Understanding ZENworks 7 Desktop Management

This section of the Administration guide introduces the major parts of Novell® ZENworks® 7 Desktop Management and explains how they work together.

Understanding the Novell Client

<div style="text-align: right">1</div>

Since the first release of Novell® ZENworks® Desktop Management (formerly called "ZENworks for Desktops"), the Novell Client™ has been an integral part of delivering zero-effort networking (ZEN) to the user's desktop. The client enables the user's Windows* workstation to securely access network resources, including NetWare® and Windows 2000/2003 servers, security, and network printers. It also integrates NetWare services such as file and print, object management in the directory, drive mapping, browsing network servers and printers, user administration on network servers, establishing rights, login scripts, and so on.

With ZENworks 7 Desktop Management, the Novell Client is not mandatory on a user's workstation because the Desktop Management Agent performs all of the functions needed to manage a workstation. For more information about the Desktop Management Agent, see Chapter 2, "Understanding the Desktop Management Agent," on page 39

This section includes the following information:

 * Section 1.1, "The Role of the Novell Client," on page 35

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

1.1 The Role of the Novell Client

ZENworks 7 Desktop Management supports the Novell Client for Windows 98 workstations (version 3.4 and later) and the Novell Client for Windows 2000/XP workstations (version 4.9 SP1a and later). When installed on workstations, earlier versions of the Novell Client (that is, the client versions used prior to ZENworks for Desktops 4) included many of the ZENworks Desktop Management components, but that is no longer the case.

Beginning with ZENworks for Desktops 4, the ZENworks Desktop Management Agent has been responsible for installing ZENworks components on user workstations, making the Desktop Management Agent a required component for ZENworks Desktop Management.

The following sections provide information about the continuing role of the Novell Client in Desktop Management functionality.

 * "The Novell Client and ZENworks Desktop Management Installation" on page 35
 * "The Novell Client and ConsoleOne Administration" on page 36
 * "Using the Novell Client in a ZENworks 7 Environment" on page 36

1.1.1 The Novell Client and ZENworks Desktop Management Installation

When you install the Desktop Management Server and the ZENworks Middle Tier Server, the installing workstation must have the required version of the Novell Client installed. The client establishes communication between the workstation and eDirectory™, making it possible for either of the two installation programs to recognize and display eDirectory trees and server objects that

help you visualize where to install Desktop Management software. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

Upgrading from Earlier Versions of ZENworks

If you intend to perform an upgrade to ZENworks 7 from ZENworks 6.5 or ZENworks for Desktops 4.*x*, workstations in your environment already have the ZENworks Desktop Management Agent installed (even if users routinely use the Novell Client to log in) along with Novell Application Launcher™ components. This makes it simple to use the Application Launcher to upgrade the Desktop Management Agent. For more information, see "Upgrading Workstations" in the "Upgrading from ZENworks for Desktops 4.x" section of the *Novell ZENworks 7 Desktop Management Installation Guide*.

1.1.2 The Novell Client and ConsoleOne Administration

Novell ConsoleOne® is a Java*-based tool used to manage your network and its resources. By default, it lets you manage:

- ◆ eDirectory objects, schema, partitions, and replicas
- ◆ NetWare server resources

When you install the Desktop Management Server, the eDirectory schema is extended to include several directory objects unique to Desktop Management, including workstations, applications, databases, and policy packages. The capabilities to configure these objects are snapped in to the ConsoleOne structure.

You can install and run ConsoleOne locally on a Windows workstation or server, or you can install it remotely on a NetWare or Windows server and run it through a mapped or shared drive pointing to that server. The Novell Client must be installed on the Windows workstation or server where you will be running ConsoleOne for administering ZENworks Desktop Management. This is because ConsoleOne is dependent on the client's NetWare libraries. For more information, see the ConsoleOne 1.3x User Guide (http://www.novell.com/documentation/lg/consol13/index.html?page=/documentation/lg/consol13/c1_enu/data/hk42s9ot.html) at the Novell Product Documentation Web site.

1.1.3 Using the Novell Client in a ZENworks 7 Environment

With ZENworks 7 Desktop Management, the Novell Client is not mandatory on a user's workstation because the Desktop Management Agent makes it possible for users to authenticate to the Desktop Management Server and benefit from ZENworks functionality when outside the corporate firewall. For more information about the Desktop Management Agent, see Chapter 2, "Understanding the Desktop Management Agent," on page 39.

The Desktop Management Agent is not a replacement for the Novell Client. For more information about using the Novell Client in a NetWare environment, see the Novell Client documentation Web site (http://www.novell.com/documentation-index/index.jsp).

If the Novell Client and the Desktop Management Agent are both installed on a workstation, the workstation login defaults to the Novell Client and all of the NetWare file system and eDirectory access is through the client.

NOTE: Users outside the firewall who have both the agent and the client installed on their workstations must use an alternative login method and will receive applications only, not Desktop Management policies. For more information about the alternative login method for authenticating to eDirectory outside the firewall when both the client and agent are installed, see "Logging in Locally to the Workstation" on page 76.

Understanding the Desktop Management Agent

2

This section contains information you can use to help you gain a high-level understanding of the role of the Desktop Management Agent and how it works.

- Section 2.1, "What is the Desktop Management Agent?," on page 39
- Section 2.2, "Getting Ready to Use the Desktop Management Agent," on page 39

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

2.1 What is the Desktop Management Agent?

Novell® ZENworks® 7 Desktop Management requires the Desktop Management Agent. With this agent installed, users who log in directly with the Novell Client™ can use ZENworks 7 Desktop Management directly, while users in an all-Windows environment or users on workstations located outside of the corporate network firewall can log in and authenticate the workstation through the ZENworks Middle Tier Server to Novell eDirectory™ using port 80 over HTTP or port 443 over HTTPS.

IMPORTANT: The Desktop Management Agent must be installed on every workstation where you want to deploy ZENworks 7 Desktop Management functionality. This includes workstations where the Novell Client is already installed.

When authenticated with the proper credentials, the workstation receives the distributed applications, schedules, policies, and various workstation inventory, remote management, and Workstation Imaging enabling files as designated by you, the administrator.

The Desktop Management Agent includes functionality for login and authentication, packaging, sending, and receiving XML requests over HTTP or HTTPS.

2.2 Getting Ready to Use the Desktop Management Agent

This section includes information you need to know if you plan to deploy the Desktop Management Agent in your network environment:

- Section 2.2.1, "Desktop Management Agent Installation Considerations," on page 40
- Section 2.2.2, "Upgrading the Desktop Management Agent," on page 40
- Section 2.2.3, "Modifying the Desktop Management Agent Login," on page 40
- Section 2.2.4, "Using the ZENworks Agent Control Panel Applet To Modify Agent Settings," on page 41
- Section 2.2.5, "Setting Up AutoAdminLogon for Windows 2000/XP," on page 45

2.2.1 Desktop Management Agent Installation Considerations

Make sure that the workstations where you install the Desktop Management Agent meet the minimum requirements for hardware and installed software. For more information, see "User Workstation Requirements" in "Preparation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The Desktop Management Agent installation lets you install various Desktop Management components on a one-time basis; that is, if you want to add or delete any of the components installed by the Agent in an earlier installation, you can use the Modify option that is available in the maintenance dialog box of the Desktop Management Agent setup.

2.2.2 Upgrading the Desktop Management Agent

The version of the Desktop Management Agent that shipped with the original *ZENworks for Desktops 4 Program* CD (`setup.exe`) is no longer supported. You must not attempt to upgrade from that version of the Desktop Management Agent.

You can upgrade the ZENworks for Desktops 4.0.1 Desktop Management Agent (and its functionality) and the ZENworks 6.5 Desktop Management Agent by installing the ZENworks 7 Desktop Management Agent.

Installing version 7 of the agent uninstalls older versions of the agent and enables ZENworks 7 functionality on your managed workstations.

For more information, see "Upgrading Workstations" in "Upgrade" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2.2.3 Modifying the Desktop Management Agent Login

If you want to modify the Desktop Management Agent for your network users, you can do so when you create the Desktop Management Agent installation for the workstations and after you import the workstations. This section includes information for both options:

- "Modifying the Login Dialog" on page 40
- "Creating Custom Bitmaps for the Graphical Interface" on page 40

Modifying the Login Dialog

If the Novell Client is not present on the installing workstation when you are installing the Desktop Management Agent, the installation program displays the Workstation Manager Settings dialog box. This dialog box can be customized. For more information about the customization options, see "Customizing the Agent Login" in "Setting Up Authentication" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

Creating Custom Bitmaps for the Graphical Interface

If you deploy the Desktop Management Agent in your network environment, you can customize the login GINA (that is, the graphical interface used for authentication) and the Welcome dialog box with your own company identity. To replace the Novell bitmaps on the Desktop Management Agent Login dialog box or the Resident Workstation Welcome dialog box, use the Workstation Policy Package > Desktop Management Agent policy. For more information, see Section 15.12,

"ZENworks Desktop Management Agent Policy (Workstation Package)," on page 213. The workstation must be imported into the eDirectory tree in order for these dialog boxes to access the customized bitmaps. When you change the bitmaps that are accessed through this policy, the new graphics are accessed when the scheduled system event occurs.The Login dialog box bitmap is sized at 390 x 75 pixels and the *Welcome* dialog box bitmap is sized at 320 x 195 pixels. The *Welcome* dialog box attribute is stored in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NWGINA
```

The Login dialog box attribute is stored in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\LgnXtier
```

NOTE: You can also log in from the Application Explorer in the Windows system tray. The graphical interface of this login GINA cannot be customized. For more information, see "Logging in Locally to the Workstation" on page 76.

2.2.4 Using the ZENworks Agent Control Panel Applet To Modify Agent Settings

When the ZENworks Management Agent is installed on user workstations, a specialized Windows Control Panel applet, *ZENworks Agent Options*, is also installed.

*Figure 2-1* *The ZENworks Agent Options Applet in the Windows Control Panel*
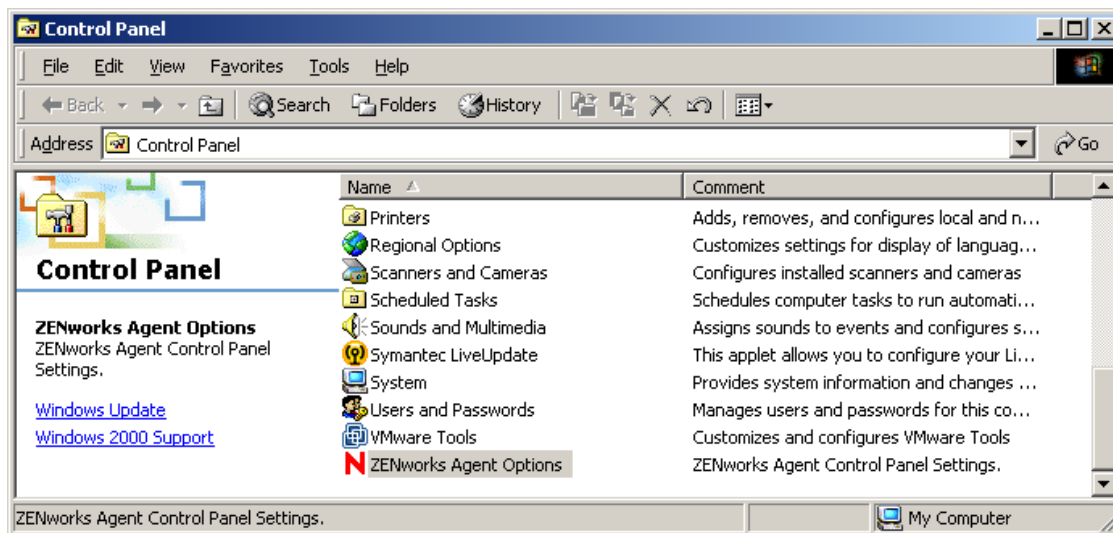
This applet provides an interface for advanced users to perform the following tasks:

- View the Middle Tier IP address they use (if any) for access to ZENworks files
- Change the eDirectory password
- Enable or disable various Workstation Manager settings

When the user double-clicks the *ZENworks Agent Options* icon in the Control Panel, the ZENworks Agent Options dialog box is displayed:

Figure 2-2 *ZENworks Agent Options Dialog Box*
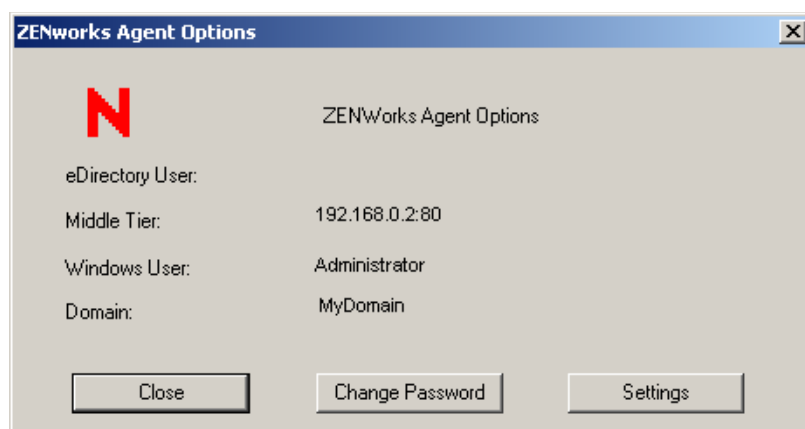
The dialog box lists the following information:

- The eDirectory username and context of the individual logged into this workstation
- The IP address or DNS name of the Middle Tier Server that this workstation uses for access through the firewall
- The Windows username of the individual logged into this workstation
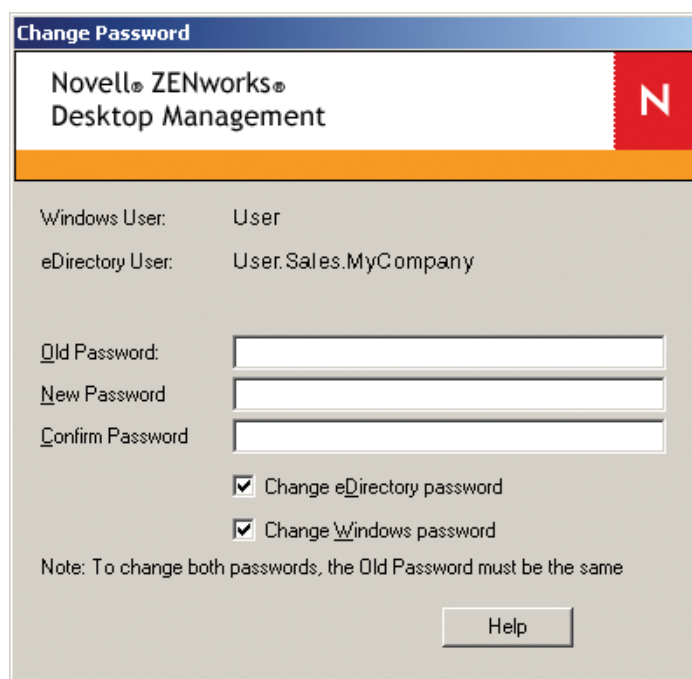- The Windows domain name to which this workstation belongs

The *Change Password* button and *Settings* button open dialog boxes where agent options can be configured.

- "Change Password Dialog Box" on page 42
- "Workstation Manager Dialog Box" on page 43

Change Password Dialog Box

The Change Password dialog box lists the eDirectory username and the Windows username of the individual who is logged in to this workstation, and includes fields where the user can change his or her password.

Figure 2-3   *Change Password Dialog Box*

The following fields in the dialog box accept user input:

Old Password: Users type their current password (Windows or eDirectory) in this field.

New Password: Users type their newly chosen password in this field.

Confirm Password: Users retype the new password in this field to confirm their choice.

The *Change eDirectory Password* check box lets the user choose whether to synchronize the eDirectory password with the newly chosen local workstation password.

The *Change Windows Password* check box lets the user choose whether to synchronize the local workstation password with the newly chosen eDirectory password.

The note in the dialog box indicates that if the user wants the same password for both eDirectory and Windows (indicated by selecting both check boxes), the current (or "old") passwords for eDirectory and Windows must already be the same (that is, they use the identical password to authenticate both locally and to eDirectory).

Workstation Manager Dialog Box

When the user clicks *Settings* in the ZENworks Agent Options dialog box, the Workstation Manager dialog box displays.

Figure 2-4 *Workstation Manager Dialog Box*
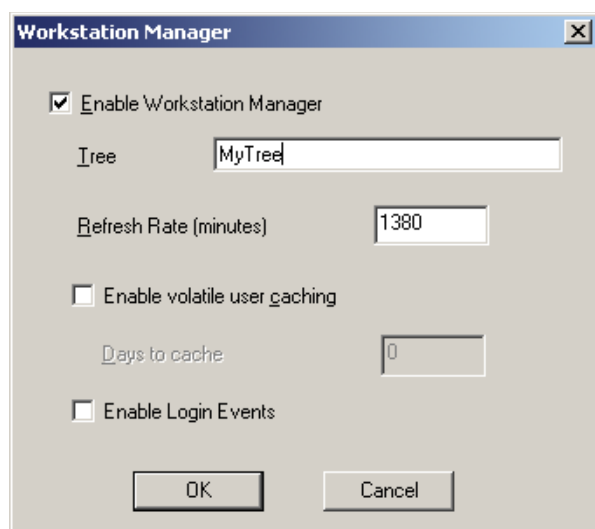
The user can configure the following settings in this dialog box:

Enable Workstation Manager: The user selects this check box to enable Workstation Manager at the next reboot.

Tree: The user specifies the name of an eDirectory tree to designate the network location where ZENworks should search for Workstation Manager policies.

Refresh Rate (Minutes): The user specifies a value (in minutes) to set the refresh rate for eDirectory. The rate determines how often the agent looks for updated information (such as new or edited policies) in eDirectory.

Enable Volatile User Caching: The user selects this check box to enable the caching of volatile user information on the workstation for a specified number of days, so that volatile users are not created or removed at every login or logout. When this option is selected, volatile users can log in faster because NWGINA does not 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.

This setting is also available in the Desktop Management Agent Policy. Because both the policy and the applet write to the same registry location, the last setting made (either in the policy or in this dialog box of the applet) before the cache flushes is the setting that takes effect.

For more information, see Section 15.12, "ZENworks Desktop Management Agent Policy (Workstation Package)," on page 213.

Days to Cache: (Conditional) This option is available only if the *Enable Volatile User Caching* check box is selected. Users specify the number of days for volatile user information to persist in the workstation's cache. When the time limit expires, all volatile user information is removed from the workstation. If the user has not logged in within the specified time period, the countdown begins again according to the number of days specified here.

Enable Login Events: Selecting this check box enables Workstation Manager to notify its policies about eDirectory logins occurring after the initial Windows login. (Usually, Workstation Manager notifies its policies of user login only at initial Windows login, so if the user logs into eDirectory later, policies are not applied.)

Activating this setting lets a user in a VPN environment initially log in locally to his or her workstation; then, when that user's VPN is up and running, he or she can log into eDirectory and their policies are applied.

By default, this check box is not selected (off), which means that the Workstation Manager service applies policies only if the user initially logs into eDirectory.

NOTE: This option was added to the dialog box starting with ZENworks 7 Desktop Management Agent with Support Pack 1.

2.2.5 Setting Up AutoAdminLogon for Windows 2000/XP

You can automate the logon process for selected Windows 2000/XP users by using the Windows Registry Editor (`regedit.exe`) to enter user ID and password credentials in the Registry database. The result for the user is immediate access to the desktop and network resources without the need to pause to enter logon information.

NOTE: You can bypass the AutoAdminLogon process and log on as a different user by holding down the Shift key after a logout or after a workstation reboot.

Using AutoAdminLogon opens your network to a serious security risk. It exposes user IDs and passwords and it lets any user who starts the workstation use the embedded credentials to obtain access to the workstation and network files—even if the workstation is locked. We recommend that you review the Microsoft* recommendations regarding when to use AutoAdminLogon before you implement it. For more information, see TID 10052847 (http://www.novell.com/support/ search.do?cmd=displayKC&docType=kc&externalId=10052847&sliceId=&dialogID=24441333&s tateId=0%200%2024443463) at the Novell Support Web site (http://support.novell.com).

IMPORTANT: If you install the Novell Client 4.9 SP1a for Windows 2000/XP on a workstation that already has the Desktop Management Agent installed and then set up AutoAdminLogon, you receive a login error because of a conflict between AutoAdminLogon and Novell Modular Authentication Services (NMAS™), installed by default by Novell Client 4.9 SP1a.

To work around the problem after the Client is installed, right-click the red N icon in the desktop system tray > click *Novell Client Properties* > *Advanced Login* > deselect *NMAS Authentication*.

This section contains the following information:

- "General Procedure for Setting Up AutoAdminLogon" on page 45
- "AutoAdminLogon Options" on page 46
- "Changing Passwords in NetWare Login with AutoAdminLogon" on page 51

General Procedure for Setting Up AutoAdminLogon

1 Start the Registry Editor (`regedit.exe`).

WARNING: Using the Registry Editor incorrectly can cause serious, system-wide problems that might require reinstalling Windows 2000/XP to correct them.

2 Locate the specified Registry keys and set the values as indicated.

If a value does not exist, click *Edit > New > String Value*, type the name of the value, then press Enter. All the values should be string values except for AutoAdminQueryNDS, which must be a DWORD value instead of a string value.

IMPORTANT: For a Windows logon only, if no DefaultPassword string is specified, the value of the AutoAdminLogon key automatically changes from 1 (True) to 0 (False), disabling the AutoAdminLogon feature after the first autoadminlogon session has occurred.

3 Exit the Registry Editor and log out of Windows 2000/XP.

AutoAdminLogon Options

This section lists the options you can choose from when you set up AutoAdminLogon.

- "Logon to Workstation Only: Client Only, Agent Only, or Both Client and Agent Installed" on page 46
- "Logon to Workstation and eDirectory: Client Only, or Both Client and Agent Installed" on page 47
- "Logon to Workstation and eDirectory: Agent Only Installed" on page 48
- "Login to NetWare Only Using Dynamic Local User (DLU) for Windows: Client Only, or Both Client and Agent Installed" on page 49
- "Logon to NetWare Only Using Dynamic Local User (DLU) for Windows: Agent Only Installed" on page 49
- "Logon to Windows and Query for NetWare: Client Only Installed" on page 50

In addition to these options for setting up AutoAdminLogon, you can also disable it. For more information, see "Disable AutoAdminLogon" on page 51. You should also be careful to use these options only for setting up user names and passwords if you want AutoAdminLogon to work properly. Be careful to caution users against resetting their own passwords. For more information, see "Changing Passwords in NetWare Login with AutoAdminLogon" on page 51.

Logon to Workstation Only: Client Only, Agent Only, or Both Client and Agent Installed

Use this option to allow users to go directly to the desktop when the workstation boots. Users are not authenticated to eDirectory. The effect is similar to the user authenticating by checking the *Workstation Only* check box in the Windows logon dialog box.

Table 2-1 *Settings for Using AutoAdminLogon: Logging on to the Workstation Only*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultDomain	Name of Domain
		or
		Name of Local Workstation
	DefaultUserName	Windows User Name
	DefaultPassword	Windows Password for the DefaultUserName specified above
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ Login	AutoAdminLogon	0

Logon to Workstation and eDirectory: Client Only, or Both Client and Agent Installed

Use this option to allow users to go directly to the desktop upon workstation bootup. No login prompts for Windows authentication or eDirectory authentication (Client or Agent) are displayed. Users are authenticated to eDirectory and to the Windows workstation. All Desktop Management policies and applications are delivered to the workstation.

Table 2-2 *Settings for using AutoAdminLogon: Logging in to the Workstation and eDirectory with the Novell Client Only Installed or with the Novell Client and ZENworks Agent Installed*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultDomain	Name of Domain
		or
		Name of Local Workstation
	DefaultUserName	Windows User Name
	DefaultPassword	Windows Password for the DefaultUserName specified above

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login	AutoAdminLogon	1
	DefaultLocationProfile	Name of the Location Profile that contains the information about the Novell User to log in to the NetWare network such as Username, Tree, Context, Server, etc.
	DefaultPassword	Novell Password for the DefaultUserName specified in the Location Profile

Location profiles let you save a user's specific login information. The profile automatically sets up login information such as the user's name, server, tree, context, login script, and other applicable information so that the user does not need to type this information.

NOTE: The NT Credential information in the Location Profile is not used. The NT user information in the registry is used instead.

Logon to Workstation and eDirectory: Agent Only Installed

Use this option to allow users to go directly to the desktop upon workstation bootup. No login prompts for Windows authentication or eDirectory authentication are displayed. Users are authenticated to eDirectory and to the Windows workstation. All Desktop Management policies and applications are delivered to the workstation.

Table 2-3 *Settings for using AutoAdminLogon: Logging in to the Workstation and eDirectory with the ZENworks Agent Only Installed*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultDomain	Name of Domain
		or
		Name of Local Workstation
	DefaultUserName	Windows User Name
	DefaultPassword	Windows Password for the DefaultUserName specified above

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ Login	AutoAdminLogon	1
	DefaultUserName	The fully-distinguished name (DN) or the common name (CN) portion of the DN that the Novell User uses to log in to eDirectory. Example: bjones or bjones.sales.novell
	DefaultPassword	Novell Password for the DefaultUserName specified in the DefaultUserName string.

Login to NetWare Only Using Dynamic Local User (DLU) for Windows: Client Only, or Both Client and Agent Installed

Use this option to allow users to go directly to the desktop upon workstation bootup. Users are authenticated to eDirectory according to the credentials entered in the registry, but they are authenticated to the Windows workstation according to the configuration of the DLU policy (no credentials for Windows are entered in the registry).

Table 2-4 Settings for using AutoAdminLogon: Logging in to NetWare Using DLU, Client Only or Both Client and Agent Installed

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	0
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ Login	AutoAdminLogon	1
	DefaultLocationProfile	Name of the Location Profile that contains the information about the Novell User to log in to the NetWare network, such as Username, Tree, Context, Server.
	DefaultPassword	Novell Password for the DefaultUserName specified in the Location Profile

Location profiles allow you to save a user's specific login information. The profile automatically sets up login information such as the user's name, server, tree, context, login script, and other applicable information so that the user does not need to type this information. In this case, the location profile must specify an eDirectory user with Dynamic Local User (DLU) privileges on the Windows 2000 workstation.

Logon to NetWare Only Using Dynamic Local User (DLU) for Windows: Agent Only Installed

Use this option to allow users to go directly to the desktop upon workstation bootup. Users are authenticated to eDirectory according to the credentials entered in the registry, but they are

authenticated to the Windows workstation according to the configuration of the DLU policy (no credentials for Windows are entered in the registry).

Table 2-5 *Settings for using AutoAdminLogon: Logging in to NetWare Using DLU, Agent Only Installed*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	0
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ Login	AutoAdminLogon	1
	DefaultUserName	The fully-distinguished name (DN) or the common name (CN) portion of the DN that the Novell User uses to log in to eDirectory. Example: bjones or bjones.sales.novell
	DefaultPassword	Novell Password for the DefaultUserName specified in the DefaultUserName string.

Logon to Windows and Query for NetWare: Client Only Installed

The following settings are applicable only if the workstation has only the Novell Client installed. They are not applicable if only the Desktop Management Agent is installed.

This option authenticates the user to the Windows workstation according to the credentials entered in the registry, but the login to NetWare requires the user to enter his or her eDirectory credentials.

Table 2-6 *Settings for using AutoAdminLogon: Logging on to Windows, Client Only Installed*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultDomain	Name of Domain
	or	or
	Local WorkstationName	Name of Local Workstation
	DefaultUserName	Windows User Name
	DefaultPassword	Windows Password for the DefaultUserName specified above

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ Login	AutoAdminLogon	0
	AutoAdminQueryNDS	1
		IMPORTANT:
		AutoAdminQueryNDS must be a DWORD value instead of a string value.

Disable AutoAdminLogon

This is the behavior setting for logon to the Windows workstation and to eDirectory. The user is prompted for Windows workstation credentials and eDirectory credentials in order to authenticate.

Table 2-7   Settings for using AutoAdminLogon: Disabling for Logon

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Micr osoft\ WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	0
HKEY_LOCAL_MACHINE\SOFTWARE\Nove ll\ Login	AutoAdminLogon	0

Changing Passwords in NetWare Login with AutoAdminLogon

Novell Client Precautions

If AutoAdminLogon is enabled, be careful when running the NetWare Login utility from the icon in the NetWare (Common) group. When run as a standalone utility from the icon, NetWare Login does not recognize that the workstation is running AutoAdminLogon.

If the primary connection's password expires when running NetWare Login from the icon, the user is given the chance to synchronize all NetWare and Windows passwords. Make sure that users do not synchronize the Windows password, because NetWare Login does not update the Registry setting for AutoAdminLogon.

Desktop Management Agent Precautions

Although you can change the login password for the Desktop Management Agent using an applet in the Windows Control Panel, doing so doesn't affect the password setting in the Windows registry. If you change the password using the applet but you don't change it in the registry, AutoAdminLogon settings fail.

For information about changing the password with the applet, see Section 2.2.4, "Using the ZENworks Agent Control Panel Applet To Modify Agent Settings," on page 41.

Understanding the ZENworks Middle Tier Server and the Desktop Management Server

3

This section contains information you can use to help you gain a high-level understanding of the role of the Novell® ZENworks® 7 Middle Tier Server and the Desktop Management Server and how to prepare to use them.

3.1 What Is the ZENworks Middle Tier Server?

The ZENworks Middle Tier Server is installed on a Windows server, a NetWare® server, or a Linux where a Web server (that is, Windows IIS on a Windows server or the Apache Web server on a NetWare server, OES Linux server, or a SLES 9 SP1 server) is already installed. The modules of the Middle Tier Server plug in to the Web server software and act as a Web service. The Middle Tier Server allows access to Novell eDirectory™ and the Windows file system (if running on a Windows server), the NetWare file system (if running on a NetWare server), or the Linux file system (if running on a SLES 9.*x*, SLES 10 (only on ZENworks 7 with SP1), or OES Linux server) for the users and workstations inside or outside the firewall.

Using ZENworks Desktop Management through the Desktop Management Agent and the Middle Tier Server, users can access their applications and policies through a Web server interface. For diagrams showing how the Middle Tier Server works, see Chapter 5, "Process Flow in ZENworks Desktop Management," on page 73.

3.2 Getting Ready to Use the ZENworks Middle Tier Server

The ZENworks Middle Tier Server can be installed on NetWare 6, NetWare 6.5, Windows 2000 servers, Windows Server 2003, SLES 9.*x*, SLES 10 (only on ZENworks 7 with SP1), or OES Linux platforms. The following sections provide details on where to find additional information about the prerequisites, installation steps, and configuration for the Middle Tier Server:

- "Preparing for the Middle Tier Server" on page 54
- "Installing ZENworks Middle Tier Server" on page 54
- "Configuring the ZENworks Middle Tier Server with NSAdmin" on page 54

3.2.1 Preparing for the Middle Tier Server

It is important that you understand the procedure for preparing to install the Middle Tier Server. We recommend that you review the following documentation:

- "Platform Support for the Desktop Management Infrastructure" in "Overview" in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- "Prerequisites for the Workstation Running the Installation" in "Preparation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- "ZENworks Middle Tier Server Limitations" in "Preparation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

This documentation includes information that details the limitations of the ZENworks Middle Tier Server, hardware and software requirements, and other installation prerequisites.

If you plan to install the ZENworks Middle Tier Server on a SLES 9.*x* server , a SLES 10 server (only on ZENworks 7 with SP1), or OES Linux server, see "Preparing a Linux Server for ZENworks Functions" in "Preparation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

3.2.2 Installing ZENworks Middle Tier Server

The procedure you should use for installing ZENworks Middle Tier Server software on a Windows or NetWare server is detailed in "Installing the ZENworks Middle Tier Server" and "Installing the Desktop Management Server and the Middle Tier Server on the Same Machine" in "Windows-Based Installation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The options you can use for installing ZENworks Middle Tier Server software on a SLES 9.*x*, SLES 10 (used for ZENworks 7 with SP1 only), or OES Linux server are detailed in "Installing ZENworks Desktop Management Services on Linux" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

3.2.3 Configuring the ZENworks Middle Tier Server with NSAdmin

When the ZENworks Middle Tier Server software is installed, it creates new registry entries on the machine where it is installed. If you want to edit or configure the configuration parameters, you can edit the registry of the NetWare or Windows server where the ZENworks Middle Tier server is installed, or you can use the NSAdmin utility to change the configuration.

IMPORTANT: Use caution when changing NetWare registry settings. Some NetWare registry entries should be changed only under direction from Novell. Changing the entries could adversely affect the Middle Tier Server, NetStorage, ZENworks Desktop Management, and your NetWare server.

You can invoke the interface of the NSAdmin utility by opening Internet Explorer and entering the NSAdmin URL in the Address box. For example:

http://*ip_address* or *dns_name*/oneNet/nsadmin

It is necessary for users accessing this utility to have the appropriate rights for access. These rights are normally configured when the Middle Tier Server is installed. For more information, see

"Required Rights for NSAdmin Access" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

IMPORTANT: Do not use a browser other than Internet Explorer (for example, Mozilla Firefox) to run the NSAdmin utility. Other browsers cannot run NSAdmin successfully.

It is not necessary to restart Tomcat or Apache or any other service in order for the changes made in NSAdmin to take effect.

If you are running the server on a port number other than port 80, use the following syntax to run the utility:

http://*ip_address or dns_name*:port/oneNet/nsadmin

If you run the server on a port number other than port 80, make sure that when you install the Desktop Management Agent, you configure the IP address for the Middle Tier Server accordingly.

The NSAdmin Web page displays a list of links in the left column that are used to access the various pages for editing and viewing Middle Tier Server configuration information in the registry. Descriptions and information for each NSAdmin page are described in the following sections.

- "General (Xtier 2.6.2 Installation)" on page 55
- "General (Xtier 3.1.x Installation)" on page 57
- "Authentication Domains (Xtier 2.6.2 installation)" on page 60
- "Authentication Domains (Xtier 3.1x Installation)" on page 61
- "WebDav Provider" on page 62
- "iFolder Storage Provider" on page 63
- "NetWare Storage Provider" on page 63
- "Current Sessions" on page 63
- "Resource Usage" on page 63
- "Statistics" on page 64

IMPORTANT: The appearance and functionality of the NSAdmin *Authenication Domains* page varies according to the version of the ZENworks Middle Tier Server you install.

- ZENworks 7 Middle Tier Server installed on NetWare and Windows servers uses Xtier 2.6.2 (see "Authentication Domains (Xtier 2.6.2 installation)" on page 60)
- ZENworks 7 Middle Tier Server installed on Linux servers uses Xtier 3.1 (see "Authentication Domains (Xtier 3.1x Installation)" on page 61)
- ZENworks 7 Middle Tier Server with SP1 installed on NetWare, Windows, or Linux servers uses Xtier 3.1.4 (see "Authentication Domains (Xtier 3.1x Installation)" on page 61)

Please consult the appropriate documentation to understand the differences between these versions of the Middle Tier.

General (Xtier 2.6.2 Installation)

The General page of the NSAdmin utility is the default display.

Figure 3-1 *The General Page of the NSAdmin Utility*

This page lets you view or edit the following configuration settings:

Proxy Username and Proxy Password: This is the admin username and password that you entered when you installed your Middle Tier Server. If you want the Middle Tier Server to use a different username and password for administrator access, enter it in the fields provided.

If you click the *Set Defaults* button, the value is set to whatever value appears in the *Default Value* column. If there is no value in the *Default Value* column, the value is set to blank (no value).

Location: This is the registered location you want users to enter as part of the Middle Tier Server URL to access the ZENworks Middle Tier Server. The default is oneNet.

If you change this registry setting on a ZENworks Middle Tier Server installed on NetWare, you must also edit a configuration file for the change to take effect. Edit the `sys:\netstorage\xsrv.conf` file and change the `/oneNet` setting in the *Location* section (first section) to the same setting you specified in NSAdmin.

Certificate Name: NetIdentity is the default certificate name. It is created automatically during the Middle Tier Server installation. If you purchased a certificate that you want to use or if you just want to use a different certificate, enter the certificate name in this field.

Any certificates used by the Middle Tier Server should reside in the same eDirectory context.

Session Timeout: This is the amount of time in seconds that the session will remain idle before it is terminated. If there is no Middle Tier Server activity for this amount of time, the user is required to log in again to the Middle Tier Server before being allowed file access.

Janitor Interval: This setting should not be changed except under direction from Novell.

Persistent Cookies: The *Persistent Cookies* setting can be turned on or off. With the value set to 0, *Persistent Cookies* is turned off. *Persistent Cookies* is turned on (the default) if there is no value or if the value is set to anything other than 0.

With *Persistent Cookies* turned off, the NetStorage or ZENworks Desktop Management session ends when the user closes the current browser or Web folder. Also, if the user has a current instance of ZENworks Desktop Management or NetStorage up in a browser window or Web folder and starts up a new browser instance or Web folder, the user is required to reauthenticate.

Turning off *Persistent Cookies* can be beneficial if you have workstations that are shared because as long as the browser instance is closed down, the next user of the workstation cannot accidentally or intentionally obtain access to your network through ZENworks Desktop Management or NetStorage.

Leaving *Persistent Cookies* turned on can be beneficial if your workstations are not shared because it prevents users from having to unnecessarily re-authenticate.

If the user selects the *Logout* option in NetStorage or ZENworks Desktop Management, the session ends regardless of whether *Persistent Cookies* is turned on or off.
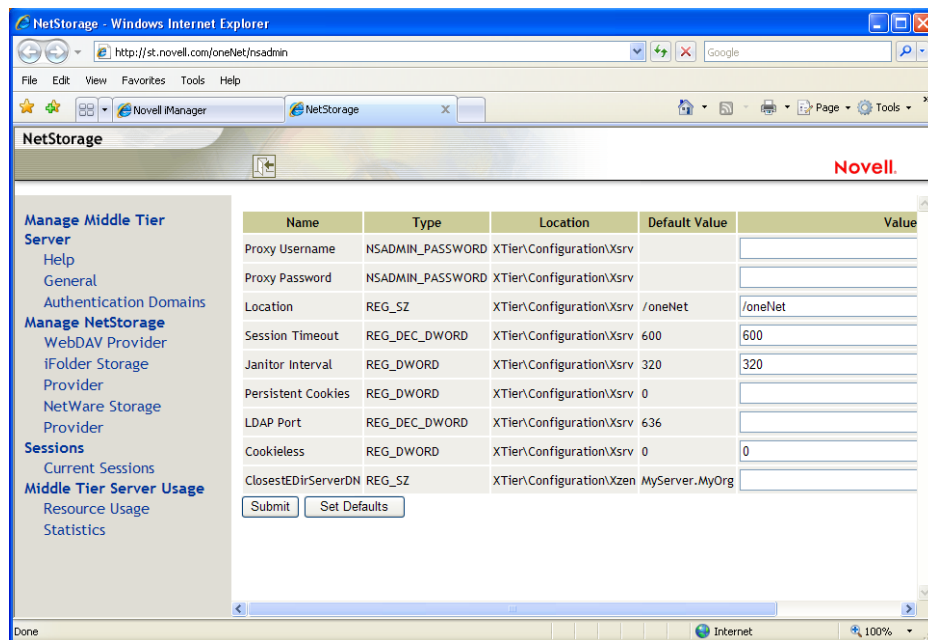
LDAP Port: Lets you change the LDAP port number if there is a conflict between Active Directory* and eDirectory for LDAP requests.

This conflict exists because the back end server is acting as a domain controller, which has Active Directory installed on it. The conflict is created by both eDirectory and Active Directory attempting to use the same default port (the default port number is 389). Active Directory normally wins the conflict. The Proxy User object type exists in eDirectory but not in Active Directory. Because of this, when the Middle Tier Server tries to bind as a Proxy User, the bind attempt fails. This is also the reason LDAP lookups fail.

General (Xtier 3.1.x Installation)

If you install the ZENworks 7 Middle Tier Server on a SLES 9.*x* server or on an OES Linux server, or if you install the ZENworks 7 with SP1 Middle Tier Server, the underlying Xtier kernel, version 3.1*x* (versus the Xtier version 2.6.2 installed with ZENworks 7 for Middle Tier installations on Windows and NetWare) displays a General page that looks like this:

Figure 3-2 *The General Page of the NSAdmin Utility When Xtier 3.1x Is Installed*

This page lets you view or edit the following configuration settings:

Proxy Username and Proxy Password: This is the admin username and password that you entered when you installed your Middle Tier Server. If you want the Middle Tier Server to use a different username and password for administrator access, enter it in the fields provided.

If you click the *Set Defaults* button, the value is set to whatever value appears in the *Default Value* column. If there is no value in the *Default Value* column, the value is set to blank (no value).

Location: This is the registered location you want users to enter as part of the Middle Tier Server URL to access the ZENworks Middle Tier Server. The default is oneNet.

If you change this registry setting on a ZENworks Middle Tier Server installed on NetWare, you must also edit a configuration file for the change to take effect. Edit the `sys:\netstorage\xsrv.conf` file and change the `/oneNet` setting in the *Location* section (first section) to the same setting you specified in NSAdmin.

Certificate Name: NetIdentity is the default certificate name. It is created automatically during the Middle Tier Server installation. If you purchased a certificate that you want to use or if you just want to use a different certificate, enter the certificate name in this field.

Any certificates used by the Middle Tier Server should reside in the same eDirectory context.

Session Timeout: This is the amount of time in seconds that the session will remain idle before it is terminated. If there is no Middle Tier Server activity for this amount of time, the user is required to log in again to the Middle Tier Server before being allowed file access.

Janitor Interval: This setting should not be changed except under direction from Novell.

Persistent Cookies: The *Persistent Cookies* setting can be turned on or off. With the value set to 0, *Persistent Cookies* is turned off. *Persistent Cookies* is turned on (the default) if there is no value or if the value is set to anything other than 0.

With *Persistent Cookies* turned off, the NetStorage or ZENworks Desktop Management session ends when the user closes the current browser or Web folder. Also, if the user has a current instance of ZENworks Desktop Management or NetStorage up in a browser window or Web folder and starts up a new browser instance or Web folder, the user is required to reauthenticate.

Turning off *Persistent Cookies* can be beneficial if you have workstations that are shared because as long as the browser instance is closed down, the next user of the workstation cannot accidentally or intentionally obtain access to your network through ZENworks Desktop Management or NetStorage.

Leaving *Persistent Cookies* turned on can be beneficial if your workstations are not shared because it prevents users from having to unnecessarily re-authenticate.

If the user selects the *Logout* option in NetStorage or ZENworks Desktop Management, the session ends regardless of whether *Persistent Cookies* is turned on or off.

LDAP Port: Lets you change the LDAP port number if there is a conflict between Active Directory* and eDirectory for LDAP requests.

This conflict exists because the back end server is acting as a domain controller, which has Active Directory installed on it. The conflict is created by both eDirectory and Active Directory attempting to use the same default port (the default port number is 389). Active Directory normally wins the conflict. The Proxy User object type exists in eDirectory but not in Active Directory. Because of this, when the Middle Tier Server tries to bind as a Proxy User, the bind attempt fails. This is also the reason LDAP lookups fail.

Cookieless: Cookieless authentication is needed for some clients that use versions of WebDav that don't support cookies. For example, Apple clients use a WebDav version that does not support cookies. The setting is used by NetStorage.

The Cookieless option can be turned either on or off. With the value set to 0, Cookieless authentication is turned off (the default). Cookieless authentication can be turned on by setting the value to 1.

ClosestEDirServerDN: If used, this option requires the distinguished name of the closest eDirectory server where needed applications distributed by ZENworks Desktop Management might reside. The default value is *MyServer.MyOrg*.

This field works in conjunction with "Site Lists" defined for Application objects in ZENworks Desktop Management. When the user has logged on through a Middle Tier Server at his or her site and clicks on an Application icon, the Middle Tier Server determines the location of the nearest eDirectory server where a needed application (defined in the site list) has been stored. The application file is then distributed to the workstation and installed. For more information about Site Lists, see Section 36.3, "Setting Up Site Lists," on page 391 in the *ZENworks 7 Desktop Management Administration Guide*.

The Site List feature is valuable when users move from one site to another and need access to applications on his or her home server, but distribution of those applications over a WAN may be time or cost prohibitive. When a closer eDirectory server contains the application(s) a user needs and site lists are set up, more efficient application distribution is realized.

Authentication Domains (Xtier 2.6.2 installation)

The Authentication Domains page lets you change or add the eDirectory server URLs and contexts that are required by the ZENworks Middle Tier Server. If you installed the ZENworks 7 Middle Tier Server on a Windows or NetWare server, it will look like this:

Figure 3-3 *The Authentication Domains Page of the NSAdmin Utility when the Middle Tier Server's Xtier Kernel, version 2.6.2, is Installed*
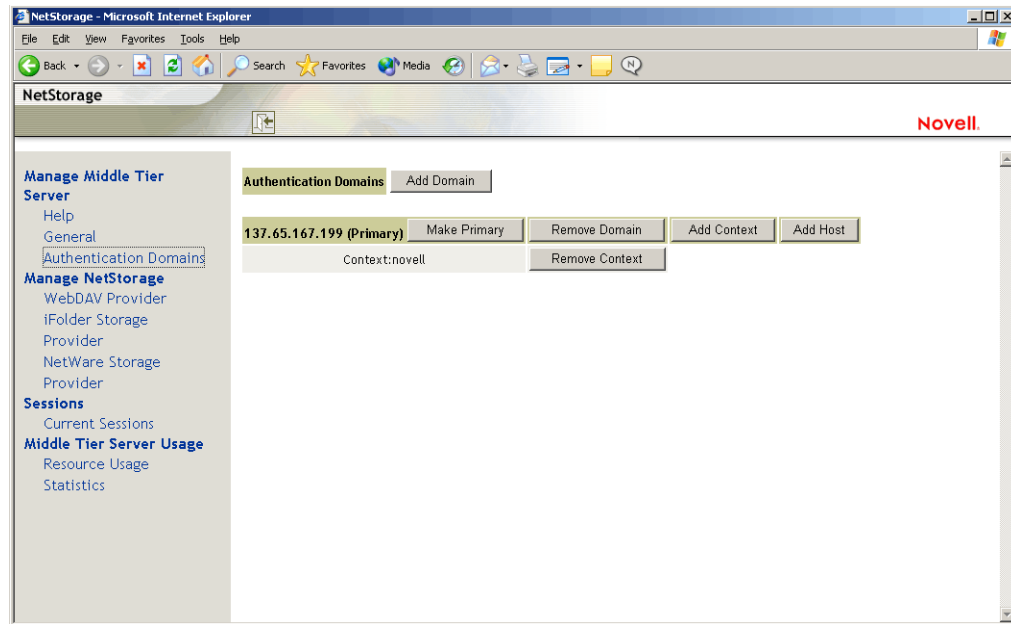
This page also lets you change the eDirectory server that is designated as the Primary. For more information about eDirectory server URLs and contexts, see the *NetStorage Administration Guide* (http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/netstor/data/h9izvdye.html) at http://www.novell.com/documentation/lg/nw6p.

The following list identifies the functions of the buttons on the Authentication Domains page:

Add Domain: Lets you add another eDirectory server IP address or DNS name.

Make Primary: Makes the eDirectory server URL listed above the button the Primary.

Remove Domain: Removes the eDirectory server URL from the list of URLs used by the Middle Tier Server.

Remove Context: Removes the context (if there is one) from the eDirectory server URL.

Add Context: Lets you add a context to the eDirectory server URL.

Add Host: Lets you list additional hosts for an Authentication Domain. Clicking the *Add Hosts* button lets you create a list of alternative hosts for the domain.

If the ZENworks Middle Tier Server cannot reach the host specified in the domain, it searches the *Other Hosts* list specified in the value field to find another server to use for authentication.

Enter DNS names or IP addresses of alternate servers separated by a comma delimiter in the *Value* field. For example, you could enter a string similar to the following:

Zenmaster.provo.novell.com,Zenmaster1.provo.novell.com

or

137.65.67.150,137.65.67.152

Authentication Domains (Xtier 3.1*x* Installation)

If you install the ZENworks 7 Middle Tier Server on a SLES 9.*x* server or on an OES Linux server, or if you install the ZENworks 7 with SP1 Middle Tier Server, the underlying Xtier kernel, version 3.1*x* (versus the Xtier version 2.6.2 installed with ZENworks 7 for Middle Tier installations on Windows and NetWare) displays an Authentication Domains page that looks like this:

Figure 3-4 *Authentication Domains Page of the NSAdmin Utility when the Middle Tier Server's Xtier Kernel, version 3.1 and later, is Installed*
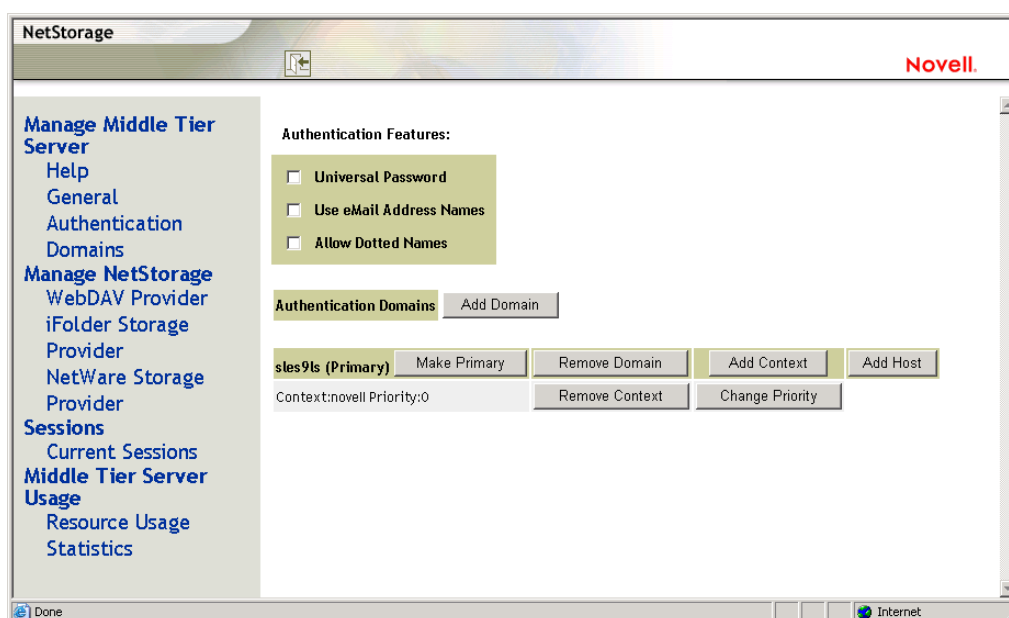
The Authentication Domains page lets you change or add the eDirectory server URLs and contexts that are required by the ZENworks Middle Tier Server.

For more information about eDirectory server URLs and contexts, see the *NetStorage Administration Guide* (http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/netstor/data/h9izvdye.html) at http://www.novell.com/documentation/lg/nw6p.

The following list identifies the functions of the buttons on the Authentication Domains page:

Universal Password: Select this check box if you want to enable Universal Password.

Use eMail Address Names: Select this check box if you want to enable e-mail address names. This allows users to log in to the network through the ZENworks Middle Tier Server by using the same syntax they might be accustomed to when sending e-mail.

Although ZENworks 7 Desktop Management does not enable e-mail or dotted name logins by default (because of the complex process used by the Middle Tier Server to find the user and because

of the network traffic this process might generate), both login methods can be used for authentication when using the Desktop Management Agent.

Authentication contexts configured for the Middle Tier must not contain any embedded dots.

NOTE: In ZENworks 7 Desktop Management with SP1, this check box is still present, but is non-functional. E-mail address name support is automatically enabled with this release.

Allow Dotted Names: Select this check box if you want to enable dotted name support. This functionality (dotted-name support) applies for the user name only, not the user's context. The ZENworks Middle Tier Server does not support authentication to a dotted name in the root context of the eDirectory tree: that is, authentication contexts configured for the Middle Tier must not contain any embedded dots. For more information, see TID 10098582 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

NOTE: In ZENworks 7 Desktop Management with SP1, this check box is still present, but is non-functional. Dotted name support is automatically enabled with this release.

Add Domain: Lets you add another eDirectory server IP address or DNS name.

Make Primary: Designates the eDirectory whose URL is displayed as the primary eDirectory server.

Remove Domain: Removes the eDirectory server URL from the list of URLs used by the Middle Tier Server.

Add Context: Lets you add a context to the eDirectory server URL.

Add Host: Lets you list additional hosts for an Authentication Domain. Clicking the *Add Hosts* button lets you create a list of alternative hosts for the domain.

If the ZENworks Middle Tier Server cannot reach the host specified in the domain, it searches the *Other Hosts* list specified in the *Value* field to find another server to use for authentication.

Enter DNS names or IP addresses of alternate servers separated by a comma delimiter in the *Value* field. For example, you could enter a string similar to the following:

Zenmaster.provo.novell.com,Zenmaster1.provo.novell.com

or

137.65.67.150,137.65.67.152

Remove Context: Removes the context (if there is one) from the eDirectory server URL.

Change Priority: Lets you change the priority for the context to the eDirectory server URL.

WebDav Provider

This page is not used for administration of the ZENworks Middle Tier Server. Do not change the values on this page.

iFolder Storage Provider

This page is not used for administration of the ZENworks Middle Tier Server. Do not change the values on this page.
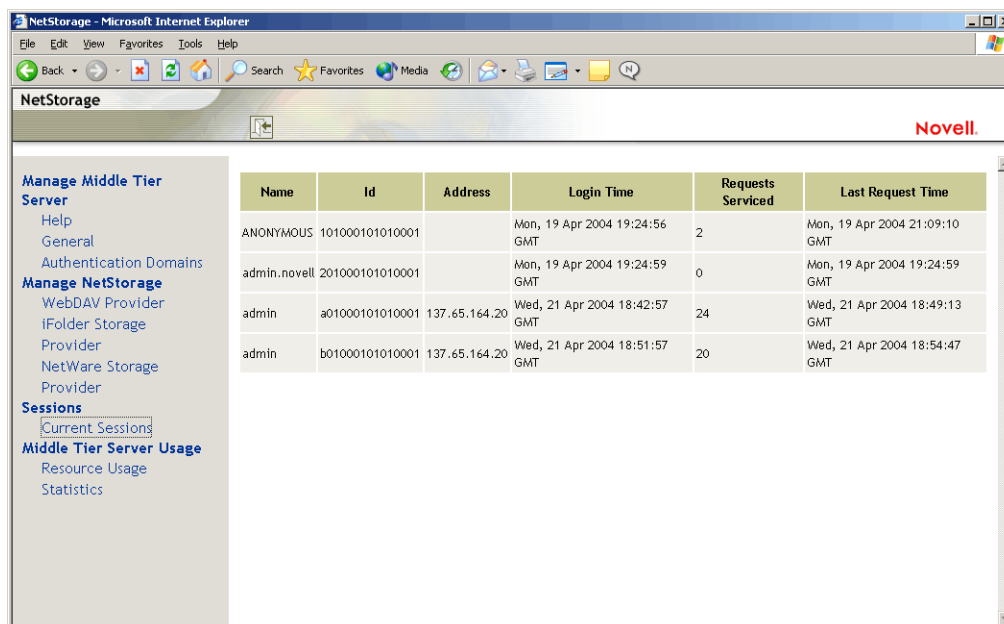
NetWare Storage Provider

This page is not used for administration of the ZENworks Middle Tier Server. Do not change the values on this page.

Current Sessions

The Current Sessions page displays a report with information on the current ZENworks Middle Tier Server sessions. The report is in XML format and can be customized with a parser to provide specific information.

Figure 3-5   *The Current Sessions Page of the NSAdmin Utility*

Resource Usage

The Resource Usage page displays a detailed report of resource utilization (memory, etc.) for the ZENworks Middle Tier Server. The report is in XML format and can be customized with a parser to provide specific information.

Figure 3-6 *The Resource Usage Page of the NSAdmin Utility*

Statistics

The Statistics page displays a report with information like server up time, login failures, and number of sessions active on the ZENworks Middle Tier Server. The report is in XML format and can be customized with a parser to provide specific information.

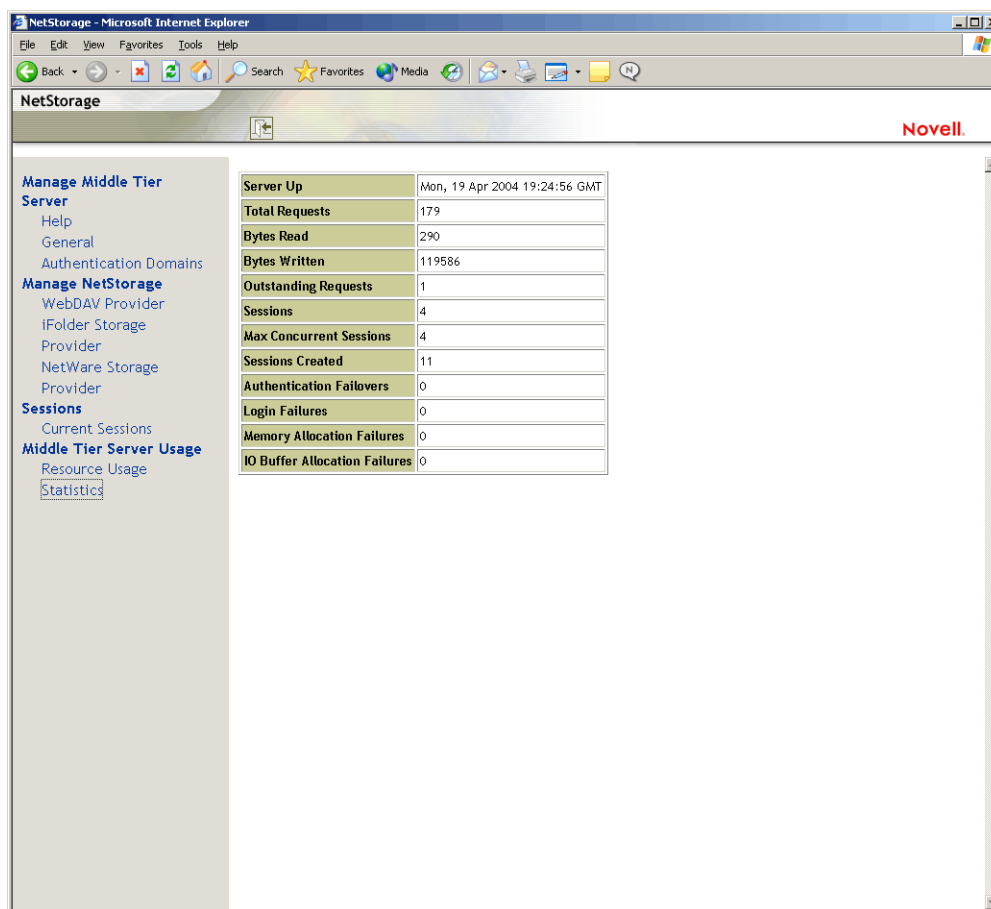**Figure 3-7** *The Statistics Page of the NSAdmin Utility*

3.3 What Is the Desktop Management Server?

The ZENworks Desktop Management Server lets you centrally create and manage policies and profiles for users and workstations on a network. These policies and profiles enable you to distribute, manage, and update applications, perform advanced inventory and remote management functions, and automatically install operating systems on the Windows workstations in your network.

The ZENworks Desktop Management Server can be installed on a Windows 2000/2003 server, a NetWare 6/6.5 server, a SLES 9 SP1 server, or an OES Linux server.

The Desktop Management Server installation program installs selected components and necessary files to the server or servers you select. These components and files are what is sometimes referred to as the "back end" of the ZENworks Desktop Management setup. The back end also includes eDirectory, ZENworks policy and application files, various Desktop Management services, and designated NetWare or Windows servers that are either members of the same tree (if eDirectory is in a NetWare environment) or members of the same Microsoft domain (if eDirectory is in a Windows environment) where the ZENworks files are located.

3.4 Getting Ready to Use the Desktop Management Server

The ZENworks Desktop Management Server can be installed on NetWare 6 SP4 servers, NetWare 6.5 SP3 servers, Windows 2000 SP2 servers, Windows Server 2003 machines, SLES 9 servers, or OES Linux servers. The following sections provide details on where to find additional information about the prerequisites, installation steps, and configuration for the Desktop Management Server:

- "Preinstallation Considerations" on page 66
- "Installing the Desktop Management Server" on page 66
- "Configuring the Desktop Management Server" on page 67

3.4.1 Preinstallation Considerations

It is important that you understand the procedure for preparing to install the Desktop Management Server. We recommend that you review the following documentation, which details the hardware and software requirements and other installation prerequisites of the Desktop Management Server installation.

- "Platform Support for the Desktop Management Infrastructure" in "Overview" in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- "Prerequisites for the Workstation Running the Installation" in "Preparation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- "Prerequisites for Installing the ZENworks Desktop Management Server" in "Preparation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- "Preparing a Linux Server for ZENworks Functions" in "Preparation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

NOTE: If the Desktop Management Server is installed on a Windows 2000/2003 server, the server must have Microsoft Active Directory installed and it must be designated as a Primary Domain Controller (PDC).

If the server has the Novell Client installed, the client must be set up to work over the IP protocol, not IPX™.

If the ZENworks Middle Tier Server is installed on a Windows 2000/2003 server and it will communicate with the Desktop Management Server installed on a Windows 2000/2003 server, both of those servers must be members of the same Microsoft domain.

3.4.2 Installing the Desktop Management Server

The procedure you should use for installing the Desktop Management Server is detailed in "Installing the ZENworks Desktop Management Server" and "Installing the Desktop Management Server and the Middle Tier Server on the Same Machine" in "Windows-Based Installation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The Desktop Management Server installation program lets you install the software to multiple servers, but because the ZENworks Middle Tier Server software installation allows for only one IP entry, not all of the Desktop Management Servers you set up can be used.

You can specify values in the *Add Host* field of the Authentication Domains page of the NSAdmin utility to add other Desktop Management Servers to which your users can background authenticate. If your primary Desktop Management Server goes down, these other servers are connected to the ZENworks Middle Tier Server without losing any ZENworks functionality. For more information, see "Authentication Domains (Xtier 2.6.2 installation)" on page 60.

The options you can use for installing ZENworks Desktop Management Server software on a SLES 9 SP1 or OES Linux server are detailed in "Installing ZENworks Desktop Management Services on Linux" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

3.4.3 Configuring the Desktop Management Server

The Desktop Management Server installation program installs selected `.jar` files to the `\consoleone` directory of the server or servers you also select. These files are the ZENworks 7 Desktop Management snap-ins that you use to manage the ZENworks objects in a directory tree.

The Desktop Management snap-ins are used by ConsoleOne®, a graphical-interface management tool that can be installed and run either on a network server you are authenticated to or to your local workstation. ConsoleOne can view eDirectory objects of ZENworks (for example, workstation objects, application objects, policies, database objects, and so on) in trees to which you are authenticated.

When you manage or create a ZENworks object using ConsoleOne, you can define the path to the server location of application files and policy files. The location of these "ZENworks files" never changes, even though the policy or other eDirectory object that defines them might be replicated throughout the eDirectory tree.

If you want to configure any component of ZENworks 7 Desktop Management, you need to identify the object with which that component is associated and then make the adjustments you want.

For details about creating or configuring the components of Desktop Management, see the appropriate section in this guide:

- Part IV, "Workstation Management," on page 139
- Part III, "Automatic Workstation Import and Removal," on page 125
- Part IV, "Workstation Management," on page 139
- Part V, "Application Management," on page 235
- Part VI, "Workstation and Server Imaging," on page 633
- Part VII, "Remote Management," on page 823
- Part VIII, "Workstation Inventory," on page 881

Understanding the ZENworks Multiple UNC Provider

4

In a Novell® ZENworks® for Desktops 4.*x* environment, accessing ZENworks policy and application files on a network server from a user desktop without using the Novell Client™ or mapped drives required the ZENworks Middle Tier Server, even if a Microsoft Client was available.

Now, in a ZENworks 7 environment, the ZENworks Multiple UNC Provider can use either the Novell Client or the Microsoft Client (through the CIFS/SMB protocol) to increase the speed of customer access to network policies and applications.

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

4.1 What Is the ZENworks Multiple UNC Provider?

The Multiple UNC Provider (MUP) is a Windows service that assists in locating network resources identified using the Uniform Naming Convention (UNC). MUP receives commands containing UNC names from applications and sends the name to each registered UNC provider. When a provider identifies a UNC name as its own, MUP automatically redirects future instances of that name to that provider. Essentially, MUP determines which client the system must use to access the requested UNC name and hands off requests to that client's redirector. The redirector then directs the resource request from the workstation to the device on the network that can provide the resource.

The ZENworks Multiple UNC Provider (ZENMUP) lets workstations establish, on a per session basis, the fastest connection available to network policies and applications based on the customer's environment and what clients they are using. When requests for files (such as group policies, applications, and inventory requests) come from the ZENworks Desktop Management Agent, ZENMUP first attempts to access those files on the identified network volume by using any installed client (calling _access on the network volume to test for existence). If this succeeds, the file system provider registered with Windows claims this network name and native file system calls are used to access all files on that network volume. If no file system provider knows about that network name, the call fails and the ZENworks Middle Tier Server is used to access files on that volume. When the successful access method is determined, that information is stored in the Windows `mup.sys` file during that session. Subsequent file access to the same volume is accomplished with a lookup on that file.

ZENMUP is automatically installed and enabled as part of the ZENworks 7 Desktop Management Agent installation. It doesn't need to be configured and cannot be disabled.
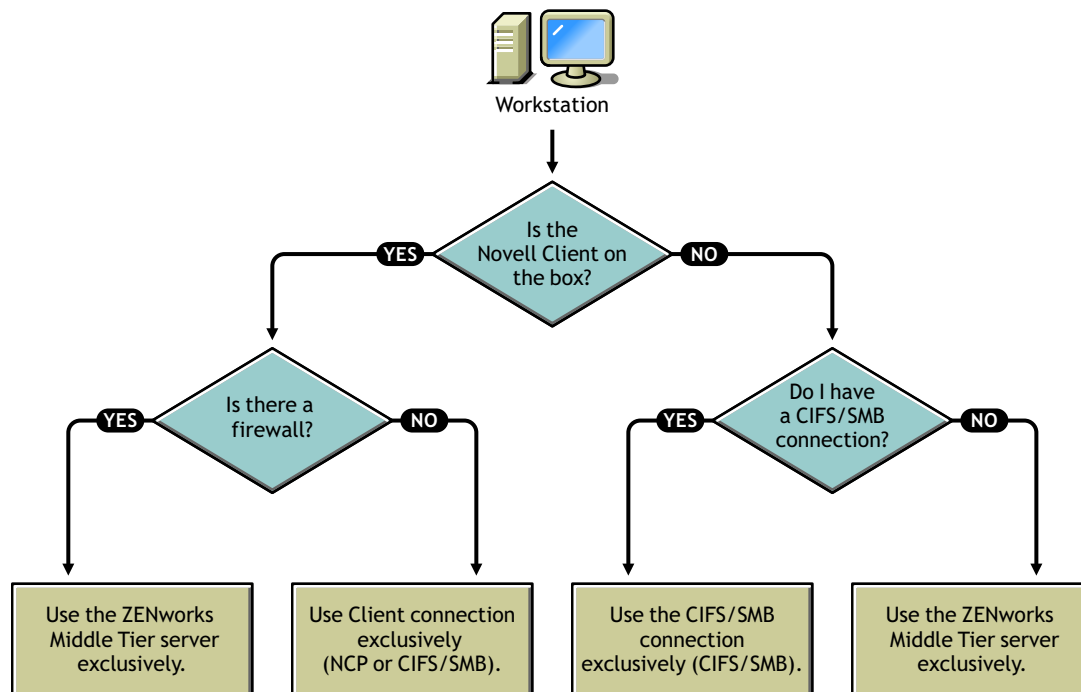
This section contains more specific information about ZENMUP in the following subsections:

4.1.1 How Does ZENMUP Work?

How ZENMUP works depends on the environment in which is it used, as outlined in the following diagram:

Figure 4-1 *How ZENMUP Logic is Invoked when a Network Connection is Established*

For more specific information about ZENMUP behavior in specific server environments, see the following sections:

ZENMUP in a NetWare Server Environment

In a NetWare® server environment, when requests for files come from a workstation, ZENMUP first checks to see if the Novell Client is installed on the workstation. If it is installed, and if no firewall is present, the client uses either the NetWare Core Protocol™ (NCP™) or a CIFS/SMB connection to access the server, depending on the network operating system where the ZENworks files are stored.

IMPORTANT: Using ZENworks 7 with versions of the Novell Client prior to 4.9 SP2, a Middle Tier connection cannot be forced by right-clicking the Application Launcher/Explorer icon and selecting *ZENworks Middle Tier Server Login* (as it could be in ZENworks 4.0.1). Upgrading to Novell Client 4.9 SP2 allows a forced Middle Tier connection in ZENworks 7. If user logins hang, you can remove the ZENworks Middle Tier login option using the Launcher Configuration setting.

If ZENMUP detects that a firewall is present, all communication is done through the ZENworks Middle Tier Server.

If no firewall is present but CIFS is running on the NetWare servers, the NetWare server attaches a - w or _w (depending on the NetWare version) to the CIFS server name to differentiate the CIFS protocol from the NCP protocol, thereby avoiding conflicts. If resources are stored on a Windows server, those resources are accessed by the Microsoft Client using a CIFS/SMB connection.

If the Novell Client is not installed on the workstation, ZENMUP checks to see if there is a CIFS/SMB connection. If there is, ZENMUP uses the CIFS/SMB connection exclusively. If there is no CIFS/SMB connection, ZENMUP uses the ZENworks Middle Tier Server to access the files.

User support inside a firewall (using CIFS only) and continual support when outside a firewall (using HTTP) requires that the Middle Tier Server's host file is configured to recognize the CIFS server name with the -w or _w.

Workstation support is limited to the Middle Tier Server. When configuring the file location, you must specify the server's NetBios name (NetWare machine name), thus forcing the connection to go through the Middle Tier Server.

ZENMUP in a Windows-only Environment

In a Windows-only environment, you must use a domain controller, and each workstation must be a member of the domain. Inside the firewall, the MS Client (CIFS) is always used for connections. Outside the firewall, the Middle Tier Server is used. Because the CIFS/SMB protocol allows Guest authentication to a network volume (with no file rights required for workstations that are not in a Windows domain), all workstations in an agent-only environment must be members of a Windows domain. This allows ZENMUP to function as designed.

ZENMUP in a Linux Server Environment

In an OES Linux server environment using NetWare-style volumes, when requests for files come from a workstation, ZENMUP checks the preferred client protocol: if the Novell Client is installed, and if no firewall is present, ZENMUP uses the NetWare Core Protocol™ (NCP™) to access the Linux server; if the Desktop Management Agent is installed exclusively, ZENMUP uses a CIFS/SMB connection to access the Linux server (if the CIFS/SMB connection fails, ZENMUP attempts an HTTP connection). Essentially, the ZENMUP interacting with OES Linux works the same as it does on a NetWare server (including the behavior inside and outside the firewall).

In a SLES 9*x* or SLES 10 server environment, Samba shares must first be set up and configured. For more information, see "Preparing a Linux Server for ZENworks Functions" in the *Novell ZENworks 7 Desktop Management Installation Guide*. When this is accomplished, the ZENMUP interacting with SLES works the same as it does on a Windows server (including the behavior inside and outside the firewall). The exception to this is that it is not necessary to set up a domain controller nor to make the workstations members of a domain.

Other ZENMUP Considerations

For each network name (server name or IP address), an entry is stored in the Windows mup.sys file telling ZENMUP which connection to use. After a connection has been made, it is saved and used for that session.

NOTE: If your authentication environment changes (for example, if your CIFS server was down during the first access attempt, then you subsequently start it), you must reboot the workstation to refresh the file entries.

ZENMUP is session-based, so any connections made during a session are released when the workstation is rebooted.

4.1.2 ZENMUP Environments Overview

For a quick overview of how ZENMUP works in different environments, see the following table:

Table 4-1 *How ZENMUP Works in Different Network Environments*

Environment	Description
NetWare servers with workstations running the Novell Client	If no firewall is present, either the NetWare Core Protocol (NCP) is used (if accessing files on a NetWare server) or a CIFS/SMB connection is used (if accessing files on a Windows server).
NetWare servers running the CIFS protocol and workstations running the MS Client and the Desktop Management Agent	User support inside the firewall uses CIFS. If ZENMUP detects no direct file access (such as when a firewall is present), all communication is directed through the ZENworks Middle Tier Server (HTTP).
Windows servers with workstations running the Desktop Management Agent only or the Desktop Management Agent and the MS Client.	There must be a domain controller, and all workstations and users must be members of the domain with the appropriate file rights on the network share where the application and policy files are located. Inside the firewall, the MS Client (CIFS) is always used. Outside the firewall, the ZENworks Middle Tier Server is used to access files.
SLES 9 or SLES 10 servers with workstations running the Desktop Management Agent only or the Desktop Management Agent and the MS Client	Samba shares must be set up for file access. Workstations must have the appropriate file rights on the network share where the application and policy files are located. Inside the firewall, the MS Client (CIFS) is always used. To access files on a SLES server outside the firewall, workstations require a Windows Middle Tier Server.
OES Linux servers with workstations running the Novell Client	If no firewall is present, either the NetWare Core Protocol (NCP) is used (if using the Novell Client to access files on an OES or NetWare server) or a CIFS/SMB connection is used (if accessing files on a Windows or SLES server).
OES servers with workstations running the ZENworks Desktop Management Agent	All communication is directed through the ZENworks Middle Tier Server unless Samba is configured to allow direct file access.

Process Flow in ZENworks Desktop Management

5

This section includes information and diagrams that explain the following fundamental processes of Novell® ZENworks® Desktop Management:

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

5.1 Authenticating to eDirectory

Before any applications or policies can be accessed by the user, the user must log in to the network (that is, log in to Novell eDirectory™) to verify login rights and to establish a connection to the network servers where the user needs to be authenticated.

IMPORTANT: LDAP authentication, which is launched when users log in and access ZENworks applications or policies, consumes two of the grace logins granted to a user when the user's password expires. Grace logins are set in ConsoleOne on the Restrictions page (password restrictions section) of the eDirectory User object.

For example, when eDirectory notifies a user that he or she has two grace logins left on a server, that user actually has no grace logins and will not be able to log in until the password is reset.

If you have installed the Novell Client™, the Desktop Management Agent, and the Middle Tier Server, there are three login scenarios:

5.1.1 Logging in Using the Novell Client

When the Novell Client is used to authenticate, all communication to eDirectory and the server file system uses the traditional Novell NCP™ protocol. The client launches as the default login GINA (Graphical Identification and Authentication) user interface. For more information about authenticating with the Novell Client, see "Using the Novell Client for Authentication" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The process of authentication to eDirectory using the 32-bit client in this scenario is illustrated in the following diagram:

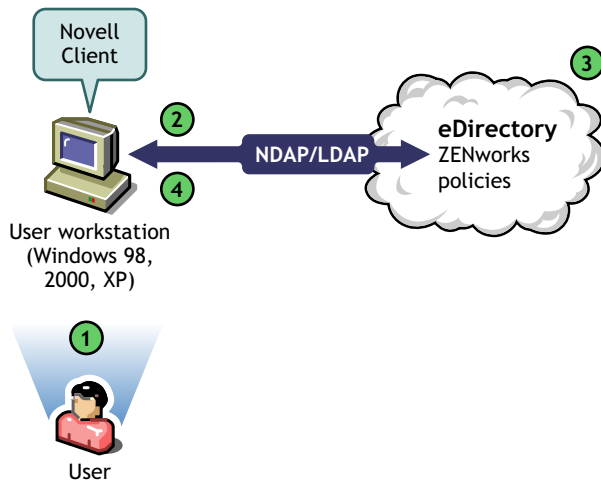**Figure 5-1** *Authentication to eDirectory Using the 32-bit Novell Client*

Table 5-1 *Steps in the eDirectory Authentication Process Using the 32-bit Novell Client*

Step	Explanation
1	A user with the appropriate rights enters eDirectory credentials in the login fields of Novell Client GINA.
2	The Novell Client sends the authentication request to eDirectory in an NDAP/LDAP packet.
3	eDirectory confirms that the login credentials are valid and sends the authentication response packet through NDAP/LDAP to the user workstation.
4	The Novell Client on the user workstation receives the response packet and confirms a successful authentication. The network connection is established.

However, if these same workstations are taken outside of the firewall, the client continues to launch as the default login GINA. Users can log in locally to their own Windows desktops, but they cannot authenticate to eDirectory through the ZENworks Middle Tier Server.

If users who have both the agent and the client installed on their machines want to authenticate and receive applications outside the firewall, they can still do so by using an alternative login method, but their workstations can receive only application files, not Desktop Management policies. For this reason, you should consider removing the client and installing only the agent on workstations that are to be used mainly outside the firewall.

For more information about the alternative login method used when the client and agent are installed together on a workstation outside the firewall, see "Logging in Locally to the Workstation" on page 76.

5.1.2 Logging in Using the Desktop Management Agent

If you install the Desktop Management Agent and you want your users to log in to the network through the agent, you need to understand how the Desktop Management Agent authenticates to the network. For more information about setting up the Desktop Management Agent for authentication, see "Using the Desktop Management Agent and the ZENworks Middle Tier Server for Authentication" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The diagram below shows the process occurring when a user authenticates to eDirectory using the Desktop Management Agent outside the firewall. The process is similar when the user is inside the firewall.

Figure 5-2   *eDirectory Authentication Using the Desktop Management Agent Behind a Firewall*
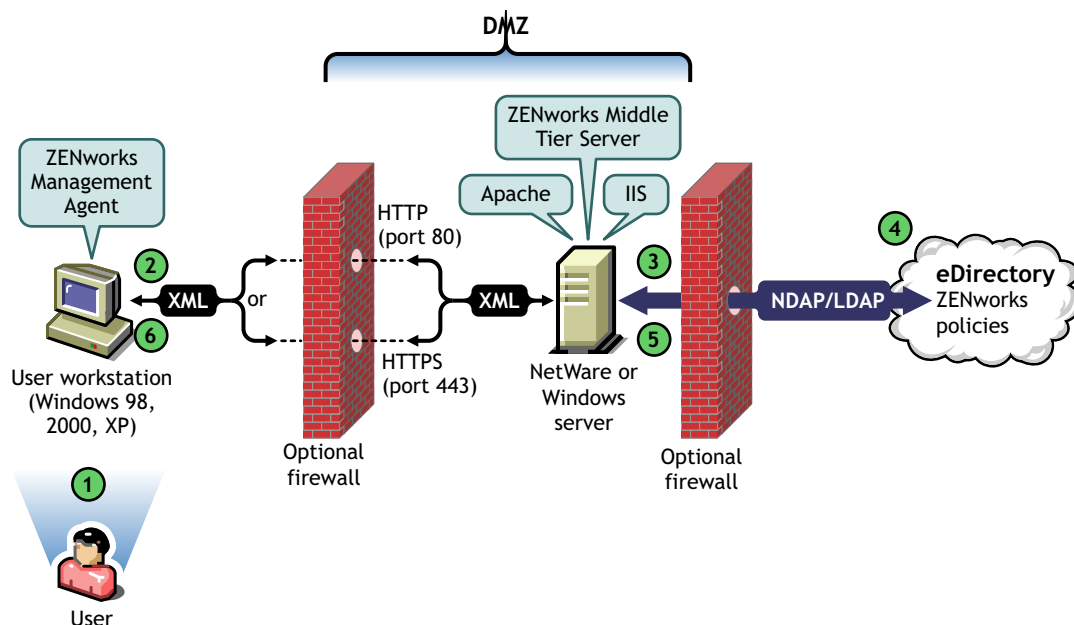

Table 5-2   *Steps of eDirectory Authentication Using the Desktop Management Agent Behind a Firewall*

Step	Explanation
1	A user accesses the ZENworks Management Agent and enters a user ID and password.
2	The agent collects the user credentials. Using public/private key and session key encryption methods, the credentials are securely passed to the ZENworks Middle Tier Server (through a corporate firewall) through HTTP or HTTPS.
	NOTE: Credentials are always secured using the techniques mentioned above whether the transport mechanism is HTTP or HTTPS.
3	The ZENworks Middle Tier Server Web service receives the credentials through the firewall, unparses them, converts them to an NDAP/LDAP packet, and then uses NDAP/LDAP to pass them through a port in the back-end firewall to eDirectory.
	NOTE: No NetWare® licenses are consumed at the ZENworks Middle Tier Server. The licensed connections are consumed by the Desktop Management Server.
4	eDirectory receives the NDAP/LDAP packet, confirms that the login credentials are valid, and sends the authentication response packet through NDAP/LDAP to the ZENworks Middle Tier Server.
5	The ZENworks Middle Tier Server encrypts the returned LDAP or NDAP packet to XML again, then sends the XML confirmation packet over HTTP or HTTPS to the ZENworks Management Agent.

Process Flow in ZENworks Desktop Management   **75**

Step	Explanation
6	The agent receives the XML packet, then unparses it and converts it to binary format, so the user at the workstation can recognize a successful login.

When eDirectory authenticates users, they are authenticated to any server in the tree where the system administrator has granted them rights.

The ZENworks Middle Tier Server uses LDAP/NDAP to authenticate to eDirectory because of the search capabilities of these protocols. If you select *Clear Text Passwords* during the installation of the ZENworks Middle Tier Server, the authentication request can use just the User ID (without its context) to search the entire tree for the authenticating user. Without a clear text password, the user must either log in using his or her fully distinguished name or you must restrict that user to an Authentication Domain, which is a particular context in the directory.

For more information about authentication and the role of the ZENworks Middle Tier Server in ZENworks file access, see Section 3.3, "What Is the Desktop Management Server?," on page 65.

5.1.3 Logging in Locally to the Workstation

If users bypass the Desktop Management Agent login by logging in to the local workstation only, they still need to authenticate to eDirectory to access their applications.

If the Application Explorer icon is displayed on the user's desktop or system tray, the user has the option (by right-clicking the icon) to log in to the ZENworks Middle Tier Server. If the user chooses to log in, the Novell Security Services login GINA is displayed.

Figure 5-3 *The Novell Security Services Login Dialog Box*
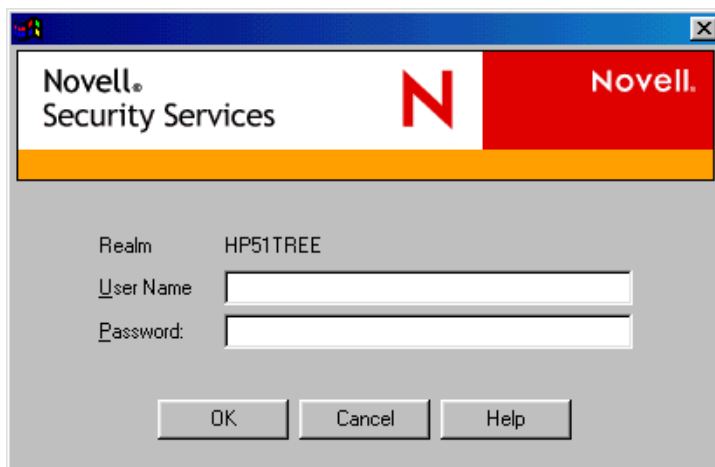
When the user enters his or her user ID and password at the Security Services login GINA, these credentials are given to the ZENworks Middle Tier Server, which passes them to eDirectory for authentication. This login GINA uses the same authentication process used by the Desktop Management Agent login GINA. For more information, see "Logging in Using the Desktop Management Agent" on page 74.

5.2 Reading Attributes from eDirectory

After the user is authenticated to eDirectory, Workstation Manager (or one of its helper `.dlls`) follows steps similar to those used to authenticate to eDirectory in order to access objects in eDirectory. The purpose of this second access is to read eDirectory for attributes; that is, settings that are configured in a directory object or container and intended for applying to the workstation.

For a simplified, step-by-step description of the authentication process, see Section 5.1, "Authenticating to eDirectory," on page 73.

5.3 Accessing Policy and Application Files

After users are authenticated, the ZENworks Desktop Management can access the policy and application files that you have defined for their use, making it possible for their workstations to be configured, managed remotely, or inventoried, and the appropriate software applications pushed to their desktops.

5.3.1 Policy Files

Policies define the capabilities or configuration of a Windows workstation. You can manage these capabilities or configurations according to the user or workstation that is authenticated to eDirectory and associated to the policy. For the most part, when you configure a policy for a workstation or user, these configurations are stored in eDirectory as attributes. These attributes are read by various `.dlls` in the client or agent, and pulled to the workstation at login time by the Workstation Manager. These configurations are stored on the workstation in its registry.

Some workstation configurations, however, are not stored in eDirectory. The iPrint, Group Policies, and Desktop Preferences policies require a defined path to files that must be accessed by the client or Desktop Management Agent and applied to the workstation. For more information about the policies that require file access, see Chapter 10, "Understanding Workstation Management," on page 141.

5.3.2 Application Files

ZENworks 7 Desktop Management lets you manage 32-bit Windows Application objects that are associated to users or workstations. Using ConsoleOne®, you can configure numerous Application objects and associate them to users, workstations, groups, or containers.

The Novell Application Launcher™ uses either the Novell Client or the ZENworks Middle Tier Server to access the application files on NetWare or Windows servers so the files can be distributed, launched, cached, or uninstalled. For more information, see Chapter 23, "Novell Application Launcher: Managing Authentication and File System Access," on page 289.

5.3.3 Accessing Files by Using a Client Inside the Firewall

The process of using a client inside the firewall to access policy or application files (from a path defined in eDirectory) is illustrated in the following diagram:

Figure 5-4 *Using the Novell Client Inside a Firewall to Access Policy or Application Files*

Table 5-3 *Steps in the Process for Using the Novell Client Inside a Firewall to Access Policy or Application Files*

Step	Explanation
1	A user with the appropriate rights enters eDirectory credentials in the login fields of Novell Client GINA and is authenticated to eDirectory through an NDAP/LDAP connection.
	For details, see Section 5.1, "Authenticating to eDirectory," on page 73.
2	The Workstation Manager or the Application Launcher installed on the workstation determines the need to access files and sends a request from the Novell Client to eDirectory in an NCP or CIFS packet.
3	The files are sent to the workstation through an NCP or CIFS packet.

5.3.4 Accessing Files by Using the Desktop Management Agent Outside the Firewall

The process of using the Desktop Management Agent outside the firewall to access policy or application files (from a path defined in eDirectory) is illustrated in the following diagram:

Figure 5-5 *The Process of Using the Desktop Management Agent to Access Policy or Application Files Outside a Firewall*
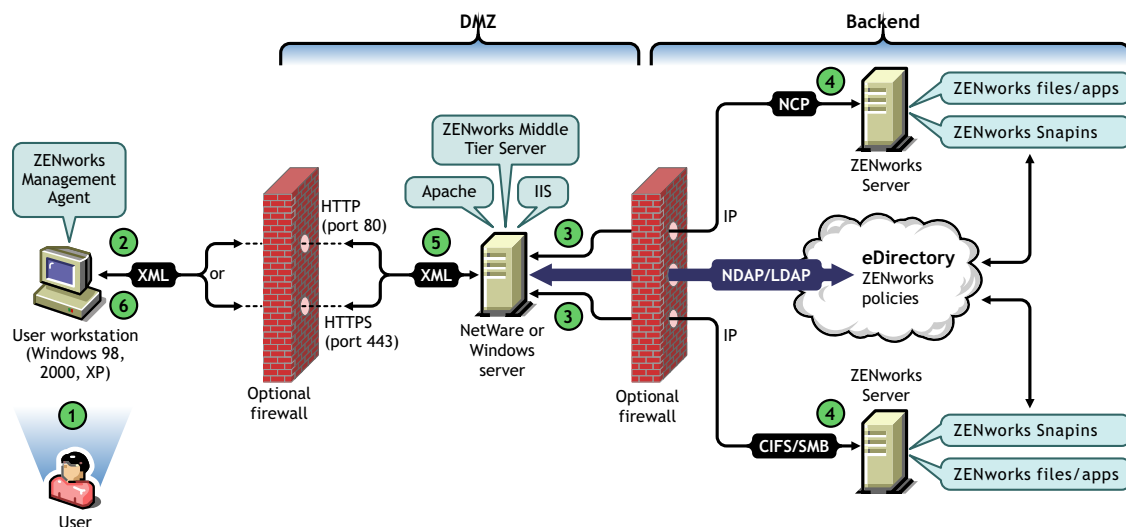
Table 5-4 *Steps in the Process of Using the Desktop Management Agent to Access Policy or Application Files Outside a Firewall*

Step	Explanation
1	A user with the appropriate rights enters eDirectory credentials in the login fields of the Novell Client GINA or the Microsoft Client GINA and is authenticated to eDirectory through an NDAP/ LDAP connection. For details, see Section 5.1, "Authenticating to eDirectory," on page 73.
2	The Workstation Manager (or one of its helper .dlls) or the Application Launcher installed on the workstation determines the need to access files and sends a request to the ZENworks Middle Tier Server in an XML packet, using the HTTP or HTTPS protocol to pass it through a designated port in the corporate firewall to the ZENworks Middle Tier Server.
3	The ZENworks Middle Tier Server Web service receives the request, unparses it, converts it to an NDAP/LDAP packet, and then uses NDAP/LDAP to connect the request to eDirectory.
4	The file location is accessed and the files are sent back to the ZENworks Middle Tier Server in an NCP or CIFS packet. CIFS can be used only if the Middle Tier Server is running on a Windows server.
5	The ZENworks Middle Tier Server converts the returned NCP or CIFS packet containing the files to XML format again, then sends the XML packet over HTTP or HTTPS to the ZENworks Management Agent.
6	The Desktop Management Agent unparses the XML packet containing the files and converts them to binary format to be applied at the workstation.

For more information about users inside the firewall accessing files, see Chapter 4, "Understanding the ZENworks Multiple UNC Provider," on page 69.

Workstation Management Does Not Use the Middle Tier if the Novell Client is Installed on the Workstation

If the Novell Client and the Desktop Management Agent are installed on a workstation (for example, a laptop workstation) and that workstation is taken outside the corporate firewall, only the traditional Novell Client login is displayed at login, and the user can log in locally by choosing *Workstation Only*.

In this scenario, Desktop Management Workstation Management does not utilize the Middle Tier to access eDirectory, and therefore Workstation Manager is in disconnected mode. This means that only cached policies are applied because Workstation Manager does not have an eDirectory connection for the User or the Workstation object. This is similar to the way Application Management works: if users log in *Workstation Only*, they see only the installed applications that are marked "disconnectable" or applications that were force-cached when they were connected.

There is one difference in this scenario between Application Management and Workstation Management. If both the Desktop Management Agent and the Novell Client are installed, and if the agent is configured with a Middle Tier Server address, users can log in to the Middle Tier through the Application Launcher after logging in *Workstation Only* using the Novell Client. In this case, the Application Launcher works in connected mode as it accesses eDirectory and the file system through the Middle Tier Server instead of the Novell Client. However, workstation associated applications do not work because Workstation Manager has already started the NAL Workstation Helper at system startup in order for cached applications to function.

NOTE: If a connection to eDirectory is established through the Novell Client after a user logs in using *Workstation Only*, within 60 seconds of the connection being made, Workstation Manager logs in as the Workstation Object and policies from the Workstation Package are retrieved.

Implementing a DHCP Option for Delivering the Middle Tier Server Address

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

Many corporate employees are often "on the road," required to travel from worksite to worksite while maintaining contact and sharing information with other individuals in the corporation. Routinely, these roaming workers use their laptop computers to help them share information.

If Novell® ZENworks® is installed in the corporate network, and if the ZENworks Management Agent is installed on a roaming user's laptop, he or she can install and run applications that process e-mail and create documents by logging in through the ZENworks Middle Tier Server.

If the corporate network's DNS is not sub-zoned, however, the roaming user might find it necessary to log in through his or her "home" Middle Tier Server, which might be hundreds of miles away and which might require the use of a WAN link. Even in cases where the roaming user tries to log in to an off-site Middle Tier and is presented with a list of Middle Tier Server names to choose from, the inconvenience, loss of time and money make this a less-than-desirable scenario.

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

A.1 Overview

This section explains how to set up a local DHCP server to send out the address of the local Middle Tier Server, making it convenient for roaming users to quickly authenticate as a local node in the corporate network and making it possible to avoid authentication through a distant Middle Tier over a slow WAN link.

When this method is properly implemented, the user's local ZENworks Management Agent uses the configured-site DHCP option to get its Middle Tier information. Based on the information provided by the local DHCP server, the workstation communicates through the Middle Tier Server to the ZENworks Management Server and eDirectory.

IMPORTANT: This method does not work unless you select the *Workstation Management* feature when you install the ZENworks Desktop Management Agent. For more information about installing the agent, see "Installing and Configuring the Desktop Management Agent" in "Windows-Based Installation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

For example, if a user's home base is Toronto, his or her laptop computer uses the Toronto Middle Tier Server when authenticating at that office. If the user travels to São Paulo, Brazil, he or she receives São Paulo Middle Tier Server information when they receive an IP address from the São Paulo DHCP server.

A.2 Creating a New DHCP Option

You need to create and enable a new predefined DHCP Option 100 named "ZENworks" at each DHCP server you will be using in the network environment. The DHCP server sends this option with a configured string value you supply (the local Middle Tier Server address or DNS name) to the agent each time a workstation running in the subnet boots and requests an IP address.

NOTE: When you create the new DHCP option (on either NetWare®, Windows, or SLES 9 SP1/OES Linux servers), make sure that you set the *Data* value as string. For more information, see TID 10092121 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10092121.htm) in the Novell Knowledgebase.

A.3 Changing the DHCP Option

Although by default the DCHP option number sought by the ZENworks Desktop Management Agent is 100, you can change the option number by adding the following DWORD value to the `HKLM\Software\Novell\ZENworks` registry key at the workstation:

`MiddleTierDhcpOptionNumber`

You can set the numeric data (that is, the option number) for this value to any number, but you also need to make sure that the data matches the DHCP option string at the server.

A.4 Checking the Middle Tier Address in the Registry

You can verify that the DHCP option you have created is being used for the Middle Tier address by looking for the following STRING value in the `HKLM\Software\Novell\ZENworks` registry key at the workstation:

`MiddleTierAddress`

You can change the data for this value to the Middle Tier address being delivered from DHCP. If you delete the key, it is re-created with the address in DHCP option on the next reboot.

Using a ZENworks Tree

B

This section contains the following information:

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

B.1 Understanding the ZENworks Tree

If you are concerned about creating change in your corporate directory structure (whether you use eDirectory® or Active Directory), you need to create a dedicated tree in eDirectory that can be used to hold the objects and configure the policies that are managed with Novell® ZENworks®. You use this dedicated "ZENworks tree" to deploy ZENworks Desktop Management without affecting the current tools, identity management processes, or authentication processes you currently have in place with your corporate tree.

After you create the ZENworks tree, you can install the ZENworks Desktop Management Server, the ZENworks Middle Tier Server there, and designate it in the ZENworks Desktop Management Agent installation program so that the ZENworks Desktop Management users and workstations are properly configured and ready to authenticate there.

Because you use the ZENworks tree exclusively for ZENworks, the Workstation objects created by ZENworks Automatic Workstation Import are to be found only in this tree. You create policies, Workstation Image objects, Database objects, and Application objects only in this tree. You can also use Nsure® Identity Manager (shipping with ZENworks 7) to synchronize User objects between your corporate tree and the ZENworks tree, making users available for association with desktop policies and applications, just as the imported workstations are available to be associated with policies and applications.

B.2 The ZENworks Tree in an Active Directory Environment

In order for ZENworks to function in a Windows (Active Directory) environment, you need to install eDirectory to synchronize with Active Directory and to manage your ZENworks objects. For more information, see "Installing in a Windows Network Environment" in "Windows-Based Installation" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

If you don't have Dynamic Local User requirements, you can configure the ZENworks Management Agent configured for pass through mode to display the Windows login when your users log in. If the Windows user credentials match those required by the ZENworks tree (after synchronizing User objects with Novell NSure® Identity Manager 2), users are authenticated to Active Directory and to the ZENworks tree. If the credentials don't match, the user is prompted for credentials again, this time with a ZENworks Management Agent login dialog box.

The following illustration shows a simplified process of using a ZENworks tree in an Active Directory environment.

Figure B-1   *Using a ZENworks Tree in an Active Directory Environment*
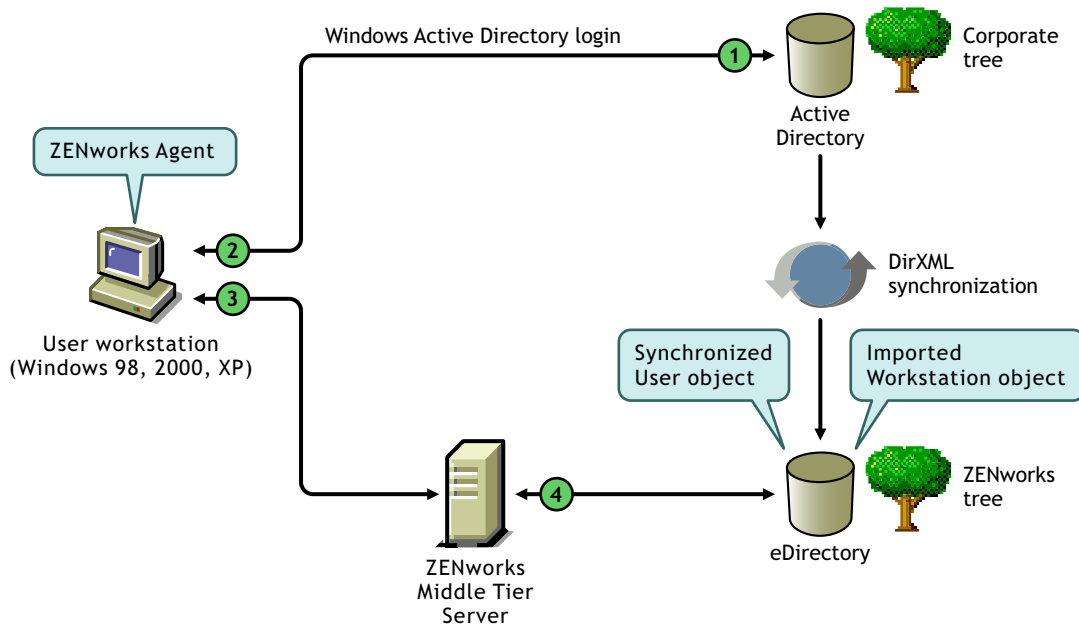
Table B-1   *Steps in the Process of Using a ZENworks Tree in an Active Directory Environment*

Step	Explanation
1	User authenticates to Active Directory.
2	The ZENworks Desktop Management Agent captures accepted user credentials.
3	The ZENworks Desktop Management Agent passes credentials to the ZENworks Middle Tier Server.
4	The user authenticates to the ZENworks tree through the ZENworks Middle Tier Server.

For more information about pass through login, see "Synchronized Passthrough Login" in "Setting Up Authentication" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

B.3 The ZENworks Tree in an eDirectory Environment

If you have an eDirectory corporate tree, you can authenticate to a separate ZENworks Tree (with User objects synchronized with the corporate tree) whether you choose to use the Novell Client or the ZENworks Management Agent in combination with the ZENworks Middle Tier Server.

This section contains the following information:

- ◆ Section B.3.1, "Using the Novell Client," on page 85
- ◆ Section B.3.2, "Using the Desktop Management Agent," on page 85

B.3.1 Using the Novell Client

When users log in using the Novell Client, its login gathers user credentials and authenticates to the corporate tree and to the designated ZENworks tree.

The following illustration shows a simplified process of using the Novell Client to authenticate to a ZENworks tree while simultaneously authenticating to the corporate tree.

Figure B-2   *Using the Novell Client to Authenticate to a ZENworks Tree*
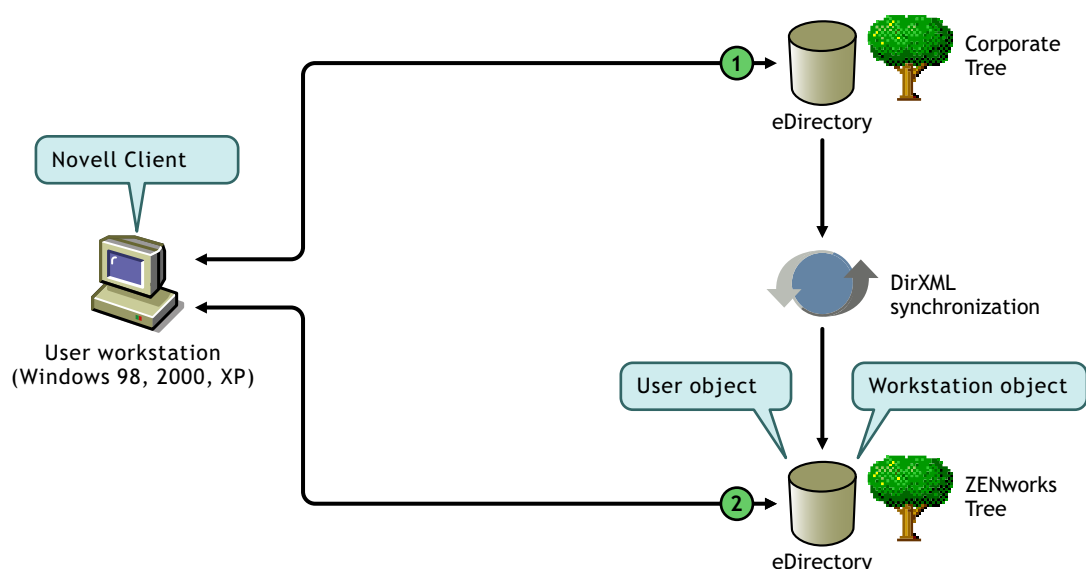
Table B-2   *Steps in the Process of Using the Novell Client to Authenticate to a ZENworks Tree*

Step	Explanation
1	The user authenticates to the corporate tree.
2	The user authenticates to the ZENworks tree.

B.3.2 Using the Desktop Management Agent

If only the ZENworks Desktop Management Agent is installed on workstations, depending on whether pass through is set up, the credentials supplied at the local login dialog box (or at the Agent login if pass through fails) are captured by the ZENworks login and are used to authenticate to both the corporate tree and to the ZENworks tree.

Authenticating to Primary and Secondary Domains

If you set up a ZENworks tree and you plan to use the Desktop Management Agent and the Middle Tier Server to authenticate, you can designate the ZENworks tree as the first authentication site or "primary authentication domain" and the corporate eDirectory tree as a subsequent authentication site, or "secondary authentication domain." For more information about setting up authentication domains, see "Authentication Domains (Xtier 2.6.2 installation)" on page 60.

If an eDirectory object exists in the primary domain and is successfully authenticated, the ZENworks Middle Tier Server looks for the presence of the same object in the secondary domain. If the object exists in the secondary domain there is a successful authentication to the secondary domain. If the object does not exist in the secondary domain, eDirectory fails the authentication to that domain only.

IMPORTANT: The context structure of the primary domain and the secondary domain must be identical (including leaf objects that might be authenticated, such as users or workstations) in order for the authentication to complete successfully.

The following illustration shows a simplified process of using the Desktop Management Agent to authenticate to a primary domain.

Figure B-3 *Using the Desktop Management Agent to Authenticate to a Primary Domain*
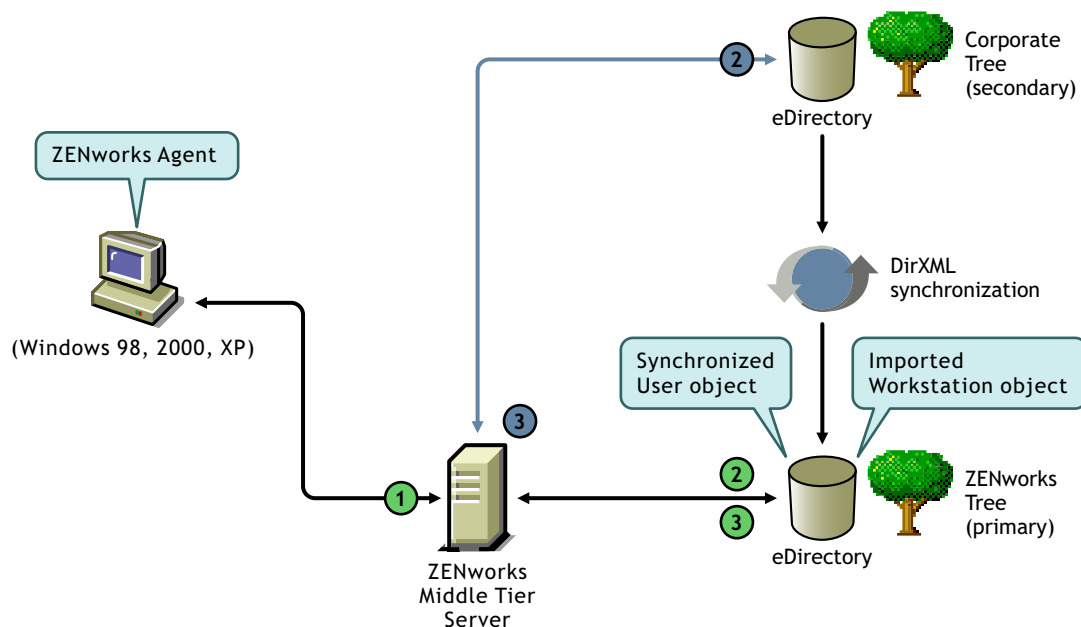
Table B-3 *Steps in the Process of Using the Desktop Management Agent to Authenticate to a Primary Domain*

Step	Explanation
1	The workstation attempts authentication.
2	The ZENworks Middle Tier Server passes credentials to the primary domain (the ZENworks tree).
2	The Middle Tier Server passes credentials to the secondary domain (the corporate tree).
3	The workstation authenticates to the ZENworks tree through the Middle Tier Server.
3	The workstation fails to authenticate through the Middle Tier Server.

The primary/secondary domain setup is particularly useful if, for example, all of your ZENworks objects, including workstations, are in the ZENworks tree, while other critical eDirectory objects (GroupWise objects, for example) are in the corporate tree. In this scenario, the primary

authentication would be to the ZENworks tree, where workstations exist, then to the corporate tree, where workstations do not exist. Many ZENworks applications and policies (Workstation Inventory policies, in particular) are associated to workstations only. If none of your policies or applications are associated with workstations, it is not necessary to designate the ZENworks tree as the primary authentication domain.

E-Mail and Dotted Name Login Support

C

If you want, you can allow users to log in to the network through the ZENworks Middle Tier Server using the same syntax they might be accustomed to when sending e-mail, or you might want them to log in with a more fully-qualified or perhaps a more simplified name that matches your authentication scheme.

IMPORTANT: This functionality (dotted-name support) applies for the user name only, not the user's context. The ZENworks Middle Tier Server does not support authentication to a dotted name in the root context of the eDirectory tree: that is, authentication contexts configured for the Middle Tier must not contain any embedded dots. For more information, see TID 10098582 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

This section explains these login methods and how to configure a workstation to use them. It includes the following information:

NOTE: A new version of the Middle Tier Server (3.1.4) released with Support Pack 1 supports dotted names and e-mail names by default (that is, it is always on), as long as LDAP search is set up correctly.

C.1 E-Mail Formatted Names

E-mail formatted names have the following characteristics:

- They are considered short names, not partial contexts or distinguished names.
- They do not contain escaped (that is, "\.") periods.
- They are found by the common name attribute in LDAP.

The following are some examples of e-mail formatted names:

tjones@example.com
tom.jones@example.com
tom.v.jones@example.com
tom@jones@miami.example.com

C.2 Non-E-Mail Formatted Names

Non-e-mail formatted names are those that:

- Begin or end with a period. Login names in this format are considered to be "fully qualified distinguished names" (FQDN).

- Include both a period and an escaped period (that is, "\."). Login names in this format are considered to be "fully qualified names."

The following are some examples of non-e-mail formatted names:

tom\.v\.jones.miami.example.acme_inc.(FQDN)
tom\.v\.jones.miami.example(FQDN)
tom.v.jones.miami.example
tom.v.jones
tom@jones

If a name includes a period, the Middle Tier Server attempts to authenticate it first as a FQDN. If that authentication fails, the Middle Tier attempts to authenticate the name with the periods escaped ("\.") beginning from left to right. If that authentication fails, the Middle Tier attempts an LDAP search from each configured base distinguished name.

C.3 Enabling E-Mail and Dotted Name Login Support

You can enable e-mail and dotted name login support in the following location of the Windows Registry:

```
HKLM\Software\Novell\Xtier\Configuration\XSrv\Authentication
Domains\DNS_or_IP_Address
```

At the authentication DNS or IP address entry under the authentication domains key, you can add DWORD values to control dotted name support and e-mail name support. The table below shows these values and their possible settings.

Table C-1 *DWORD Values and Settings Used to Control Dotted Name and e-Mail Name Support*

Type of Login Name Support	Setting
Dotted Name Support	1 or 0 (default)
E-Mail Name Support	1 or 0 (default)

At the context entry under the authentication DNS or IP address key, you can add DWORD values to control whether the entered name is attempted as an appendage to the context and whether to attempt an LDAP search from the context. The table below shows these values and their possible settings.

Table C-2 *DWORD Values and Settings Used to Control Dotted name and e-Mail Name Searches*

Type of Search Attempt	Setting
Append Context	1 (default) or 0
LDAP Search	1 (default) or 0

If you specify the Dotted Name Support value as 1 (enabled) at the authentication domain entry, then LDAP Search at the authentication context is always attempted.

NOTE: The registry does not allow a "\" in a key name. This means you cannot use a dotted context in the configuration.

NOTE: A new version of the Middle Tier Server (3.1.4) released with Support Pack 1 supports dotted names and e-mail names by default (that is, it is always on), as long as LDAP search is set up correctly.

Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users

D

Kerberos*, an authentication protocol developed at MIT, requires entities (for example, a user and a network service) that need to communicate over an insecure network to prove their identity to one another so that secure authentication can take place.

The Kerberos protocol has been proven to be highly trusted and valuable security tool for providing secure network authentication. Kerberos functionality is included natively in a Windows* Active Directory* environment, but there are administrators who want to use Kerberos with Novell® eDirectory® (in conjunction with the dynamic local user (DLU) accounts created by ZENworks®Desktop Management) in their NetWare® or Linux environments.

Kerberos requires the use of a Key Distribution Center (KDC) to act as a trusted third party between these entities. Novell has created a proprietary, Linux-based implementation of the KDC that makes eDirectory® its core authentication and identity authority and allows full Kerberos authentication of ZENworks DLU accounts. The Novell Kerberos KDC provides a single point of management, with the advantage of eDirectory replication and security capabilities. It moves Kerberos-specific data to eDirectory and provides Kerberos services using a KDC that accesses data stored in eDirectory.

The information in this section describes how to set up the Novell Kerberos KDC for use in a ZENworks DLU environment.

If you want more specific information about the Novell Kerberos KDC, see the Novell Kerberos KDC documentation (http://www.novell.com/documentation/kdc/) on the Novell product documentation Web site.

This section includes the following information:

- Section D.1, "Kerberos Terms," on page 93
- Section D.2, "Kerberos KDC Services," on page 94
- Section D.3, "Things to Know Before Setting Up the Novell Kerberos KDC for ZENworks DLU," on page 95
- Section D.4, "Setting Up the Novell Kerberos KDC for ZENworks DLU," on page 95

D.1 Kerberos Terms

The following table lists some of the terms that you need to understand as you set up the Novell Kerberos KDC.

Table D-1 *Important Kerberos Terms*

Kerberos Term	Definition
Key (also referred to as Secret Key)	An encryption key shared by a principal and the KDC, distributed outside the system, with a long lifetime. In the case of a user's principal, the key is derived from a password.
Principal	An entity in the network. Each entity corresponds to a principal.
Realm	A logical grouping of principals.
Service	A resource provided to network clients, such as a server holding a ZENworks policy or an application.
Service ticket	A record required to access services in the network.
Session key	A temporary encryption key used between two principals, with a lifetime limited to the duration of a single login session.
Ticket	A record that helps a client authenticate itself to a server. It contains information such as client's identity, a session key, a timestamp, and other information---all sealed using the server's secret key.
Ticket Granting Ticket (TGT)	The initial ticket obtained after a successful login. This ticket is used to get the service ticket to access a service.

D.2 Kerberos KDC Services

A KDC contains the identities and keys of every principal in the network that it must service within its realm. This principal information is stored in a local database within the KDC. In the Novell Kerberos KDC, the principal and realm information is stored in eDirectory.

The following tables list some of the services provided by a typical KDC (including the Novell Kerberos KDC):

- Table D-2, "Basic KDC Services and Their Purpose," on page 94
- Table D-3, "KDC Services Used to Manage KDC and Kerberos Principals," on page 95

Table D-2 *Basic KDC Services and Their Purpose*

Basic KDC Service	Purpose
Authentication Server (AS)	Issues authentication credentials known as Ticket Granting Tickets (TGT) to users while logging in.
Ticket Granting Server (TGS)	Issues service tickets to the users in response to their requests accompanied by TGT so that they can access various services in the realm.

Table D-3 *KDC Services Used to Manage KDC and Kerberos Principals*

KDC Service	Purpose
Kerberos Administration Server	Server component for maintaining Kerberos principals, policies, and service key tables (keytabs). This server responds to the requests from the `kadmin` and `kpasswd` utilities.
Kerberos Administration Utilities	Client component (such as `kadmin`, `kadmin.local`, and `kdb5_util`) for maintaining Kerberos realms, principals, policies, and service key tables.
Kerberos Password Server	Server component of the Kerberos Password utility for changing passwords of Kerberos principals.
Kerberos Client Utilities	Utilities such as `kinit` and `kpasswd`, which are used for various operations like login and changing passwords.

D.3 Things to Know Before Setting Up the Novell Kerberos KDC for ZENworks DLU

Before you begin the setup of the Novell Kerberos KDC for ZENworks DLU, you need to know the following:

- Time synchronization is required to be able to have a working Kerberos environment, make sure that the workstation time varies no more that five minutes from the server time.

- The Kerberos configuration file is located at `/etc/krb5.conf`.

- Kerberos credentials must stay in sync with eDirectory credentials in order to authenticate the user.

- Similar to Active Directory, there is a two step process used for preparing an end user account for Kerberos. Just as in Active Directory, you need to manually add the user principal to the server and then you need to add the workstation principal to the server. In Active Directory this is done when a workstation is added to the domain. With the Novell KDC, you need to use `ksetup.exe` to configure the workstation and then use `kadmin.local` (installed with the Novell KDC) to add it to the server using a process similar to adding a user principal.

- Commands are case sensitive. Make sure the commands are entered correctly.

D.4 Setting Up the Novell Kerberos KDC for ZENworks DLU

This section includes the following information:

NOTE: You need to know the following about the sample setup shown below:

- The Kerberos Realm name is `KERBEROS.YOURCOMPANY.COM.`

- The Kerberos username is `testuser.`

- Kerberos workstation is `testworkstation`.
- The eDirectory root context is `Novell`.
- The Kerberos user context is `Users.Novell`.
- The supported encryption types are `des-cbc-crc` and `hmac`. These are exclusive.
- Commands are case sensitive. Make sure that the commands are entered correctly.

D.4.1 Setting Up the Linux Server

Use the following sample procedure for setting up the KDC to run Kerberos authentication on a SLES 9 (or later) server:

1 Install Novell eDirectory 8.8.1 for Linux, available from the *ZENworks 7 Desktop Management with SP1 Companion 1* CD.

2 Download (http://download.novell.com/Download?buildid=SqdluPPy8KE~) the Novell Kerberos KDC for Linux from the Novell Download site.

3 Using the documentation for the Novell Kerberos KDC (http://www.novell.com/documentation/kdc/), install the Novell Kerberos KDC for Linux.

4 Enter the following commands to set up the proper search paths, based on the installation location of the Novell Kerberos KDC:

```
export PATH=/opt/novell/kerberos/bin/:/opt/novell/kerberos/
sbin/:$PATH
```

```
export LD_LIBRARY_PATH=/opt/novell/kerberos/lib/:/opt/novell/
lib/:$LD_LIBRARY_PATH
```

5 Enter the following command to start the Kerberos daemon:

```
/etc/init.d/krb5kdc start
```

6 Run `kadmin.local` from the shell, then run the following commands for each user and workstation that you want to add to the Kerberos realm:

Command	Comments
`addprinc -x userdn=cn=testuser,ou=Users,o=Novell -e des-cbc-crc:normal,rc4-hmac:normal -pw password testuser`	- Type for each user (`testuser.Users.Novell`) in eDirectory, to create a corresponding Kerberos user principal - The command maps the eDirectory user (`testuser.Users.Novell`) to the kerberos user (`testuser`) - Make sure that the password for this newly created user principal is the same as the password for the user in eDirectory.

Command	Comments
`addprinc -x containerdn=o=Novell -e rc4-hmac:normal,des-cbc-crc:normal -pw` *password* `host/ testworkstation.kerberos.yourcompany.com`	◆ Type for each workstation (`testworkstation`). ◆ Make sure that the password for this newly created workstation principal is the same as the password set with `/SetComputerPassword` in `ksetup.exe` on the Windows workstation.

7 From a new shell, run `tail -f /var/log/krb5kdc.log` before you attempt to connect to the Kerberos server. This command displays all messages or errors in the transaction.

NOTE: In this sample setup, `testuser.Users.Novell` is a user in eDirectory. The workstation (`testworkstation`) is a workstation to add to the Kerberos realm / domain, not necessarily in eDirectory.

D.4.2 Setting Up the KDC for Windows Workstations

Use the following sample procedure for setting up the KDC to run Kerberos authentication on Windows workstations:

1 Download (http://download.microsoft.com/) the `ksetup.exe` utility from Microsoft. The utility is included in the support tools for Windows workstations.

2 Set up the workstation's Kerberos information:

  2a (Optional) Run the following commands from the Windows command line:

Command	Comment
`ksetup /SetRealm` *UPPERCASE_REALM_NAME*	Obtain the Realm Name from the `/etc/ krb5.conf` file.
`ksetup.exe /AddKdc` *UPPERCASE_REALM_NAME KDC_DNS_name*	This command associates the Kerberos server to the Realm where the computer belongs so that the workstation recognizes the server that it needs to contact.
`ksetup.exe /AddKpasswd` *UPPERCASE_REALM_NAME Kerberos_Password_Server_DNS_name*	This command allows access to the Password Server so that you can change Kerberos user passwords from the workstation GINA.

Command	Comment
`ksetup.exe /SetComputerPassword` `computer_password_for_Kerberos_authentication`	This command sets the workstation password to authenticate to the Kerberos server. The password must be the same on both the workstation and the server.

2b (Optional) Run a batch filewith the following configuration (modified according to your Kerberos server) from the Windows command line:

```
@echo off
ksetup.exe /SetRealm KERBEROS.YOURCOMPANY.COM
ksetup.exe /AddKdc KERBEROS.YOURCOMPANY.COM
your_kerberos_server.your_company.com
ksetup.exe /SetComputerPassword password
ksetup.exe /AddKpasswd KERBEROS.YOURCOMPANY.COM novell
ksetup.exe /MapUser testuser@KERBEROS.YOURCOMPANY.COM testuser
ksetup.exe
```

3 Reboot the workstation.

D.4.3 Setup Options

Although ZENworks DLU can do so, you have the option of adding users to the Windows Kerberos registry mappings (local users to kerberos user). Use the following procedure to add users:

1 Run the following command:

```
ksetup.exe /MapUser testuser@KERBEROS.YOURCOMPANY.COM testuser
```

The functionality for enabling DLU on the workstation is set in the Windows Registry at `HKLM\Software\Novell\NWGina\Security`. The DWORD value is `AllowKerberosLoginWithDLU`. When enabled, the setting is 1.

Ports Used by ZENworks 7 Desktop Management

E

This appendix includes information regarding the IP ports used by Novell® ZENworks® Desktop Management, including those that should be open and available for use by various ZENworks components.

Table E-1   *Ports Used by ZENworks 7 Desktop Management*

ZENworks Component Using the Port(s)	Port(s) Used	Service	Protocols
ZENworks Middle Tier Server to Source File Server	524	NCP	TCP, UDP
ZENworks Middle Tier Server to Authentication Domain	389, 636	LDAP	TCP
ZENworks Middle Tier Server to Source File Server	445	CIFS	
ZENworks Middle Tier Server to Desktop Management Server - AWI	8039		
Novell Application Launcher™ using NCP (server and client)	524	NCP	TCP, UDP
Web Server (Middle Tier Server to the Internet)	80, 8080, 443, 8089	HTTP, HTTPS	TCP
Remote Control	80	HTTP	TCP, UDP
Remote Control	524	NCP	TCP, UDP
Remote Control Management Agent (client)	1761 (configureable)		TCP, UDP
Remote Control Listener Port (from ConsoleOne®)	1762 (configureable)		TCP
Service Location Protocol (server)	427		TCP, UDP
Service Location Protocol (client - ephemeral)	1024-1500		UDP
ZENworks Preboot Services: DHCP and Proxy DHCP Servers - PXE (server)	67		TCP, UDP
ZENworks Preboot Services: DHCP and Proxy DHCP Servers - Client Requests (server)	68		TCP, UDP
ZENworks PXE TFTP Server	69		UDP
PXE RPC Port Map Server (Sun RPC)	111		UDP
MTFTP Listener (server)	360		UDP
PXE (Windows Server)	524		

ZENworks Component Using the Port(s)	Port(s) Used	Service	Protocols
PXE Imaging Server Engine	997		
ZENworks Imaging Server	998		TCP
ZENworks Preboot Services: DHCP and Proxy DHCP Servers	4011		UDP
PXE Transaction Server	18753		UDP
Workstation Import Server (AWI server)	8039		TCP
MS SQL Inventory Database JDBC Driver (server)	1433		
Oracle Inventory Database JDBC Driver (server)	1521		
ZENworks Inventory Database (server)	2544		TCP
ZENworks Inventory Database (server)	2638 (configureable)	sybaseanywhere	TCP
ZENworks Inventory Sybase Database	2639 (configureable)		TCP
ZENworks Inventory Sybase Database	2640 (configureable)		TCP
ZEnworks Inventory Service	8080	HTTP	TCP
ZEnworks Inventory Proxy Port	65000		TCP

Documentation Updates

F

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 Personality Migration.

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:

F.1 February 9, 2007

Updates were made to the following sections. The changes are explained below.

F.1.1 Appendix C: E-Mail and Dotted Name Login Support

The following changes were made in this section:

Location	Change
Appendix C, "E-Mail and Dotted Name Login Support," on page 89	Added a note explaining that the limitations on e-mail and dotted name support were lifted with Support Pack 1. The Support Pack fully supports these login methods.

F.1.2 Understanding the ZENworks Middle Tier Server and the Desktop Management Server

The following changes were made in this section:

Location	Change
"General (Xtier 3.1.x Installation)" on page 57	Added this section to explain two new configuration fields in the NSadmin tool.

F.2 October 30, 2006

Updates were made to the following sections. The changes are explained below.

- Section F.2.1, "Appendix C: E-Mail and Dotted Name Login Support," on page 102
- Section F.2.2, "Getting Ready to Use the Desktop Management Agent," on page 102

F.2.1 Appendix C: E-Mail and Dotted Name Login Support

The following changes were made in this section:

Location	Change
Section C.3, "Enabling E-Mail and Dotted Name Login Support," on page 90	Added a paragraph showing the Windows Registry key that is modified to enable e-mail and dotted name login support.

F.2.2 Getting Ready to Use the Desktop Management Agent

The following changes were made in this section:

Location	Change
Section 2.2.4, "Using the ZENworks Agent Control Panel Applet To Modify Agent Settings," on page 41	Added this section to explain a previously undocumented applet.

F.3 July 14, 2006 (Support Pack 1)

The following note was added to each section:

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

Updates were also made to the following sections. The changes are explained below.

- Section F.3.1, "Appendix D: Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users," on page 103

- Section F.3.2, "Understanding the ZENworks Middle Tier Server and the Desktop Management Server," on page 103

F.3.1 Appendix D: Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users

The following changes were made in this section:

Location	Change
Appendix D, "Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users," on page 93	Newly-added appendix.

F.3.2 Understanding the ZENworks Middle Tier Server and the Desktop Management Server

The following changes were made in this section:

Location	Change
Section 3.2.3, "Configuring the ZENworks Middle Tier Server with NSAdmin," on page 54	Added the following sentence: "It is not necessary to restart Tomcat or Apache or any other service in order for the changes made in NSAdmin to take effect."

F.4 January 31, 2006

Updates were made to the following sections. The changes are explained below.

- Section F.4.1, "Appendix E: Ports Used by ZENworks 7 Desktop Management," on page 103

F.4.1 Appendix E: Ports Used by ZENworks 7 Desktop Management

The following changes were made in this section:

Location	Change
Appendix E, "Ports Used by ZENworks 7 Desktop Management," on page 99	Newly-added appendix.

F.5 December 23, 2005

Updates were made to the following sections. The changes are explained below.

- Section F.5.1, "Understanding the ZENworks Middle Tier Server and the Desktop Management Server," on page 104

F.5.1 Understanding the ZENworks Middle Tier Server and the Desktop Management Server

The following changes were made in this section:

Location	Change
Section 3.1, "What Is the ZENworks Middle Tier Server?," on page 53	Added information to reflect the installation of ZENworks Middle Tier Server on OES Linux and SLES 9 SP1 servers.

F.6 December 9, 2005

The page design in the guide was reformatted to comply with revised Novell documentation standards.