropriate for the tasks that a user or a group of users performs. The mandatory user profile does not save changes to the desktop settings made by the user. Users can modify the desktop settings of the computer while they are logged on, but none of these changes are saved when they log off. The mandatory profile settings are downloaded to the local computer each time the user logs on.

A mandatory user profile is a roaming profile, following the user wherever he or she logs on. It is created in ConsoleOne using the same procedure used to create roaming profiles (see Section 15.8.1, "Setting Up the Windows Desktop Preferences Policy in ConsoleOne," on page 198) but with some important differences:

- Make sure you set the appropriate access permissions for the user or groups of users that will use this profile. This is most easily done by storing the profile in a network directory location where all users have Read rights.

- When the user profile, `ntuser.dat`, has been stored in the designated network location, rename it to `ntuser.man`. User profiles become mandatory (Read Only) when you rename them with the `.man` extension.

15.9 Windows Group Policy (User and Workstation Packages)

You can specify and edit group policies for Windows 2000/XP workstations (User and Workstation Package) and for Windows 2000/2003 Terminal Servers (User Package only).

NOTE: The Windows Group policy is contained in both the User Package and in the Workstation Package. When you configure the Windows Group policy in the User Package, the policy applies to all associated users regardless of the workstation they use. When you configure the Windows Group policy in the Workstation Package, the policy applies to all users who log in to an associated workstation.

The following sections contain additional information:

15.9.1 Understanding the Windows Group Policy

The Windows Group policy is an extension of extensible policies for Windows 2000/XP and Active Directory. There is some cross-over in policy settings between the Windows Group policy and Desktop Management extensible policies, such as under *User Configuration > Administrative Templates*. For more information about extensible policies, see Section 15.2, "Computer/User Extensible Policies (Workstation/User Packages)," on page 180.

NOTE: You should not configure group policies on a Windows 2000 Domain Controller using ConsoleOne. To edit group policies through ConsoleOne, you should use a Windows 2000 workstation to edit Windows 2000 group policies and a Windows XP workstation to edit Windows XP group policies.

If a workstation is a member of an Active Directory domain but is disconnected from the domain, Windows Group policies contained in both the User and Workstation packages do not apply.

Using ZENworks Desktop Management to distribute Group policies to workstations or users where Group policies are already distributed by Active Directory (or vice versa) is not supported because of the unpredictable behavior that occurs. ZENworks Desktop Management does support distributing Active Directory settings. For more information, see Section 15.9.5, "Importing Windows Group Policies (User and Workstation Packages)," on page 211.

For the following reasons, you must use UNC paths rather than mapped drives for importing this policy to Desktop Management:

- Users could change their login scripts, altering drive mappings
- Workstation objects are often logged in before users are, so there are no drive mappings available

With UNC paths, as long as the server is available, the policy is found.

Group policies have changed significantly since the ZENworks for Desktops 3 initial release. Review the following sections for more information:

- "Additive Group Policies" on page 202
- "Revision Checking" on page 203
- "Group Policy Caching" on page 203
- "Persistent and Volatile Settings" on page 203
- "Using Group Policies on Terminal Servers" on page 203

Additive Group Policies

Group policies are now additive. This means that settings from multiple Windows Group policies are cumulatively effective, rather than individually. Settings from multiple Windows Group policies can affect users and workstations. Policies start with the local Windows Group policy settings and are applied in reverse of the policy search order. This means that a setting in a policy applied first has lowest priority and its value is overwritten by any other policy with the same setting.

Security settings are not additive; they are set by the last effective policy.

Revision Checking

Windows Group policies now track the revision of the policies in effect. As long as the list of effective policies and their revisions remains the same, Windows Group policies are not processed, but use the cached Group policy.

NOTE: Each time the *Edit Policies* button is clicked, the revision of a Windows Group policy changes, causing the policies to be reprocessed.

Group Policy Caching

The last-processed Windows Group policy is cached locally. This helps reduce network traffic by processing Windows Group policies only if necessary. If UserA logs in on a new machine, his or her effective Group policies are processed and then cached.

If UserA logs out and UserB logs in, and if UserB has the same effective Group policies as UserA, the locally-cached Group policy is restored instead of reprocessing Windows Group policies. If the list of effective policies is different or if the revision is changed on any policy, the Windows Group policies are reprocessed.

New functionality has been added to the Desktop Management Windows Group policy implementation. The Windows Group policy settings in both the User Package and in the Workstation Package can remain in effect even when the workstation is disconnected from the network.

Persistent and Volatile Settings

The administrator determines if Windows Group policies are persistent or volatile. The persistent setting indicates that when the Windows Group policies are set, they remain set—even if a user happens to log in only to a workstation and not to the network.

The volatile setting indicates that the original local Windows Group policy settings will be restored when:

- The user logs out (the user Group policy settings are removed)
- The system shuts down (the workstation Group policy settings are removed)

Using Group Policies on Terminal Servers

You can configure Windows Group policies in a User Package for Windows 2000 and Windows 2003 Terminal Servers. You can also use the Window 2000-2003 Terminal Server platform page if you want to set policies that apply to both platforms to make managing Terminal Servers easier.

When configuring Windows Group policies for Terminal Servers, consider the following:

- **Applied Settings Types:** Only the *User Configuration* settings under *Applied Settings Types* apply to Terminal Servers. The *Computer Configuration* and *Security Settings* options are not available for Terminal Servers.
- **Logoff Scripts:** Logoff scripts are not supported in a Terminal Server environment.

15.9.2 Configuring the Windows Group Policy in the User Package

1 In ConsoleOne, right-click the User Package, click *Properties*, then click the appropriate platform page.

When choosing the appropriate platform page, take the following into account:

- **Windows NT:** For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

- **Windows NT-2000-XP platform page:** Because of the differences between Windows 2000 and Windows XP in regards to how security settings are saved, you cannot use the Windows NT-2000-XP platform page to edit the Windows Group policy. For Windows 2000, security settings are saved in the `gpttml.inf` file; for Windows XP, security settings are saved in the `xpsec.dat` file. Both files are located in the `\group policies\machine\microsoft\windows nt\secedit` directory.

  In ZENworks 7, the *Edit* option on the Windows NT-2000-XP platform page has been disabled; you must use one of the specific platform pages to edit group policies.

2 Select the check box under the *Enabled* column for the Windows Group policy.

This both selects and enables the policy.

3 Click *Properties* to display the Windows Group Policies page.

4 Specify the network location for new or existing group policies.

Make sure that users have sufficient rights to access this network location.

If you use an environment variable in the *Network location of existing/new group policies* field, you must first set the environment variable on the management workstation on which you are

running ConsoleOne and on any workstations that receive the group policy. You must also exit and restart ConsoleOne before the variable is recognized.

5 (Conditional) If you want to import group policies from Active Directory, click *Import Policy*.

For more information, see Section 15.9.5, "Importing Windows Group Policies (User and Workstation Packages)," on page 211.

6 (Conditional) If you want to edit existing group policies, click *Edit Policies*.

For more information, see Section 15.9.4, "Editing Existing Windows Group Policies (User and Workstation Packages)," on page 209.

7 (Optional) Select the *Group Policies remain in effect on user logout* check box to indicate that the pushed group policies remain in effect on the local Windows desktop after the user logs out.

IMPORTANT: We do not recommend using both the *Group policies remain in effect on user logout* settings and the *Cache User Configuration* settings in an environment in which the user Group policies are pushed to different users on common workstations.

---

8 (Optional) Select the *Cache User Configuration* check box.

Caching user configuration settings is different than enabling the *Group Policies remain in effect on user logout* check box.

Setting the *Group policies remain in effect on user logout* option enables the administrator to retain the group policy settings of the last logged-in user. The limitation with this approach is that any user who logs in locally (workstation only) receives the Group policy settings of the last person who logged in to the network on that workstation. If an administrator was the last user to log in to the network on a particular workstation, any subsequent local logins result in the user receiving the administrator's policy settings.

To avoid this situation, you can enable the *Cache User Configuration* check box to allow each user's settings to be cached.

Consider the following before you enable caching of settings in the User Package's Windows Group policy:

- The cache user settings functionality works with both NetWare or Windows on the back end. If you are using a Windows server on the back end, consider the following:
  - The user must be logged in with a local user account, not a cached domain account. Windows Group policy settings apply to domain accounts as long as the user is logging in to the domain. When the user does not log in to the domain, but uses a cached domain account, the Desktop Management Windows Group policy settings do not apply.
  - If you store Group policy files on an Active Directory server, the Active Directory username and password must match the eDirectory credentials.
- Users must have unique local user accounts. The Windows Group policy settings are cached in the local user's profile, so users with different effective Windows Group policies must have different local user accounts.
- Each user must have a profile on the machine in which to cache the settings. You can provide this profile by using local user accounts or by using Dynamic Local User (DLU) accounts; however, the account cannot be removed. If the DLU policy removes the local user account (either by a using a volatile user account or by using an expired cached volatile user account), the user cannot log in locally.
- Only the settings contained in the `\user\registry.pol` file are cached. This is roughly equivalent to the *User Settings* in the Group Policy editor with the exception of

the logon/logoff scripts (they are stored in the Scripts folder under \user, and therefore not cached).

Selecting the *Cache User Configuration* check box causes the user configuration settings of each user's effective Windows Group policies to be stored in each user's local profile. When each user logs in locally, the user settings are read from the cached copy of the registry.pol in that user's profile and are applied. The only settings cached are those stored in the registry.pol file in the \user folder. Other settings are not cached, including logon/logoff scripts, computer settings, and security settings.

> **IMPORTANT:** We do not recommend using both the *Group Policies remain in effect on user logout* settings and the *Cache User Configuration* settings in an environment in which the user Group policies are pushed to different users on common workstations.

9 In the *Applied Settings Types* group box, enable the desired options.

These options allow Windows user, computer, and security settings to be pushed with a User or Workstation policy. This differs from earlier releases in which user settings were pushed with User Packages and computer and security settings were pushed with Workstation Packages.

User Configuration: Select to push settings under *User Configuration* with the Windows Group policy.

Computer Configuration: Select to push settings under *Computer Configuration* (except *Security Settings*) with the Windows Group policy.

Security Settings: Select to push Windows security settings with the Windows Group policy. Selecting this option applies all security settings under *Computer Configuration > Windows Settings > Security Settings*, including *Account Policies*, *Local Policies*, *Public Key Policies*, and *IP Security Policies on Local Machine*. You cannot choose to push individual policies and policies are not additive.

Only the *User Configuration* settings under *Applied Settings Types* apply to Terminal Servers. The *Computer Configuration* and *Security Settings* options are not available for Terminal Servers.

10 Click the *Policy Schedule* tab > select a schedule type:

Package Schedule
Event
Daily
Weekly
Monthly
Yearly

You can click *Advanced Settings* to set additional settings such as *Completion*, *Fault*, *Impersonation*, *Priority*, and *Time Limit*. For detailed information on each of these settings, click the *Help* button on each page.

11 Click *OK* to save the policy.

12 When you have finished configuring all of the policies for this package, continue with the steps under Section 15.13, "Associating the User or Workstation Package," on page 216 to associate the policy package.

15.9.3 Configuring the Windows Group Policy in the Workstation Package

1 In ConsoleOne, right-click the Workstation Package, click *Properties*, then click the appropriate platform page.

When choosing the appropriate platform page, take the following into account:

- **Windows NT:** For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

- **Windows NT-2000-XP platform page:** Because of the differences between Windows 2000 and Windows XP in regards to how security settings are saved, you cannot use the Windows NT-2000-XP platform page to edit the Windows Group policy. For Windows 2000, security settings are saved in the `gpttml.inf` file; for Windows XP, security settings are saved in the `xpsec.dat` file. Both files are located in the `\group policies\machine\microsoft\windows nt\secedit` directory.

  In ZENworks 7, the *Edit* option on the Windows NT-2000-XP platform page has been disabled; you must use one of the specific platform pages to edit group policies.

2 Select the check box under the *Enabled* column for the Windows Group policy.

This both selects and enables the policy.

3 Click *Properties* to display the Windows Group Policies page.

4 Specify the network location for new or existing group policies.

Make sure that users have sufficient rights to access this network location.

If you use an environment variable in the *Network location of existing/new Group Policies* field, you must first set the environment variable on the management workstation on which you

are running ConsoleOne and on any workstations that receive the group policy. You must also exit and restart ConsoleOne before the variable is recognized.

5 (Conditional) If you want to import group policies from Active Directory, click *Import Policy*.

For more information, see .

6 (Conditional) If you want to edit existing group policies, click *Edit Policies*.

For more information, see .

7 (Optional) Select the *Persist workstation settings* check box.

Selecting this option specifies that all workstation settings that Desktop Management supports (user, machine, and security settings) in the Workstation Package's Windows group policy can remain in effect (are cached) regardless of network connectivity.

Consider the following before you enable caching of settings in the Workstation Package's Windows group policy:

  ◆ The persistent workstation settings functionality works with both NetWare or Windows on the back end. If you are using a Windows server on the back end and you store Windows Group policy files on a Windows server, the workstation must be a member of that domain.

  ◆ In order to use persistent workstation settings, you cannot enable the *Group Policy LoopBack Support* option in the Windows Group policy associated to the workstations for which you want to cache settings (this includes either the *Replace Mode* or the *Merge Mode* options). By not enabling loopback support, the configuration in the user's policy always takes precedence over the configuration in the Workstation Package's Windows Group policy if conflicting settings exist.

Selecting the *Persist Workstation Settings* check box causes the workstation's effective Windows Group policy settings that are already stored in `windows_directory\system32\group policy.wkscache` to be applied, even if that workstation is unable to log in to the network as the Workstation object (for example, when the workstation is disconnected from the network).

8 In the *Applied Settings Types* group box, enable the desired options.

These options allow Windows user, computer, and security settings to be pushed with a User or Workstation policy. This differs from earlier releases in which user settings were pushed with User Packages and computer and security settings were pushed with Workstation Packages.

User Configuration: Select this option to push settings under *User Configuration* with the Windows Group policy.

Computer Configuration: Select this option to push settings under *Computer Configuration* (except *Security Settings*) with the Windows Group policy.

Security Settings: Select this option to push Windows security settings with the Windows Group policy. Selecting this option applies all security settings under *Computer Configuration > Windows Settings > Security Settings*, including *Account Policies*, *Local Policies*, *Public Key Policies*, and *IP Security Policies on Local Machine*. You cannot choose to push individual policies and policies are not additive.

9 (Optional) Select the *Group Policy Loopback Support* check box, then select a mode.

Enabling this option gives precedence to Workstation Package policies over User Package policies. Loopback support has two modes, replace and merge:

Don't Apply User's Policy Settings (Replace Mode): Select this option to ignore all User policy settings; Workstation policy settings are applied.

Apply Workstation's Policy Settings Last (Merge Mode): Select this option to apply User policy settings first and then Workstation policy settings. This lets you apply user settings but override conflicting settings with workstation settings. If a user setting does not conflict, it remains in effect.

10 Click the *Policy Schedule* tab > select a schedule type:

Package Schedule
Event
Daily
Weekly
Monthly
Yearly

Because the Windows desktop files finish loading before group policy settings are loaded, some group policies in the Workstation Package might exhibit odd behavior if they are scheduled to run at user login. Specifically, any changes to desktop settings (for example, hide My Network Place, hide all icons on desktop, etc.) do not occur, and programs won't run if you have scheduled them to run at user login through use of a login script. If the user logs off and back on, the settings display correctly.

To prevent this behavior, do not configure group policies in the Workstation Package to run at user login. Instead, configure them to run at system startup, on a daily basis, or on some other regular schedule.

If you configure group policies to run startup scripts and you schedule those policies to run at system startup, you should select the *Persist Workstation Settings* option in Step 7 on page 208. Because Windows 2000/XP looks for and runs startup scripts before Workstation Manager authenticates and applies policies, group policies that you configure to run startup scripts might fail to run when scheduled to run at system startup. If you select the *Persist Workstation Settings* option, the Workstation Package group policy settings (and startup scripts) are cached and can be applied correctly at the next system startup.

You can click *Advanced Settings* to set additional settings such as *Completion*, *Fault*, *Impersonation*, *Priority*, and *Time Limit*. For detailed information on each of these settings, click the *Help* button on each page.

11 Click *OK* to save the policy.

12 When you have finished configuring all of the policies for this package, continue with the steps under Section 15.13, "Associating the User or Workstation Package," on page 216 to associate the policy package.

15.9.4 Editing Existing Windows Group Policies (User and Workstation Packages)

1 In ConsoleOne, right-click the User or Workstation Package, click *Properties*, then click the appropriate platform page.

2 Select the check box under the *Enabled* column for the Windows Group policy.

This both selects and enables the policy.

3 Click *Properties* to display the Windows Group Policies page.

4 Specify the network location for new or existing group policies.

5 Click *Edit Policies*.

When you click the *Edit Policies* button, the Microsoft Management Console editor is launched, where you can edit a User Package policy or a Workstation Package policy. For more information, click *Help* in the dialog boxes. After you have finished editing the policy, click the *Close* button.

When you edit group policies, be aware of the following:

 - **Directory Path:** Make sure you have selected the correct directory path because you could destroy data. All of the files in the selected directory as well as the \adm, \user, and \machine subdirectories are deleted before the Active Directory group policy is copied to it.

   NOTE: If the Network Location of Existing/New Group Policies path is set to a Linux file server, permission must be set from a Linux machine to allow read rights for users and workstations.

 - **Security Settings that Cannot be Edited in Windows XP:** Because of changes in Windows XP, you cannot currently edit the following Windows XP Security settings using Desktop Management:

   - Under *Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy*:

     Password Must Meet Complexity Requirements
     Store Password Using Reversible Encryption

   - Under *Security Settings > Local Policies > Security Options*:

     Network Access: Allow Anonymous SID/Name Translation
     Accounts: Administrator Account Status
     Accounts: Guest Account Status

 - **Operating System Version and Service Pack Level Checking in ZENworks 7:** New functionality has been added to ZENworks 7 to check the operating system version and service pack level while editing group policies on all platforms on which you can edit group policies (Windows 2000, Windows XP, and Windows Server 2003). For example, if a group policy was created on a Windows XP SP1 or earlier workstation and you attempt to edit it on a Windows XP SP2 workstation, ZENworks displays a warning dialog box. ZENworks also prohibits you from editing a group policy that was created on a Windows XP SP2 workstation if you are using a workstation with either Windows XP or Windows XP SP1 installed.

 - **Disabling Group Policy Settings using ZENworks 7:** In ZENworks 7, new functionality has been included to let you disable certain group policy settings without preventing future editing of the policy.

   In previous versions of ZENworks, disabling certain settings disabled the group policy editor, preventing you from editing that policy in the future. These settings include the following (depending on the OS and service pack level, not all settings might be present):

   - Under *User Configuration > Administrative Templates > Windows Components > Microsoft Management Console*:

     Restrict the user from entering author mode
     Restrict users to the explicitly permitted list of snap-ins

◆ Under *User Configuration > Administrative Templates > Windows Components > Microsoft Management Console > Restricted/Permitted Snap-ins > Group Policy*:

  Group Policy Management
  Group Policy Object Editor

◆ Under *User Configuration > Administrative Templates > Windows Components > Microsoft Management Console > Restricted/Permitted Snap-ins > Group Policy > Group Policy snap-in extensions*:

  Administrative Templates (Computers)
  Administrative Templates (Users)
  Folder Redirection
  Internet Explorer Maintenance
  Remote Installation Services
  Scripts (Logon/Logoff)
  Scripts (Startup/Shutdown)
  Security Settings
  Software Installation (Computers)
  Software Installation (Users)
  Wireless network (IEEE 802.11) Policies

If you disable any of these settings and then attempt to edit the policy, an error message displays stating that the snap-in has been restricted by policy. In addition, the group policy editor does not open.

To avoid this problem in ZENworks 7, these settings are removed from the group policy and saved in a temporary local location. When you close the editor, the settings in the temporary file are merged with the settings in the newly configured group policy. If you made any changes to these settings while using the editor and they conflict with those settings that were saved in the temporary file, the new settings take precedence over the original settings that were moved to the temporary file.

6 Click *OK* to save the policy.

15.9.5 Importing Windows Group Policies (User and Workstation Packages)

1 In ConsoleOne, right-click the User or Workstation Package, click *Properties*, then click the appropriate platform page.

2 Select the check box under the *Enabled* column for the Windows Group policy.

This both selects and enables the policy.

3 Click *Properties* to display the Windows Group Policies page.

4 Specify the network location for new or existing group policies.

5 If you want to import group policies from Active Directory, click *Import Policy*, then fill in the fields.

  5a Select an import option:

  Import Whole Active Directory Folder: Lets you import all group policies in the Active Directory folder. If you select this option, use the *Source Location* field to specify the UNC path to the folder containing group policies created by Active Directory that you want to migrate to the directory listed in the *Destination location of migrated group policies* field. You must know or browse for the Unique Name of the directory from where

you import the Active Directory group policy. You can find the Unique Name by examining the properties of the Active Directory Group policy.

Import Security Settings: Lets you import security settings from a file. If you select this option, use the *Source Location* field to specify the UNC path to the file containing the security settings created by Active Directory that you want to migrate to the directory listed in the *Destination location of migrated group policies* field. You must know or browse for the Unique Name of the file that you import into the group policy.

Imported security settings let administrators set only certain security settings without affecting all remaining security settings. Security settings can be imported from an Active Directory Group policy or can be created with the Security Templates snap-in in the Microsoft Management Console (MMC). For more information, see "Creating Security Settings Using the Security Templates Snap-In in the Microsoft Management Console (MMC)" on page 212.

When you import an Active Directory Group policy containing security settings or import a security settings file, the imported settings are saved in a new file called `zensec.inf.`

The security settings in `zensec.inf` are used instead of the regular security settings displayed when editing the Group policy in MMC. The security settings shown in MMC are not accurate and any changes made are not applied. If imported security settings are detected while editing a Group policy, a message box informs the user that the security settings in `zensec.inf` will be used in place of the regular security settings and give the user the option of displaying the settings in the `zensec.inf` file.

IMPORTANT: You should use UNC paths rather than mapped drives for group policies.

5b Click *Import*.

This copies the Active Directory group policy or file to the directory specified in the Destination Location of Migrated Group Policies field. If the specified directory does not exist, it is created.

WARNING: Make sure you have selected the correct directory path in the Destination Location of Migrated Group Policies field because you could destroy data. All of the files in the selected directory as well as the `\adm,` `\user,` and `\machine` subdirectories are deleted before the Active Directory group policy is copied to it.

---

6 Click *OK* to save the policy.

Creating Security Settings Using the Security Templates Snap-In in the Microsoft Management Console (MMC)

We recommend that you create new security settings rather than editing existing settings in the MMC. If you edit existing security settings, they might contain default settings that you do not need and might take a significant amount of time to process. You can avoid this problem by generating new settings.

NOTE: You must be logged on as an administrator or a member of the Administrators group to create security templates. Network policy settings might also prevent you from creating security templates.

To create new security settings using the Security Templates snap-in:

1 Click the *Start* button, then click *Run*.

2 Type `mmc`, then click *OK*.

3 Click *File > Add/Remove Snap-in* to display the Add/Remove Snap-in dialog box.

4 In the Standalone page, click *Add*.

5 In the Add Standalone Snap-in dialog box, click S*ecurity Templates*, click *Add*, then click *Close* to close the Add Standalone Snap-in dialog box.

6 In the Add Remove Snap-in dialog box, click *OK*.

7 (Optional) In the console tree, right-click Security Templates, click *New Template Search Path*, then select the new location.

A folder with the path of the new location appears in the console tree.

8 Right-click the folder where you want to store the new template, then click *New Template*.

9 Type a template name and description, then click *OK*.

10 In the console tree, double-click the new security template to display the security areas and navigate until the security setting you want to configure is in the right pane.

11 Double-click the security setting you want to configure, select the *Define This Policy* setting in the *Template* check box, edit the settings, then click *OK*.

15.10 Workstation Imaging Policy (Workstation Package)

Sets the parameters for imaging workstations. This policy is found on each of the platform pages. For general imaging information, see Part VI, "Workstation and Server Imaging," on page 633.

The setup procedure that is applicable to you depends on your imaging deployment strategy. For more information, see Chapter 58, "Setting Up Imaging Policies," on page 705.

15.11 Workstation Inventory Policy (Workstation Package)

Sets what hardware and software inventory data you want to view for each workstation. For more detailed information, see Part VIII, "Workstation Inventory," on page 881.

15.12 ZENworks Desktop Management Agent Policy (Workstation Package)

The ZENworks Desktop Management Agent policy lets you configure the Desktop Management Agent, which lets you use Desktop Management without using the Novell Client. The Desktop Management Agent lets users access the Desktop Management Middle Tier server using a DNS name or IP address. In order to use the ZENworks Desktop Management Agent policy, you must have the Desktop Management Agents installed; you cannot use this policy in an environment that has only the Novell Client installed. For more information, see Part I, "Understanding ZENworks 7 Desktop Management," on page 33.

To set up the ZENworks Desktop Management Agent policy:

1 In ConsoleOne, right-click the Workstation Package, click *Properties*, then click the appropriate platform page.

For more information about Desktop Management support for the Windows NT platform, see "Interoperability with Windows NT 4 Workstations" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2 Select the check box under the *Enabled* column for the ZENworks Desktop Management Agent policy.

This both selects and enables the policy.

3 Click *Properties* to display the Settings page.
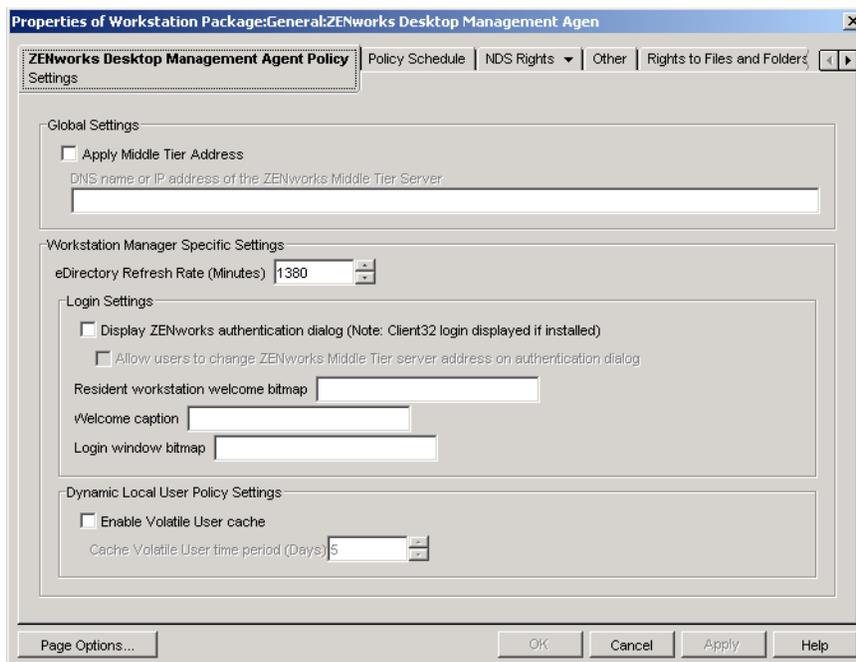
4 Select the *Apply Middle Tier address* check box, then fill in the fields:

DNS Name or IP Address of the ZENworks Management Middle Tier Server: Specify the DNS name or IP address of the Middle Tier Server.

The DNS name or IP address you specify in this location identifies the access point that all Desktop Management components (Workstation Inventory, Workstation Management, Application Management, and Remote Management) use to function outside of the firewall.

Only non-blank values are passed on to the associated workstations. If you leave the *DNS name or IP address of the Middle Tier Server* field blank, this setting is not affected on the associated workstations.

If you change the DNS name or IP address in this location, this setting is applied to all associated workstations the next time they start up. Therefore, in a clientless environment, be sure to provide adequate time for associated workstations to transition to the new DNS name or IP address before removing access to the previous location.

eDirectory Refresh Rate (Minutes): Use the arrows to set the refresh rate for eDirectory. The rate you set determines how often the agent looks for updated information in eDirectory, such as new or edited policies.

Display ZENworks Authentication Dialog: Select this check box if you want the ZENworks authentication dialog box to display during startup.

Allow Users to Change ZENworks Middle Tier Server Address on Authentication Dialog: Select this check box if you want to allow users to change the Middle Tier Server address to point to another Middle Tier Server. If this box is selected, users can click the *Options* button in the ZENworks authentication dialog box and specify another Middle Tier server's address.

Resident Workstation Welcome Bitmap: Specify the name of the bitmap file that appears on the welcome screen when you start Windows NT/2000/XP. You can specify any file located in the associated workstations' Windows NT/2000/XP directory. You can also leave this field blank if you do not want to use a bitmap.

Welcome Caption: Specify the text that appears in the header on the welcome screen when you start Windows NT/2000/XP.

Login Window Bitmap: Specify the name of the bitmap file that appears in the login window. You can specify any file located in the associated workstations' Windows NT/2000/XP directory. You can also leave this field blank if you do not want to use a bitmap.

Enable Volatile User Cache: Select this check box to enable the volatile user cache. This option allows for volatile user information that has previously been cached on a workstation to remain on the workstation for a specified period. Therefore, volatile users are not created or removed at every login or logout. This promotes faster logins for volatile users because NWGINA does not need to spend cycles re-creating the user desktop.

The Dynamic Local User (DLU) policy settings configure users created on Windows NT/2000/XP workstations after they have authenticated to eDirectory.

The cache makes it possible for a user to continue using the workstation even when the workstation is disconnected from the network and the user is not a registered user on the workstation.

Cache Volatile User Time Period (Days): Use the arrows to select how often you want to remove volatile user information. When the time limit expires and if the user has not authenticated to eDirectory within the specified time period, all volatile user information is removed from the workstation. However, if the user authenticates to eDirectory within the specified time period, the countdown begin again according to the number of days you specify using this option.

5 Click the *Policy Schedule* tab.
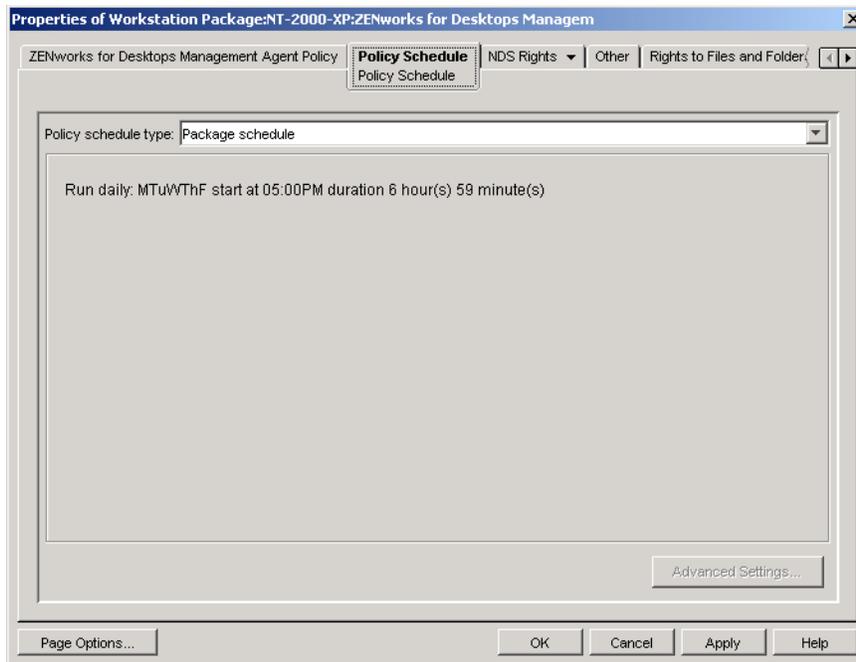
6 Select a schedule type:

Package Schedule
Event
Daily
Weekly
Monthly
Yearly

Click the *Help* button on the Schedule tab for more information about each schedule.

7 Click *OK* to save the policy.

8 Repeat Step 1 through Step 7 for each platform where you want to set a ZENworks Desktop Management Agent policy.

9 When you have finished configuring all of the policies for this package, continue with the steps under Section 15.13, "Associating the User or Workstation Package," on page 216 to associate the policy package.

15.13 Associating the User or Workstation Package

The policies you configured and enabled are not in effect until you associate their policy package with a container object.

1 In ConsoleOne, right-click the User Package or Workstation Package, then click *Properties*.

2 Click the *Associations* tab > *Add*.

3 Browse for and select the container, group, user, or workstation object for associating the package, then click *OK*.

Generating Policy Reports

16

Novell® ZENworks® 7 Desktop Management provides two predefined reports through ConsoleOne® for effective policies and policy package associations.

You can run either report based on a selected container, and you can include its subcontainers.

Report results are automatically displayed in Notepad and are saved as text files in the \temp directory of the workstation where you are running ConsoleOne.

The following sections provide information on Desktop Management reporting:

- ◆ Section 16.1, "The Effective Policies Report," on page 217
- ◆ Section 16.2, "The Package Associations Report," on page 217

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

16.1 The Effective Policies Report

The Effective Policies report shows which policies are currently in effect for the listed objects. It provides the following information:

Version
Tree
Container
Object DN
Platform
Effective Policy DN

To run a report on the effective policies:

1 In ConsoleOne, click *Tools > ZENworks Utilities > Report Policies and Packages*.

2 In the *Report From* field, browse for a context for the report.

3 To include all subcontainers in that context, click *Include Subcontainers*.

4 Click *Effective Policies Report*, then click *OK*.

The report results are displayed in Notepad and are automatically saved to \temp\effectivepolicies.txt on the user's workstation.

16.2 The Package Associations Report

The Package Associations report shows which policy packages are associated with the listed containers, subcontainers, and objects. It provides the following information:

Tree
Container
Package DN

Association

To run a report on policy package associations:

1 In ConsoleOne, click *Tools > ZENworks Utilities > Report Policies and Packages*.

2 In the *Report From* field, browse for a context for the report.

3 To include all subcontainers in that context, click *Include Subcontainers*.

4 Click *Package Association Report*, then click *OK*.

The report results are displayed in Notepad and are automatically saved to `\temp\packageassociations.txt` on the user's workstation.

Copying Policy Packages

Novell® ZENworks® 7 Desktop Management provides a utility to help you copy policy packages from one directory container to another. You can run the Copy Policy Packages utility via a ConsoleOne® snap-in or you can use a version of the utility based on Windows.

The following sections contain step-by-step instructions to help you run the Copy Policy Packages utility:

- Section 17.1, "Using the ConsoleOne Copy Policy Packages Utility," on page 219
- Section 17.2, "Using the Windows Copy Policy Packages Utility," on page 219

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

17.1 Using the ConsoleOne Copy Policy Packages Utility

The Copy Policy Packages utility can be run via a ConsoleOne snap-in. The snap-in consists of the `zencopypol.jar` and `zencopypolreg.jar` files.

To run the Copy Policy Packages utility from ConsoleOne:

1 In ConsoleOne, click *Tools* > *ZENworks Utilities* > *Copy Policy Packages*.

2 Browse to and select a policy package or container that contains policy packages.

3 Browse to and select a container where you want to copy this policy package.

4 Click *Add* to add the container to the *Selected Container* list.

   To copy the policy package or container to multiple containers, repeat Step 3 and Step 4.

5 Click *OK*.

17.2 Using the Windows Copy Policy Packages Utility

The Windows-based Copy Policy Packages utility is found in the *windows_drive*\sys\public\mgmt\consoleone\1.2\bin directory.

To run the Copy Policy Packages utility from Windows:

1 Double-click `copypol.exe`.

2 Specify the name of a policy package or container that contains policy packages that you want to copy from one Novell eDirectory™ container to another.

3 Specify a container name.

4 Click *Add* to add the container name to the *Selected Container* list.

   To copy the policy package or container to multiple containers, repeat Step 3 and Step 4.

5 Click *OK*.

The Windows-based Copy Policy Packages utility can also run from the Windows command line. You can copy a policy package from one container to another or you can copy all of the policy packages from one container to another container.

To copy a policy package from one container to another, use the following syntax:

```
copypol policy_package_DN /d destination_container
```

To copy all of the policy packages from one container to a different container, use the following syntax:

```
copypol container_DN /d destination_container
```

You can use the following command line switches:

Table 17-1   *List of Command Line Switches for Use with the Windows Copy Policy Packages Utility*

Switch	Description
/d	Specifies the destination container where the policy packages will be copied
/h	Runs the Copy Policy Packages utility in hidden mode
/r	Replaces the policy package in the destination container if a policy package with the same name already exists in that container
/t	Specifies the tree to copy the policy packages to
/v	Lets you view a log file to verify the results of the copy process

Workstation Scheduler

The Novell® ZENworks® 7 Desktop Management Scheduler allows you to set up different actions to run on a workstation. You can run actions on a workstation using policies or manually using the Scheduler. In previous versions of ZENworks for Desktops, the Scheduler was available on the Windows taskbar. Because many system administrators do not want users to be able to access the Scheduler, it is no longer displayed in the taskbar. The Scheduler (`wmsched.exe`), however, is installed as part of the Workstation Client installation.

This section contains the following topics to help you understand and use the workstation Scheduler manually; for further information on how to manage the workstation scheduler using policies, see Section 15.6, "Scheduled Action Policy (User and Workstation Packages)," on page 195:

- Section 18.1, "Understanding Workstation Scheduler," on page 221
- Section 18.2, "Using Workstation Scheduler," on page 222

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

18.1 Understanding Workstation Scheduler

This section contains the following topics:

- "Actions" on page 221
- "Rights for Running Actions" on page 222
- "Using the Scheduler in Windows 2000/XP" on page 222
- "Microsoft SAGE Compatibility" on page 222

18.1.1 Actions

An action is an object that contains a list of one or more action items (for example, `.exe` files `.dll` files, ActiveX*, and JavaScript*). The action applies only to the workstation from which you are running the workstation Scheduler.

Actions and action items can be given a priority, allowing you to specify which action or action item should run first, second, and so forth. You can also schedule actions to automatically run when a workstation event occurs or periodically at a certain time.

You determine the amount of time each action or action item has to complete. If the action cannot occur at the specified time, you can indicate whether to discontinue it, retry it every minute, or have it rescheduled.

If the action does not complete within a specified amount of time, you can indicate that the action should be terminated. If the action does complete successfully, you can indicate that the action should not be run again.

You can also specify if an action should dial a number before any action item runs.

If you have the necessary rights, you can view and edit details or properties associated with an action. You can also delete an action, disable or enable an action, or run an action immediately even if it was scheduled to run at a later date or time or upon the occurrence of a given event.

You can remove, disable or enable, reorder, and view or modify properties associated with action items.

18.1.2 Rights for Running Actions

For actions to have the proper rights to modify the workstation's environment, you must have the appropriate workstation access rights.

18.1.3 Using the Scheduler in Windows 2000/XP

In Windows 2000/XP, a user does not need to be logged in to the workstation or the network for the action to happen. The action takes place even when no one is at the workstation. However, the workstation must be powered on for the action to occur. If the workstation is not on when an action starts, Scheduler reschedules the action within a block of time called the startup block of time. If the workstation is not turned on within this time, you can indicate that the action be retried every minute, rescheduled to occur during the next interval, or dropped.

18.1.4 Microsoft SAGE Compatibility

The Scheduler is compatible with Microsoft SAGE for Windows 98 and can run SAGE-aware programs.

18.2 Using Workstation Scheduler

This section contains the following topics:

- "Adding an Action" on page 222
- "Adding an Action Item" on page 224
- "Disabling or Enabling an Action" on page 225
- "Disabling or Enabling an Action Item" on page 225
- "Removing an Action" on page 225
- "Removing an Action Item" on page 225
- "Running an Action Immediately" on page 225
- "Scheduling an Action to Run" on page 226
- "Setting Advanced Action Properties" on page 228
- "Viewing or Editing the Details or Properties of an Action" on page 228
- "Viewing or Editing the Details or Properties of an Action Item" on page 228
- "Viewing or Editing User-Defined Action Item Properties" on page 229

18.2.1 Adding an Action

Setting up an action item requires that you add the action item to the list of action items. The network administrator (or other user with the Supervisor right) can do this in ConsoleOne® and then

push the action item to one or more user workstations. Users can also set up action items to run on their individual workstations by using the workstation Scheduler.

1 Load the Scheduler (run `wmsched.exe`).

2 Click *Add* to display the Action Properties dialog box.

3 On the General page, fill in the fields:

Name: The name of the action. In ConsoleOne, the name includes the action object's full context. In the workstation Scheduler, the name is whatever you enter in this field.

Priority: The order in which the action is run. Higher priority actions run first. If two actions have the same priority, the first one encountered in the action list (contained in the window that is first displayed when the Scheduler is loaded) runs first. The priority selected applies to all action items contained in this action, unless the action item overrides it.

Impersonation: The workstation access rights to grant to all action items contained by this action. (Windows NT/2000/XP only.)

Action Remains Persistent after Reboot: The action is saved to the workstation, allowing the Scheduler to reactivate the action at the appointed time when the workstation is rebooted. If this option is not selected, the action is lost when you exit Windows NT/2000/XP.

4 On the Actions page, click *Add*.

5 In the Item Properties dialog box, fill in the fields:

Name: Specify the name of the program to run. This program must exist on the user's path to be run as an action item.

Working Directory: The working directory is automatically set when you specify an action item. It is set to the directory that the action item is in. You can specify a different working directory by entering the path in this field.

Parameters: The information the system can use for command line arguments to be sent to the application. For example, if you want to launch `notepad.exe` and have it automatically open the `readme.txt` file, put `readme.txt` in the Parameters field.

Priority: Both actions and action items have four priorities available: *Action Default*, *Above Normal*, *Normal*, and *Below Normal*. Action items can assume the same priority as the Action object that contains them; in other words, they take on the action's default priority. Alternatively, they can override the default by using one of the three other priority settings.

If the action occurs during normal business hours, it should be assigned a *Below Normal* priority so it does not affect the user's workstation performance.

If two or more actions or action items have the same priority, the first one defined (the one that appears first in the list) has precedence over the others.

6 Select the *Terminate action if still running after ? minutes* check box, then select the desired number of minutes.

This option terminates the action if it is still running after the number of minutes you specify. The action is then rescheduled to run at the next scheduled time.

The number of minutes you specify in the *Minutes* field should be the total time required by the action itself as well as by all action items associated with the action, where applicable. If you do not specify sufficient time for the action and all associated action items to run, your action items might not have enough time to complete their tasks.

7 Click *OK* twice.

The action is added to the *Action* list on the Scheduler. You can now do any of the following:

- ◆ Specify when this action should take place (Schedule page).
- ◆ Add items to this action (Items page).
- ◆ Specify what happens if this action cannot occur (Advanced page).

18.2.2 Adding an Action Item

This process assumes that you have previously created an action to contain the action items. If you have not yet created an action, see "Adding an Action" on page 222.

1 In the Scheduler, select an action, click *Properties*, click *Items*, then click *Add*.

2 In the Item Properties dialog box, fill in the fields:

Name: Browse to or enter the name of the program to run. This program must exist on the user's path to run as an action item.

Working Directory: The working directory is automatically set when you browse for an action item. It is set to the directory that the action item is in. You can specify a different working directory by providing the path in this field.

The *Working Directory* field must specify a local device. Network paths cannot be used as working directories.

Parameters: The information the system can use for command line arguments to be sent to the application. For example, if you want to launch `notepad.exe` and have it automatically open the readme.txt file, put `readme.txt` in the *Parameters* field.

If you are adding an action item that is a DOS batch file, a DOS window must be opened to run it. The DOS window closes when the batch file has finished running if you include the `/c` parameter. You must add the `/c` parameter, followed by a space, in front of the name of the batch file in the *Parameters* field.

For example, to run a DOS batch file called `test_c.bat`, make the following entries in the Item Properties dialog box for the action item when you add the action item:

- ◆ *Name*: `CMD.exe` (the name of the Windows NT/2000/XP command that opens a DOS window) or START (the name of the Windows 98 command that opens a DOS window).
- ◆ *Working Directory*: Leave this field blank unless you need to specify where either cmd.exe or start is located.
- ◆ *Parameters*: `/c test_c.bat`. You must include the full filename with its extension, and you must use the `/c` parameter if you want the DOS window to close as soon as the batch file has finished running.
- ◆ *Priority*: Leave at Action Default, or choose one of the other settings.

Priority: Both actions and action items have four priorities available: *Action Default*, *Above Normal*, *Normal*, and *Below Normal*. Action items can assume the same priority as the Action object that contains them; in other words, they take on the action's default priority. Alternatively, they can override the default by using one of the three other priority settings.

If the action occurs during normal business hours, it should be assigned a *Below Normal* priority so it does not affect the user's workstation performance.

If two or more actions or action items have the same priority, the first one defined (the one that appears first in the list) has precedence over the others.

3 Select the *terminate action if still running after ? minutes* check box, then select the desired number of minutes.

This option terminates the action if it is still running after the number of minutes you specify. The action is then rescheduled to run at the next scheduled time.

The number of minutes you specify in the *Minutes* field should be the total time required by the action itself as well as by all action items associated with the action, where applicable. If you do not specify sufficient time for the action and all associated action items to run, your action items might not have enough time to complete their tasks.

4 To save the settings and continue editing the action, click *Apply*.

or

When you are done with the action item's properties, click *OK*.

The action item now appears in the *Action item* list.

If any action items are scheduled to run now and you click *OK* or *Apply*, they run.

5 Repeat Step 2 through Step 4 until you have finished adding items.

18.2.3 Disabling or Enabling an Action

1 Load the Scheduler (run `wmsched.exe`).

2 Click an action.

3 Click *Enable/Disable*.

18.2.4 Disabling or Enabling an Action Item

1 Load the Scheduler (run `wmsched.exe`).

2 Click an action, then click *Properties*.

3 Click the Items page, select an action item, then click *Disable/Enable*.

18.2.5 Removing an Action

This procedure cannot be undone. When you click *Remove*, you are not prompted to verify the removal of the action. If you remove an action that you need later, you must add it again.

1 Click an action.

2 Click *Remove*.

18.2.6 Removing an Action Item

This procedure cannot be undone. When you click *Remove*, you are not prompted to verify the removal of the action item. If you remove an action item that you need later, you must add it again.

1 Click an action, then click *Properties*.

2 Click *Items*, select an action item, then click *Remove*.

18.2.7 Running an Action Immediately

1 Click an Action.

2 Click *Run Now*.

18.2.8 Scheduling an Action to Run

Use the fields on the Schedule page to specify when the action should run and to provide details that the system needs about when the action runs.

The Schedule page contains five scheduling options: *Event*, *Daily*, *Weekly*, *Monthly*, and *Yearly*. The option you choose and the settings you associate with it determine when the action is run.

You can use only one scheduling option at a time. For example, if the *Daily* option is selected, all other options are ignored unless you use the options found on the *Advanced* tab.

Time units are shown according to a 24-hour clock (for example, 9:00 for 9 a.m. and 13:30 for 1:30 p.m.).

The Scheduler ignores the scheduling information until the action can be started successfully.

To schedule an item:

1 Select the action you want to schedule.

2 Click *Properties > Schedule*.

3 Select the desired scheduling option:

 ◆ **Event:** Event scheduling allows you to determine what kind of workstation event causes your action to run. To schedule the action based on an event, click *Event* and choose from the following list of recognized events:

 Scheduler Service Startup: Runs the action when the Scheduler starts up. You cannot choose the *Scheduler Service Startup* event to start the action if you are going to run the action with the rights of an interactive user. When these events take place, the interactive user is not yet authenticated. *Scheduler Service Startup* requires System rights.

 User Login: Runs the action after the user has successfully logged in but before the login scripts are executed.

 User Desktop Is Active: Runs the action after the login scripts have completed (does not apply to Windows 98).

 Workstation Is Locked: Runs the action when the workstation is locked (does not apply to Windows 98).

 Workstation Is Unlocked: Runs the action when the workstation is unlocked (does not apply to Windows 98).

 Screen Saver Is Activated: Runs the action when the screen saver is activated.

 User Logout: Runs the action before logout is completed.

 System Shutdown: Runs the action after all other applications have successfully closed, but before the system shuts down. You cannot choose the *System Shutdown* event to start the action if you are going to run the action with the rights of an interactive user. When these events take place, the interactive user is no longer authenticated. *System Shutdown* requires System rights.

 ◆ **Daily:** Lets you schedule an action to occur on one or more days between the specified start and end times. Optionally, it allows you to repeat the action at regular intervals after the action successfully starts. For example, on Monday, Wednesday, and Friday, you could

start the action between 12:30 and 13:00 and run it every 10 minutes. To schedule the action based on a daily basis, click *Daily* and choose from the following options:

Run this Action on the Following Days: Specify the days of the week when the action is to run.

Start the Action Between the Hours of ? (HH:MM): Specify a range of time within which this action can be started.

Repeat the Action Every ? (HH:MM:SS): Specify the length of time the system is to wait before it repeats this action.

- **Weekly:** Lets you schedule an action on a particular day of the week. To schedule an action on a weekly basis, click *Weekly* and choose from the following options:

Run this Action Once a Week On: Identifies day of the week when you want the action to run.

Start this Action Between the Hours of ? (HH:MM): Identifies the exact hour (HH) and minute (MM) to start this action.

- **Monthly:** Lets you choose the day of the month when this action runs, as well as the time to start this action. For example, you can choose to run this action on every fourth day of the month, between the hours of 8:00 and 10:15. You specify the time range using a 24-hour clock. If you prefer, you can choose to have the action run on the last day of the month, regardless of how many days there are in the month. To schedule the action on a monthly basis, click *Monthly* and choose from the following options:

Run this Action Once a Month on Day __ of the Month: Specify the day of the month on which the system is to automatically run this action. Click one of the available option buttons:

  - **On Day _ of the Month:** This action runs on the specified day.

  - **On the Last Day of the Month:** This action runs on the last day of the month regardless of how many days there are in the month.

Start this Action Between the Hours of ? (HH:MM): Specify the exact hour (HH) and minute (MM) this action is to start.

- **Yearly:** Lets you determine the time and the day of the month to perform the action. To schedule the action on a yearly basis, click *Yearly* and choose from the following options:

Run the Action Once a Year on Day ? of ?: Specify the day of the month and the month of the year for the action to run.

Start the Action between the Hours of ? and ?: Using a 24-hour clock, specify the hour and minute of the earliest time this action is to be started, and then the hour and minute of the latest time this action is to be started. For example, choose 17:30 to begin the action no earlier than 5:30 p.m. and 20:00 to begin the action no later than 8:00 p.m.

4 Click *OK*.

The schedule you define applies to every action item contained in the action and overrides the package schedule.

18.2.9 Setting Advanced Action Properties

Use the fields on the Advanced page to determine what happens to the action's schedule if it did not complete or run within the given time, or when it successfully completes.

1 Click an action > *Properties* > *Advanced*.

2 Specify what should happen if the system cannot run the action:

- ◆ **Disable the Action:** Disables the action so it does not run again (unless you enable it again).

- ◆ **Retry Every Minute:** Causes the system to keep trying to run this action every 60 seconds.

- ◆ **Ignore the Error and Reschedule Normally:** Causes any error that occurred while the action was running to be ignored and the action to be rescheduled for a later date/time.

3 Select the *Disable the action after completion* check box to disable the rescheduling mechanism for this action after all action items have started successfully.

4 Select the *Terminate action if still running after ? minutes* check box, then select the number of minutes.

This feature terminates the action if it is still running after the number of minutes you specify. The action is then rescheduled to run at the next scheduled time.

To set a time limit on how long the action should run, select the check box. The number of minutes that you specify in the *Minutes* field should be the total time required by the action itself as well as by all action items associated with the action, where applicable. If you do not specify sufficient time for the action and all associated action items to run, your action items might not have enough time to complete their tasks.

This feature prevents an action that has stopped responding or running without completing from continuously tying up the system. However, selecting this option only affects actions that are not currently running. You cannot use this check box to terminate an action that has already been loaded by the Scheduler and is currently running. Also, if the action you are running (such as a DOS batch file) opened a DOS window, the DOS window is not automatically closed after the action has completed, unless you added the /c parameter in the *Parameters* field when you originally added the action item.

18.2.10 Viewing or Editing the Details or Properties of an Action

1 Click an action, then click *Properties*.

2 Click one of the pages containing the details or properties associated with this action.

3 Make the necessary changes.

4 Click *OK*.

18.2.11 Viewing or Editing the Details or Properties of an Action Item

1 Click an action, then click *Properties*.

2 Click *Item*, select an action item, then click *Properties*.

3 Make the necessary changes.

4 Click *OK*.

18.2.12 Viewing or Editing User-Defined Action Item Properties

1 Open the Scheduler on a workstation.

2 Select an action item > click *Properties*.

3 Make the necessary changes.

4 Click *OK*.

Documentation Updates

This section contains information on documentation content changes that have been made in this section of the *Administration* guide since the initial release of Novell® ZENworks® 7 (August 26, 2005). The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: `.html` and `.pdf`. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for ZENworks 7 Workstation Management.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page.

The documentation was updated on the following dates:

- Section I.1, "February 9, 2007," on page 231
- Section I.2, "July 14, 2006 (Support Pack 1)," on page 232
- Section I.3, "April 28, 2006," on page 232
- Section I.4, "February 28, 2006," on page 232
- Section I.5, "December 9, 2005," on page 233

I.1 February 9, 2007

Updates were made to the following section. The changes are explained below.

- Section I.1.1, "Windows Desktop Preferences Policy (User Package)," on page 231

I.1.1 Windows Desktop Preferences Policy (User Package)

The following updates were made in this section:

Location	Change
Section 15.8, "Windows Desktop Preferences Policy (User Package)," on page 198	- Added definitions for the different types of user profiles. - Added information about how to create a mandatory user profile. - Relocated information about "accommodating roaming profiles on slow networks" in a separate subsection.

I.2 July 14, 2006 (Support Pack 1)

Updates were made to the following section:

* Section 15.9.4, "Editing Existing Windows Group Policies (User and Workstation Packages)," on page 209

I.2.1 Windows Group Policies

The following updates were made in this section:

Location	Change
Section 15.9.4, "Editing Existing Windows Group Policies (User and Workstation Packages)," on page 209	Added a note to warn users that if the Network Location of Existing/New Group Policies path is set to a Linux file server, permission must be set from a Linux machine to allow read rights for users and workstations.

I.3 April 28, 2006

Updates were made to the following sections. The changes are explained below.

* Section 13.1, "Dictionary Update Policy," on page 157
* Section 15.4, "Novell iPrint Policy (User and Workstation Packages)," on page 190

I.3.1 Dictionary Update Policy

The following updates were made in this section:

Location	Change
Section 13.1, "Dictionary Update Policy," on page 157	Added a section documenting the Dictionary Update Policy.

I.3.2 Novell iPrint Policy (User and Workstation Packages)

The following updates were made in this section:

Location	Change
Section 15.4, "Novell iPrint Policy (User and Workstation Packages)," on page 190	Deleted outdated information on using the Novell iPrint Policy on Windows 2000 terminal servers.

I.4 February 28, 2006

Updates were made to the following sections. The changes are explained below.

* Section I.4.1, "ZENworks Windows Group Policy (User and Workstation Packages)," on page 233

I.4.1 ZENworks Windows Group Policy (User and Workstation Packages)

The following updates were made in this section:

Location	Change
Section 15.9.1, "Understanding the Windows Group Policy," on page 202	Added a paragraph to warn users that using ZENworks Group Policies and Group Policies configured in Active Directory in the same environment is not supported.

I.5 December 9, 2005

The page design of the entire guide was reformatted to comply with revised Novell documentation standards.

Updates were made to the following sections. The changes are explained below.

- Section I.5.1, "Setting Up User and Workstation Package Policies," on page 233

I.5.1 Setting Up User and Workstation Package Policies

The following updates were made in this section:

Location	Change
Section 15.9.4, "Editing Existing Windows Group Policies (User and Workstation Packages)," on page 209	One of the subsections in this part of the documentation, entitled "Using Windows XP SP2 and ZENworks 7" was deleted because the scenario is no longer viable because of a fix in the code.