

administration guide

Novell[®] Client[™] 2 for Windows Vista*/2008

April 14, 2009

www.novell.com



Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007-2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see [the Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the [Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	9
1 Overview of the Novell Client 2 for Windows Vista/2008	11
1.1 Features and Benefits	11
1.2 How the Novell Client 2 for Windows Vista/2008 Differs from the Novell Client for Windows XP/2003	13
1.2.1 Novell Client for Windows XP/2003 Features Not Included in the Novell Client for Windows Vista/2008	13
1.2.2 Service Location Protocol (SLP) Differences	14
1.2.3 LDAP Contextless Login Differences	16
1.3 Novell Products Not Supported with the Novell Client 2 for Windows Vista/2008	16
1.4 Novell Features Not Included in the Novell Client 2 for Windows Vista/2008	16
2 Advanced Installation Options	17
2.1 Understanding the Basic Novell Client Installation (setup.exe)	17
2.1.1 Selecting a Language	18
2.2 Understanding the Novell Client Install Manager (nciman.exe)	21
2.2.1 Creating the Novell Client Properties File	21
2.3 Using the Install.ini File	22
2.4 Understanding Automatic Client Update (acu.exe)	23
2.4.1 Setting Up the Novell Client Update Agent	24
2.5 Selecting a Network Server Distribution Option	25
2.5.1 Distributing the Novell Client Using Login Scripts	25
2.5.2 Sample Client Installation Login Script	25
2.6 Pre-distributing a Trusted Publisher Certificate for the Novell Client Installation	26
3 Authenticating to a Novell Network	29
3.1 Windows Vista and Windows Server 2008 Credential Providers	29
3.2 Novell Credential Provider	31
3.2.1 Logon	31
3.2.2 Locking and Unlocking the Workstation	33
3.2.3 Fast User Switching	33
3.2.4 Logon Using Windows Server 2008 Terminal Services	34
3.3 Logging in When eDirectory and Windows Credentials Are Not Synchronized	35
3.4 Changing Passwords	36
3.4.1 Changing Your Password When Authenticated to eDirectory	36
3.4.2 Changing Your Password When Not Authenticated to eDirectory	38
4 Setting Client Properties	39
4.1 Setting Properties During Installation	39
4.2 Setting Properties on a Single Workstation after Installation	40
4.2.1 Client Settings	41
4.2.2 Login Profiles Settings	41
4.2.3 Advanced Login Settings	43
4.2.4 Update Agent Settings	46
4.2.5 Service Location Settings	47

4.2.6	Advanced Settings	48
4.2.7	Advanced Menu Settings	50
4.2.8	LDAP Contextless Login Settings	53
4.2.9	Name Services Settings	54
4.3	Setting Properties on Multiple Workstations after Installation	55
5	Managing File Security	57
5.1	Checking File or Folder Rights	57
5.2	Changing Trustee Rights	58
5.3	Adding a Trustee	59
5.4	Removing a Trustee	60
5.5	Combining Multiple Trustees	60
6	Managing Passwords	63
6.1	Creating Strong Passwords	64
6.2	Displaying Password Requirements for End Users	64
6.3	Using Forgotten Password Self-Service	66
6.3.1	Using the "Did You Forget Your Password?" Link	66
6.3.2	Using Hints for Remembering Passwords	69
6.4	Setting Up Passwords in Windows	71
7	Security Considerations	73
7.1	Security Features	73
7.2	Known Security Threats	74
7.3	Security Characteristics	74
7.3.1	Identification and Authentication	74
7.3.2	Authorization and Access Control	75
7.3.3	Roles	75
7.3.4	Security Auditing	75
7.4	Other Security Considerations	75
8	Managing Login	77
8.1	Setting Up Login Scripts	77
8.2	Setting Up Login Restrictions	77
8.3	Customizing the Novell Login	79
8.4	Logging In to the Network	81
8.5	Logging Out of the Network	81
8.6	Setting Up Login Profiles	81
8.6.1	Creating a System Login Profile	84
8.6.2	Creating a System Login Profile for Use on Multiple Workstations	85
8.6.3	Viewing or Editing a System Login Profile's Properties	87
8.6.4	Removing a System Login Profile	88
8.6.5	Enabling the Use of DHCP In a System Login Profile	88
8.7	Setting Up LDAP Contextless Login and LDAP Treeless Login	90
8.7.1	Setting Up Novell LDAP Services for eDirectory	91
8.7.2	Setting Up LDAP Contextless Login on One Workstation	94
8.7.3	Setting Up LDAP Contextless Login on Multiple Workstations	96
8.7.4	Logging In Using LDAP Contextless Login	96
8.7.5	LDAP Contextless Login Differences in the Novell Client for Windows Vista/2008	97
8.8	Configuring 802.1X Authentication	97
8.8.1	Enabling 802.1X Authentication	98

8.8.2	Enabling Wired 802.1X Authentication on Windows Vista	99
8.9	Enabling AutoAdminLogon	101
8.9.1	Enabling a Windows-Only Login	101
8.9.2	Enabling an eDirectory AutoAdminLogon	102
8.10	Enabling TSClntAutoAdminLogon	102
8.10.1	Enabling the TSClntAutoAdminLogon policy	103

A Documentation Updates 105

About This Guide

This guide describes how to configure the Novell® Client™ 2 for Windows Vista/2008 software and contains the following sections:

- ◆ Chapter 1, “Overview of the Novell Client 2 for Windows Vista/2008,” on page 11
- ◆ Chapter 2, “Advanced Installation Options,” on page 17
- ◆ Chapter 3, “Authenticating to a Novell Network,” on page 29
- ◆ Chapter 4, “Setting Client Properties,” on page 39
- ◆ Chapter 5, “Managing File Security,” on page 57
- ◆ Chapter 6, “Managing Passwords,” on page 63
- ◆ Chapter 8, “Managing Login,” on page 77
- ◆ Chapter 7, “Security Considerations,” on page 73

Audience

This guide is intended for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the latest version of this documentation, see the [Novell Client online documentation \(http://www.novell.com/documentation/vista_client/index.html\)](http://www.novell.com/documentation/vista_client/index.html) Web site.

Additional Documentation

For information on installing the Novell Client 2 for Windows Vista/2008, see the *Novell Client 2 for Windows Vista/2008 Installation Quick Start*.

For information on using the Novell Client 2 for Windows Vista/2008, see the *Novell Client 2 for Windows Vista/2008 User Guide*.

For information on login scripts, see the *Novell Login Scripts Guide (http://www.novell.com/documentation/linux_client/login/data/front.html)*.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

Overview of the Novell Client 2 for Windows Vista/2008

1

The Novell® Client™ 2 for Windows Vista/2008 provides Windows connectivity to NetWare® and OES Linux* servers.. With the Novell Client, you can browse through authorized Novell directories, transfer files, and use advanced Novell services directly from a Windows Vista workstation or a Windows 2008 server.

After it is installed on workstations, the Novell Client lets users enjoy the full range of Novell services, including authentication via Novell eDirectory™, network browsing and service resolution, and secure and reliable file system access. All services are delivered through industry-standard protocols. The Client also supports the Novell traditional NCP™ protocol.

The Novell Client for Windows Vista/2008 is a separate release from the current Novell Client 4.91 for Windows XP/2003. The Novell Client for Windows Vista/2008 supports both the x86 and x64 versions of Windows Vista and has many of the same features as the Novell Client 4.91 for Windows 2000/XP. A separate iPrint Client that can be installed as a standalone item and used for printing is also available from Novell.

This section contains the following information:

- ♦ [Section 1.1, “Features and Benefits,” on page 11](#)
- ♦ [Section 1.2, “How the Novell Client 2 for Windows Vista/2008 Differs from the Novell Client for Windows XP/2003,” on page 13](#)
- ♦ [Section 1.3, “Novell Products Not Supported with the Novell Client 2 for Windows Vista/2008,” on page 16](#)
- ♦ [Section 1.4, “Novell Features Not Included in the Novell Client 2 for Windows Vista/2008,” on page 16](#)

1.1 Features and Benefits

- ♦ Support for Novell Open Enterprise Server (OES) 1, OES 2, NetWare 5.1, NetWare 6.0, and NetWare 6.5
- ♦ File system integration with NSS and non-NSS volumes via NCP
- ♦ Login script processing
- ♦ Notification area (Red N) options

Many of the Novell Client features are available when you right-click the **N** icon in the notification area of the taskbar, located in the bottom right portion of your screen. For more information, see “[Using the Novell Client for Windows Vista/2008 Red N Menu](#)” in the *Novell Client for Windows Vista/2008 User Guide*.

- ♦ Integrated login with Windows (single username and password)

The Novell Client for Windows Vista/2008 provides a single, synchronized login to the Windows desktop and the Novell network. Users enter their names and passwords only once to access all the resources they are authorized to use.

- ♦ Integrated eDirectory login support for Windows Terminal Services

- ◆ Integrated eDirectory login and script support for TS Remote Applications
- ◆ NMAS™ client integration
- ◆ Forgotten password recovery options for eDirectory

You can provides users with the ability to recover from a forgotten password without contacting the help desk. For more information, see [Section 6.3, “Using Forgotten Password Self-Service,” on page 66.](#)

- ◆ LDAP contextless login support

LDAP contextless login makes it unnecessary for your users to manage or know about changes to their organization’s name or its placement in the hierarchy. Because users no longer need to enter their context to authenticate, the context can be changed on the back end as many times as necessary without the users knowing and without the costs associated with managing and supporting these changes.

For more information, see [Section 8.7, “Setting Up LDAP Contextless Login and LDAP Treeless Login,” on page 90](#) and [Section 1.2.3, “LDAP Contextless Login Differences,” on page 16.](#)

- ◆ DFS junctions
- ◆ Support for 802.1x wireless authentication

See [Section 8.8, “Configuring 802.1X Authentication,” on page 97](#) for more information.

- ◆ DHCP-based configuration options

The Novell Client is able to use DHCP-supplied configuration values for the Novell login profile's *Tree*, *Context* and/or *Server* fields. For more information, see section “[Enabling the Use of DHCP In a Personal Login Profile](#)” in the *Novell Client 2 for Windows Vista/2008 User Guide*.

In addition, the OpenSLP support in the Novell Client is able to retrieve DHCP-supplied configuration information for the SLP Directory Agent and/or SLP Scope to use."

- ◆ SLP (moved to OpenSLP instead of the proprietary SRVLOC)

For more information, see [Section 1.2.2, “Service Location Protocol \(SLP\) Differences,” on page 14.](#)

- ◆ Shell extensions for Windows’ file browser
- ◆ File caching/shared open mode support
- ◆ Auto-reconnect for NCP connections
- ◆ Cluster failover support for NCP connections
- ◆ Novell Client settings management and install-time pre-configuration

1.2 How the Novell Client 2 for Windows Vista/2008 Differs from the Novell Client for Windows XP/2003

Using the Novell Client 2 for Windows Vista/2008 differs in a few ways from using the Novell Client for Windows XP/2003. For users and network administrators who are familiar with the Novell Client for Windows XP/2003, knowing these differences can help the transition to Windows Vista run more smoothly.

- ♦ [Section 1.2.1, “Novell Client for Windows XP/2003 Features Not Included in the Novell Client for Windows Vista/2008,” on page 13](#)
- ♦ [Section 1.2.2, “Service Location Protocol \(SLP\) Differences,” on page 14](#)
- ♦ [Section 1.2.3, “LDAP Contextless Login Differences,” on page 16](#)

1.2.1 Novell Client for Windows XP/2003 Features Not Included in the Novell Client for Windows Vista/2008

The following Novell Client for Windows XP/2003 features are not included in the Novell Client for Windows Vista/2008:

- ♦ Compatibility with any version of Windows other than Windows Vista or Windows Server 2008.

The Novell Client 4.91 for Windows continues to support Windows XP and 2003.

- ♦ Compatibility to NetWare 5.0 and all prior versions.
- ♦ Novell Graphical Login at Windows boot.

There is no direct concept of this in Windows Vista, because the Graphical Identification and Authentication (GINA) credential input extension model was replaced by the credential provider model. For more information, see [Create Custom Login Experiences With Credential Providers For Windows Vista \(http://msdn.microsoft.com/msdnmag/issues/07/01/CredentialProviders/default.aspx\)](http://msdn.microsoft.com/msdnmag/issues/07/01/CredentialProviders/default.aspx) and [Chapter 3, “Authenticating to a Novell Network,” on page 29](#).

- ♦ Queue-based or NDPS[®] printing support.
Printing support is provided by iPrint
- ♦ 16-bit applications and libraries.
- ♦ Compatibility Mode Driver (CMD).
- ♦ NetWare IP (NWIP).
- ♦ IPX/SPX[™] protocols and API libraries.
- ♦ Catalog Services version of contextless login.
- ♦ NetIdentity Client.
- ♦ Bindery-mode authentication.
- ♦ UNC path handling (NWFilter).

1.2.2 Service Location Protocol (SLP) Differences

Both the Novell Client 2 for Windows Vista/2008 and the Novell Client for Linux* use the OpenSLP User Agent (UA) for performing Service Location Protocol (SLP) based name resolution. OpenSLP is an open source effort to maintain a standards-compliant SLP User Agent (UA) and Directory Agent (DA) implementation. More information on OpenSLP can be found at <http://openslp.org> (<http://openslp.org>).

For Novell Client 4.91 for Windows XP/2003 users, there are noticeable differences between how the Novell Client 4.x SRVLOC SLP User Agent (UA) operates and how the OpenSLP LIBSLP UA operates. This section describes some of the significant known differences between the two SLP User Agents.

- ♦ “Novell Client 4.x SRVLOC User Agent” on page 14
- ♦ “Novell Client 2 for Windows Vista/2008 OpenSLP LIBSLP User Agent” on page 15

Novell Client 4.x SRVLOC User Agent

By default, the following behaviors occur with the Novell Client 4.x for Windows XP/2003 SRVLOC User Agent (UA):

- ♦ The SRVLOC UA initiates discovery of new SLP Directory Agents (DAs) as soon as Windows provides notification that a new TCPIP network interface was created (that is, as soon as each network interface indicates it is physically connected and also has an IP address assigned to it). SRVLOC initiates a DHCP Inform request for SLP configuration information and/or a multicast query for SLP DAs at that time, as appropriate, and saves the SLP DA information learned from each interface.

Any SLP DAs that were manually configured on the workstation are considered global, and apply to all interfaces. Any SLP DAs that are learned through DHCP or by multicast are associated with the specific interface over which they were learned. When a network interface becomes disconnected, the SLP DA information associated with that interface is also removed.

- ♦ When the Novell Client issues a name resolution request through SRVLOC, all SLP scopes that the SRVLOC UA has been configured with or learned from DAs are used when making the request. For example, if a Novell Client 4.x machine knows of scopes “CORPORATE” and “PARTNER,” a name resolution request is made for both “CORPORATE” and “PARTNER” on any DAs that declared that they support these scopes.
- ♦ If the SRVLOC UA was configured to support both SLP v2 and SLP v1 and the SLP v2 DAs did not return answers for a query, or the DAs did not support the scopes being queried, the SRVLOC UA issues an unscoped SLP v1 query to any SLP v1 DAs or by multicast to determine whether the service was registered in the SLP v1 unscoped scope.
- ♦ The SRVLOC UA supports diagnostic and status information that can be queried programmatically. The `SLPINFO.EXE` tool queries and presents this information to aid in confirming and troubleshooting SLP configurations.
- ♦ When unicasting directly to an SLP DA, the SRVLOC UA uses UDP datagram communication unless the answer being returned by the DA cannot fit within a UDP datagram. In such an event, a TCP connection to the SLP DA is created long enough to obtain the large result.
- ♦ To work around the issue described in [TID 10095884: Novell Client is unable to communicate with OpenSLP Directory Agent over SLPv2](http://support.novell.com/docs/Tids/Solutions/10095884.html) (<http://support.novell.com/docs/Tids/Solutions/10095884.html>), the SRVLOC UA allows setting a “Use SingleEquals in Where (V2)” policy to cause a single equals character to be used in predicate strings.

Novell Client 2 for Windows Vista/2008 OpenSLP LIBSLP User Agent

By default, the following behaviors occur with the OpenSLP LIBSLP User Agent (UA) used in the Novell Client 2 for Windows Vista/2008:

- ♦ The OpenSLP UA does not perform “preemptive discovery” of SLP Directory Agents (DAs). Instead, the OpenSLP UA waits until there is an actual name resolution request to perform, at which point SLP DA discovery by DHCP and multicast can occur. Both DHCP Inform discovery of SLP configuration information and multicast-based discovery of DAs and services occur over all active interfaces.
- ♦ The OpenSLP discovery process attempts SLP scope and DA discovery in a specific order: first, by manually configured DA and scope information; second, by DHCP-supplied DA and scope information; and finally, by DA and scope information learned from multicast. This order is important because the OpenSLP DA discovery process stops as soon as one or more DAs are successfully found.
- ♦ During the DA discovery process, the OpenSLP UA intends to find and use just one DA. The OpenSLP UA looks for a DA that supports any one of the scopes the OpenSLP UA is currently configured to use. For example, if the OpenSLP UA currently knows of scopes “CORPORATE” and “PARTNER,” OpenSLP looks for any DA that supports “CORPORATE” or any DA that supports “PARTNER.”

Whichever DA the OpenSLP UA finds first is the only DA (and therefore the only scope) that the OpenSLP UA uses to obtain answers from. The OpenSLP UA does not query both the DAs serving “CORPORATE” and the DAs serving “PARTNER.” The UA queries only one or the other.

While the OpenSLP UA supports configuration with multiple scopes and DAs, the OpenSLP UA only expects to find or use one of those scopes (and therefore, only those DAs supporting that scope) within a given network environment.

There is some merit in manually configuring an OpenSLP UA workstation with a list of more than one scope and more than one DA if the workstation physically moves between networks that require one scope versus the other. DHCP-delivered SLP configuration information can achieve the same goal by delivering only the scope name and DA address information appropriate for the network environment that the DHCP server serves.

- ♦ The OpenSLP UA is designed for SLP v2 operation only.
- ♦ Neither the OpenSLP UA nor the manner in which the Novell Client 2 for Windows Vista/2008 employs it currently supports the level of diagnostic information that `SLPINFO.EXE` provided. The OpenSLP project supports logging in general, but currently only supports logging in the OpenSLP DA, not the OpenSLP UA.

As such, capturing a network traffic LAN trace of a workstation's SLP interaction is usually the most effective tool for troubleshooting SLP-related actions on a Novell Client for Windows Vista workstation or Windows 2008 server.

- ♦ When unicasting directly to an SLP DA, the OpenSLP UA always uses TCP connections to the SLP DA. UDP is still used for multicast and broadcast discovery and queries, but DA connections are TCP-only.
- ♦ The OpenSLP UA (or more specifically, the SLPNSP name service provider used by the Novell Client 2 for Windows Vista/2008 and the Novell Client for Linux) does not yet provide a solution for the issue of using a single equals character in a predicate string.

1.2.3 LDAP Contextless Login Differences

The LDAP Contextless Login feature in the Novell Client 2 for Windows Vista/2008 includes the following limitations for those familiar with the Novell Client 4.x for Windows XP/2003.

- ♦ The options to search by attributes other than username (for example, phone number or e-mail address) have been disabled for the Novell Client 2 for Windows Vista/2008 release.

1.3 Novell Products Not Supported with the Novell Client 2 for Windows Vista/2008

The following Novell products are not supported on Windows Vista or with the Novell Client 2 for Windows Vista/2008:

- ♦ ConsoleOne®
- ♦ NetWare Administrator utility (`nwadm32.exe`)

1.4 Novell Features Not Included in the Novell Client 2 for Windows Vista/2008

The following Novell features are not included in the Novell Client 2 for Windows Vista/2008:

- ♦ Workstation Manager (there are no bundled ZENworks components as there are in the Novell Client 4.9x for Windows XP/2003)
- ♦ Novell Management Agent infrastructure components
- ♦ BorderManager® infrastructure components (Client Trust)
- ♦ Common Authentication Service Adapter (CASA)

Advanced Installation Options

2

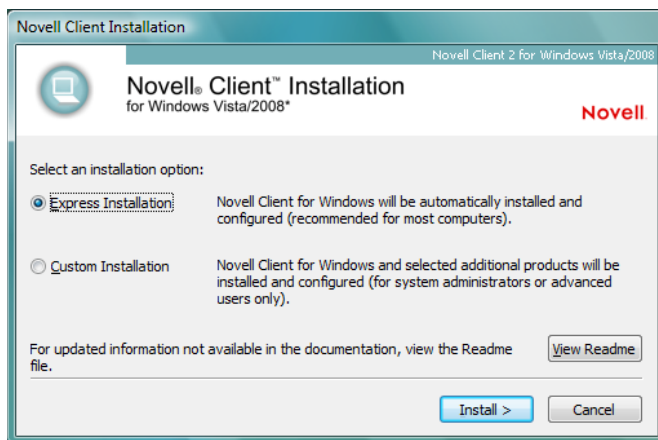
This section explains some advanced Novell® Client™ 2 for Windows Vista/2008 installation options and procedures. For information on installing the Novell Client for Windows Vista/2008 on a single workstation, see the “[Novell Client 2 for Windows Vista/2008 Installation Quick Start](#).”

- ◆ [Section 2.1, “Understanding the Basic Novell Client Installation \(setup.exe\),” on page 17](#)
- ◆ [Section 2.2, “Understanding the Novell Client Install Manager \(nciman.exe\),” on page 21](#)
- ◆ [Section 2.3, “Using the Install.ini File,” on page 22](#)
- ◆ [Section 2.4, “Understanding Automatic Client Update \(acu.exe\),” on page 23](#)
- ◆ [Section 2.5, “Selecting a Network Server Distribution Option,” on page 25](#)
- ◆ [Section 2.6, “Pre-distributing a Trusted Publisher Certificate for the Novell Client Installation,” on page 26](#)

2.1 Understanding the Basic Novell Client Installation (setup.exe)

To install the Novell Client software, use `setup.exe`, located in the `C:\Novell\Novell Client for Windows Vista-2008` directory (created when you unzipped the Novell Client for Windows Vista/2008 download file).

Figure 2-1 Express Novell Client Installation



The Novell Client Express Installation automatically installs and configures the Novell Client for Windows Vista/2008. The Custom Installation lets you choose whether or not to install Novell Modular Authentication Services (NMAS™) and Novell International Cryptographic Infrastructure (NICI) when you install the Client.

The `setup.exe` installation process can also be modified by using the following command line switches:

Table 2-1 *Novell Setup.exe Switches*

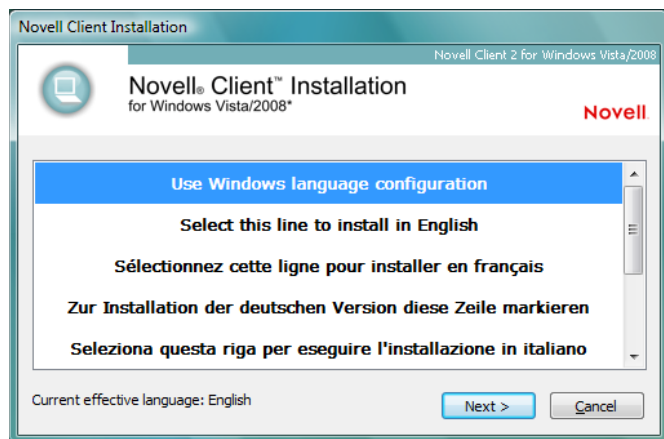
Switch	Description
/ACU	Directs <code>setup.exe</code> to perform an upgrade of the currently installed Client software if the version to be installed is a later one.
/NCPF	Applies the Novell Client property page settings specified in the default <code>NovellClientProperties.txt</code> file. Use the Novell Client Install Manager (<code>nciman.exe</code>) to create this file. See “Creating the Novell Client Properties File” on page 21 for more information.
/NCPF:filename	Applies the Novell Client property page settings specified in <i>filename</i> . Use the Novell Client Install Manager (<code>nciman.exe</code>) to create this file. See “Creating the Novell Client Properties File” on page 21 for more information.

/ACU and /NCPF can be specified together at the command line. For more information, see [“Using Optional Parameters to Install the Novell Client”](#) in the *Novell Client for Windows Vista/2008 Installation Quick Start*.

2.1.1 Selecting a Language

The Novell Client for Windows Vista/2008 installation contains a language selection dialog box. The language choice made in this dialog box determines the language that `setup.exe` uses, and also becomes the language selection for the installed Novell Client for Windows Vista/2008.

Figure 2-2 *Language Selection Dialog Box*



This section contains information on how this dialog box operates, using single language and multiple language versions of Windows Vista, and the languages that are available for selection.

- ♦ [“How the Language Selection Dialog Box Works” on page 19](#)
- ♦ [“Using Single-Language Versions of Windows Vista” on page 19](#)
- ♦ [“Using Multiple-Language Versions of Windows Vista” on page 19](#)
- ♦ [“Available Language Selections” on page 19](#)

How the Language Selection Dialog Box Works

On new installations, the default choice in the language selection dialog box is *Use Windows language configuration*. The language selection list also includes the available Novell Client for Windows Vista/2008 languages (for example, *Select this line to install in English* and *Select this line to install in French*).

Selecting the *Use Windows language configuration* option causes the Novell Client for Windows Vista/2008 to try and match the language the Windows Vista user interface is using. The Novell Client for Windows Vista/2008 consults the Windows Multilingual User Interface (MUI) configuration and determines if any of the Novell Client for Windows Vista/2008 languages match the current MUI preferred or fallback languages.

For the initial release of the Novell Client for Windows Vista/2008, the language selection dialog box in `setup.exe` is the only way you can make a Client language configuration change. To make a new Novell Client for Windows Vista/2008 language selection, you must run `setup.exe` again and choose a different language.

Using Single-Language Versions of Windows Vista

On single-language versions of Windows Vista, selecting the *Use Windows language configuration* option is no different than selecting a specific Novell Client for Windows Vista/2008 language. For example, if you are running the German version of the Windows Vista Business Edition, selecting either *Use Windows language configuration* or *Select this line to install in German* results in German being used as the language for both the Novell Client for Windows Vista/2008 installation and the installed version of the Client.

Using Multiple-Language Versions of Windows Vista

On multiple-language versions of Windows Vista, such as the Windows Vista Ultimate Edition with one or more additional Multilingual User Interface (MUI) language packs installed, the Windows user interface language can be individually selected for each Windows user on the machine (using the *Change Display Language* option in the Windows Vista Control Panel).

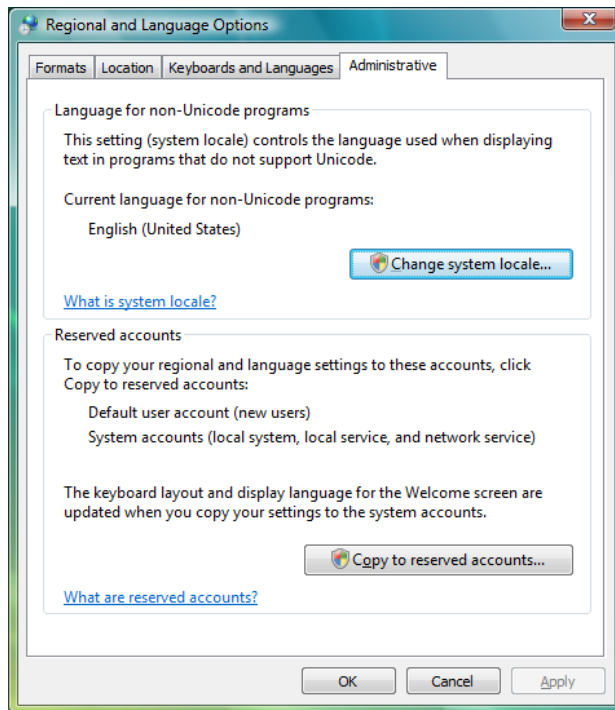
If *Use Windows language configuration* is selected during the Novell Client for Windows Vista/2008 installation, the current Windows MUI language configuration is consulted each time the Novell Client language is queried. If the Windows MUI language configuration changes (for example, if a user changes his or her preferred Windows display language, or a different user who has a different preferred Windows display language logs in), the Novell Client re-evaluates the current Windows MUI language selections and determine which of the available Novell Client languages best matches the new and current MUI language.

Available Language Selections

In the Novell Client for Windows Vista/2008 language selection dialog box, you might notice that not all of the available Novell Client for Windows Vista/2008 languages are offered for selection. For example, on a Windows Vista Business Edition (Japanese) machine, only *Select this line to install in English* and *Select this line to install in Japanese* are offered, along with the *Use Windows language configuration* option.

This is because some components of the Novell Client for Windows Vista/2008 are not yet completely based on Unicode*. Until all of the major and required Novell Client for Windows Vista/2008 user interfaces operate in Unicode, the Client is limited to those languages that can be correctly rendered through the current Windows ANSI code page (what the Windows *Regional and Language Options* Control Panel dialog box refers to as *Language for non-Unicode programs*).

Figure 2-3 *Regional and Language Options Dialog Box*



In general, this means that users of the English, French, German, Italian, Portuguese, and Spanish versions of Windows Vista can select any one of these languages for the Novell Client for Windows Vista/2008 language. This is because all of these languages share the same ANSI code page and can successfully render all the other offered languages. Users of the Japanese, Polish, and Russian versions of Windows Vista, however, can select only their own language or English. For example, a Russian version of Windows Vista will display a language selection list with only *Use Windows language configuration*, *Select this line to install in English*, and *Select this line to install in Russian*.

Even on a multi-language version of Windows, such as Windows Vista Ultimate Edition with one or more additional Multilingual User Interface (MUI) language packs installed, there is still only one system-wide *Language for non-Unicode programs* (meaning that there is still only one system-wide ANSI code page selected in Windows at any given time). As such, even if a Windows Vista Ultimate Edition (Russian) machine successfully installs and uses a German MUI language pack for Windows Vista, the Novell Client for Windows Vista/2008 language selection dialog box still only offers English and Russian as options. This is because the Novell Client for Windows Vista/2008 language choices are based on the current Windows configuration for the *Language for non-Unicode programs* setting and not on which MUI language packs are installed or in use.

The Windows Vista *Language for non-Unicode programs* option can be changed to a different language, which then affects which languages the Novell Client for Windows Vista/2008 installation can offer for selection. This is a system-wide setting that affects all non-Unicode applications and not just the Novell Client for Windows Vista/2008.

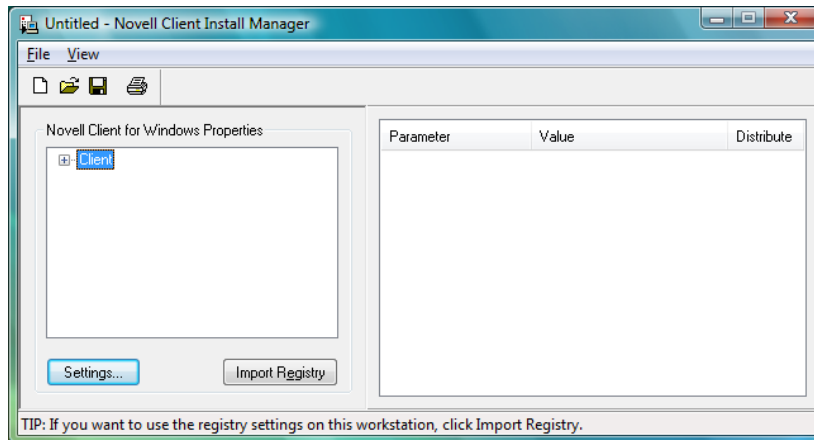
2.2 Understanding the Novell Client Install Manager (nciman.exe)

The Novell Client Install Manager (`nciman.exe`) lets you generate a properties file, used by the Client install utility (`setup.exe` or `acu.exe`), to configure the Novell Client **Property Page settings** during installation. You can create different properties files for different groups of workstations and specify their use by indicating the name of the desired file at the command line. For more information, see **“Creating the Novell Client Properties File” on page 21**.

The Novell Client Install Manager is located in `C:\Novell\Novell Client for Windows Vista/2008\Admin` (created when you unzipped the Novell Client for Windows Vista/2008 download file).

The Novell Client Properties file must be copied to the root directory of the Client build (`C:\Novell\Novell Client for Windows Vista-2008`) before installation. `NovellClientProperties.txt` is the default filename, but you can save a properties file with any name you want.

Figure 2-4 Novell Client Install Manager



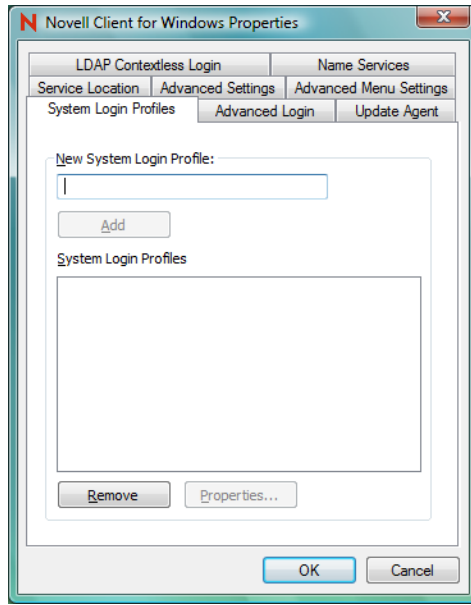
2.2.1 Creating the Novell Client Properties File

The Novell Client installation (`setup.exe` and `acu.exe`) applies a properties file generated by the Novell Client Install Manager in order to configure Novell Client settings during installation.

You can import the settings from a workstation that has been previously configured and save them to a properties file. After you set up the workstation, click *File > Import Registry* in the Novell Client Install Manager to import the settings.

If you are installing the client with the default settings, you do not need to create or modify the configuration file. Skip this process and proceed to **Chapter 4, “Setting Client Properties,” on page 39**.

- 1 Start the Novell Client Install Manager (`nciman.exe`), located in the `C:\Novell\Novell Client for Windows Vista-2008\Admin` folder.
- 2 Double-click *Client* to open the Novell Client for Windows Properties dialog box



3 Modify the Client properties as needed.

For example, if your network uses LDAP, you can enable **LDAP Contextless Login**.

For more information on the Client properties, see **Chapter 4, “Setting Client Properties,”** on **page 39**.

4 Click *File > Save*, then specify a name for the Novell Client properties file.

You can use any filename (for example, `workstation_properties.txt`).

5 Copy this file to the root directory of the Client build (`C:\Novell\Novell Client for Windows Vista-2008`).

2.3 Using the Install.ini File

If you only want to change the behavior of the install components (`setup.exe`, `acu.exe`, and `cuagent.exe`), you do not need to create a Novell Client properties file. All you need to do is open the `install.ini` file, located in the root directory of the Client build (`C:\Novell\Novell Client for Windows Vista-2008`), make the desired changes, and save it. When the install components run, they read the file and change the appropriate behavior.

The `Install.ini` file lets you configure the following settings:

Option	Description	Settings
[NovellClient]	Specifies settings that apply to one or more of the install utilities.	MajorInternalVersion= MinorInternalVersion= NovellClientPropertiesFile=

Option	Description	Settings
[Setup]	Specifies settings that apply only to the install program (<code>setup.exe</code>).	DisplayLanguageSelection= DefaultLanguageSelection= DisplayLicenseAgreement= DisplayInitialDialog= DisplayBackground= CreateSystemRestorePoint= InstallNMAS= InstallNICI= ForceReboot= DisplayRebootDialog=
[ACU]	Specifies settings that apply only to the Automatic Client Upgrade utility (<code>acu.exe</code>).	DisplayUpgradeDialog= Message=
[UpdateAgent]	Specifies settings that apply only to the Client Update Agent utility (<code>cuagent.exe</code>).	Disabled= DisplayUpdateDialog= DisplayUpdateLocation= Message=

2.4 Understanding Automatic Client Update (acu.exe)

The Automatic Client Update utility (`acu.exe`) determines whether the client needs to be updated and allows you to specify several installation options.

ACU's actions are determined by `install.ini`, a text file that can be modified to change the behavior of the installation utilities. ACU can also accept information from a properties file you can create by using the Novell Client Install Manager (`nciman.exe`). For more information, see [“Creating the Novell Client Properties File” on page 21](#).

IMPORTANT: If you use a Novell Client properties file to configure the Novell Client with `acu.exe`, you must specify the name of the properties file in the `NovellClientPropertiesFile=` line of the `[NovellClient]` section of the `install.ini` file.

ACU can be launched from within the login script. ACU determines if an update of the Novell Client is required and then launches the Setup utility (`setup.exe`). Launching ACU from the login script saves network bandwidth during login because the Setup utility runs only if the Client needs to be updated.

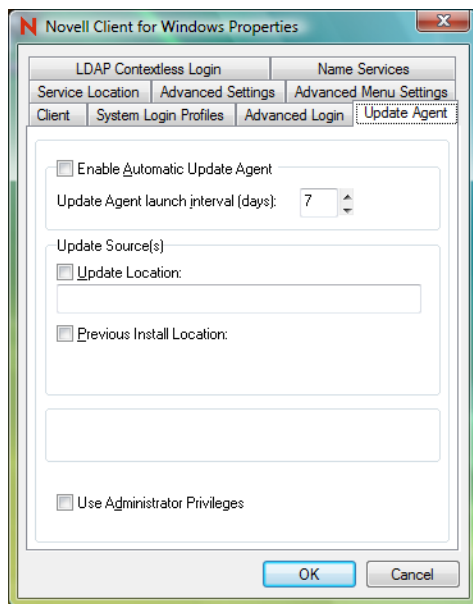
2.4.1 Setting Up the Novell Client Update Agent

You can simplify future client software upgrades by enabling the Novell Client Update Agent. The Update Agent can be run manually at any time from the Red N menu (see “[Updating the Novell Client](#)” in the *Novell Client for Windows Vista/2008 Users Guide* for more information), or it can be run automatically when users log in to the network.

If it is run automatically, the Update Agent determines if the preconfigured number of days have elapsed since the last upgrade check and then checks the specified location for a newer version of the client. If a newer version is found, the new install is launched. You can preconfigure the interval of days as well as the location of the newer client version.

IMPORTANT: Before workstations can check to see if updates are available, the Update Agent must be configured during the Client installation or from the Novell Client Property Pages.

- 1 Create a Novell Client properties file by running the Novell Client Install Manager utility (`nciman.exe`).
See “[Creating the Novell Client Properties File](#)” on page 21.
- 2 Double-click *Client*, then click the *Update Agent* tab.



- 3 (Optional) Select the *Enable Automatic Update Agent* option and specify the launch interval.
- 4 Select *Update Location*, then specify the Update Location path (mapped drive or UNC path).
- 5 (Optional) Select *Previous Install Location*.

This causes the Previous Install Location to be used if the Update Location cannot be found. If the Update Agent should use only the Previous Install Location, deselect the *Update Location* option.

- 6 (Optional) Select *Use Administrator Privileges* to run the Novell Client Update Agent service on the workstation, then click *OK*.

When the Update Agent is run, it uses the service to obtain the required privileges to install the Client. This allows non-administrator users to update the Client. If *Use Administrator Privileges* is not selected, the Update is performed using the privileges of the logged in user.

7 Click *File > Save*.

You can use any filename.

8 Copy this file to the root directory of the Client build.

2.5 Selecting a Network Server Distribution Option


After you have set up your network installation of the Novell Client, you must decide how to distribute the install files. You can modify the login script to launch installation files, distribute the files through ZENworks[®], or use another method you have available on your network.

For more information on using login scripts, see “[Distributing the Novell Client Using Login Scripts](#)” on page 25. For more information on using ZENworks, see the documentation associated with the installed version of ZENworks.

- [Section 2.5.1, “Distributing the Novell Client Using Login Scripts,”](#) on page 25
- [Section 2.5.2, “Sample Client Installation Login Script,”](#) on page 25

2.5.1 Distributing the Novell Client Using Login Scripts

You need to modify login scripts for users whose workstations are upgraded. To upgrade workstations for users in a container, modify that container's login script. To upgrade workstations for users in a profile, modify that profile's login script. To upgrade specific users' workstations, modify those users' login scripts.

- 1 In Novell iManager, make sure you are in the Roles and Tasks view by clicking  on the top button bar.
- 2 Select *Users > Modify User*
- 3 Specify a username and context, then click *OK*.
- 4 Click *General > Login Script*.
- 5 Type the login script commands and information in the *Login script* box.

For a sample of the login script commands that you need to add to the scripts, see “[Sample Client Installation Login Script](#)” on page 25.

IMPORTANT: Make sure that you edit the sample login script to match the server names, directory paths, and specifications of your own network.

For additional information on all login script commands, see the *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html).

- 6 To save the login script, click *OK*.

2.5.2 Sample Client Installation Login Script

The following sample shows the commands that you add to the login script in order to install the client software from the network. The sample includes text for installing across an internal network.

NOTE: In this sample, the text that is necessary to the script is represented in uppercase letters. The information that you should customize for your network is in lowercase letters.

```
REM ***** Windows Vista *****
IF OS = "WINNT" AND OS_VERSION = "V6.00"
    WRITE "Updating Novell Client for Windows Vista/2008."
    #\\server1\sys\public\client\acu.exe
    IF "%ERROR_LEVEL" = "1" THEN
        EXIT
    END
END
END
```

2.6 Pre-distributing a Trusted Publisher Certificate for the Novell Client Installation

The Novell Client for Windows Vista/2008 uses Microsoft* Authenticode* digital signatures to verify Novell, Inc. as the publisher of Novell Client drivers, as is required by the latest versions of Windows. During the Novell Client installation, Windows presents an approval dialog box which lets you confirm whether software from *Publisher: Novell, Inc.* should be installed.

An *Always trust software from Novell, Inc.* option is also available. If you select this option, Windows Vista adds the Novell, Inc. certificate to the Windows *Trusted Publishers* certificate list for the current Windows machine. The next time this Windows machine encounters driver software signed with the same Novell, Inc. certificate, Windows proceeds with installation rather than prompting you again for confirmation.

If you want to keep Windows Vista from presenting this installation approval (for the Novell Client or for any other driver software using publisher-signed Authenticode signatures), you can pre-distribute the publisher's public certificate used for Authenticode signing to the Windows machines *Trusted Publishers* certificate list prior to installation of the driver software.

For the Novell Client, the certificate used for Authenticode signing is the Verisign* public certificate for Novell, Inc. The best way to obtain the correct certificate for use in the *Trusted Publishers* list is to install the Novell Client on a Windows machine, then select the *Always trust software from Novell, Inc.* option when prompted. Then use the Microsoft Certificate Management Console (`certmgr.msc`) to export the Novell, Inc. certificate visible in this Windows machine's *Trusted Publishers* certificate list.

The exported certificate can be used to pre-distribute Novell, Inc. as a *Trusted Publishers* certificate on Windows machines using any of the methods Microsoft makes available for pre-loading certificates used by Authenticode-signed software. This includes Microsoft support for distributing certificates during unattended installations of Windows, or through the use of Group Policies.

For more information on the options provided by Microsoft Windows for distributing software publisher certificates, see the "Deploying Authenticode Digital Certificates in an Enterprise" section of *Using Authenticode to Digitally Sign Driver Packages for Windows Server 2003* (<http://www.microsoft.com/whdc/driver/install/authenticode.msp#>) (`Authenticode.doc`), and the following Microsoft Windows Group Policy documentation:

- ♦ Windows Server* Group Policy (Server 2008) (<http://www.microsoft.com/grouppolicy/>)
- ♦ Windows Server Group Policy (Server 2003) (<http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/default.msp#>)

Certificates have an expiration date, and the certificate a software publisher uses will eventually change as the current certificate reaches expiration and a renewed certificate is obtained. For example, the certificate currently used to sign Novell Client for Windows Vista/2008 is valid until 2010, so pre-distributing this certificate will work for future Novell Client software releases until the year 2010.

Authenticating to a Novell Network

3

This section describes the methods used on Windows Vista and Windows Server 2008 to authenticate to a Novell® network. Previous versions of the Novell Client™ used a custom authentication component called the Graphical Identification and Authentication (GINA) dynamic link library to provide authentication services on Windows operating systems prior to Vista. The GINA technology is not available on the the Windows Vista and Windows Server 2008 platforms, having been replaced by a new method of collecting logon credentials called Credential Providers.

- ♦ [Section 3.1, “Windows Vista and Windows Server 2008 Credential Providers,” on page 29](#)
- ♦ [Section 3.2, “Novell Credential Provider,” on page 31](#)
- ♦ [Section 3.3, “Logging in When eDirectory and Windows Credentials Are Not Synchronized,” on page 35](#)
- ♦ [Section 3.4, “Changing Passwords,” on page 36](#)

3.1 Windows Vista and Windows Server 2008 Credential Providers

Credential Providers are in-process COM objects used to collect credentials for authentication. Credential Providers describe the credential information required for authentication to the Local Security Authority (LSA) or to an application. For an interactive user logon, this credential information is presented to the user in the form of a “tile” that contains informational and editable fields. Users interact with the tile by entering their usernames and passwords, then clicking a right-arrow button.

Figure 3-1 *Windows Vista Welcome Screen*



In Windows Vista and Windows Server 2008, the Winlogon process launches the LogonUI process after it receives a SAS event. LogonUI queries each Credential Provider for the number of credential tiles that it wants to display. A Credential Provider might, for example, display a tile for each local machine user. One of these tiles can be configured to be the default tile initially displayed to the user. After LogonUI is finished querying the Credential Providers for their tiles, it displays all of the enumerated tiles to the user. After the user supplies information for the requested fields, LogonUI submits the credentials for authentication.

Credential Providers are not enforcement mechanisms. They are used only to gather and serialize credentials. The Local Security Authority and authentication packages enforce security. Credential Providers are responsible for:

- ◆ Describing the credential information required for authentication.
- ◆ Handling communication and logic with external authentication authorities.
- ◆ Packaging credentials for interactive network logon.

Even though multiple Credential Providers can be displayed to a user on a machine, only the one selected by the user is allowed to provide credentials to the interactive logon process.

For more information, see [Create Custom Login Experiences With Credential Providers For Windows Vista \(http://msdn.microsoft.com/msdnmag/issues/07/01/CredentialProviders/default.aspx\)](http://msdn.microsoft.com/msdnmag/issues/07/01/CredentialProviders/default.aspx)

3.2 Novell Credential Provider

The Novell Credential Provider provides tiles that allow credential gathering for network and local workstation logon.

- ♦ [Section 3.2.1, “Logon,” on page 31](#)
- ♦ [Section 3.2.2, “Locking and Unlocking the Workstation,” on page 33](#)
- ♦ [Section 3.2.3, “Fast User Switching,” on page 33](#)
- ♦ [Section 3.2.4, “Logon Using Windows Server 2008 Terminal Services,” on page 34](#)

3.2.1 Logon

Because it is not possible to provide a logon tile that represents each individual user in a Novell eDirectory™ tree, only two logon tiles are displayed on the desktop.

Figure 3-2 *Windows Vista Welcome Screen When the Novell Client is Installed*



The first logon tile represents the last user who successfully logged on interactively. This tile is provided as a convenience for the single-user workstation, because it allows a user to log on interactively by simply entering his or her password.

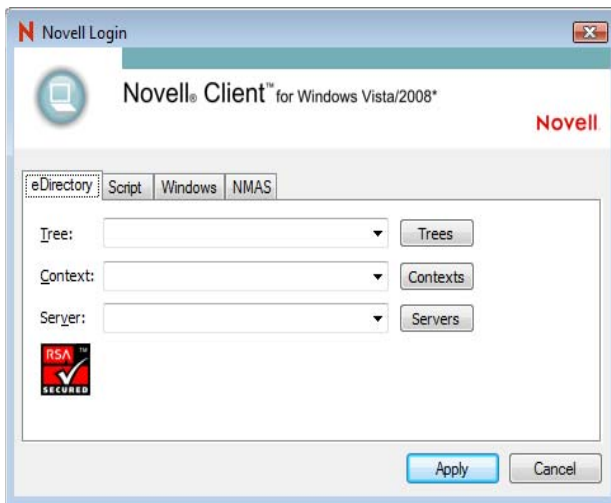
The second logon tile allows the user to specify all necessary local and network credential information. This lets any eDirectory user log on interactively.

Figure 3-3 Novell Client for Windows Vista/2008 Logon Screen



Each logon tile also allows the user to log in to only the local machine and bypass the network logon (using the *Computer Only Logon* option). The Novell logon tile also provides a link (*Show Advanced Options*) that allows users to interact with the Novell Client for Windows Advanced Options dialog box, which lets users specify the eDirectory tree, context, and server they want to log in to.

Figure 3-4 Novell Client Login Advanced Options Dialog Box



3.2.2 Locking and Unlocking the Workstation

The Credential Provider supports locking and unlocking the Windows Vista workstation. When the workstation is locked, a logon tile is displayed that represents the locked user's account. The user is required to enter the network and workstation passwords to unlock the workstation.

Figure 3-5 Novell Client for Windows Vista/2008 Unlock Computer Screen



3.2.3 Fast User Switching

The Credential Provider supports fast user switching. Fast user switching allows two or more users to be logged into the workstation simultaneously. It also allows a user to switch to a different user account without closing programs and files. When a user chooses to switch users (by clicking the Start button, clicking the arrow next to the lock button, then clicking *Switch User*), the Credential Provider displays a tile representing each logged-in user. It also displays the generic Novell Logon tile that allows a new user to log on interactively.

Figure 3-6 Novell Client for Windows Vista/2008 Switch User Screen



To switch to a new user:

- 1 Click the *Start* button, then click the arrow next to the lock button.
- 2 Click *Switch User*.
- 3 Click the Novell Logon tile.
- 4 Specify the credentials for a new user logon (either to eDirectory and Windows, or to Windows only by selecting the *Computer Only Logon* link), then click the right-arrow button.

NOTE: When logging in to a Windows Vista workstation using the Novell Credential Provider, Novell connections made during the login will persist only if you are not currently logged in to the workstation. If your Vista account is already logged in, you will be restored to that existing session when you log back in to the workstation. This applies to both Fast User Switching and connecting via Remote Desktop Connection.

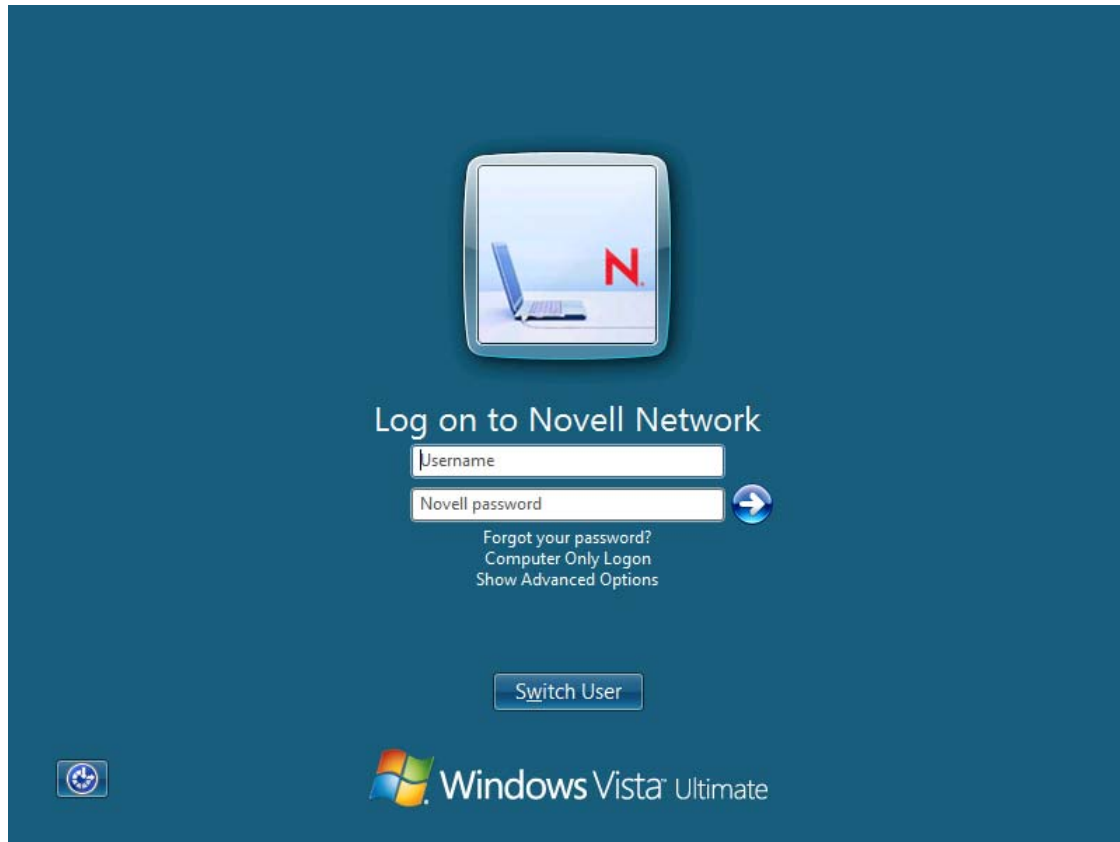
3.2.4 Logon Using Windows Server 2008 Terminal Services

On Windows Server 2008, specifically once Terminal Services has been installed, the Credential Provider switches to a mode in which the previous logged-on user is not displayed, nor are currently logged-on users displayed. This is intended to match Microsoft default credential provider behavior, which exhibits these same behaviors once Terminal Services is installed on Windows Server 2008.

Even though existing logged-on user sessions are not enumerated as visible tiles, it is still possible to re-connect with existing logged-on user sessions by specifying login information which ultimately matches the Windows account of the existing logged-on user session. (And, in the case of Windows Terminal Service Remote Applications, must also match the same TS RemoteApp as the current logon session is running.)

However, this behavior is entirely dependent upon the Windows Server 2008 policy *Restrict Terminal Services users to a single remote session*. If users are not restricted to a single session, logging on with the Windows credentials of an existing logged-on session will still create an additional logon session instead of re-connecting to the existing logged-on user session."

Figure 3-7 Novell Client Credential Provider with Terminal Services Enabled



3.3 Logging in When eDirectory and Windows Credentials Are Not Synchronized

If your eDirectory account password is not in sync with the Windows Vista account password when logging in through the Novell Client for Windows Vista/2008 credential provider, you will see a screen confirming that the eDirectory (Novell) login succeeded and letting you enter the Windows Vista account password.

Figure 3-8 Novell Client for Windows Vista/2008 Account Logon Screen



If you specify the correct Windows Vista account password and continue with the login, the Novell Client then logs you in to both eDirectory and Windows.

If users have the permissions necessary to change their Windows account password, and it's desired that the eDirectory account password and Windows account password match during future logons, selecting the *Change your Windows password to match your Novell password after a successful login* checkbox will synchronize the account passwords after the correct credentials have been provided.

3.4 Changing Passwords

The Credential Provider lets you change a Novell password as well as a Windows Vista password.

- ♦ [Section 3.4.1, “Changing Your Password When Authenticated to eDirectory,” on page 36](#)
- ♦ [Section 3.4.2, “Changing Your Password When Not Authenticated to eDirectory,” on page 38](#)

3.4.1 Changing Your Password When Authenticated to eDirectory

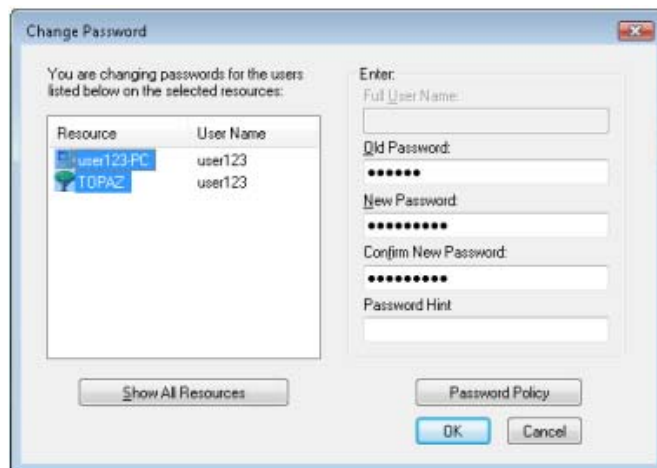
- 1 Press Ctrl+Alt+Delete, then click *Change a password*.
- 2 Click the logon tile.
- 3 Type your current Novell password in the *Old password* field, type your new password in the *New password* field, then retype the new password in the *Confirm new password* field.



4 Press Enter.

After the old password is verified, and if the new passwords you specified match, the Novell Change Password dialog box opens.

5 Select which resources you want the password change to go to.



For example, you can change your Novell password and your Windows Vista password, or you can change only your Novell password.

6 Click *OK*.

You will receive a message telling you that your password has been changed.

7 Click *OK* to close the message.

3.4.2 Changing Your Password When Not Authenticated to eDirectory

- 1 Press Ctrl+Alt+Delete, then click *Change a password*.
- 2 Click the logon tile.
- 3 Type your current password in the *Old password* field, type your new password in the *New password* field, then retype the new password in the *Confirm new password* field.



- 4 Press Enter.
You will receive a message telling you that your password has been changed.
- 5 Click *OK* to close the message.

Setting Client Properties

You can optimize the Novell® Client™ 2 for Windows Vista/2008 for your network by using property pages to configure Client parameters.

By default, the Client is configured for high speed with moderate use of memory and data protection. You can adjust the Client to optimize its performance in any of these areas. However, optimizing the Client in one area might lessen performance in other areas.

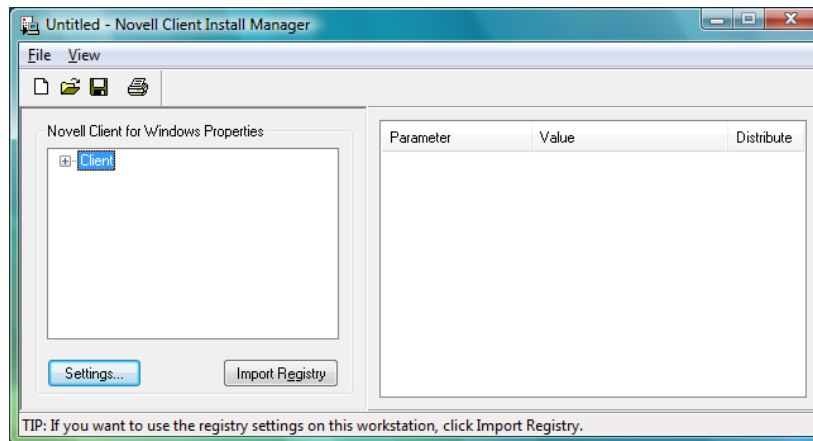
This section discusses the following ways to set properties:

- ♦ [Setting Properties During Installation \(page 39\)](#)
- ♦ [Setting Properties on a Single Workstation after Installation \(page 40\)](#)
- ♦ [Setting Properties on Multiple Workstations after Installation \(page 55\)](#)

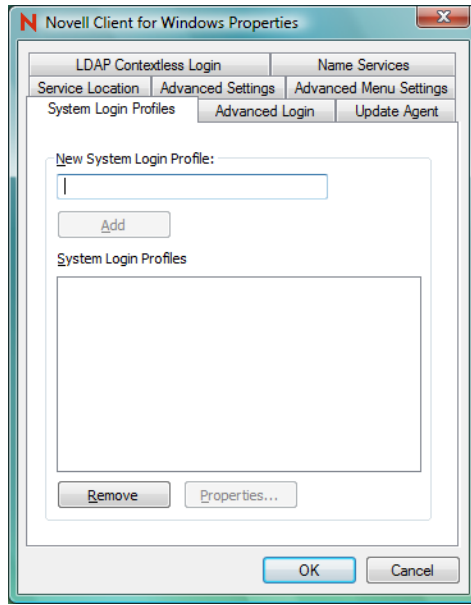
4.1 Setting Properties During Installation

Use the Novell Client Install Manager to set properties for one or more workstations before an install. This method saves you from setting each workstation individually.

- 1 Start the Novell Client Install Manager (`nciman.exe`) located in the `C:\Novell\Novell Client for Windows Vista-2008\Admin` folder (created when you unzipped the Novell Client for Windows Vista/2008 download file).



- 2 Click *Settings* to open the Novell Client for Windows Properties dialog box.



- 3 Modify the Novell Client parameters you want, then click *OK*.

The parameters that you set appear in the *Summary* list box on the right side of the Novell Client Install Manager.

For more detailed information on these options, see [Section 4.2, “Setting Properties on a Single Workstation after Installation,”](#) on page 40.

- 4 Click *File > Save*.

You can save the file with any filename that you want to use. For example, you could save the file with the name `novell.txt` and then specify it in the `NovellClientPropertiesFile=` line of the `Install.ini` file, or use it at the command line by specifying the `/NCPF:novell.txt` option.

TIP: You can configure one workstation the way you want other workstations to be configured, then use the Novell Client Install Manager to import the settings from that workstation’s registry and save them to the properties file you will use during the install. After you set up the workstation, click *Import Registry* to import the settings into the Novell Client Install Manager.

4.2 Setting Properties on a Single Workstation after Installation

- 1 At the user’s workstation, right-click the **N** icon in the notification area of the taskbar.
- 2 Click *Novell Client Properties*.
- 3 Set any of the following properties that you want to change:
 - ♦ **Client**
 - ♦ **System Login Profiles**
 - ♦ **Advanced Login**
 - ♦ **Update Agent**
 - ♦ **Service Location**

- ◆ [Advanced Settings](#)
- ◆ [Advanced Menu Settings](#)
- ◆ [LDAP Contextless Login](#)
- ◆ [Name Services](#)

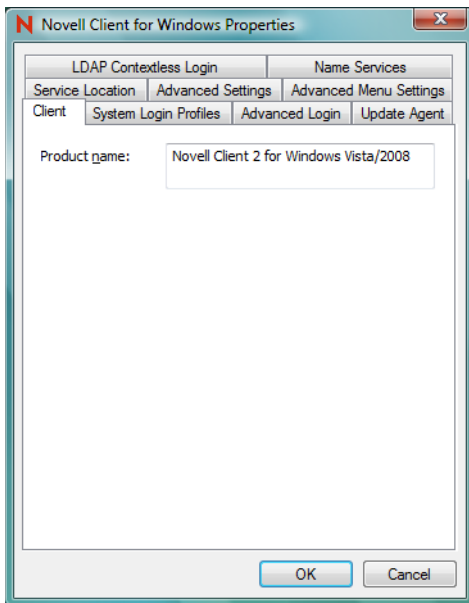
4 Click *OK* to set the changes and close the property pages.

4.2.1 Client Settings

Use the Client property page in the Novell Client for Windows Properties dialog box to view which version of the Novell Client you are running.

This page contains one option, *Product name*, which displays the product name and version.

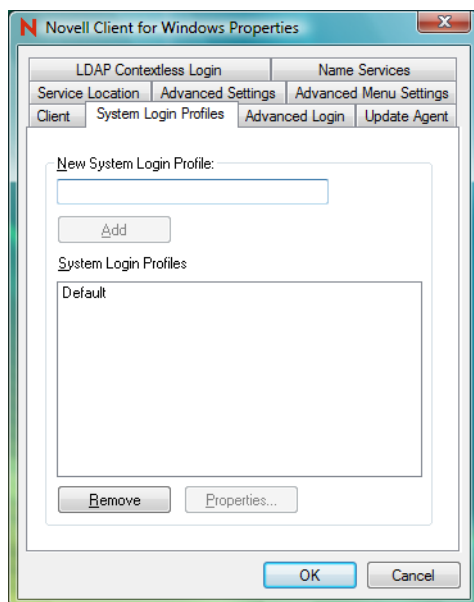
Figure 4-1 Client Property Page



4.2.2 Login Profiles Settings

Use the System Login Profiles property page in the Novell Client for Windows Properties dialog box to create one or more system login profiles that a user can select when logging in. When the user selects the profile, the profile automatically sets up login information such as the user's name, server, context, login script, and other applicable information so that the user does not need to type this information. For more detailed information, see [Section 8.6, “Setting Up Login Profiles,”](#) on [page 81](#).

Figure 4-2 *System Login Profiles Property Page*



- ♦ “Adding a System Login Profile” on page 42
- ♦ “Viewing or Editing a System Login Profile's Properties” on page 42
- ♦ “Removing a System Login Profile” on page 43

Adding a System Login Profile

- 1 Right-click the **N** icon in the notification area of the taskbar.
- 2 Click *Novell Client Properties*, then click the *System Login Profiles* tabbed page.
- 3 Type the name of the profile you want to add in the *New System Login Profile* text box.
- 4 Click *Add*.
- 5 In the Novell Login dialog box, specify the login information you want for this profile, such as the user's name, server, and context.
- 6 Click *OK* to close the Novell Login dialog box, then click *OK* to close the Novell Client Properties dialog box.

Viewing or Editing a System Login Profile's Properties

- 1 Right-click the **N** icon in the notification area of the taskbar.
- 2 Click *Novell Client Properties*, then click the *System Login Profiles* tabbed page.
- 3 In the *System Login Profiles* list, select the name of a profile.
- 4 Click *Properties*.
- 5 In the Novell Login dialog box, view or modify the login information you want for this profile, such as the user's name, server, and context.
- 6 Click *OK* to close the Novell Login dialog box, then click *OK* to close the Novell Client Properties dialog box.

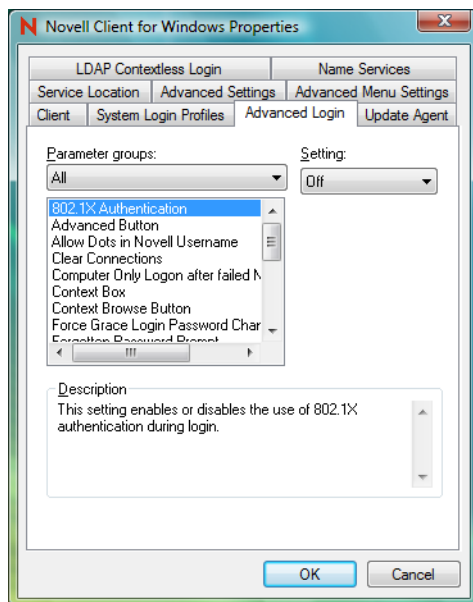
Removing a System Login Profile

- 1 Right-click the **N** icon in the notification area of the taskbar.
- 2 Click *Novell Client Properties*, then click the *System Login Profiles* tabbed page.
- 3 In the *System Login Profiles* list, select the name of the profile you want to remove.
- 4 Click *Remove*.
- 5 Click *OK* to close the Novell Client Properties dialog box.

4.2.3 Advanced Login Settings

Use the Advanced Login property page in the Novell Client for Windows Properties dialog box to configure user login settings.

Figure 4-3 *Advanced Login Property Page*



Use the *Parameter groups* drop-down list to display all the advanced login parameters or to sort the parameters by function (*Execution Options*, *Password*, and *Shown on Login*). Select the parameter you want, then use the *Setting* option to configure the parameter. For most parameters, this consists of simply turning it On or Off. Some parameters require a filename or text or number setting. A short description of each parameter is available in the *Description* field when you select the parameter.

The Advanced Login parameters include the following:

- ♦ **802.1X Authentication:** Enables or disables the use of 802.1X authentication during login. For more information, see [Section 8.8, “Configuring 802.1X Authentication,” on page 97](#).
- ♦ **Advanced Button:** Specifies whether the *Advanced* button on the Login dialog box is enabled. This button leads to various tabs that help you to specify advanced login parameters.

- ♦ **Allow Dots in Novell Username:** If this setting is On, any periods entered in the Novell username are treated as part of the name, rather than as context delimiters. The user cannot enter the context as part of the username, but must enter it separately. This makes it possible for the user to log in with a username such as John.Smith to both Novell and Windows Vista.
- ♦ **Allow Roaming User Profile Paths to non-Windows servers:** Enables or disables the Windows *Do not check for user ownership of Roaming Profile Folders* policy. By default, Windows attempts to enhance profile security by checking the permissions on a remote roaming profile directory. But the check is performed in a Windows-specific manner, and this fails when the roaming profile path is to a Novell or other non-Windows-compatible resource. Setting this parameter to *On* allows roaming profile paths to Novell and other non-Windows server by disabling this Windows-specific security check. Note this policy is defined and controlled by Windows and not the Novell Client, so group policies and other Windows management tools may also set or change this policy (CompatibleRUPSecurity).
- ♦ **Clear Connections:** Specifies whether the *Clear Connections* check box appears in the Login dialog box. The check box allows you to clear all previous connections when you create a new connection to the network.
- ♦ **Computer Only Logon:** Specifies whether the Computer Only Logon option is shown when the Novell Logon option is presented by the Welcome screen. The Computer Only Logon option is used to log in to the Windows workstation without logging in to the Novell network.
- ♦ **Computer Only Logon after failed Novell Logon:** Allows the user to log on to the computer after a failed Novell Logon attempt.
- ♦ **Computer Only Logon Default:** Determines whether the Novell Client will default to the Computer Only Logon mode. *Automatic* means the Novell Client will remember when Computer Only Logon was the mode previously selected, and will continue defaulting to Computer Only Logon until Novell Logon mode is interactively selected again. *Always* means the Computer Only Logon will always be the default mode presented, even if Novell Logon was the previous mode used. *Never* means that Novell Logon will always be the default mode presented, even if Computer Only Logon was the previous mode used.
- ♦ **Context Box:** Specifies whether the *Context* field is displayed on the Login dialog box.
- ♦ **Context Browse Button:** Specifies whether the *Contexts* browse button is displayed in the Login dialog box.
- ♦ **Default bitmap for Novell Login dialog:** Specifies the path and filename for a bitmap that will be used on the Novell Login dialog in place of the default Novell Client bitmap. Custom bitmap sizes can be used, but will affect the overall size of the Novell Login dialog.
- ♦ **Default bitmap for Welcome screen tiles:** Specifies the path and filename for a bitmap that will be used on the Welcome screen tiles whenever a user-specific bitmap is not yet known. Note that Windows imposes the size limit on any bitmap used for a Welcome screen tile, and will stretch / deform the bitmap provided to conform to that limit as needed.
- ♦ **Force Grace Login Password Change:** This setting forces users to change their passwords at the last grace login. With this setting activated, when the password expires, the password must be changed in order to successfully log in.
- ♦ **Forgotten Password Prompt:** Specifies whether the *Did you forget your password?* prompt is displayed in the Login dialog box. This prompt provides an option to recover from a forgotten password based on an administrator-defined password policy. See [Section 6.3, "Using Forgotten Password Self-Service,"](#) on page 66 for more information.

- ♦ **Last Logged On User:** Specifies whether the last logged on user is displayed along with the Novell Logon when logging on to the computer. Note this does not override the fact that the last logged on user is not displayed on Windows Server 2008 when Terminal Services are installed.
- ♦ **Login Profile List:** Specifies whether the *Login Profiles* drop-down list on the Novell Login dialog box is enabled.
- ♦ **Login Windows password synchronization option default:** This is the default state of the *Change your Windows password to match your Novell password* functionality that occurs during login to both eDirectory and Windows when the passwords are not already synchronized. This setting controls the default synchronization behavior that will occur, regardless of whether the "Show login Windows password synchronization option" is allow the checkbox to be shown to the user or not.
- ♦ **Login With Non-Novell Credential Provider:** This setting controls whether a Novell login will still be attempted after the Windows logon, in cases where the Novell Client's credential provider was not used during the Windows logon.
- ♦ **NMAS Authentication:** If this setting is On, Novell Modular Authentication Services (NMAS™) is enabled during login. NMAS authentication adds additional security to the network. However, if your network does not use NMAS, login might take additional time and you might want to disable NMAS authentication by changing this setting to Off.
- ♦ **Novell Logon:** Enables the Novell Logon option (tile) when logging on to the computer.
- ♦ **Prompt for Novell login during Windows AutoAdminLogon:** If the Novell Login parameter is enabled, and Windows is configured to perform a Windows-only AutoAdminLogon as a specific user account, enabling this setting causes a Novell login to interactively prompt for eDirectory login information to be used in addition to the AutoAdminLogon-defined Windows login.
- ♦ **Server Connection Retries:** This parameter controls the number of times that Login tries to establish a connection to a server. If Login tries to connect to a server and fails, it waits 1 second and then tries to connect again. It continues to do this until the number of retries has been reached. It is recommended that this setting be no higher than 20.
- ♦ **Show login Windows password synchronization option:** Specifies whether the *Change your Windows password to match your Novell password* option is shown when logging in to both eDirectory and Windows when the passwords are not already synchronized.
- ♦ **Tree Box:** Specifies whether the *Tree* field is displayed on the Login dialog box.
- ♦ **Tree Browse Button:** Specifies whether the *Trees* browse button is displayed on the Login dialog box.
- ♦ **Variables Button:** Specifies whether the *Variables* button in the Login dialog box is enabled. The button allows you to enter login script variables to be used when the user logs in.
- ♦ **Windows Password Synchronization:** With this feature enabled, the user can change the Novell password, and the Windows password is set to the same value. Turning it off leaves the passwords separate unless they are synchronized through some other means (for example, Novell Identity Manager).

4.2.4 Update Agent Settings

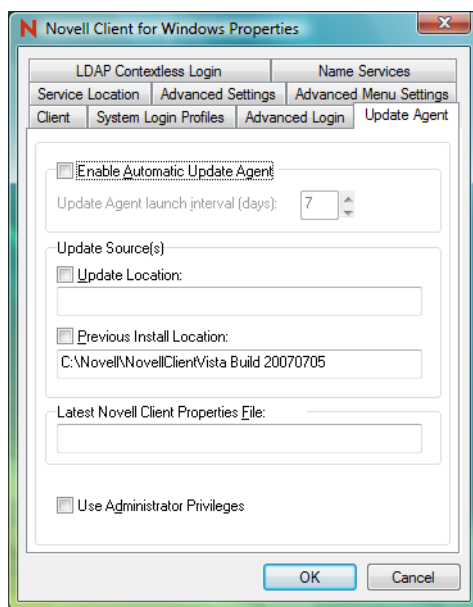
The Novell Client Update Agent provides a workstation-initiated (manual or automatic) update of the Novell Client software. It launches `acu.exe` from a specified location. Update Agent can be run manually from the Red N menu or it can be configured to automatically check for updates at specified intervals.

If it is configured to check automatically, each time a user logs in to the network, Update Agent runs and determines if the preconfigured number of days have elapsed since the last upgrade check, then checks the specified location for a newer version of the client. If a newer version is found, ACU then launches the appropriate installation process.

Before workstations can check to see if updates are available, the Update Agent must be configured during a software installation. Or, you can configure the Update Agent on each machine locally through the Novell Client Property Pages.

The Update Agent is configured by modifying the Update Agent property page settings or (optionally) the `Install.ini` file. Because the Update Agent launches ACU, which in turn launches `setup.exe`, all of the configuration changes made to these subsequent utilities are used in the same way they would be when not running the Update Agent. For more information, see [Setting Up the Novell Client Update Agent](#).

Figure 4-4 Update Agent Property Page



This page contains the following options:

- ◆ **Enable Automatic Update Agent:** Select this check box to enable the automatic update agent, then use the *Update Agent launch interval* option to set the interval (in days) that the Novell Client Update Agent will check for a new version of the Novell Client.
- ◆ **Update Source(s):** Select the *Update Location* check box to enable the Novell Client Update Agent to look for a new version of the Novell Client in the designated update location.

The Update Agent checks for updates: first, in the *Update Location*; and second, in the *Previous Install Location*.

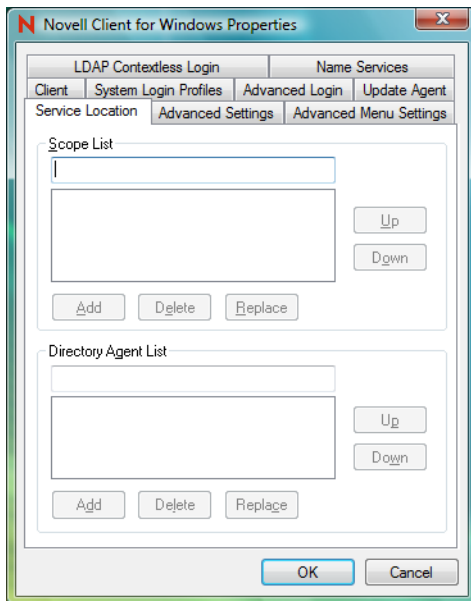
The Update Agent looks in each enabled location for a valid set of Client installation files. Make sure that you have the latest Client installation files in the first location that the Update Agent searches.

- ♦ **Latest Novell Client Properties File:** Displays the name, date, and time of the most recent Novell Client properties file used to apply Client settings on this workstation. For more information, see [Section 2.2.1, “Creating the Novell Client Properties File,” on page 21](#).
- ♦ **Use Administrator Privileges:** If this option is selected, the Update Agent uses the Novell Client Update Agent service to install the Client. The service runs with elevated privileges required for a non-administrator to install the Client. If this setting is not selected, the user must be able to elevate to an administrator user to complete the Client installation.

4.2.5 Service Location Settings

Use the Service Location property page in the Novell Client for Windows Properties dialog box to manage a list of scope names to be reported to SLP applications for a workstation and a list of SLP Directory Agent addresses.

Figure 4-5 Service Location Property Page



This page contains the following options:

- ♦ **Scope List:** A list of scope names to be reported to SLP applications on a workstation. Multiple scope names are allowed. The list order reflects the preference order. Scopes can also be configured via DHCP or discovered dynamically from Directory Agents.

A scope is like a collection of services within a logical group. You might want to use a scope to create a group of directory agents and services registered with these directory agents in a large organization.

To add a scope to the list, specify a name, then click *Add*. To remove a scope from the list, select a name in the *Scope* list, then click *Delete*. To replace a scope in the list with a new scope, type the name of the new scope, select the name of the item you want to replace, then click *Replace*. Use the *Up* and *Down* buttons to move a scope up or down in the list.

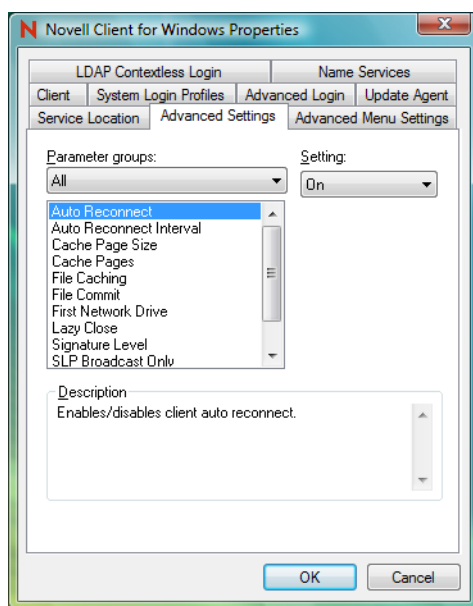
- ♦ **Directory Agent List:** A list of SLP Directory Agent addresses. Multiple Directory Agent addresses are allowed. Each address is a fully qualified domain name (DNS), or a dotted decimal IP address. Directory Agents can also be configured via DHCP, or discovered dynamically.

To add a Directory Agent to the list, specify a name, then click *Add*. To remove a Directory Agent from the list, select a name in the Directory Agent list, then click *Delete*. To replace a Directory Agent in the list with a new Directory Agent, type the name of the new Directory Agent, select the name of the item you want to replace, then click *Replace*. Use the *Up* and *Down* buttons to move a Directory Agent up or down in the list.

4.2.6 Advanced Settings

Use the Advanced Settings property page in the Novell Client for Windows Properties dialog box to configure connection, packet management, performance, cache, and SLP settings.

Figure 4-6 Advanced Settings Property Page



Use the *Parameter* groups drop-down list to display all the Advanced Settings parameters or to sort the parameters by function (Connections, Packet Management, Performance, Cache, and SLP). Select the parameter you want, then use the *Setting* option to configure the parameter. For most parameters, this consists of simply turning it On or Off. Some parameters require a number setting. A short description of each parameter is available in the *Description* field when you select the parameter.

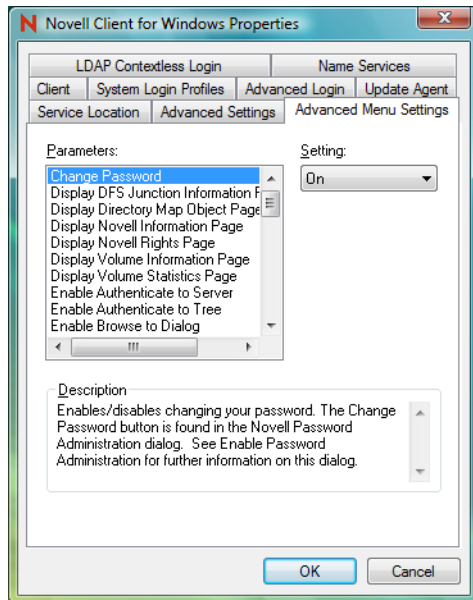
The Advanced Settings parameters include the following:

- ◆ **Auto Reconnect:** Enables or disables Novell Client auto reconnect.
- ◆ **Auto Reconnect Interval:** Specifies the delay in seconds between Client reconnect attempts.
- ◆ **Cache Page Size:** Specifies the size of a cache page in kilobytes. This setting multiplied by the **Cache Pages** is the amount of physical memory consumed by the cache. It is the largest read-ahead or write-behind that will be performed.
- ◆ **Cache Pages:** Specifies the number of available cache pages. This setting multiplied by the **Cache Page Size** is the amount of physical memory consumed by the cache.
- ◆ **File Caching:** This controls whether the Client caches files locally or not.
- ◆ **File Commit:** Controls whether buffers flushed by an application are committed to disk on the server. Setting this value to On ensures data integrity at the expense of performance by ensuring that file buffers are committed to disk on the server when an application flushes its file buffers.
- ◆ **First Network Drive:** This parameter sets the first network drive to the drive letter of choice when you connect to a Novell server. The first network drive applies to any user logging in to the network using the workstation where it is set.
- ◆ **Lazy Close:** Delays the file close on the network, allowing the file to be reopened without accessing the network.
- ◆ **Receive Broadcast Messages:** Tells the client which broadcast message, if any, to receive. You can choose one of the following settings: All (receive all broadcast messages), Server Only (receives broadcast messages sent by the server only), or None (do not receive any broadcast messages).
- ◆ **Signature Level:** Determines the level of enhanced security support. Enhanced security includes the use of a message digest algorithm and a per connection/per request session state. The values are as follows: 0 = disabled, 1 = Enabled but not preferred, 2 = Preferred, 3 = Required. Setting the value of this parameter to 2 or 3 increases security but decreases performance.
- ◆ **SLP Broadcast Only:** Enables or disables a broadcast only network for this SLP agent. If this option is set to On, the SLP agent must send only broadcast messages (in other words, it forces broadcasts to be used instead of multicasts). If this option is set to Off, the SLP agent can send multicast messages.
- ◆ **SLP Maximum Results:** Specifies the maximum number of results to accumulate and return for a synchronous request before the timeout, or the maximum number of results to return through a callback if the request results are reported asynchronously.
- ◆ **UNC Path Filter:** Enables or disables the UNC Path Filter. Filters requests for UNC path resolution sent to the Client for Microsoft Networks (Microsoft redirector). When enabled, UNC path queries sent to the Microsoft redirector will first be filtered by the Novell Client to determine if the server name is known to be a Novell resource. If it is determined to be a Novell resource, the UNC path request will not be allowed to proceed to the Microsoft redirector. This can help avoid unnecessary delays caused by repeated failing attempts to access the Novell resources as though it might be a Windows server.

4.2.7 Advanced Menu Settings

Use the Advanced Menu Settings property page in the Novell Client for Windows Properties dialog box to determine which options are available to users on the Red N menu when they right-click the **N** icon in the notification area of the taskbar, or in other context menus.

Figure 4-7 Advanced Menu Settings Property Page



Select the parameter you want, then use the *Setting* drop-down menu to turn the parameter On or Off. A short description of each parameter is available in the *Description* field when you select the parameter.

The Advanced Menu Settings parameters include the following:

- ♦ **Change Password:** Enables or disables the ability of users to change their passwords. The *Change Password* button is found in the Novell Password Administration dialog box. See [Enable Password Administration](#) for more information on this dialog box.
- ♦ **Display DFS Junction Information Page:** Display or hide the *DFS Junction Information* tab. The *DFS Junction Information* tab is found by selecting *Properties* from the context menu of a DFS Junction on a Novell server.
- ♦ **Display Directory Map Object Page:** Display or hide the Directory Map Object page. The Directory Map Object page is accessed by selecting *Properties* from the context menu of the selected Directory Map Object icon in the Network folder.
- ♦ **Display Novell Information Page:** Display or hide the *Novell Information* tab. The *Novell Information* tab is found by selecting *Properties* from the context menu of a volume, directory, or file on a Novell server.
- ♦ **Display Novell Rights Page:** Display or hide the *Novell Rights* tab. The *Novell Rights* tab is found by selecting *Properties* from the context menu of a volume, directory, or file on a Novell server.
- ♦ **Display Volume Information Page:** Display or hide the *Volume Information* tab. The *Volume Information* tab is found by selecting *Properties* from the context menu of a volume.

- ♦ **Display Volume Statistics Page:** Display or hide the *Volume Statistics* tab. The *Volume Statistics* tab is found by selecting *Properties* from the context menu of a volume.
- ♦ **Enable Authenticate to Server:** Enables or disables authenticating to a server. The *Authenticate* menu item is displayed in the context menu of a server.
- ♦ **Enable Authenticate to Tree:** Enables or disables authentication to a tree. The *Authenticate* menu item is displayed in the context menu of a tree.
- ♦ **Enable Browse To Dialog:** Enables or disables the Browse To dialog box. This menu item is displayed in the context menu of the Red N icon.
- ♦ **Enable Challenge/Response Administration:** Enables or disables the *Challenge/Response Administration* item in the *User Administration* menu. For more information, see “[Configuring Challenge/Response Settings](#)” on page 68.
- ♦ **Enable Change Context Dialog:** Enables or disables the Change Context dialog box. This menu item is found in the context menu of the selected container in the Network folder.
- ♦ **Enable Group Membership Dialog:** Enables or disables the *Group Membership* item in the *User Administration* menu. See “[Configuring Your User Account](#)” in the *Novell Client for Windows Vista/2008 User Guide* for more information on this menu.
- ♦ **Enable Inherited Rights Dialog:** Enables or disables the Inherited Rights dialog box. This dialog box can be reached from a menu item in the context menu of a volume or directory or under the *Novell Utilities* menu item in the Red N menu.
- ♦ **Enable Login Account Information:** Enables or disables the *Login Account Information* item in the *User Administration* menu. See “[Configuring Your User Account](#)” in the *Novell Client for Windows Vista/2008 User Guide* for more information on this menu.
- ♦ **Enable Login Dialog:** Enables or disables the Login dialog box. This menu item is displayed in the context menu of the Red N icon and in the context menu of the Network folder.
- ♦ **Enable Login to Server:** Enables or disables logging in to a server. The *Login to Server* menu item is displayed in the context menu of the selected server.
- ♦ **Enable Logout of Server:** Enables or disables logging out of a server. The *Logout* menu item is displayed in the context menu of a server. Subsequently, the *Detach* button when a server is selected in Novell Connections is also enabled or disabled according to this parameter.
- ♦ **Enable Logout of Tree:** Enables or disables logging out of a tree. The *Logout* menu item is displayed in the context menu of a tree. Subsequently, the *Detach* button when a tree is selected in Novell Connections is also enabled or disabled according to this parameter.
- ♦ **Enable Map Dialog:** Enables or disables the Network Drive Mapping dialog box.
- ♦ **Enable Mapped Drive Disconnect Dialog:** Enables or disables the Disconnect dialog box.
- ♦ **Enable Modify Container Script:** Enables or disables the *Modify Container Script* menu item. This item is displayed in the context menu of the selected container.
- ♦ **Enable NDS Mailing Information:** Enables or disables the *Mailing Information* item in the *User Administration* menu. See “[Configuring Your User Account](#)” in the *Novell Client for Windows Vista/2008 User Guide* for more information on this menu.
- ♦ **Enable NDS Personal Information:** Enables or disables the *Personal Information* item in the *User Administration* menu. See “[Configuring Your User Account](#)” in the *Novell Client for Windows Vista/2008 User Guide* for more information on this menu.
- ♦ **Enable NDS Work Information:** Enables or disables the *Work Information* item in the *User Administration* menu. See “[Configuring Your User Account](#)” in the *Novell Client for Windows Vista/2008 User Guide* for more information on this menu.

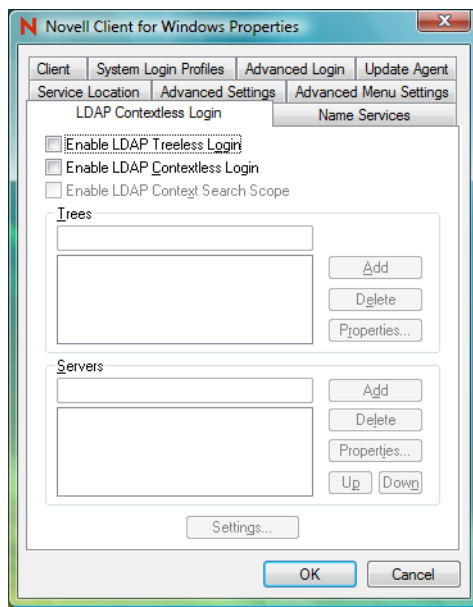
- ♦ **Enable Novell Client Help:** Enable or disables the Novell Client help. This menu item is displayed in the context menu of the Red N icon.
- ♦ **Enable Novell Client Properties:** Enables or disables viewing the Novell Client property pages. This menu item is displayed in the context menu of the Red N icon.
- ♦ **Enable Novell Connections Dialog:** Enables or disables the Novell Connections dialog box. This menu item is displayed in the context menu of the Red N icon and in the context menu of the Network folder.
- ♦ **Enable Novell Copy Dialog:** Enables or disables the Novell File Copy dialog box. This menu item is displayed in the context menu of the selected directory or file.
- ♦ **Enable Novell Utilities:** Enables or disables the Novell Utilities. This menu item is displayed in the context menu of the Red N icon.
- ♦ **Enable Object Properties Dialog:** Enables or disables the Object Properties dialog box. This menu item is displayed in the *Novell Utilities* menu. See “[Using Novell Utilities](#)” in the *Novell Client for Windows Vista/2008 User Guide* for more information on this menu.
- ♦ **Enable Password Administration:** Enables or disables password administration.
- ♦ **Enable Purge Dialog:** Enables or disables the [Purge Files](#) dialog box. This menu item is displayed in the context menu of the selected volume or directory on a server.
- ♦ **Enable Salvage Dialog:** Enables or disables the [Salvage](#) dialog box. This menu item is displayed in the context menu of the selected volume or directory on a server.
- ♦ **Enable Send Message:** Specifies whether the Send Message function is enabled. This function is accessed from the Context menu for the selected server in Network Neighborhood.
- ♦ **Enable Send Message to Server Dialog:** Enable/disable the send message to server dialog. This menu item is displayed within the server context menu item Send Message. See the Enable Send Message Dialog setting for further information on this menu.
- ♦ **Enable Send Message to User Dialog:** Enable/disable the send message to user dialog. This menu item is displayed within the server context menu item Send Message. See the Enable Send Message Dialog setting for further information on this menu.
- ♦ **Enable Systray Config Dialog:** Enables or disables the [Configure System Tray](#) dialog box. This menu item (*Configure System Tray Icon*) is displayed on the Red N menu in the notification area of the taskbar.
- ♦ **Enable Trustee Rights Dialog:** Enables or disables the Trustee Rights dialog box. This dialog box can be reached from a menu item in the context menu of a volume or directory or under the *Novell Utilities* submenu on the Red N icon.
- ♦ **Enable Update Novell Client:** Enables or disables the *Update Novell Client* menu item. This menu item is displayed in the context menu of the Red N icon.
- ♦ **Filter User List:** Enables or disables showing only users objects in the Send Message dialog box.
- ♦ **Show Current Connections:** Shows or hides the current connections displayed in the Novell Resource Browser and in the Network folder.
- ♦ **Show Edit Login Script Item:** Specifies whether the *Edit Login Script* item is available in the *User Administration* menu. See “[Configuring Your User Account](#)” in the *Novell Client for Windows Vista/2008 User Guide* for more information on this menu.

- ♦ **Show Novell System Tray Icon:** If this parameter is enabled, the Red N icon appears in the notification area of the taskbar, located in the bottom right portion of the Windows Vista screen. Right-click the Red N icon to select from a list of Novell Client options.
- ♦ **Show User Administration Menu:** Enables or disables the menu item for user administration. This menu item is displayed in the context menu of the selected server or tree in the Network folder.

4.2.8 LDAP Contextless Login Settings

Use the LDAP Contextless Login property page in the Novell Client for Windows Properties dialog box to let users log in to the network without specifying a tree name or context. For more detailed information, see [Section 8.7, “Setting Up LDAP Contextless Login and LDAP Treeless Login,”](#) on page 90.

Figure 4-8 LDAP Contextless Login Property Page



This page contains the following options:

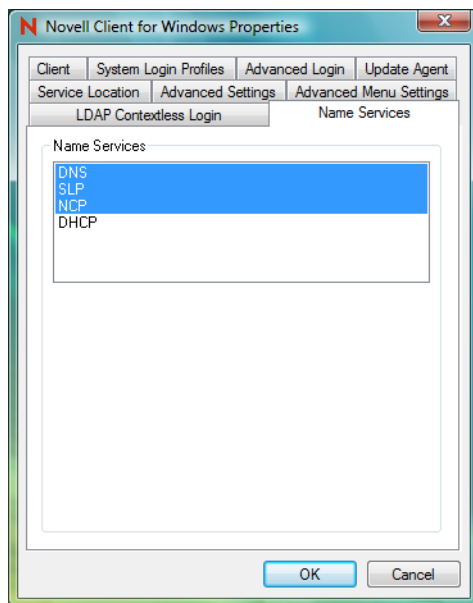
- ♦ **Enable LDAP Treeless Login:** To enable treeless login, select this check box. Treeless login makes it possible to log in to the network without specifying a tree.
- ♦ **Enable LDAP Contextless Login:** To enable LDAP contextless login, select this check box. You must have LDAP Services for eDirectory installed on your corporate server hosting the corporate tree to take advantage of LDAP contextless login.
- ♦ **Enable LDAP Context Search Scope:** Use this option to limit the search scope to a specific context or to a specific context and subtree.
- ♦ **Trees:** Lists the eDirectory trees running LDAP Services that will be searched during login. To add a tree to the list, specify a tree name in the *Trees* field, then click *Add*. To delete one or more trees from the list, select the trees and click *Delete*. These trees are no longer searched during login. To set a tree’s context scope information, select a tree from the list, then click *Properties*. You can limit the scope of the search by selecting *Search Context Only* in the Tree Properties dialog box.

- ♦ **Servers:** Lists the servers associated with the tree running LDAP Services.
To add a server, enter a server name in the *Servers* box, then click *Add*. Servers are searched in the order they appear in this list. You can rearrange the search order by clicking *Up* or *Down*. To delete one or more LDAP servers, select the servers and then click *Delete*. To set the LDAP server timeout and data encryption settings, select the server from the list, then click *Properties*.
- ♦ **Settings:** Opens the LDAP Contextless Login Parameters dialog box. Select the parameter you want, then use the *Settings* option to configure the parameter. For most parameters, this consists of simply turning it On or Off. Some parameters give you other configuration options. A short description of each parameter is available in the *Description* field when you select the parameter.

4.2.9 Name Services Settings

Use the Name Services property page in the Novell Client for Windows Properties dialog box to specify which name service protocols are used to attempt to resolve names.

Figure 4-9 Name Services Property Page



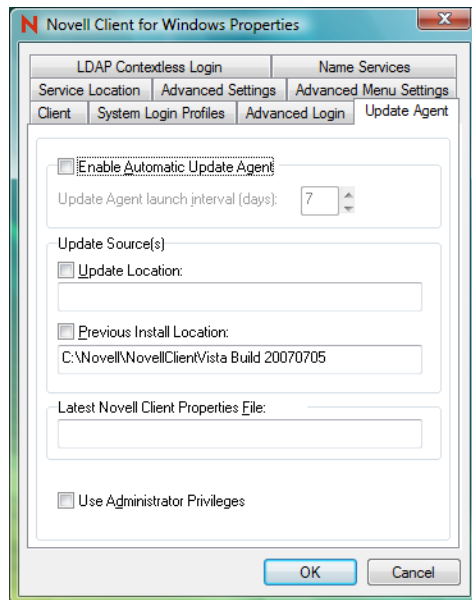
All configured name service providers are queried asynchronously in order to resolve the name to an address. They are first queried with a cache flag that allows name service providers (NSP) who maintain a cache to attempt to resolve the name. If no NSP resolves the name then they are queried again without the cache flag, allowing all NSPs to attempt to resolve the name. NetWare Core Protocol™ uses information contained in the active NCP™ connections. Service Location Protocol queries SLP for eDirectory and Bindery names.

4.3 Setting Properties on Multiple Workstations after Installation

You can use the Novell Client Update Agent to set properties on multiple workstations after installation.

- 1 Make sure that the Update Agent is configured on each workstation and that the *Update Location* has been specified.

You can check the Update Agent settings in the Novell Client for Windows Properties dialog box (right-click the **N** icon in the notification area of the taskbar > *Novell Client Properties* > *Update Agent*).



The Update Agent can be configured during installation or after installation by enabling it on each workstation.

- 2 Use the Novell Client Install Manager to create a Novell Client properties file with the desired property settings.

See [Section 2.2.1, “Creating the Novell Client Properties File,”](#) on page 21 for more information.

- 3 Copy the properties file to the root directory of the Client build specified in the *Update Location* field or the *Previous Install Location* field.
- 4 Modify the `Install.ini` file (located in the root directory of the Client build) in the update location so that the `[NovellClient]` section has the following settings:

```
NovellClientPropertiesFile=name_of_the_properties_file.txt
```

Replace `name_of_the_properties_file.txt` with only a filename, because the Update Agent does not accept paths. The file must exist in the directory that the Update Agent is trying to update from.

- 5 (Optional) Make any additional changes to the `Install.ini` file.
- 6 Run the Update Agent from the workstation.

After settings are updated, the pathname, date, and time of the Novell Client properties file is displayed in the *Last Novell Client Properties File* field on the Update Agent property page.

Managing File Security

5

Novell® Open Enterprise Server (OES) and NetWare® networks restrict access to network files and folders based on user accounts. For example, a user connected to the network using the Administrator account can delete or rename a file that other users can only open and edit.

The Novell file system keeps track of the rights that users have to files and directories on the network. When users try to access any file on the network, Novell File Services (NFS) either grants access or prohibits certain things that users can do with the file.

For more information on the specific rights on NetWare and OES servers, see “File Services” (<http://www.novell.com/documentation/oes/implgde/data/filesvcs.html>) in the *Novell OES Planning and Implementation Guide*.

For additional information on file system attributes, see the *File Systems Management Guide for OES* (http://www.novell.com/documentation/oes/stor_filesys/data/hn0r5fzo.html).

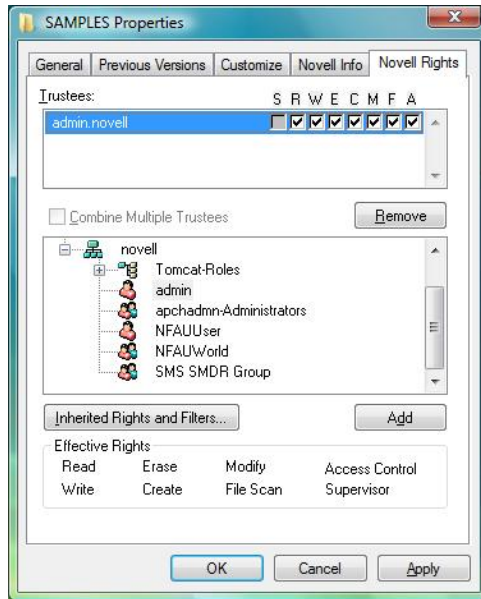
Rights are granted and revoked by creating trustee assignments. For more information, see [Section 5.2, “Changing Trustee Rights,” on page 58](#). File rights apply only to the file that they are assigned to. The rights can be inherited from the folder that contains the file. Folder rights apply not only to the folder but also to the files and folders it contains.

This section explains the following:

- ♦ [Checking File or Folder Rights \(page 57\)](#)
- ♦ [Changing Trustee Rights \(page 58\)](#)
- ♦ [Combining Multiple Trustees \(page 60\)](#)

5.1 Checking File or Folder Rights

- 1 In Windows explorer, right-click a Novell file system directory or file.
- 2 Click *Properties*.
- 3 Click the *Novell Rights* tab.



4 View the information.

The *Trustees* list shows the users or groups that have been granted rights to work with this file or folder. The trustees rights to the folder also apply to all the files and subfolders it contains unless the rights are explicitly redefined at the file or subfolder level.

The rights that each trustee has are shown by check marks under the letters. If you are viewing the properties of multiple files, the trustees and rights shown are the combined trustees and rights for all the files.

Effective Rights displays your rights for this file or folder. Users can receive rights in a number of ways, such as explicit trustee assignments, inheritance, and security equivalence (see [eDirectory Rights Concepts \(http://www.novell.com/documentation/edir88/edir88/data/fbachi_fb.html\)](http://www.novell.com/documentation/edir88/edir88/data/fbachi_fb.html) in the *Novell eDirectory 8.8 Administration Guide* for more information). Rights can also be limited by Inherited Rights Filters and changed or revoked by lower trustee assignments. The net result of all these actions—the rights a user can employ—are called *effective rights*.

5 To view a list of rights and filters inherited by this file or directory, click *Inherited Rights and Filters*.

All rights assignments on directories are inheritable. You can block such inheritance on individual subordinate items so that the rights aren't effective on those items, no matter who the trustee is. One exception is that the Supervisor right cannot be blocked.

6 Click *OK*.

5.2 Changing Trustee Rights

The assignment of rights involves a trustee and a target object. The trustee represents the user or set of users that are receiving the authority. The target represents those network resources the users have authority over. You must have the Access Control right to change trustee assignments.

- 1 In Windows Explorer, right-click a Novell file system directory or file.
- 2 Click *Properties*.

- 3 Click the *Novell Rights* tabbed page.
- 4 In the *Trustees* list, select the trustee whose rights you want to change.
- 5 Select or deselect the rights you want to assign for this trustee.

For each trustee in the list, there is a set of eight check boxes, one for each right that can be assigned. If a check box is selected, the trustee has that right. The following rights can be set for each trustee:

- ♦ **Read:** For a directory, grants the right to open files in the directory and read the contents or run the programs. For a file, grants the right to open and read the file.
- ♦ **Write:** For a directory, grants the right to open and change the contents of files in the directory. For a file, grants the right to open and write to the file.
- ♦ **Erase:** Grants the right to delete the directory or file.
- ♦ **Create:** For a directory, grants the right to create new files and directories in the directory. For a file, grants the right to create a file and to salvage a file after it has been deleted.
- ♦ **Modify:** Grants the right to change the attributes or name of the directory or file, but does not grant the right to change its contents (changing the contents requires the Write right).
- ♦ **File Scan:** Grants the right to view directory and file names in the file system structure, including the directory structure from that file to the root directory.
- ♦ **Access Control:** Grants the right to add and remove trustees for directories and files and modify their trustee assignments and Inherited Rights Filters.
- ♦ **Supervisor:** Grants all rights to the directory or file and any subordinate items. The Supervisor right cannot be blocked by an Inherited Rights Filter. Users with this right can grant or deny other users rights to the directory or file.

- 6 Click *OK*.

Trustee assignments override inherited rights. To change an Inherited Rights Filter, click *Inherited Rights and Filters*.

5.3 Adding a Trustee

When you add a trustee to a Novell file system directory or file, you grant a user (the trustee) rights to that directory or file. You must have the Access Control right to add a trustee.

- 1 In Windows Explorer, right-click the Novell file or directory that you want to add a trustee to.
- 2 Click *Properties*.
- 3 Click the *Novell Rights* tab.
- 4 In the tree diagram, locate the eDirectory™ user object that you want to add as a trustee, then click *Add*.
- 5 Set the rights for this user by selecting the boxes under the letters on the right of the *Trustees* list.

The following rights can be set for each trustee:

- ♦ **Read:** For a directory, grants the right to open files in the directory and read the contents or run the programs. For a file, grants the right to open and read the file.
- ♦ **Write:** For a directory, grants the right to open and change the contents of files in the directory. For a file, grants the right to open and write to the file.
- ♦ **Erase:** Grants the right to delete the directory or file.

- ♦ **Create:** For a directory, grants the right to create new files and directories in the directory. For a file, grants the right to create a file and to salvage a file after it has been deleted.
- ♦ **Modify:** Grants the right to change the attributes or name of the directory or file, but does not grant the right to change its contents (changing the contents requires the Write right).
- ♦ **File Scan:** Grants the right to view directory and file names in the file system structure, including the directory structure from that file to the root directory.
- ♦ **Access Control:** Grants the right to add and remove trustees for directories and files and modify their trustee assignments and Inherited Rights Filters.
- ♦ **Supervisor:** Grants all rights to the directory or file and any subordinate items. The Supervisor right cannot be blocked by an Inherited Rights Filter. Users with this right can grant or deny other users rights to the directory or file.

6 Click *OK*.

5.4 Removing a Trustee

When you remove a trustee of a Novell file system directory or file, you delete a user's rights to that directory or file. You must have the Access Control right to remove a trustee.

- 1 In Windows Explorer, right-click the Novell file or directory whose trustee you want to remove.
- 2 Click *Properties*.
- 3 Click the *Novell Rights* tab.
- 4 In the *Trustees* list, select the trustee you want to remove.
- 5 Click *Remove*, then click *OK*.

5.5 Combining Multiple Trustees

As an administrator, you might need to apply the same trustee assignments to a group of selected files. You can combine trustee assignments by selecting the *Combine multiple Trustees* option on the Novell Rights page.

For example, Kim is a trustee of FILEA and FILEB. Kim has Read, File Scan, and Access Control rights for FILEA and Read and File Scan rights for FILEB. Nancy has Read and File Scan rights for FILEA.

If you give a new user named Michael the Read, Write, and File Scan rights for both FILEA and FILEB and, at the same time, you want to give similar trustee rights to Kim and Nancy, you would select Combine Multiple Trustees. The following would then be true:

- ♦ Kim has Read and File Scan rights to both FILEA and FILEB. Her Access Control right is lost because the combined rights are based on the rights given to Michael.
- ♦ Nancy has Read and File Scan rights to both FILEA and FILEB. She has gained Read and File Scan rights to FILEB because the combined rights are based on the rights given to Michael.
- ♦ Michael has Read, Write, and File Scan rights to both FILEA and FILEB.

To combine multiple trustees:

- 1 In Windows Explorer, select all the Novell files or directories that you want to combine rights for.

- 2** Right-click the files or directories, then click *Properties*.
- 3** Click the *Novell Rights* tab.
- 4** Click *Combine Multiple Trustees*, then click *OK*.

Managing Passwords

6

Starting with NetWare® 6.5 and eDirectory™ 8.7.3, Novell provides password management tools that help administrators secure the network with stronger passwords and reduce password management by enabling end users to manage their own passwords. This set of tools is referred to as Universal Password.

With Universal Password, users can employ a single username and password to access networks, applications, devices, Internet sites, online services, portals, and more. Administrators can reduce or eliminate the task of resetting user passwords when they are forgotten or lost. Universal Password also manages multiple types of password authentication methods from disparate systems and provides extended password management capabilities. Universal Password is made possible by Novell Modular Authentication Services (NMAS™), an advanced authentication technology that allows for multiple methods of authentication, including simple passwords, smart cards, biometrics, tokens, and digital certificates.

Universal Password uses eDirectory plus NMAS to create a password that is used for access to all resources. This common password type—taking the place of the combination of simple passwords, NDS® passwords, and enhanced passwords in eDirectory—allows for the enforcement of strong password policies, such as minimum or maximum number of characters, a combination of alphabetic and numeric characters, and forced password reset.

In addition, password policies let users set a hint for their passwords. If a password is entered incorrectly or is forgotten, users can click the *Password Help* button and retrieve the hint they entered to help them remember their password. This reduces administrator time spent resetting forgotten passwords.

For more information on deploying universal passwords, see “[Deploying Universal Password](http://www.novell.com/documentation/password_management31/pwm_administration/data/allq21t.html#allq21t)” (http://www.novell.com/documentation/password_management31/pwm_administration/data/allq21t.html#allq21t) and “[Managing Passwords by Using Password Policies](http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html#ampxjj0)” (http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html#ampxjj0) in the *Novell Password Management Administration Guide*. It is important that you understand the requirements for using these advanced password policies before rolling out any password changes to your network.

The Novell® Client™ 2 for Windows Vista/2008 takes advantage of several of the features provided in Universal Password, including the following:


- ♦ Stronger password policies set in iManager.
- ♦ Display of password requirements on the Change Passwords dialog box so that users know what policies you have set for passwords.
- ♦ Access to password hints to help users remember their passwords.
- ♦ Support for changing passwords.
- ♦ Challenge-response for password reset.

6.1 Creating Strong Passwords

Password policies allow you to set strong password policies such as a minimum or maximum number of characters, a combination of alphabetic and numeric characters, and forced password reset. You set password policies in Novell iManager and then assign them to users. Administering passwords by using Novell iManager automatically sets the Universal Password to be synchronized to simple and NDS password values for backwards compatibility. The NMAS task in iManager allows for granular management of individual passwords and authentication methods that are installed and configured in the system.

For more information on setting up password policies in iManager, see “[Managing Passwords by Using Password Policies](http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html#ampxjj0)” (http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html#ampxjj0) in the *Novell Password Management Administration Guide*. Make sure that you read this documentation and understand the requirements before rolling out any password changes to your network.

Then, use the Password Policy Wizard in iManager to set up the policies.

- 1 Make sure you have completed the steps in “[Prerequisite Tasks for Using Password Policies](http://www.novell.com/documentation/password_management31/pwm_administration/data/bo59drg.html#bo59drg)” (http://www.novell.com/documentation/password_management31/pwm_administration/data/bo59drg.html#bo59drg) in the *Novell Password Management Administration Guide*. These steps prepare you to use all the features of password policies.
- 2 In iManager, make sure you are in the Roles and Tasks view by clicking  on the top button bar, then select *Passwords > Password Policies* in the navigation panel on the left.
- 3 Click *New* to create a new Password policy.
- 4 Follow the steps in the wizard to create Advanced Password Rules, Universal Password Configuration Options, and Forgotten Password selections for the policy.

For information about each step, see the online help as well as the information in “[Managing Passwords by Using Password Policies](http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html#ampxjj0)” (http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html#ampxjj0) in the *Novell Password Management Administration Guide*.

6.2 Displaying Password Requirements for End Users

Password policies ensure that passwords adhere to administrator-defined criteria. The user can examine these criteria by clicking the *Password Policy* or *Policy* button in any of the Change Password dialog boxes.

Figure 6-1 Change Password Dialog Box

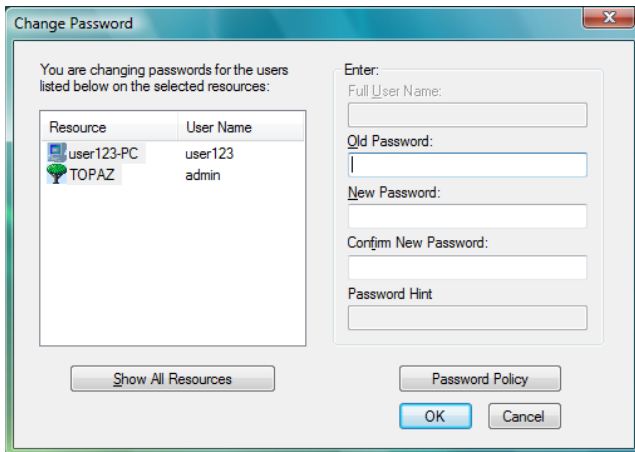
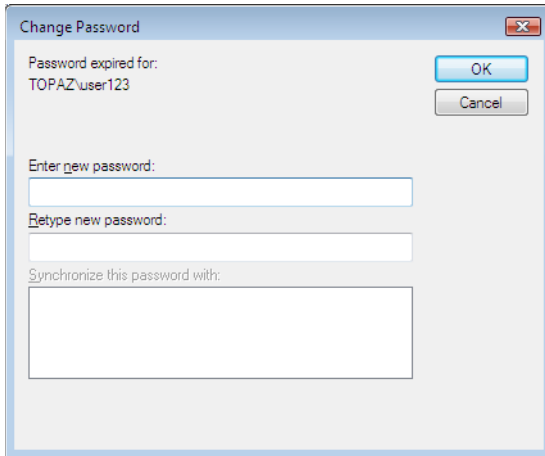
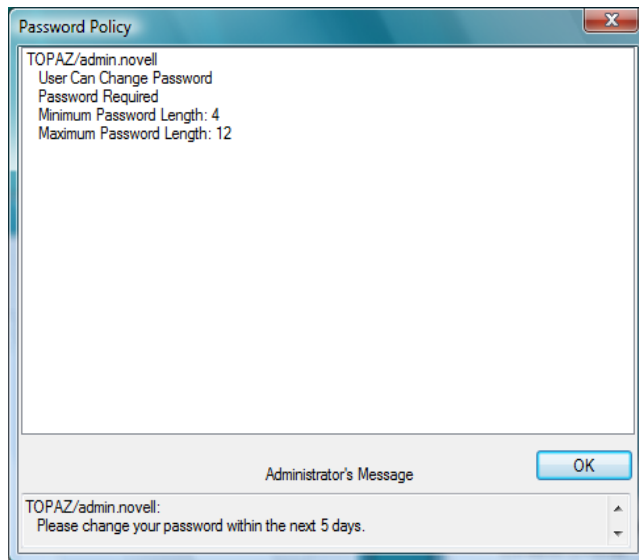


Figure 6-2 Change Expired Password Dialog Box



The following is an example of the password criteria displayed when you click the *Password Policy* button in the Change Password dialog box.

Figure 6-3 Novell Client Password Policy



6.3 Using Forgotten Password Self-Service

You can use the Password Policy Wizard in iManager to create a Password policy, which provides users with the ability to recover from a forgotten password without contacting the help desk.

The following features are supported:

- ◆ “Using the “Did You Forget Your Password?” Link” on page 66
- ◆ “Using Hints for Remembering Passwords” on page 69

IMPORTANT: Before using Password Self-Service, review the information about “[Managing Passwords by Using Password Policies](http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html#ampxjj0)” (http://www.novell.com/documentation/password_management31/pwm_administration/data/ampxjj0.html#ampxjj0) in the *Novell Password Management Administration Guide*.

Other applications that use the Universal Password might be able to use additional features, such as Reset Self-Service and Challenge Sets.

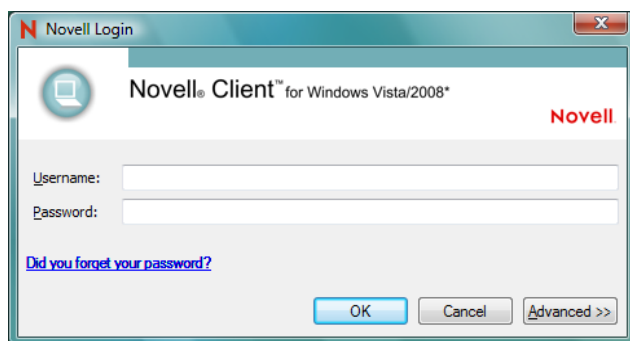
6.3.1 Using the “Did You Forget Your Password?” Link

When you click the *Did you forget your password?* link in the Novell Login dialog box, the system invokes the Forgotten Password Policy specific to the user. The following three options are supported by the Novell Client for Windows:

- ◆ Display a password hint.
- ◆ Authenticate via Challenge/Response and show a password reminder (requires eDirectory 8.8 or later).
- ◆ Authenticate via Challenge/Response and reset the password.

NOTE: The Novell Client does not support forgotten actions that involve e-mailing the password or the hint to the user.

Figure 6-4 Novell Client Login Dialog Box



NOTE: The Client prompts users to populate the Challenge/Response set if they log in and the sets have not been entered.

The workstation administrator can choose to display or not display the *Did you forget your password?* link on the Novell Login dialog box.

- 1 Right-click the Red N, then click *Novell Client Properties*.
- 2 Click the *Advanced Login* tab.
- 3 Set the *Forgotten Password Prompt* option to On or Off.

Before the *Did you forget your password?* link can work, you must complete the following:

- “Configuring Password Self-Service” on page 67
- “Configuring Challenge/Response Settings” on page 68

If you click the link before Password Self-Service is set up, you receive an error. If the administrator changed or set up a new policy, you are prompted on log in.

IMPORTANT: Not all features of Forgotten Password Self-Service are implemented with the Novell Client at this time, including e-mailing passwords and hints.

Configuring Password Self-Service

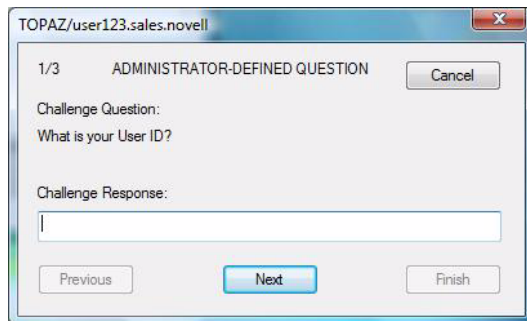
Before users can use the *Did you forget your password?* link, the administrator must configure Password Self-Service and the user must enter the optional information (password hint or responses to challenge questions). The administrator should also upgrade to eDirectory 8.8 or later. See “Password Self-Service” (http://www.novell.com/documentation/password_management/pwm_administration/data/bqf5d1r.html) in the *Novell Password Management Administration Guide* for more information.

Configuring Challenge/Response Settings

After the administrator configures the challenge sets and password policies, users need to provide their information for the challenge sets in either of the following two ways:

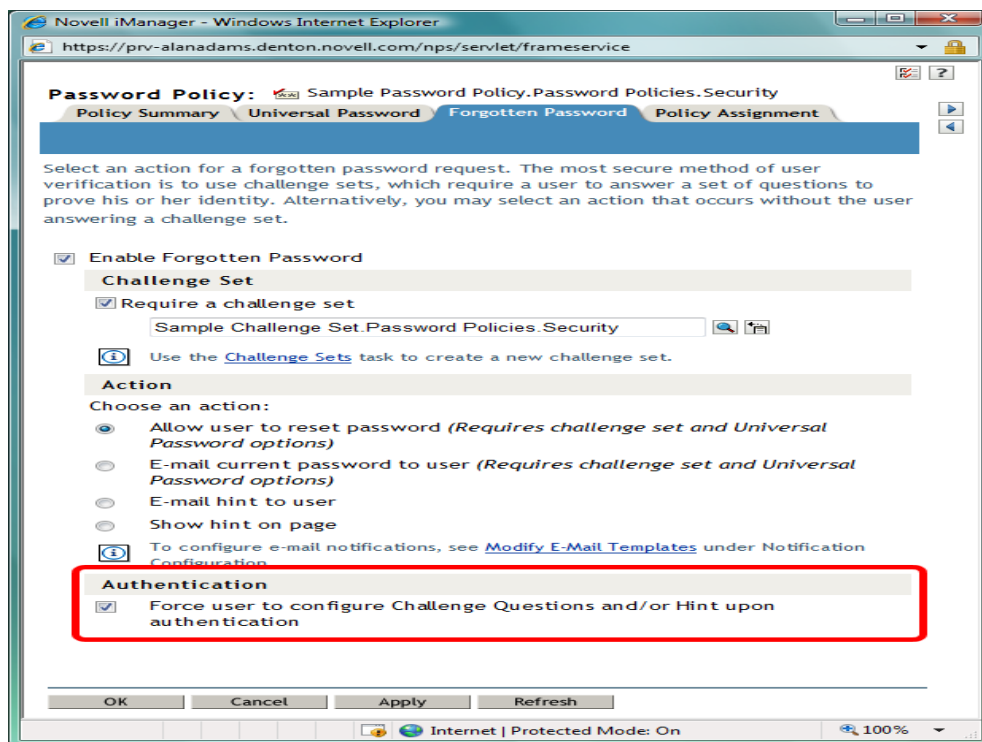
- ♦ Right-click the Red N (N), then click *User Administration > Challenge/Response Administration*. Depending on how the administrator configured the challenge sets, users enter their information in the dialog boxes presented. For example, if the administrator specifies four questions in the challenge set, users enter information in four different dialog boxes.

Figure 6-5 Sample Challenge/Response Dialog Box



- ♦ If the administrator selected the *Force user to configure Challenge Questions and/or Hint upon authentication* option on the Forgotten Password page in iManager, the client prompts users to enter this information when they log in and their challenge set information is missing or out of date.

Figure 6-6 Forgotten Password Page in iManager



The challenge/response questions allow for any response, such as a word, a sentence, or a phrase. Because it might be difficult to correctly type a phrase or sentence when the text is hidden, answers are not hidden with asterisks by default, like passwords usually are. However, as an added layer of security, you can configure the challenge/response LCM to hide the user's responses to the challenge questions. For example, when this functionality is enabled, instead of the user's response reading "my son charlie" in plain text, the response reads "*** ** * *****."

To configure the challenge/response LCM to hide the user's responses to the challenge questions:

- 1 Create the following registry key:

```
HKLM\SOFTWARE\Novell\NMAS\MethodData\challenge_response
```

- 2 Create a DWORD registry value named `mask_responses`, and set it to one of the following values:

0 - FALSE, don't mask responses (default value)

1- TRUE, mask responses

If a user forgets the answers to his or her challenge/response questions, the Novell Client does provide a way to reset the answers. Right-click **N**, then click *User Administration for > Challenge/Response Administration*. The user can then enter new responses in the dialog boxes presented.

6.3.2 Using Hints for Remembering Passwords

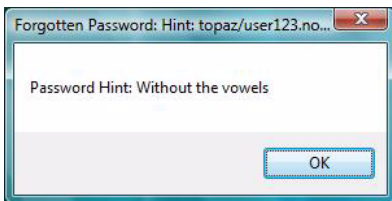
If you specify a Forgotten Password Action that requires a password hint, users are required to enter a hint that is a reminder of their password. The password hint is checked to make sure that it does not contain the user's password. Users must enter a new hint every time they change a password.

Figure 6-7 Change Password Dialog Box



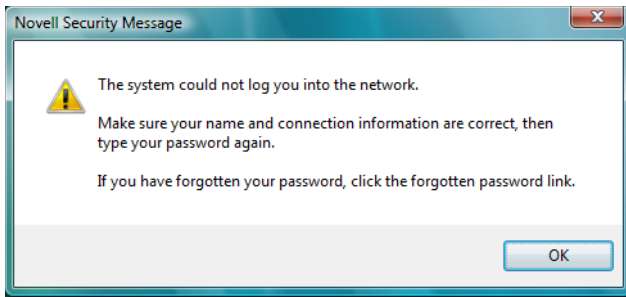
If a user clicks the *Did you forget your password?* link in the Novell Login dialog box, the user is asked to answer their challenge questions. When the series of challenge questions is answered correctly, a dialog box containing the password hint is displayed.

Figure 6-8 Forgotten Password Hint Dialog Box



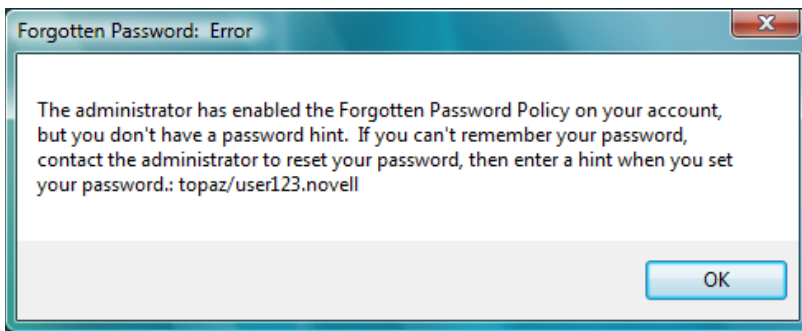
If a user enters an erroneous password, the login program displays a message with a prompt to retype the password or click the *Did you forget your password?* link.

Figure 6-9 Password Error Dialog Box



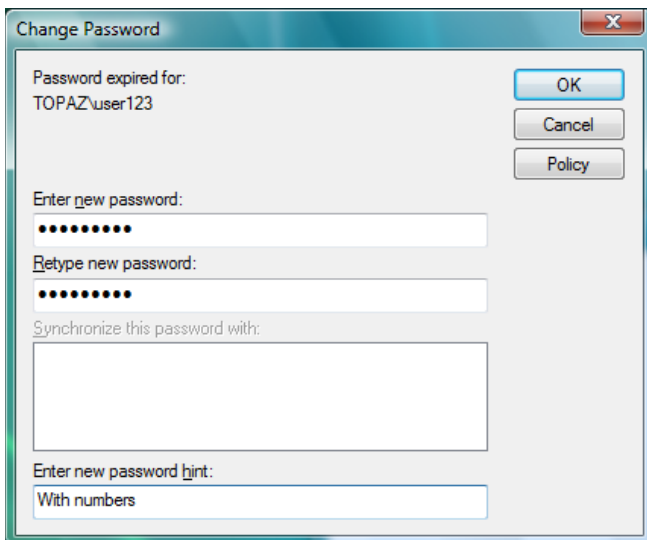
If the policy action is to show a hint but the user did not enter a hint for the current password, an error message is displayed telling the user to contact the system administrator to reset the password and to enter a hint the next time the password is set.

Figure 6-10 Forgotten Password Error Dialog Box



Users can also create a hint at any time using the Change Password window available at login, or by pressing Ctrl+Alt+Delete, then clicking *Change Password*.

Figure 6-11 Change Password Dialog Box



6.4 Setting Up Passwords in Windows

We recommend that you configure workstations to not use any of the Microsoft password restrictions available in User Manager. The Novell Client works best if password restrictions are set in eDirectory.

Security Considerations

7

This section contains the following topics:

- ♦ [Section 7.1, “Security Features,” on page 73](#)
- ♦ [Section 7.2, “Known Security Threats,” on page 74](#)
- ♦ [Section 7.3, “Security Characteristics,” on page 74](#)
- ♦ [Section 7.4, “Other Security Considerations,” on page 75](#)

7.1 Security Features

The following table contains a summary of the Novell® Client™ 2 for Windows Vista/2008 security features:

Table 7-1 *Novell Client for Windows Vista/2008 Security Features*

Feature	Yes/No	Details
Users are authenticated	Yes	GUI and command line login utilities support authentication of NCP™ and LDAP connections via user authentication into eDirectory™. NCP protocol authentication is supported via RSA, and LDAP authentication is supported via SSL and the Simple Bind protocol.
Servers, devices, and/or services are authenticated	Yes	Connections to servers are authenticated via user-supplied credentials. No device authentication is supported directly by the Client.
Access to information is controlled	Yes	
Roles are used to control access	Yes	
Logging and/or security auditing is done	Yes	
Data on the wire is encrypted by default	No	No wire encryption is supplied by this product.
Data stored is encrypted	Yes	
Passwords, keys, and any other authentication materials are stored encrypted	Yes	Passwords and other authentication materials in temporary storage are encrypted to prevent in-memory scanners.
Security is on by default	Yes	There are no configuration options to enable or disable with the exception of packet signing. Packet signing is enabled by default.
FIPS 140-2 compliant	Unknown	MSCAPI is not a FIPS 140-2 certified API, but this is deemed unimportant because customers have not expressed a requirement for FIPS 140 compliance.

7.2 Known Security Threats

The following section provides a list of known security threats for the Novell Client for Windows Vista/2008, an indication of how difficult it would be to exploit the threat, and what the consequences would be for a customer.

Table 7-2 *Known Security Threats*

Description	Consequence	Likelihood	Difficulty
Repetitive password cracking attempts	Intruder detection lockout	Low	Hard
“Stale” passwords	Password expiration, grace login enforcement	High	Hard
Attempted access out-of-hours or from unauthorized locations	Date/Time and Location restrictions at login	Medium	Easy
Port scanners	Unsuccessful pass of Nessus scans; possible port hijacking	Medium	Possible
Man-in-the-middle attacks	NCP request sequencing, packet signing	Low	Hard
Wire frame examination and manipulation	Same protections as with other Novell products utilizing NCP and RSA-based authentication	Low	Hard
Memory scanning for sensitive data	All buffers containing sensitive data (passwords) are short-term in nature and are zeroed and/or freed immediately after use.	Low	Hard

7.3 Security Characteristics

- ♦ [Section 7.3.1, “Identification and Authentication,” on page 74](#)
- ♦ [Section 7.3.2, “Authorization and Access Control,” on page 75](#)
- ♦ [Section 7.3.3, “Roles,” on page 75](#)
- ♦ [Section 7.3.4, “Security Auditing,” on page 75](#)

7.3.1 Identification and Authentication

This product uses X-Tier* to authenticate users via user identity information stored in eDirectory and resource authorization and access control provided by eDirectory. The product takes a username and password supplied directly by the user and transfers that information to X-Tier for use within its supported authentication mechanisms (via X-Tier’s plug-in authentication module architecture). If configured to do so, this product authenticates to eDirectory through SSL and LDAP Simple Bind Protocol.

This product does not itself authenticate to another product, system, or service. No portion of this product authenticates to another.

7.3.2 Authorization and Access Control

This product allows the protections supplied by eDirectory for access control to be fully realized for those resources that are contained within eDirectory. Access to resources is protected based on user identity (as stored within eDirectory). The VFS, daemon, and X-Tier work together to compare ACLs for a given file system path or object retrieved from eDirectory to the identity and session scope established for the identity that owns a given connection.

The VFS acts as a proxy to the local file system (via redirection of its local mount point) to make such decisions for network-based file system paths or objects.

7.3.3 Roles

This product does not define or manage roles. It simply makes use of roles that have already been defined elsewhere and treats role access privileges in the same way as any user identity.

Because the product has a VFS module running in the kernel, it does not require root access for users to create mount points (as do NCPFS and other similar open source offerings to date). The product does not require use of SETUID for any of its operations.

7.3.4 Security Auditing

No security auditing is performed by this product.

7.4 Other Security Considerations

If admin is compromised, all network access could also be compromised. For example, if a malicious entity gets administrator access, it might be able to steal user credentials and authenticate to the network with those credentials.

Managing Login

8

You can customize the Novell® Client™ 2 for Windows Vista/2008 login environment to suit your network and have greater control over what users can access during login.

- ◆ [Section 8.1, “Setting Up Login Scripts,” on page 77](#)
- ◆ [Section 8.2, “Setting Up Login Restrictions,” on page 77](#)
- ◆ [Section 8.3, “Customizing the Novell Login,” on page 79](#)
- ◆ [Section 8.4, “Logging In to the Network,” on page 81](#)
- ◆ [Section 8.5, “Logging Out of the Network,” on page 81](#)
- ◆ [Section 8.6, “Setting Up Login Profiles,” on page 81](#)
- ◆ [Section 8.7, “Setting Up LDAP Contextless Login and LDAP Treeless Login,” on page 90](#)
- ◆ [Section 8.8, “Configuring 802.1X Authentication,” on page 97](#)
- ◆ [Section 8.9, “Enabling AutoAdminLogon,” on page 101](#)
- ◆ [Section 8.10, “Enabling TSClientAutoAdminLogon,” on page 102](#)

8.1 Setting Up Login Scripts

When a user successfully logs in to the network, one or more login scripts are executed that automatically set up the workstation environment. Login scripts are similar to batch files and are executed by the Novell LOGIN utility. You can use login scripts to map drives and search drives to directories, display messages, set environment variables, and execute programs or menus.

For more information on setting up login scripts, see the *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html).

8.2 Setting Up Login Restrictions

Login restrictions are limitations you set on user accounts in order to control access to the network. These restrictions can be set in Novell iManager for each user and include the following:

- ◆ Requiring a password. You can specify its minimum length, whether it must be changed and how often, whether it must be unique, and whether the user can change it. You can also require strong passwords. See [Chapter 6, “Managing Passwords,” on page 63](#).
- ◆ Setting the number of logins with an expired password and the number of incorrect login attempts allowed.
- ◆ Setting account limits such as an account balance or expiration date.
- ◆ Limiting disk space for each user by specifying the maximum blocks available for each user on a volume.
- ◆ Specifying the number of simultaneous connections a user can have.
- ◆ Specifying (by node address) which workstations users can log in on.
- ◆ Restricting the times when users can log in (you can assign all users the same hours, or you can restrict users individually).

When a user violates login restrictions by entering an incorrect password or by exceeding the number of logins with an expired password, the account is disabled and no one can log in using that username. This prevents unauthorized users from logging in.


To manage user login restrictions:

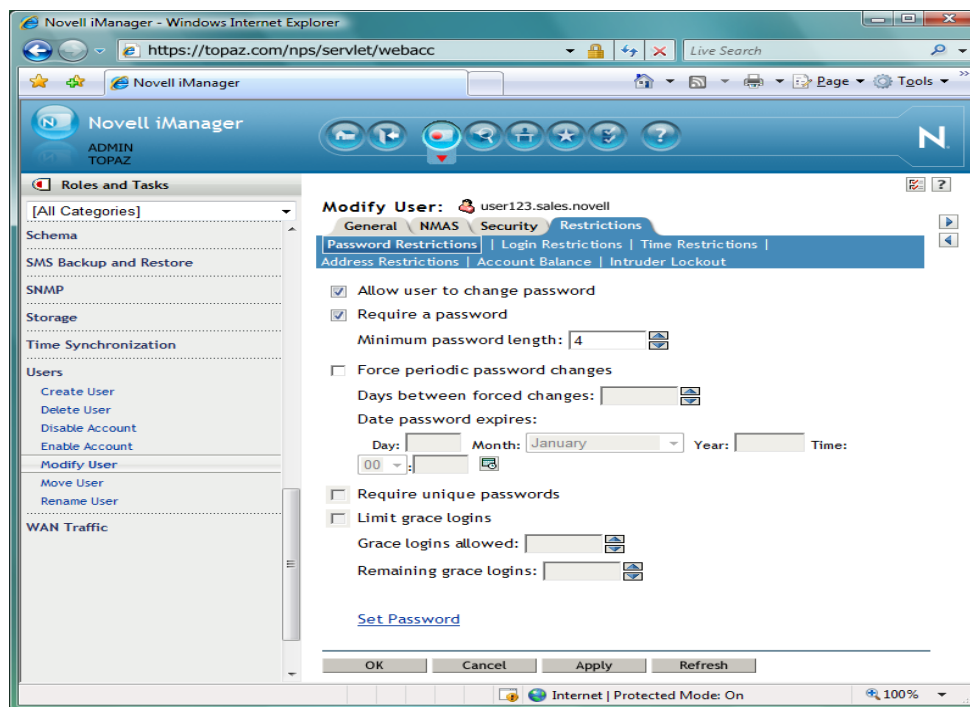
- 1 Launch iManager by entering the following in the *Address* field of a network browser:

`http://server_IP_address/iManager.html`

- 2 Log in using your username and password.

You will have access only to those features you have rights to. To have full access to all Novell iManager features, you must log in as Supervisor/Administrator of the tree.

- 3 Make sure you are in the Roles and Tasks view by clicking  on the top button bar, then select *Users > Modify User* in the navigation panel on the left.
- 4 Type the name and context of the User object you want to modify, or use the search feature to find it, then click *OK*.
- 5 Click the *Restrictions* tab (or drop-down list, depending on the browser you are using).



The following options appear. They open pages that display various properties:

- ◆ Password Restrictions
- ◆ Login Restrictions
- ◆ Time Restrictions
- ◆ Address Restrictions
- ◆ Account Balance
- ◆ Intruder Lockout

- 6 Make your changes, then click *Apply* to preview or *OK* to save.

8.3 Customizing the Novell Login

The Novell Login process can be customized to use the features that you want users to have access to. Customizing gives you control over the following:

- ◆ NMAS™ authentication

NMAS authentication adds additional security to the network. However, if your network does not use NMAS, login might take additional time and you might want to disable NMAS authentication.

For more information, see “Disabling NMAS on the Server” in the *Novell Modular Authentication Services 3.0 Administration Guide* (<http://www.novell.com/documentation/nmas30/index.html?page=/documentation/nmas30/admin/data/am4bbpx.html>).

IMPORTANT: You can use the `Install.ini` file to control the installation of NMAS. In the `[Setup]` section of the `Install.ini` file, there are `InstallNICI` and `InstallNMAS` options. If you change these options to No (they are set to Yes by default), NICI and NMAS are not installed when you install the Client. See [Section 2.3, “Using the Install.ini File,” on page 22](#) for more information.

- ◆ Novell Login dialog box customization

The dialog box can be customized to control the availability of certain login options. This gives you control over how users log in.

- ◆ *Advanced* button

If you have set up several login profiles and do not want users to change the data in various login fields (such as Tree, Context, Server, and Run Scripts), you can hide the *Advanced* button.

- ◆ *Clear current connections* check box

If you want all connections to be cleared every time users log in, or if you don't want any connections to be cleared, you can set the value in the location profile and then hide the *Clear current connections* check box.

NOTE: The *Clear current connections* option is never visible during initial login, because an initial login automatically clears all connections.

- ◆ *Context* field

If the Novell Login dialog box is being used to log in to a specific tree, you can disable the *Context* field to prevent users from changing the context.

- ◆ *Contexts* browse button

If the Novell Login dialog box is being used to log in to a specific tree, you can disable the *Contexts* browse button to prevent users from changing the context.

- ◆ *Did you forget your password?* prompt

This prompt gives users the ability to recover from a forgotten password without contacting the help desk. See [Section 6.3, “Using Forgotten Password Self-Service,” on page 66](#) for more information on configuring the Forgotten Password feature.

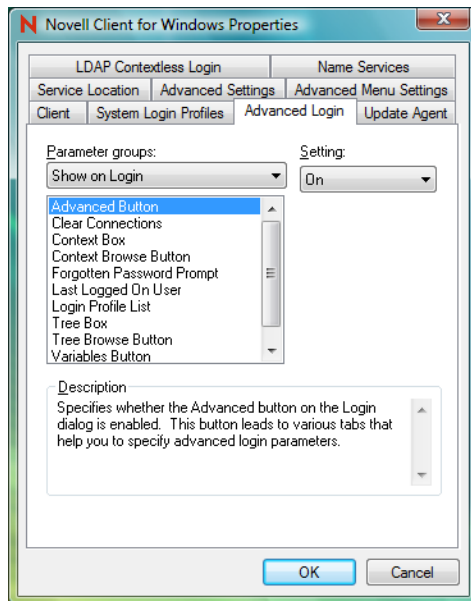
- ◆ Last logged on user

You can specify whether the last logged on user is displayed along with the Novell Logon when a user logs on to a computer.

- ◆ *Login Profile* drop-down list at the top of the dialog box
The *Login Profile* drop-down list can be set to Off (always hide the Login Profile list), On (always display the Login Profile list) or Automatic (only display the Login Profile list if it contains more than one Login Profile).
- ◆ *Tree* field
If the Novell Login dialog box is being used to log in to a specific tree, you can disable the *Tree* field to prevent users from changing the tree.
- ◆ *Trees* browse button
If the Novell Login dialog box is being used to log in to a specific tree, you can disable the *Trees* browse button to prevent the user from changing the tree.
- ◆ *Variables* button on the Script tabbed page
If you use %2, %3, %4, or %5 in the login script, you might want to set these values in the location profile but not allow users to change them. In this case, it might be helpful to hide the *Variables* button.

To show or hide any Login dialog box option:

- 1 Right-click the Red N icon (N) in the notification area of the taskbar, then click *Novell Client Properties*.
- 2 Click *Advanced Login*.
- 3 Select *Show on Login* in the *Parameter groups* drop-down list.



- 4 Select the parameter you want, then select *On* or *Off* in the *Setting* drop-down list.
A short description of each parameter is available in the *Description* field when you select the parameter. For more information, see [Section 4.2.3, “Advanced Login Settings,”](#) on page 43.
- 5 Click *OK*.

8.4 Logging In to the Network

There are several ways to initiate a Novell Client login after users have already logged in to a Novell server or to the local workstation:

- ♦ Right-click the Red N icon (**N**) in the notification area of the taskbar, then click *Novell Login*.
- ♦ In the Network folder, double-click the desired Novell tree or server.
- ♦ In the Network folder, right-click the desired Novell tree or server, then click *Open*.
- ♦ Run `loginw32.exe` from the command prompt.
This file is located in the `C:\Windows\System32` folder.
- ♦ Include `loginw32.exe` in the Windows Vista startup folder.
This causes the Novell Client Login to run automatically at workstation startup and shows the Novell Login screen when Windows Vista first opens.

8.5 Logging Out of the Network

To log in to different Novell services while logging out of other servers or clearing the current connections, use the Novell Client Login dialog box and select the *Clear Current Connections* option.

If you want to log out of both the Windows Vista workstation and Novell, press Ctrl+Alt+Del and then click *Logoff*.

To log out of a specific server, right-click the Network folder, click *NetWare Connections*, select the server or tree, then click *Detach*. Or, right-click the Red N menu, click *Novell Connections*, select the server or tree, and then click *Detach*.

8.6 Setting Up Login Profiles

Login profiles let you save the information from a user's individual login. When the user selects this profile during login, the profile automatically sets up the login information you specify, such as the user's name, server, tree, context, login script, and other applicable information so that the user does not need to enter this information.

Login profiles are especially useful for users who log in from multiple places. Users can have separate profiles for the office, home, laptop, or any other workstation they use. This simplifies the login process so that users don't need to remember their login information for each workstation. Using multiple login profiles also gives you control over what users can access from each workstation.

On a single workstation, you can create login profiles that are customized for a particular user. The Novell Client for Windows Vista/2008 also allows different users on the same machine to have their own login profiles. You can also use the Novell Client Install Manager (`nciman.exe`) to create login profiles that are more general in nature and deliver them during the installation of the Novell Client. And as an administrator, you can define a set of system login profile templates that contain the information most commonly needed for your environment. These profiles form the basis for individualized profiles for your users.

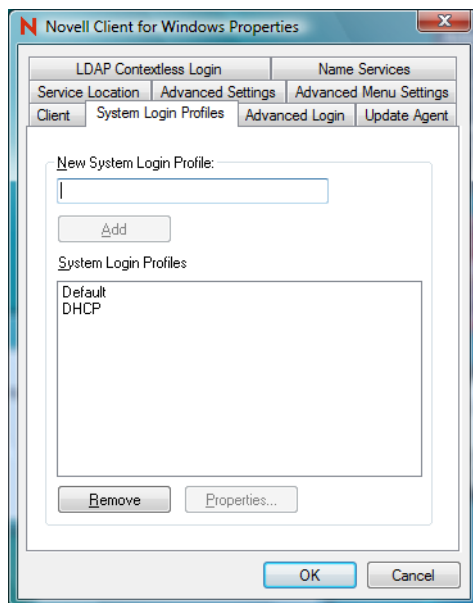
Users can add, edit, or delete their own login profiles as needed without affecting other users or modifying the system templates (see “[Managing Your Login Profiles](#)” in the *Novell Client for Windows Vista/2008 User Guide* for more information). An application can invoke login with some parameters and allow others to be supplied from the login profile.

System Login Profiles and User Login Profiles

All login profiles that don't belong to a specific user belong to the system and are available to all users on that system. A system can have a default profile, and each user on the system can have a default profile. System default profiles names have angle brackets around them (for example, <Default>), while user profile names do not (for example, Default).

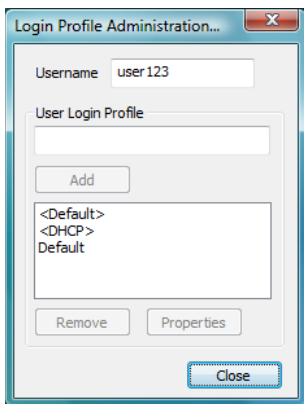
You can edit system profiles (and only system profiles) on the *System Login Profiles* tab in the Novell Client for Windows Properties dialog box (right-click the Red N icon in the notification area of the taskbar, click *Novell Client Properties*, then click the *System Login Profiles* tab). The system profiles in this list appear without angle brackets.

Figure 8-1 *System Login Profiles*



When you edit user profiles (right-click the Red N icon in the notification area of the taskbar, click *User Administration for*, then click *Login Profile Administration*), you will see both system profiles (with angle brackets) and user profiles (without angle brackets) in the list of profiles. Only the user profiles are directly editable. You can select a system profile in the Login Profile Administration dialog box to edit, but when you save the profile, it is saved as a user profile with the same name as the system profile, but without the brackets.

Figure 8-2 *User Login Profiles*

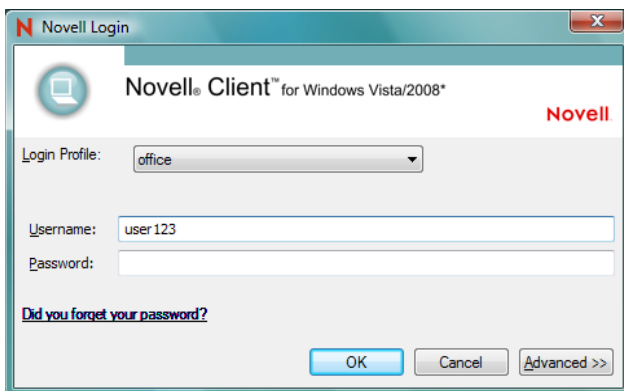


The system login profiles provide a template for users to create custom profiles. You cannot modify a system template from the Login Profile Administration dialog box on the *User Administration for* submenu. For example, if both a <Default> and a Default profile appear in the list, you can only edit the Default profile. If, however, you want to use the values in the <Default> system profile to replace the values in the Default user profile, you can delete Default, select <Default> to edit in the Login Profile Administration dialog box, then save the profile, which then creates a new user profile named Default. Users can then modify Default as desired.

Using Login Profiles During Login

When users log in using the Novell Login dialog box, they can select the login profile they want to use from the *Login Profile* drop-down list. You can use the *Advanced Login* tab in the Novell Client for Windows Properties dialog box to specify if the Login Profile drop-down list is available or not.

Figure 8-3 *Novell Login Dialog Box with the “office” Login Profile Selected*



If a system profile (for example, <Default>) is the only profile with that name on the *Login Profile* drop-down list, and if it is a complete profile, users can select that profile and log in with it. But if, for example, both a <Default> system profile and a Default user profile appear on the list, selecting <Default> causes the Default user profile to be used instead because user profiles always supercede system profiles if they both have the same name.

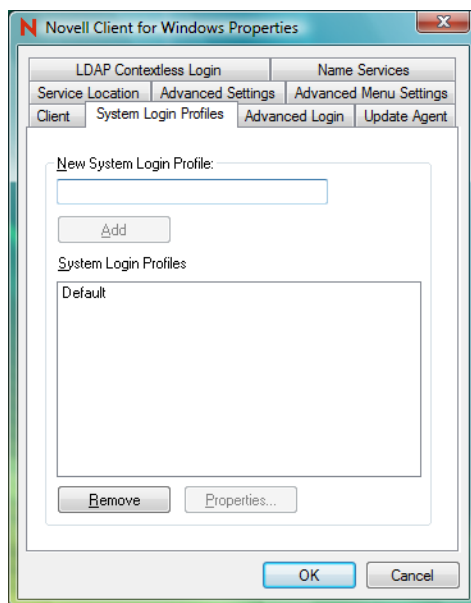
- ◆ [Section 8.6.1, “Creating a System Login Profile,” on page 84](#)
- ◆ [Section 8.6.2, “Creating a System Login Profile for Use on Multiple Workstations,” on page 85](#)

- ◆ Section 8.6.3, “Viewing or Editing a System Login Profile's Properties,” on page 87
- ◆ Section 8.6.4, “Removing a System Login Profile,” on page 88
- ◆ Section 8.6.5, “Enabling the Use of DHCP In a System Login Profile,” on page 88

For information on creating and editing user login profiles, see “Managing Your Login Profiles” in the *Novell Client for Windows Vista/2008 User Guide*.

8.6.1 Creating a System Login Profile

- 1 Right-click the Red N icon (N) in the notification area of the taskbar.
- 2 Click *Novell Client Properties*, then click the *System Login Profiles* tab.

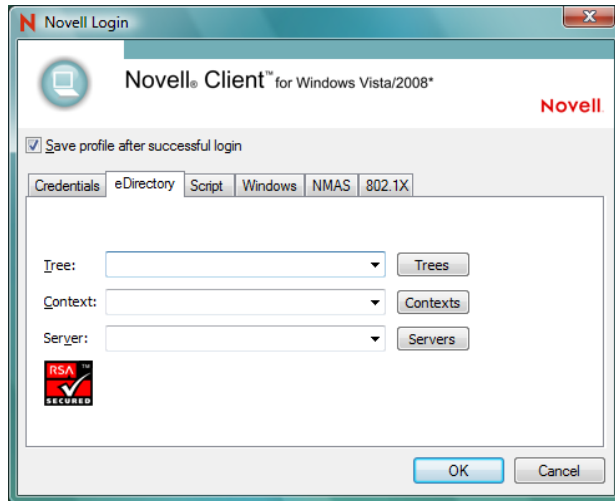


- 3 Type the name of the profile you want to add in the *New System Login Profile* text box, then click *Add*.

The name you specify here will appear with angle brackets (to indicate that it is a system login profile) in the Novell Login dialog box and the **Login Profile Administration** dialog box.

You can give a system login profile the same name as a user login profile (the system login profile will show up with angle brackets around it), but be aware that during login if a user selects a system login profile that has the same name as a user login profile, the user login profile will be used because user profiles always supersede system profiles when they have the same name.

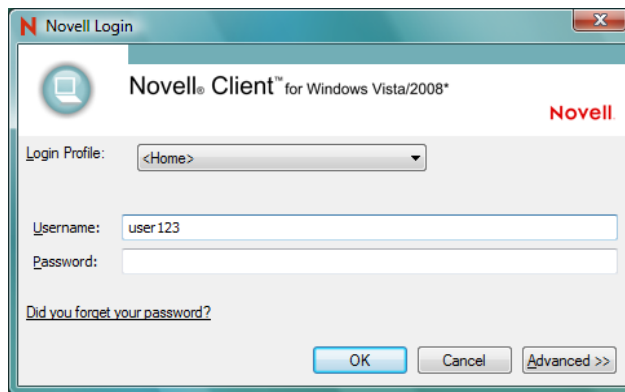
- 4 In the Novell Login dialog box, specify the login information you want for this profile, such as a tree, context, and server.



- 5 Click *OK* to close the Novell Login dialog box, then click *OK* to close the Novell Client Properties dialog box.

When a user logs in using the Novell Login dialog box, he or she can select the system login profile from the *Login Profile* drop-down list.

Figure 8-4 Novell Login Dialog Box with a System Login Profile Selected

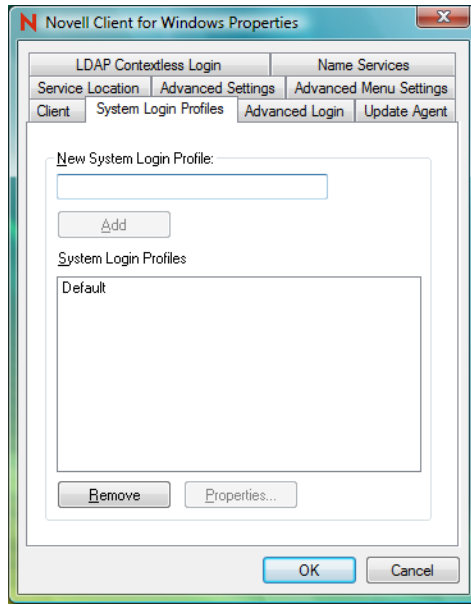


8.6.2 Creating a System Login Profile for Use on Multiple Workstations

Login Profiles are one of many settings that can be predefined by using a Novell Client properties file that is applied during installation of the Novell Client. For more information, see [“Creating the Novell Client Properties File” on page 21](#).

To create a system login profile that can be distributed by the Novell Client Install Manager:

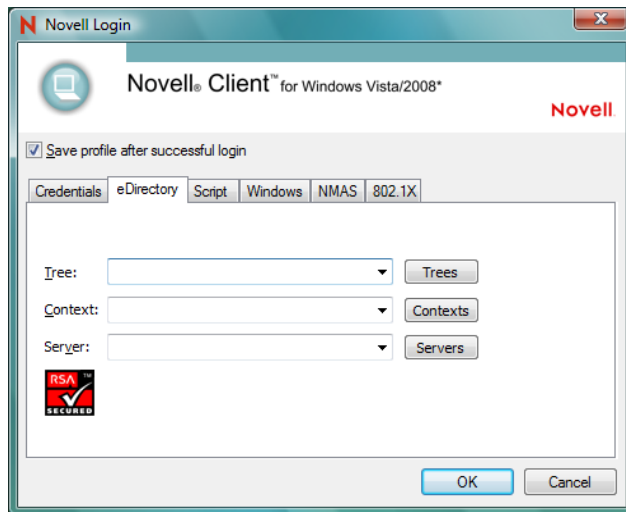
- 1 Start the Novell Client Install Manager (`nciman.exe`), located in the `C:\Novell\Novell Client for Windows Vista-2008\Admin` folder.
- 2 In the *Novell Client for Windows Properties* box, double-click *Client* to open the Novell Client for Windows Properties dialog box, then click the *System Login Profiles* tabbed page.



- 3 Type the name of the profile you want to add in the *New System Login Profile* text box, then click *Add*.

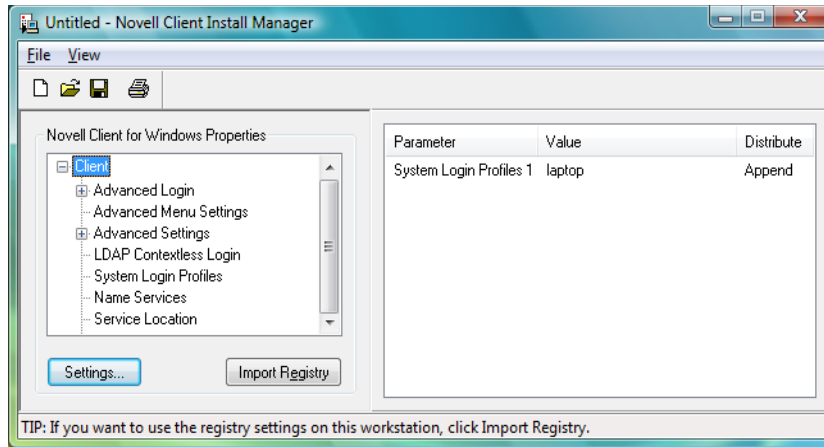
To create the Default system profile, enter `Default` as the new profile name.

- 4 In the Novell Login dialog box, specify the login information you want for this profile, such as the tree, context, and server.



- 5 Click *OK* to close the Novell Login dialog box, then click *OK* to close the Novell Client for Windows Properties dialog box.

A parameter for the login profile you just created appears in the *Parameter* list in the Novell Client Install Manager.



- 6 Right-click the system login profile parameter, then click *Distribute (Append)*.
- 7 Select whether to append or replace any existing login profiles already on the workstations.

Appending an existing login profile merges the settings in this file with the settings that exist in the login profile already on a workstation. Replacing overwrites any existing login profile with this one.

By default, the new login profile item is automatically appended to any login profile that might exist on a workstation.

WARNING: If you right-click the login profile parameter and select *Clear List and Distribute(Never)*, the login profile you just created is deleted.

- 8 Modify any other Client properties as needed.

For more information, see [“Creating the Novell Client Properties File” on page 21](#).
- 9 Click *File > Save*, then specify a name for the Novell Client properties file.

You can use any filename (for example, `workstation_properties.txt`).
- 10 Copy this file to the root directory of the Client build (`C:\Novell\Novell Client for Windows Vista-2008`).

This file can be specified as input to **ACU**, the **Update Agent**, or `setup.exe` during the next Client installation/upgrade. For more information on distribution methods, see [Chapter 2, “Advanced Installation Options,” on page 17](#).

8.6.3 Viewing or Editing a System Login Profile's Properties

- 1 Right-click the **N** icon in the notification area of the taskbar.
- 2 Click *Novell Client Properties*, then click the *System Login Profiles* tabbed page.
- 3 In the *System Login Profiles* list, select the name of a profile.
- 4 Click *Properties*.
- 5 In the Novell Login dialog box, view or modify the login information you want for this profile, such as the user's name, server, and context.
- 6 Click *OK* to close the Novell Login dialog box, then click *OK* to close the Novell Client Properties dialog box.

8.6.4 Removing a System Login Profile

- 1 Right-click the **N** icon in the notification area of the taskbar.
- 2 Click *Novell Client Properties*, then click the *System Login Profiles* tabbed page.
- 3 In the *System Login Profiles* list, select the name of the profile you want to remove.
- 4 Click *Remove*.
- 5 Click *OK* to close the Novell Client Properties dialog box.

8.6.5 Enabling the Use of DHCP In a System Login Profile

If a DHCP server is set up on your network, the DHCP server can inform the Novell Client of network-specific configuration information.

You can easily configure Novell DHCP servers (NetWare 5 and later) to distribute this information to the clients. For more information, see the *Novell DNS/DHCP Administration Guide for Linux* (http://www.novell.com/documentation/oes2/ntwk_dnshcp_nw/data/front.html#front) or the *Novell DNS/DHCP Administration Guide for NetWare* (http://www.novell.com/documentation/oes/dhcp_enu/data/front.html).

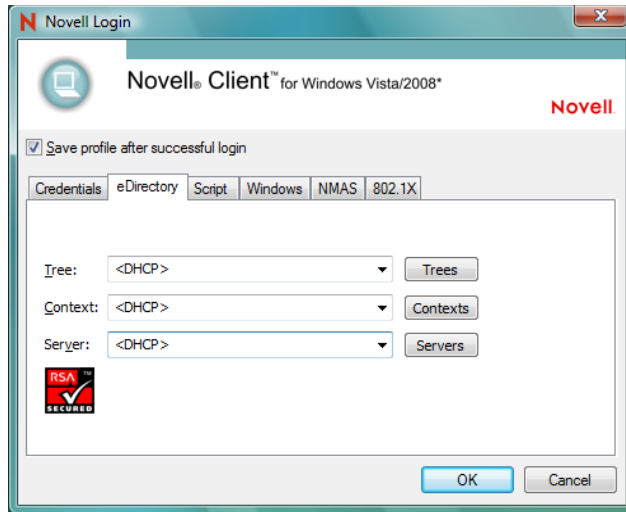
Clients obtain configuration information from DHCP even when you statically configure the clients' IP addresses or when the DHCP server used to supply the information is different from the DHCP server supplying an IP address to the clients.

Unlike the Novell Client for Windows XP/2003, the use of information from DHCP options 85, 86, and 87 is not enabled through a *DHCP Settings* tab in the Novell Client Properties dialog box. Using information from DHCP in the Novell Client for Windows Vista/2008 is enabled directly from the *Tree:*, *Context:*, and *Server:* fields in the login profile. You can enable use of DHCP information when creating a new profile or when editing an existing profile.

- 1 Right-click the **N** icon in the notification area of the taskbar.
- 2 Click *Novell Client Properties*, then click the *System Login Profiles* tabbed page.

NOTE: Users can create their own DHCP profiles by using the *Login Profile Administration* option on the Red N menu. See “**Enabling the Use of DHCP In a Personal Login Profile**” in the *Novell Client for Windows Vista/2008 User Guide* for more information.

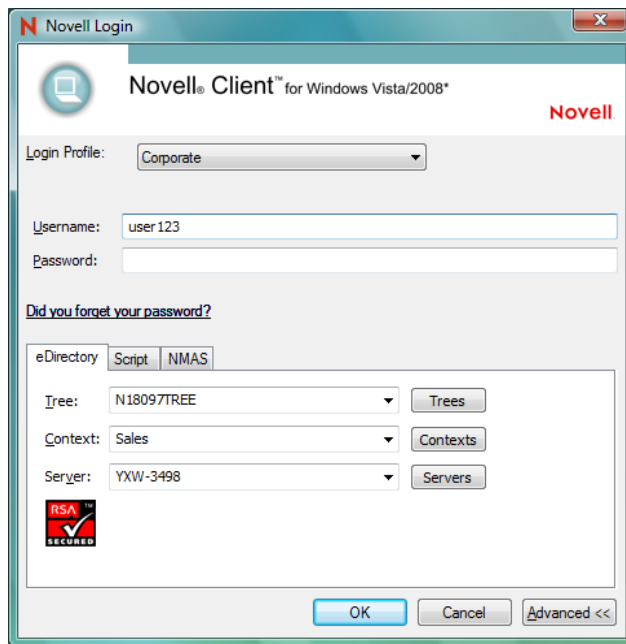
- 3 Type the name of the profile you want to add (for example, *Corporate*) in the *New System Login Profile* text box, then click *Add*.
- 4 In the fields you want to be filled by DHCP, select *<DHCP>* from the drop-down menu.



5 Click *OK* twice.

The next time a user opens the Novell Login dialog box, the DHCP-enabled profile is available as an option on the *Login Profile* drop-down menu.

Select the DHCP-enabled profile from the *Login Profile* drop-down menu to automatically populate the fields that were given the <DHCP> option in **Step 4** with whatever the DHCP server sends.



NOTE: When using the login profile to perform a Novell login, users can overwrite the values displayed by DHCP, but the changes are in effect only for that specific login. If <DHCP> is chosen as an option in a login profile for Tree, Context, or Server, it cannot be removed by simply editing the field when logging in or by saving the profile on successful login. Any values entered in these fields during login are not saved when <DHCP> is enabled for that field. If users want to

permanently change the values in that field, they must edit the login profile using either the System Profile Manager (*System Login Profiles* tab on the Novell Client Properties dialog box) or the User Profile Manager (*Login Profile Administration* option on the Red N menu).

8.7 Setting Up LDAP Contextless Login and LDAP Treeless Login

LDAP Contextless Login facilitates the merging of several trees in to one global tree. Without LDAP Contextless Login, users must change their context information in the Novell Login dialog box when changes take place in the tree structure. This can result in increased IT costs to manage and support the changes. LDAP Contextless Login makes it easier for users to work in the new global tree because it is unnecessary for the users to manage or know about changes to their organization's name or its placement in the hierarchy. Because users no longer need to enter their context to authenticate, the context can be changed on the back end as many times as necessary without the users knowing and without the costs associated with managing and supporting these changes.

The Lightweight Directory Access Protocol (LDAP) is an Internet communications protocol that lets client applications access directory information. It is based on the X.500 Directory Access Protocol (DAP) but is less complex than a traditional client and can be used with any other directory service that follows the X.500 standard. Lightweight Directory Access Protocol (LDAP) Services for Novell eDirectory™ is a server application that lets LDAP clients access information stored in eDirectory.

If your network has LDAP Services for Novell eDirectory set up on your eDirectory tree and you are running Novell eDirectory 8.5 or later, users who are logging in to the network from Windows can log in to the network without entering their context in the Novell Login dialog box. To log in, users need to know only their username, password, and the name of the tree that is running LDAP Services. Optionally, you can also have users log in to the network without specifying the eDirectory tree name.

User objects can be located in the tree by username or e-mail address. You can also enable wildcard searches. If wildcard searches bring up multiple usernames, the user is prompted to select his or her username.

Generally, when a user connects to the network using LDAP, the connection is made through an LDAP client. Now, the Novell Client Login acts as an LDAP client and connects to the network. All LDAP clients bind (connect) to Novell eDirectory as one of the following types of users:

- ◆ [Public] User (Anonymous Bind)
- ◆ Proxy User (Proxy User Anonymous Bind)
- ◆ NDS® or eDirectory User (NDS User Bind)

NOTE: The NDS User Bind is not used by LDAP Contextless Login.

The type of bind and the rights assigned to the corresponding User object determine the content that the LDAP client can access. LDAP clients access a directory by building a request and sending it to the directory. When an LDAP client sends a request through LDAP Services for eDirectory, eDirectory completes the request for only those attributes that the LDAP client has the appropriate access rights to. There are additional restrictions that can be set to further secure connections.

This documentation assumes that you are familiar with LDAP. It contains links to information about LDAP and eDirectory; it is not meant to replace or supersede the documentation about LDAP running on eDirectory. If you are unfamiliar with LDAP, you should familiarize yourself with LDAP and how it operates in your network.

For more information on LDAP for Novell eDirectory, see “[Understanding How LDAP Works with eDirectory](http://www.novell.com/documentation/edir88/edir88/data/h0000007.html#h0000007)” (<http://www.novell.com/documentation/edir88/edir88/data/h0000007.html#h0000007>) in the *Novell eDirectory 8.8 Administration Guide*.

Before users can log in to the network without their context or tree information, you must complete the following steps:

- 1 Set up Novell LDAP Services for eDirectory.
See “[Setting Up Novell LDAP Services for eDirectory](#)” on page 91.
- 2 Do one of the following:
 - ♦ If you are installing Novell Client software on a few workstations, install the software and then configure the Novell Client property pages so that the LDAP port number and SSL settings in the client properties match the settings on your LDAP server. See “[Setting Up LDAP Contextless Login on One Workstation](#)” on page 94.
 - ♦ If you are installing Novell Client software on multiple workstations, preconfigure the LDAP contextless login property pages prior to installing the Client software so that the LDAP port number and SSL settings in the Client properties match the settings on your LDAP server (see “[Setting Up LDAP Contextless Login on Multiple Workstations](#)” on page 96). Then install the Client software.
- 3 Inform users about contextless login.
See “[Logging In Using LDAP Contextless Login](#)” on page 96.

If you experience problems with LDAP Contextless Login, check the Server and Group object configurations. Most problems occur in the access rights given to the Proxy User. You can use any LDAP browser available from the Internet to check the access rights. Browse to the user and verify that you can read the inetOrgPerson property and other properties you are searching for, such as CN and MAIL. If these cannot be seen through the LDAP browser by logging in anonymously, contextless login cannot perform the proper searches to resolve the User object’s context in the tree.

8.7.1 Setting Up Novell LDAP Services for eDirectory

Before users can take advantage of LDAP Contextless Login, the network must be running Novell LDAP Services for eDirectory 8.5 or later and you must complete the following steps:

- 1 Install and configure the LDAP Services for eDirectory on the LDAP server.
See “[Understanding LDAP Services for Novell eDirectory](http://www.novell.com/documentation/edir88/edir88/data/a4wyf4a.html#a4wyf4a)” (<http://www.novell.com/documentation/edir88/edir88/data/a4wyf4a.html#a4wyf4a>) and “[Configuring LDAP Services for Novell eDirectory](http://www.novell.com/documentation/edir88/edir88/data/ahlmb7h.html#ahlmb7h)” (<http://www.novell.com/documentation/edir88/edir88/data/ahlmb7h.html#ahlmb7h>) in the *Novell eDirectory 8.8 Administration Guide*.
- 2 Do one of the following:
 - ♦ Grant the Read right to the Public Object. See “[Connecting As a \[Public\] User](#)” on page 92.
 - ♦ Create a Proxy User Object that has the correct rights. See “[Connecting As a Proxy User](#)” on page 92.

Connecting As a [Public] User

An anonymous bind is a connection that does not contain a username or password. If an LDAP client without a name and password binds to LDAP Services for eDirectory and the service is not configured to use a Proxy User, the user is authenticated to eDirectory as user [Public].

User [Public] is a nonauthenticated eDirectory user. By default, user [Public] is assigned the Browse right to the objects in the eDirectory tree. The default Browse right for user [Public] allows users to browse eDirectory objects but blocks user access to the majority of object attributes.

The default [Public] rights are typically too limited for most LDAP clients. Although you can change the [Public] rights, changing them gives these rights to all users. Because of this, we recommend that you use the Proxy User Anonymous Bind. For more information, see [“Connecting As a Proxy User” on page 92](#).

To give user [Public] access to object attributes, you must do the following in iManager:

- 1 Make user [Public] a trustee of the appropriate container or containers.
- 2 Grant the Read right to user [Public].

Without the Read right, user [Public] cannot search containers for the User object information.

You can grant the Read right to the specific attributes that LDAP Contextless Login searches for User objects or you can grant rights to all attributes. For example, you can grant rights only to the e-mail address or telephone number; when LDAP Contextless Login searches the tree as user [Public], it searches only these attributes.

Connecting As a Proxy User

A Proxy User Anonymous Bind is an anonymous connection linked to an eDirectory username. If an LDAP client binds to LDAP for eDirectory anonymously, and the protocol is configured to use a Proxy User, the user is authenticated to eDirectory as the Proxy User. The name is then configured in both LDAP Services for eDirectory and in eDirectory.

The key concepts of Proxy User Anonymous Binds are as follows:

- ♦ All LDAP client access through anonymous binds is assigned through the Proxy User object.
- ♦ The Proxy User must have a null password and must not have any password restrictions (such as password change intervals). Do not force the password to expire or allow the Proxy User to change passwords.
- ♦ You can limit the locations that the Proxy User can log in from by setting address restrictions for the Proxy User object.
- ♦ The Proxy User object must be created in eDirectory and assigned rights to the eDirectory objects you want to publish. The default user rights provide Read access to a limited set of objects and attributes. Assign the Proxy User Read and Search rights to all objects and attributes in each subtree where access is needed.
- ♦ The Proxy User object must be enabled on the General page of the LDAP Group object that configures LDAP Services for eDirectory. Because of this, there is only one Proxy User object for all servers in an LDAP group.
- ♦ You can grant a Proxy User object rights to All Properties (default) or Selected Properties. In order for contextless login or treeless login to work, the Read right must be granted so that LDAP can search the container or tree for the User object. Typically, you assign the Proxy user

rights to the root of the tree so that LDAP can view the attributes of the User objects throughout the tree. However, you might want to restrict access by assigning the Read right only to individual Organizational Units that you want LDAP to search.

For more information, see “Configuring LDAP Objects” (<http://www.novell.com/documentation/edir88/edir88/data/agq8auc.html#agq8auc>) in the *Novell eDirectory 8.8 Administration Guide*.

NOTE: LDAP Contextless Login requires clear text passwords to be enabled for LDAP. This does not affect the eDirectory password required during Login. They remain encrypted.

To give the Proxy User rights to only selected properties on eDirectory 8.7 or later, complete the following steps:


NOTE: LDAP Contextless Login works with eDirectory 8.5 or later. However, these steps apply specifically to eDirectory 8.7. If you are using a compatible version other than eDirectory 8.7, check the documentation that corresponds to your version for steps.

- 1 Launch iManager by entering the following in the *Address* field of a network browser:

```
http://server_IP_address/iManager.html
```

- 2 Log in using your username and password.

You have access only to those features you have rights to. To have full access to all Novell iManager features, you must log in as Supervisor/Administrator of the tree.

- 3 Make sure you are in the Roles and Tasks view by clicking  on the top button bar, then select *Rights > Modify Trustees* in the navigation panel on the left.
- 4 Specify the top container the Proxy User is to have rights over or click the *Browse* button to browse to the container in question, then click *OK*.
- 5 On the Modify Trustees page, click *Add Trustee*.
- 6 Browse to and click the Proxy User’s object, then click *OK*.
- 7 On the Modify Trustees page, click *Assigned Rights* for the Proxy User.
- 8 Select the *All Attributes Rights* and *Entry Rights* options, then click *Delete Property*.
- 9 Click *Add Property*, then select the *Show All Properties in Schema* option.
- 10 Select an inheritable right for the Proxy User, such as mailstop (in the lowercase section of the list) or Title, then click *OK*.
To add additional inheritable rights, repeat **Step 9** and **Step 10**.
- 11 Click *Done*.


To implement proxy user anonymous binds on eDirectory 8.7 or later, you must create the Proxy User object in eDirectory and assign the appropriate rights to that user. Assign the Proxy User Read and Browse rights to all objects and attributes in each subtree where access is needed. You also need to enable the Proxy User in LDAP Services for eDirectory by specifying the same proxy username.

- 1 Launch iManager by entering the following in the Address field of a network browser:

```
http://server_IP_address/iManager.html
```

- 2 Log in using your username and password.


You have access only to those features you have rights to. To have full access to all Novell iManager features, you must log in as Supervisor/Administrator of the tree.

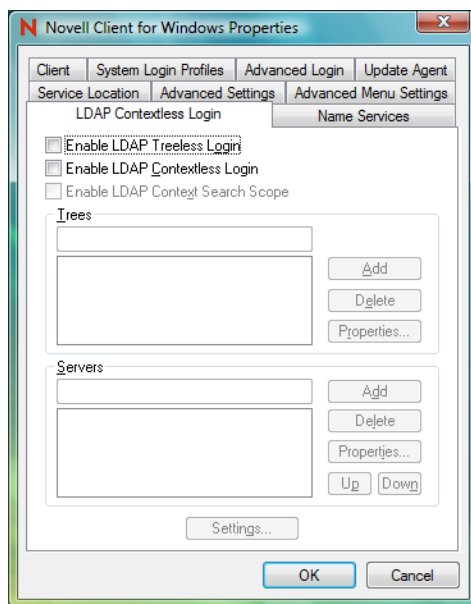
- 3 Make sure you are in the Roles and Tasks view by clicking  on the top button bar, then select *LDAP > LDAP Options* in the navigation panel on the left.
- 4 On the LDAP Options page, click the name of an LDAP Group object to configure.
- 5 In the Authentication Options area, type the name and context of an eDirectory User object in the *Proxy user* field.
- 6 Click *OK*.

8.7.2 Setting Up LDAP Contextless Login on One Workstation

After you have set up the LDAP Group object and assigned the correct rights to the User object that is associated with the proxy username, you need to set up LDAP Contextless Login on the workstations.

If you want to install on a few workstations, complete these steps. If you want to install on many workstations, see “[Setting Up LDAP Contextless Login on Multiple Workstations](#)” on page 96.

- 1 At the user’s workstation, right-click the Red N icon () in the notification area of the taskbar, then click *Novell Client Properties*.
- 2 Click the *LDAP Contextless Login* tab.



- 3 Do one of the following:
 - ♦ To enable treeless login, select *Enable LDAP Treeless Login*. The *Enable LDAP Contextless Login* is automatically selected for you because you must set up contextless login to enable treeless login.
 - ♦ To enable only LDAP contextless login, select *Enable LDAP Contextless Login*.
- 4 In the *Trees* field, specify the name of an eDirectory tree running LDAP services, then click *Add*.
- 5 In the *Servers* field, specify the IP address or DNS names of the server running LDAP services, then click *Add*.

Order is important for speed and efficiency because servers are queried for their tree until one is found that matches the tree specified by the user.

- 6** (Conditional) If this is the first time this server has been added to the list, check the server properties on the LDAP Server Properties page that appears to make sure that the timeout settings and data encryption settings are correct.

If you are using Secure Socket Layer (SSL) to establish a secure connection, you must specify the path and name of the certificate on the workstation. You should also check to make sure that the correct port number is specified.

- 7** (Conditional) If there are additional servers running LDAP, repeat **Step 5** and **Step 6** for each server.
- 8** (Optional) Start searching for users in a certain context.

8a Select *Enable Context Search Scope*.

8b Select the tree, then click *Properties*.

8c Do one of the following:

- ◆ To enable a search in the specified context and any containers in that context, select *Search Context and Subtree*.
- ◆ To enable a search in the specified context only, select *Search Context Only*.

8d Type the distinguished context delimited by commas (standard LDAP format), then click *Add*.

For example: OU=TOKYO,O=DIGITALAIRLINE

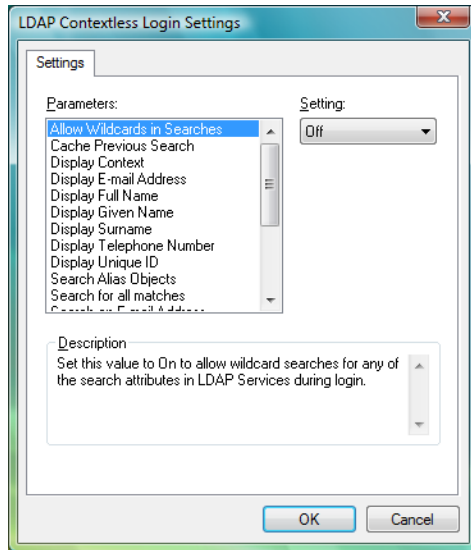
TIP: The LDAP property page does not ensure that this context is correct. If users have problems logging in, check that you typed this information correctly.

8e (Optional) Add multiple contexts to be searched by repeating **Step 8d** for each context.

The servers and contexts are searched in order. You can set the order they are searched by selecting a server or context, then clicking *Up* or *Down* to move its position in the search list.

- 9** Click *OK*.
- 10** (Optional) Specify additional eDirectory trees to use by repeating **Step 4** through **Step 9** for each tree.
- 11** (Optional) Set the optional search and display parameters that LDAP Contextless login uses to search the eDirectory tree for users by clicking *Settings*.

For example, because users do not need to specify their context, you might want to disable the Display Context parameter so that the context is not displayed during login.



Select the parameter you want, then use the *Setting* drop-down menu to turn the parameter On or Off. A short description of each parameter is available in the *Description* field when you select the parameter.

IMPORTANT: If you set the *Cache Previous Search* parameter to On, any wildcard searches you perform will conflict with this cache. For example, if you search for “mabels” and A.N is resolved as the context and then you search for “mabels” in a B.N context, mabels.B.N would never be resolved (even with wildcards) because mabels.A.N was resolved and cached first. You could clear the cache and allow mabels.B.N to resolve, but then mabels.A.N would not resolve.

The *Allow Wildcards in Searches* and *Cache Previous Search* parameters cannot be used together. If the *Allow Wildcards in Searches* parameter is On, the *Cache Previous Search* parameter is not used (even if you turn it On).

- 12 Click *OK* to make the changes and close the property page.

8.7.3 Setting Up LDAP Contextless Login on Multiple Workstations

As with all property page settings, you can set these properties for multiple workstations both before and after installation. For more information, see [Section 4.1, “Setting Properties During Installation,”](#) on page 39 and [Section 4.3, “Setting Properties on Multiple Workstations after Installation,”](#) on page 55.

8.7.4 Logging In Using LDAP Contextless Login

When users log in to the network using LDAP Contextless Login, they must specify the necessary information based on the options you specified in the [LDAP Contextless Login Settings](#) dialog box, the password, and the name of the tree running LDAP Services for eDirectory. The context information is added automatically to the Novell Login dialog box when the username is found.

If you choose to allow wildcard searches, users can perform a wildcard search and the LDAP database lists all possible users that meet the wildcard search criteria.

The Novell Client login dialog, on the *eDirectory* tab shown in the *Show Advanced Options* or *Advanced* section, will display status text to confirm whether the eDirectory tree name currently entered in the *Tree* field does or does not qualify as a tree for which LDAP Contextless Login will be attempted, based on the current LDAP Contextless Login configuration. This status text is only shown when the LDAP Contextless Login feature of the Novell Client has been enabled, either in a treeless or tree-specific mode.

8.7.5 LDAP Contextless Login Differences in the Novell Client for Windows Vista/2008

The LDAP Contextless Login feature in the Novell Client for Windows Vista/2008 includes the following limitations for those familiar with the Novell Client 4.x for Windows XP/2003.

- ♦ When invoking *Show Advanced Options* from the Novell credential provider (the login dialog box seen at boot time and when logging out of Windows Vista), the LDAP Contextless Login lookup cannot be triggered when viewing the *eDirectory* tab. If LDAP Contextless Login is enabled, a lookup is performed after the user attempts to log in to eDirectory from the credential provider.

This is different from the LDAP Contextless Login behavior when running `LOGINW32 . EXE` or selecting the *Novell Login* option from the Red N menu on the desktop. In those instances, you can see the effect of the LDAP Contextless Login lookup prior to actually proceeding with the eDirectory login.

- ♦ The options to search by attributes other than username (for example, phone number or e-mail address) have been disabled for the Novell Client for Windows Vista/2008 release.

8.8 Configuring 802.1X Authentication

The Novell Client 2 for Windows Vista/2008 includes an Extensible Authentication Protocol (EAP) plug-in to the Microsoft Windows Vista supplicant, which lets users authenticate through RADIUS to wireless access points and wired switches for added network security. Using FreeRADIUS as the RADIUS server, users can authenticate to their local machines, to eDirectory, and to 802.1X with the same set of credentials for a single sign-on experience.

When 802.1X authentication is enabled, the username and password entered in the Novell Login dialog box are first passed to the EAP plug-in module. An exchange of messages (PEAP/MSCHAPv2) between the Windows supplicant, the wireless access point/wired switch, and the RADIUS server allows network access if the correct credentials were entered. After the 802.1X authentication has succeeded, both the eDirectory and local logins take place just as they have in previous versions of the Novell Clients. If the 802.1X authentication fails, no access to the network is given, and the user will not be able to access the network.

The 802.1x authentication feature supports both wired and wireless connections. Only password-based authentication is supported (the Novell Client for Windows Vista/2008 supports only PEAP with MSCHAPv2). Biometrics (non password-based) authentication types are not supported with this release. If you want certificate support, the Microsoft EAP plug-ins are sufficient and no Novell-specific EAP support is required.

The ability to browse for trees and servers in the Novell Login dialog box is not supported because the 802.1X port blocks all network access.

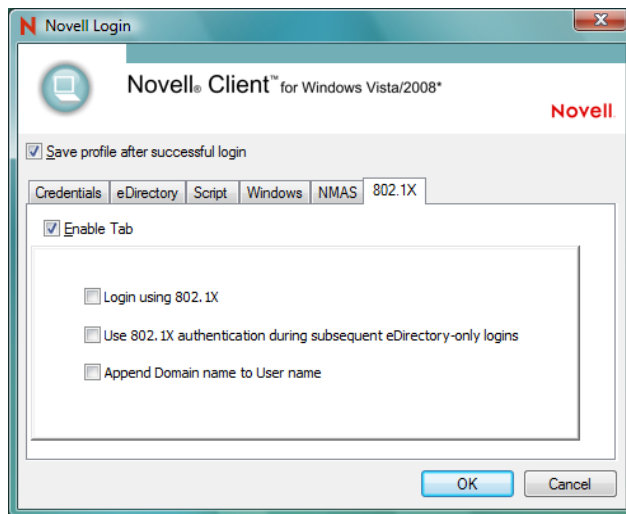
TIP: We recommend testing this functionality with user accounts that don't expire. There is a possibility that grace login messages won't display to users, which means that users might unknowingly exhaust their grace logins.

This configuration is intended for use only with the native 802.1x supplicant provided with Windows. We recommend that you install only the driver for your wireless adapter (that is, that you do not install other supplicants or utilities that come with wireless adapters). This is because such utilities often disable the wireless service in Windows. You should also make sure that the *Use Windows to configure your wireless network* setting is always enabled (to do this, right-click the wireless connection).

- ♦ [Section 8.8.1, “Enabling 802.1X Authentication,” on page 98](#)
- ♦ [Section 8.8.2, “Enabling Wired 802.1X Authentication on Windows Vista,” on page 99](#)

8.8.1 Enabling 802.1X Authentication

- 1 Right-click the Red N icon (N) in the notification area of the taskbar, then click *Novell Client Properties*.
- 2 In the Novell Client for Windows Properties dialog box, click the *System Login Profiles* tab.
- 3 Select *Default* in the *Location Profiles* box, then click *Properties*.
- 4 Select *Default* in the *Service Instance* drop-down list, then click *Properties*.
- 5 Click the *802.1X* tab, then select *Enable Tab*.



- 6 Select *Login using 802.1X*.

You can also select any of the following options:

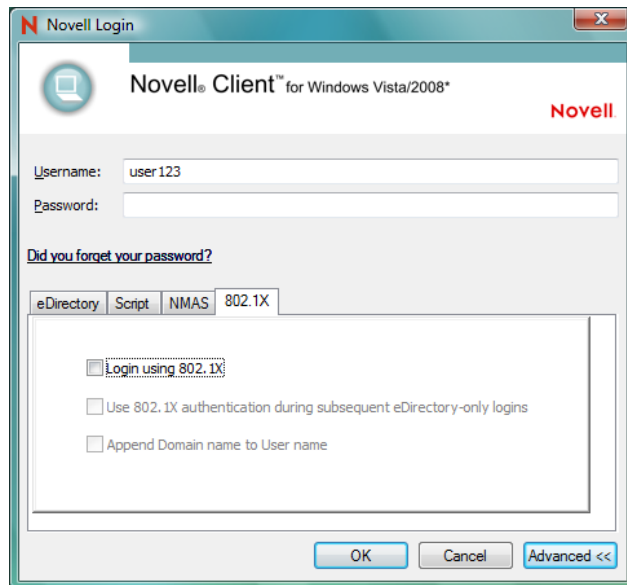
Use 802.1X authentication during subsequent eDirectory-only logins: Causes 802.1X authentication to take place when a user logs in from the Red N, even if he or she is already logged in to the Windows workstation. If the user is not logged in, 802.1X authentication takes place even if this option is not selected.

Append Domain name to User name: Prepends the user's domain to the username when the username is submitted to 802.1X. The format is DomainName/username. Use this option if the RADIUS server expects the domain name to precede the username. This options is normally used when IAS/AD is the RADIUS backend.

NOTE: Contextless login runs after you click *OK*.

- 7 Click *OK* three times.
- 8 Reboot the workstation for the changes to take effect.

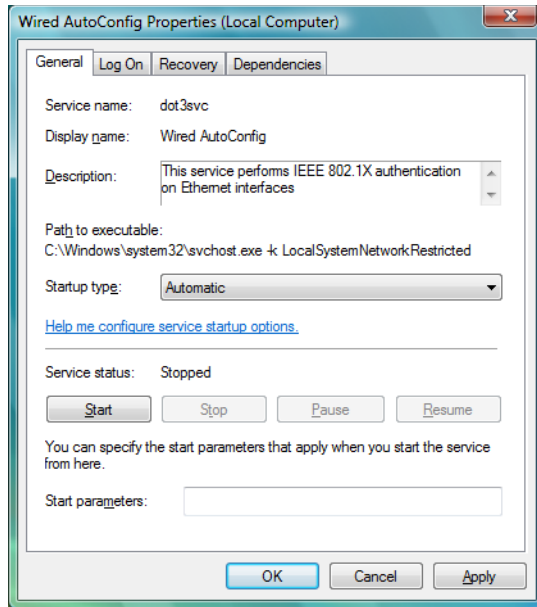
After it is enabled, an *802.1X* tab appears on the Novell Login dialog box when you click the *Advanced* tab. Use the options on the tab (see [Step 6](#)) to control 802.1X authentication at login time.



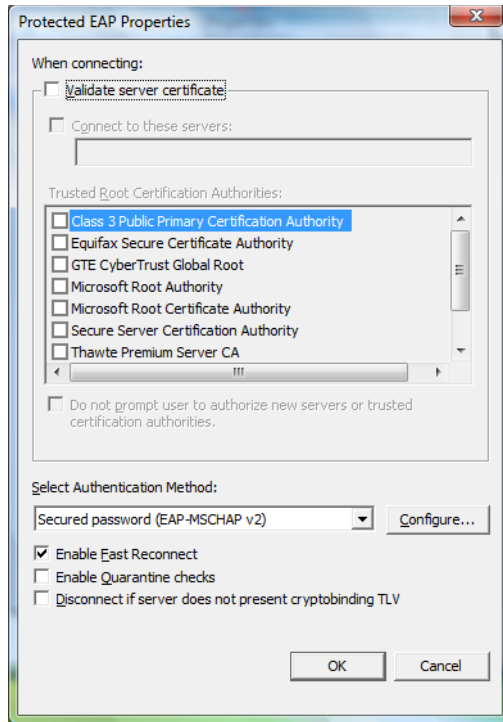
8.8.2 Enabling Wired 802.1X Authentication on Windows Vista

To enable wired 802.1x authentication on Windows Vista, perform the following procedure. You must be logged in as an administrator to perform these steps.

- 1 Click the *Start* button in the lower left corner of the Windows Vista desktop, then click *Control Panel*.
- 2 Click *System and Maintenance*, click *Administrative Tools*, then double-click *Services*.
- 3 In the list of services, double-click *Wired AutoConfig*.
- 4 From the *Startup type* drop-down list, select *Automatic*.



- 5 Click the *Start* button under *Service status*, then click *OK*.
- 6 Close the *Services* and *Administrative Tools* windows.
- 7 In the Windows Vista Control Panel, click *Network and Internet*, then click *Network and Sharing Center*.
- 8 Click *Manage network connections* in the left navigation panel.
- 9 Right-click your LAN connection, click *Properties*, and then click the *Authentication* tab.
- 10 From the *Choose a network authentication method* drop-down list, select *Protected EAP (PEAP)*, and then click *Settings*.
- 11 In the Protected EAP Properties dialog box, clear the *Validate server certificate* check box.



- 12 Click *OK* twice.
- 13 Close the Network Connections window.

8.9 Enabling AutoAdminLogon

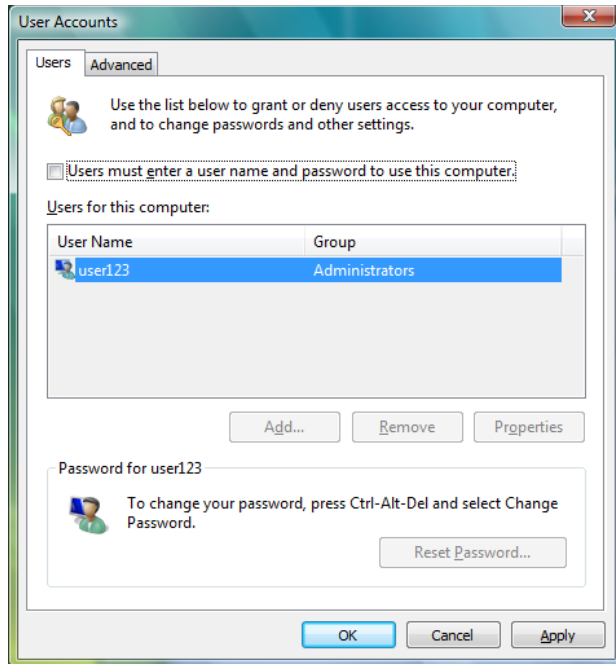
The AutoAdminLogon feature lets you log in to the desktop and eDirectory without being prompted to enter login credentials.

- ♦ [Section 8.9.1, “Enabling a Windows-Only Login,” on page 101](#)
- ♦ [Section 8.9.2, “Enabling an eDirectory AutoAdminLogon,” on page 102](#)

NOTE: With the initial release of the Novell Client for Windows Vista/2008, there is no way to perform only an eDirectory auto admin logon.

8.9.1 Enabling a Windows-Only Login

- 1 Click the Start button, then type `netplwiz.exe` (or `control.exe userpasswords2`) in the *Start Search* field.
- 2 Press Enter to open the User Accounts dialog box.
- 3 On the *Users* tabbed page, select the user that you want to enable AutoAdminLogon for in the *Users for this computer* list.
- 4 Deselect *Users must enter a user name and password to use this computer*.



- 5 Click *OK*.
- 6 When prompted, enter the password for the selected user, then click *OK*.
After the machine is rebooted, a Windows-only logon occurs for the specified user.

8.9.2 Enabling an eDirectory AutoAdminLogon

- 1 Click the *Start* button, then type `regedit.exe` in the *Start Search* field.
- 2 Press *Enter* to open the Registry Editor.
- 3 Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login`, then add the following:

Value Type=REG_SZ, Name=AutoAdminLogon, Data=1

Value Type=REG_SZ, Name=DefaultUserName, Data=eDirectory username

Value Type=REG_SZ, Name=DefaultLocationProfile, Data=profile to use (that is, Default)

Value Type=REG_SZ, Name=DefaultPassword, Data=the user's eDirectory password

NOTE: If the Windows password is the same as the eDirectory password, the last value is not necessary. In the future, a way to securely store the eDirectory password might be provided.

- 4 Close the Registry Editor.

8.10 Enabling TSClientAutoAdminLogon

Normally, without the Novell Client for Windows Vista/2008 installed, a terminal services client will pass a specific Windows account name, password, and domain name from the terminal client workstation to be used in establishing and logging on to Windows within the terminal session.

When the Novell Client for Windows Vista/2008 is installed, by default this behavior is unchanged. Correct Windows credentials passed from the terminal client workstation still result in a Windows-only account logon within the terminal session.

If the "TSClientAutoAdminLogon" policy is established, in addition to the the Windows account logon using these credentials provided from the terminal client, the Windows account username and Windows account password will "merged" with a specified Novell Client login profile, and will be attempted for eDirectory login in addition to the Windows account logon. Provided that the eDirectory user account name and password are already in sync with the Windows account username and password, this will result in a successful and transparent login to both eDirectory and Windows using the credentials provided from the terminal client workstation, where only a Windows account logon would have normally occurred.

NOTE: Although this behavior has greatest impact for Windows Server 2008 Terminal Services configurations, the TSClientAutoAdminLogon policy also has the same operational behavior for Remote Desktop usage on Windows Vista workstations. Normally Windows account credentials pre-supplied in the terminal client connection result in a Windows-only account logon via Remote Desktop. If the TSClientAutoAdminLogon policy is established on the Windows Vista workstation, the same Remote Desktop connection will attempt a transparent eDirectory and Windows account logon using the Windows account credentials provided from the terminal client workstation.

8.10.1 Enabling the TSClientAutoAdminLogon policy

- 1 Click the *Start* button, then type `regedit.exe` in the *Start Search* field.
- 2 Press Enter to open the Registry Editor.
- 3 Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login`, then add the following:

```
Value Type=REG_SZ, Name=TSClientAutoAdminLogon, Data=1  
Value Type=REG_SZ, Name=DefaultLoginProfile, Data=name of profile to use
```

Typically, the profile policy name is `Default`.
- 4 Close the Registry Editor.

Documentation Updates

A

The *Novell® Client™ 2 for Windows Vista/2008 Administration Guide* has been updated since the initial product release as shown below.

April 14, 2009

Section	Change
Section 2.2, “Understanding the Novell Client Install Manager (nciman.exe),” on page 21	Replaced an invalid forward slash (/) with a dash (-) in the Vista-2008 directory name examples.
Section 3.3, “Logging in When eDirectory and Windows Credentials Are Not Synchronized,” on page 35	Removed a typo from the title of Figure 3-8.
Section 4.2.1, “Client Settings,” on page 41	Removed information about options that are no longer part of this tab.
Section 4.2.3, “Advanced Login Settings,” on page 43	Corrected a minor typo.
Section 4.2.7, “Advanced Menu Settings,” on page 50	Adjusted alphabetical order of list items.
Section 8.6.2, “Creating a System Login Profile for Use on Multiple Workstations,” on page 85	Replaced an invalid forward slash (/) with a dash (-) in the Vista-2008 directory name examples.

