Client for Open Enterprise Server
Administration Guide

Legal Notices

Contents

About This Guide

This guide describes how to configure the Client for Open Enterprise Server and contains the following sections:

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 and enter your comments there.

Documentation Updates

For the latest version of this documentation, see the Client for Open Enterprise Server Web site.

Additional Documentation

For information on installing the Client for Open Enterprise Server, see the *Client for Open Enterprise Server Installation Quick Start*.

For information on using the Client for Open Enterprise Server, see the *Client for Open Enterprise Server Installation Quick Start*.

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

1 Overview of the Client for Open Enterprise Server

The Client for Open Enterprise Server provides Windows connectivity to NetWare and OES Linux servers. With the Client for Open Enterprise Server, you can browse through authorized directories, transfer files, and use advanced services directly from Windows 11, Windows 10, Windows 8, or Windows 7 workstations, Windows 2012 server, Windows 2016 server, Windows 2019 server or a Windows 2022 server.

After it is installed on workstations, the Client for Open Enterprise Server lets users enjoy the full range of OES services, including authentication via NetIQ 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 traditional NCP protocol.

The Client for Open Enterprise Server for Windows is a separate release from the Novell Client 4.91 for Windows XP/2003. The Client for Open Enterprise Server for Windows supports both the x86 and x64 versions of Windows 11, Windows 10, Windows 8, and Windows 7 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.

In this guide, the Client for Open Enterprise Server is referred to as the Client.

This section contains the following information:

1.1 Features and Benefits

- Support for accessing NCP volumes that are greater than 16 TB. For more information, see in the Support for Volumes Greater than 16 TB in the OES 2015: NCP Server for Linux Administration Guide.
- Support for Open Enterprise Server (OES) 2018, 2015, OES 11, OES 2, and NetWare 6.5
- File system integration with NSS and non-NSS volumes via NCP
- Login script processing
- Notification area (Client System Tray Icon) options

  Many of the Client for Open Enterprise Server features are available when you right-click the ⬜ icon in the notification area of the taskbar, located in the bottom right portion of your screen. For more information, see "Using the Client for Open Enterprise Server" in the *Client for Open Enterprise Server User Guide*.

- Integrated login with Windows (single username and password)

  The Client for Open Enterprise Server for Windows provides a single, synchronized login to the Windows desktop and the 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 96.

- 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 8.8, "Setting Up LDAP Contextless Login and LDAP Treeless Login," on page 124 and Section 1.3.3, "LDAP Contextless Login Differences," on page 18.

- DFS junctions

- Support for 802.1x wireless authentication

  See Section 8.9, "Configuring 802.1X Authentication," on page 132 for more information.

- DHCP-based configuration options

  The Client is able to use DHCP-supplied configuration values for the 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 *Client for Open Enterprise Server User Guide*.

  In addition, the OpenSLP support in the Client for Open Enterprise Server 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 1.3.2, "Service Location Protocol (SLP) Differences," on page 16.

- Shell extensions for Windows' file browser

- File caching/shared open mode support

- Auto-reconnect for NCP connections

- Cluster failover support for NCP connections

- Client for Open Enterprise Server settings management and install-time pre-configuration

1.2 Rebranding Changes

Novell is now part of Micro Focus. Products across the portfolio are now being rebranded to reflect Micro Focus or a more appropriate name. This corporate change impacts the name of products and components, user interfaces, logos, and so on. As a result of this corporate change, the new name for `Novell Client` is `Client for Open Enterprise Server`.

The documentation update to reflect these changes (such as names and screenshots) is being done in a phased manner.Until all the guides in the documentation library are modified, Novell Client and Client for Open Enterprise Server are used interchangeably.

The screenshot provides an overview of the change to the user interfaces, logos, and so on. However, all the client functionality remains the same.

Figure 1-1 *Overview of Client for Open Enterprise Server*

The following is a list of changes in the "Client for Open Enterprise Server 2 SP4 (IR3)" and later, as compared to the "Novell Client 2 SP4 for Windows (IR2)" and all previous releases:

◆ In "Novell Client for Windows", when the downloaded file was unzipped, by default all files were extracted to a "C:\Novell" directory such as "C:\Novell\Novell Client 2 SP4 for Windows (IR2)". In "Client for Open Enterprise Server", when the downloaded file is unzipped, by default all files are extracted to a "C:\Micro Focus" directory such as "C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)".

◆ In "Novell Client for Windows", the menu in the Windows taskbar notification area to perform client services such as login, map a drive, etc., was displayed using the Novell "red 'N' icon". In "Client for Open Enterprise Server", this is replaced with the Micro Focus icon and is referred to as the "Client System Tray icon" in documentation."
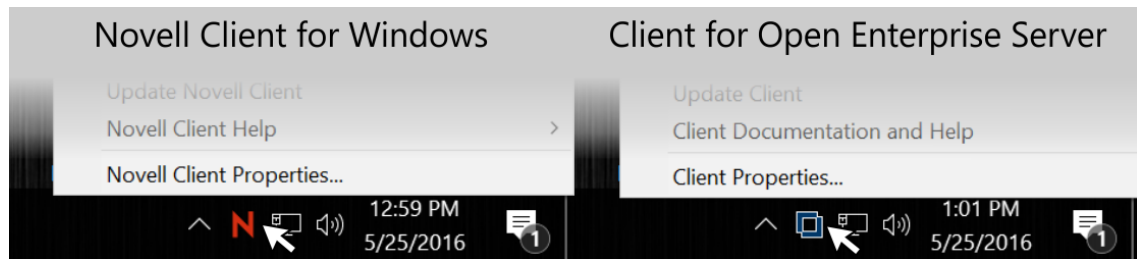
◆ In "Novell Client for Windows", to uninstall the client using the Windows control panel or "Settings" application, the entry name "Novell Client for Windows" was looked for. In "Client for Open Enterprise Server", look for the entry name "Client for Open Enterprise Server".

◆ In "Client for Open Enterprise Server", all the previous Novell bitmaps and images are replaced with "Micro Focus" branded bitmaps and images.

◆ In "Client for Open Enterprise Server", some of the menu items and setting names are changed, but the functionality still remains the same. The following in the list of items that are changed from "Novell Client for Windows" to "Client for Open Enterprise Server".

Novell Client for Windows	Client for Open Enterprise Server
Novell Client	Client for Open Enterprise Server
Novell Login	OES Login
Novell Connections	OES Connections
Novell Map Network Drive	OES Map Network Drive
Novell Utilities	OES Utilities
Update Novell Client	Update Client
Novell Client Properties	Client Properties
Novell Copy	OES Copy
Netware Copy	OES Copy
Novell Info	OES Info
Novell Rights	OES Rights
Novell Volume Statistics	OES Volume Statistics
Novell Volume Information	OES Volume Information
Novell File Copy Utility	Client File Copy Utility
NDS objects	eDirectory objects

In Client Properties:

Novell Client for Windows	Client for Open Enterprise Server
Allow Dot in Novell Username	Allow Dot in Network Username
Novell Logon	Client Logon
Default Bitmap for Novell Login Dialog	Default Bitmap for Novell Login Dialog
Login with Non-Novell Credential Provider	Login with Third-Party Credential Provider
Prompt for Novell Login during Windows AutoAdminLogon	Prompt for Network Login during Windows AutoAdminLogon
Display Novell Information Page	Display OES Information Page
Display Novell Rights Page	Display OES Rights Page
Display Volume Information Page	Display OES Volume Information Page
Display Volume Statistics Page	Display OES Volume Statistics Page
Enable Novell Client Help	Enable Client Help
Enable Novell Client Properties	Enable Client Properties
Enable Novell Connections Dialog	Enable OES Connections Dialog
Enable Novell Copy Dialog	Enable OES Copy Dialog
Enable Novell Utilities	Enable OES Utilities
Show Novell System Tray Icon	Show Client System Tray Icon
Latest Novell Client Properties File	Latest Client Properties File
Computer Only Logon after failed Novell Logon	Computer Only Logon after failed Network Logon

In Client Credential Provider:

Novell Client for Windows	Client for Open Enterprise Server
Logon to Novell Network	Logon to OES Network
Novell Password	Network Password
Novell Logon	Network Logon
"Novell Logon" tile is the name of the blank "enter a different username to logon" tile.	"Other User" tile is the name of the blank "enter a different username to logon" tile.
Change your Windows Password to match your Novell Password after a successful login.	Change your Windows Password to match your Network Password after a successful login.

◆ Note there are many file names, Program Files directory names, and registry keys in Client for Open Enterprise Server that continue to reflect the "Novell" or "Novell Client" branding. The goal was to not make changes that would affect application-level compatibility or existing customer-defined scripts that were working with the previous Novell Client for Windows. Any

customer scripts or applications that are dependent on the existing file names, directory names or registry setting names used in the Novell Client for Windows continues to work successfully with the Client for Open Enterprise Server.

1.3 How the Client for Open Enterprise Server Differs from the Novell Client for Windows XP/2003

Using the Client for Open Enterprise Server 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 10, Windows 8, and Windows 7 run more smoothly.

- Section 1.3.1, "Novell Client for Windows XP/2003 Features Not Included in the Client for Open Enterprise Server," on page 15
- Section 1.3.2, "Service Location Protocol (SLP) Differences," on page 16
- Section 1.3.3, "LDAP Contextless Login Differences," on page 18

1.3.1 Novell Client for Windows XP/2003 Features Not Included in the Client for Open Enterprise Server

The following Novell Client for Windows XP/2003 features are not included in the Client for Open Enterprise Server:

- Compatibility with any version of Windows other than Windows 10, Windows 8, Windows 7, Windows Server 2012 or Windows Server 2008 R2.

  The Novell Client 4.91 for Windows continues to support Windows XP and 2003.
- Compatibility to NetWare 5.0 and all prior versions.
- Graphical Login at Windows boot.

  There is no direct concept of this in Windows 10, Windows 8, and Windows 7, 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/en-us/magazine/cc163489.aspx) and Chapter 3, "Authenticating to a OES Network," on page 45.
- 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).

1.3.2 Service Location Protocol (SLP) Differences

The Client for Open Enterprise Server 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 describe some of the significant known differences between the two SLP User Agents.

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 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 Novell Client is unable to communicate with OpenSLP Directory Agent over SLPv2 (http://www.novell.com/support/kb/doc.php?id=7000053), the SRVLOC UA allows setting a "Use SingleEquals in Where (V2)" policy to cause a single equals character to be used in predicate strings.

- DHCP-based SLP configuration information is retrieved by the SRVLOC UA through the Client NWDHCP.SYS driver. DHCP-based SLP configuration can be successfully retrieved even when the Windows network adapter is not using DHCP for its IPv4 address configuration, and instead has a static IPv4 address assignment.

Client for Open Enterprise Server OpenSLP LIBSLP User Agent

By default, the following behaviors occur with the OpenSLP LIBSLP User Agent (UA) used in the Client for Open Enterprise Server:

- 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 muticast-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.

- As of Novell Client 2 SP2 (IR4) and later, the Client includes an SLPINFO.EXE tool for displaying the workstation discovered SLP Directory Agents and SLP Scopes. Differences in the underlying OpenSLP LIBSLP User Agent implementation prevent the diagnostic information from being as granular as the Novell Client for Windows XP/2003 SRVLOC User Agent.

- 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 Client for Open Enterprise Server) does not yet provide a solution for the issue of using a single equals character in a predicate string.

- DHCP-based SLP configuration information is retrieved by the OpenSLP UA through the Microsoft DHCP Client Service included with the Windows operating system. The Microsoft DHCP Client Service only supports retrieving DHCP-based configuration information when the Windows network adapter itself is configured to acquire IPv4 address information via DHCP. If the Windows network adapter is configured with a static IPv4 address, the SLP DA and/or SLP scope list will need to be manually configured on the machine, as the it will not retrieve SLP configuration information via DHCP. Or the machine will need to successfully learn SLP DA and scopes via multicast every time the machine boots. For more information, see Novell Client 2 does not retrieve SLP information when using static IPv4 address.

1.3.3   LDAP Contextless Login Differences

The LDAP Contextless Login feature in the Client for Open Enterprise Server 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 Client for Open Enterprise Server release.

1.4   Features Not Included in the Client for Open Enterprise Server

The following features are not included:

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

2 Advanced Installation Options

This section explains some advanced installation options and procedures. For information on installing the Client on a single workstation, see the "Client for Open Enterprise Server Installation Quick Start."

2.1 Understanding the Basic Client Installation (setup.exe)

To install the Client software, use `setup.exe`, located in the `C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)` directory (created when you unzipped the Client downloaded file).

Figure 2-1 Express Client Installation
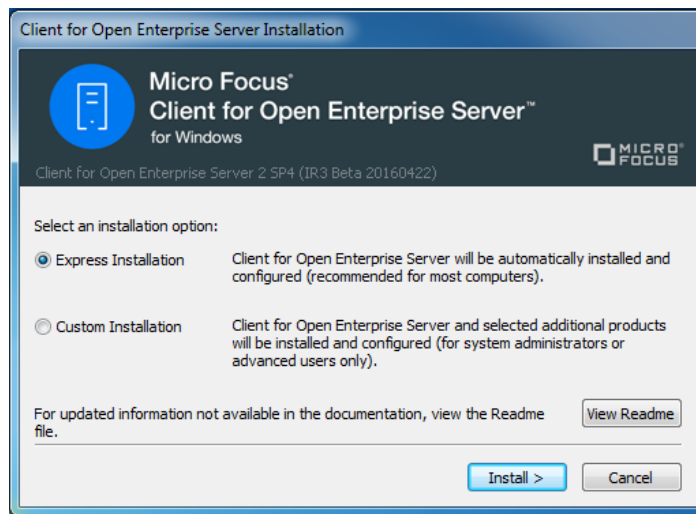
The Client Express Installation automatically installs and configures the Client for Open Enterprise Server. The Custom Installation lets you choose whether or not to install the following when you install the Client:

- Novell Modular Authentication Services (NMAS)

- Novell International Cryptographic Infrastructure (NICI)
- Advanced Authentication Client
- Advanced Authentication Device Services

Along with the preceded components, the Client for Open Enterprise Server installs the Microsoft Visual C++ 2010 Redistributable Package by default. If NMAS and NICI are chosen to install when you install the Client for Open Enterprise Server 2 SP4 (IR9) or later, then the Microsoft Visual C++ 2012 Redistributable Package is also installed.

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

Table 2-1 *Setup.exe Switches*

Switch	Description
/ACU	Directs `setup.exe` to perform an upgrade of the currently installed Client software if the version to be installed is a later one.
/NCPF	Applies the Client property page settings specified in the default `NovellClientProperties.txt` file. Use the Client Install Manager (`nciman.exe`) to create this file. See "Creating the Client Properties File" on page 24 for more information.
/NCPF:*filename*	Applies the Client property page settings specified in *filename*. Use the Client Install Manager (`nciman.exe`) to create this file. See "Creating the Client Properties File" on page 24 for more information.

/ACU and /NCPF can be specified together at the command line. For more information, see "Using Optional Parameters to Install the Client " in the *Client for Open Enterprise Server Quick Start*.

2.1.1   Selecting a Language

The Client 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 Client.

Figure 2-2 *Language Selection Dialog Box*
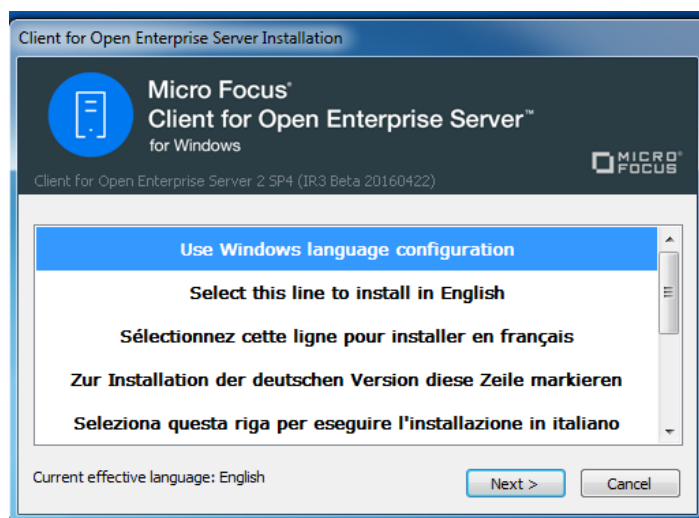
This section contains information on how this dialog box operates, using single language and multiple language versions of Windows 10, Windows 8, and Windows 7, and the languages that are available for selection.

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 other available languages which Client for OES supports (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 Client to try and match the language the Windows 10, Windows 8, or Windows 7 user interface is using. The Client consults the Windows Multilingual User Interface (MUI) configuration and determines if any of the Client for OES languages match the current MUI preferred or fallback languages.

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

Using Single-Language Versions of Windows 10, Windows 8, and Windows 7

On single-language versions of Windows 10, Windows 8, and Windows 7, selecting the **Use Windows language configuration** option is no different than selecting a specific Client's supported language. For example, if you are running the German version of the Windows 7 Professional 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 Client for OES installation and the installed version of the Client.

Using Multiple-Language Versions of Windows10, Windows 8, and Windows 7

On multiple-language versions of Windows 10, Windows 8, and Windows 7, such as the Windows 7 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 7 Control Panel).

If **Use Windows language configuration** is selected during the Client installation, the current Windows MUI language configuration is consulted each time the 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 Client re-evaluates the current Windows MUI language selections and determine which of the available Client languages best matches the new and current MUI language.

Available Language Selections

In the Client language selection dialog box, you might notice that not all of the available Client 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 Client are not yet completely based on Unicode. Until all of the major and required Client 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*
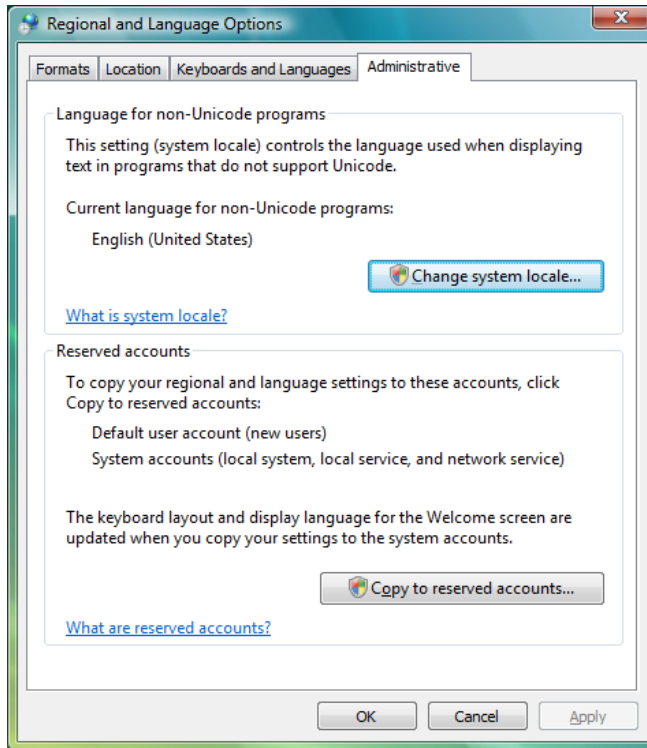
In general, this means that users of the English, French, German, Italian, Portuguese, and Spanish versions of Windows 10, Windows 8, and Windows 7 can select any one of these languages for the Client language. This is because all of these languages share the same ANSI code page and can successfully render all the other offered languages. Users of the Japanese, Polish, and Russian versions of Windows 7 and 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 Client language selection dialog box still only offers English and Russian as options. This is because the Client 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 **Language for non-Unicode programs** option can be changed to a different language, which then affects which languages the Client installation can offer for selection. This is a system-wide setting that affects all non-Unicode applications and not just the Client.

2.2 Understanding the Client Install Manager (nciman.exe)

The Client Install Manager (`nciman.exe`) lets you generate a properties file, used by the Client install utility (`setup.exe` or `acu.exe`), to configures the 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 Client Properties File" on page 24.

The Client Install Manager is located in `C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)\Admin` (created when you unzipped the Client download file).

The Client Properties file must be copied to the root directory of the Client build (`C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)`) before installation. `NovellClientProperties.txt` is the default filename, but you can save a properties file with any name you want.

Figure 2-4 *Client Install Manager*
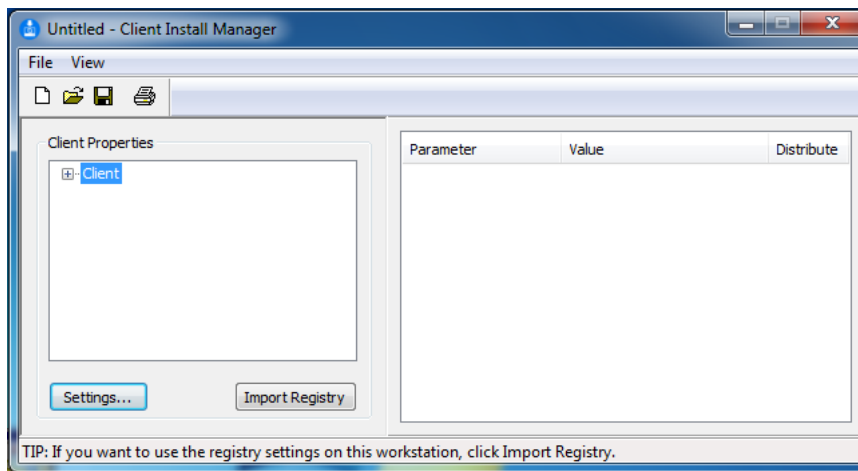
2.2.1 Creating the Client Properties File

The Client installation (`setup.exe` and `acu.exe`) applies a properties file generated by the Client Install Manager in order to configure 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 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 65.

1 Start the Client Install Manager (`nciman.exe`), located in the `C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)\Admin` folder.

2 Double-click **Client** to open the Properties dialog box
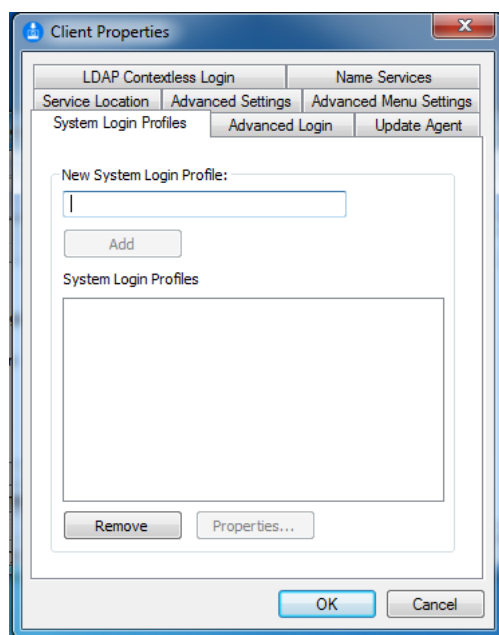
3 Modify the Client properties as needed.

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 65.

4 Click **File > Save**, then specify a name for the 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:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)`).

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 Client properties file. All you need to do is open the `install.ini` file, located in the root directory of the Client build (`C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)`), 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 (setup.exe).	DisplayLanguageSelection=
		DefaultLanguageSelection=
		DisplayLicenseAgreement=
		DisplayInitialDialog=
		DisplayBackground=
		CreateSystemRestorePoint=
		InstallNMAS=
		InstallNICI=
		ForceReboot=
		DisplayRebootDialog=
		LocalDirectory=
		InstallAdvancedAuthentication=
		InstallAdvancedAuthenticationDeviceServices=
		AdvancedAuthenticationClientDiscoveryHost=
		AdvancedAuthenticationClientEventName=
[ACU]	Specifies settings that apply only to the Automatic Client Upgrade utility (acu.exe).	DisplayUpgradeDialog=
		Message=
	.	
[UpdateAgent]	Specifies settings that apply only to the Client Update Agent utility (cuagent.exe).	Disabled=
		DisplayUpdateDialog=
		DisplayUpdateLocation=
	.	Message=

NOTE: The .INI file parsing performed by Microsoft on the Windows platform does not support duplicate section names, nor does it support duplicate setting names within a section. Only the first section found with a given name will be used, and only the first instance of a setting name within that section will be recognized.

Meaning the settings presented in the INSTALL.INI will need to be modified within the existing sections, as they were distributed in the INSTALL.INI. Moving or duplicating the settings to another area of the file will not result in the intended processing.

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 Client Install Manager (`nciman.exe`). For more information, see "Creating the Client Properties File" on page 24.

IMPORTANT: If you use a Client properties file to configure the 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 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 Client Update Agent

You can simplify future client software upgrades by enabling the Client Update Agent. The Update Agent can be run manually at any time from the Client Tray Application ▢(see "Updating the Client for Open Enterprise Server" in the *Client for Open Enterprise Server User 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 Client Property Pages.

---

1 Create a Client properties file by running the Client Install Manager utility (`nciman.exe`).

   See "Creating the Client Properties File" on page 24.

2 Double-click **Client**, then click the **Update Agent** tab.
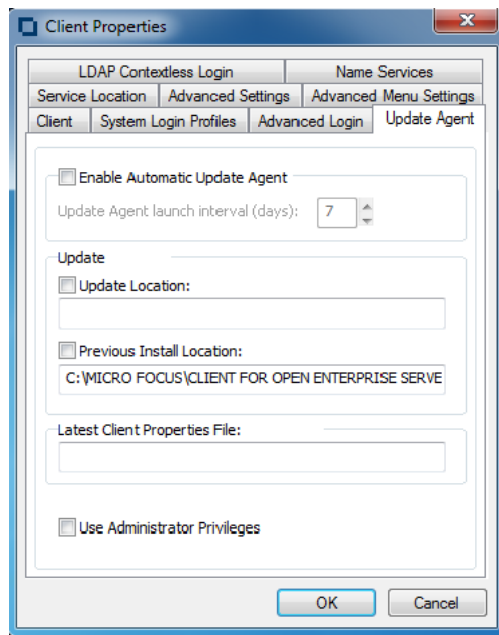
3 (Optional) Select the **Enable Automatic Update Agent** option and specify the launch interval.

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 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 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 Client Using Login Scripts" on page 29. For more information on using ZENworks, see the documentation associated with the installed version of ZENworks.

- Section 2.5.1, "Distributing the Client Using Login Scripts," on page 29
- Section 2.5.2, "Sample Client Installation Login Script," on page 29

2.5.1 Distributing the 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 29.

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 7 *****
IF OS = "WINNT" AND OS_VERSION = "V6.00"
   WRITE "Updating Novell Client for Windows."
   #\\server1\sys\public\client\acu.exe
   IF "%ERROR_LEVEL" = "1" THEN
       EXIT
   END
END
```

2.6 Signing Requirements for the Client Installation

 ◆ Section 2.6.1, "Signing Requirements on Windows 10 Platforms," on page 30
 ◆ Section 2.6.2, "Pre-distributing a Trusted Publisher Certificate for the Client Installation," on page 30
 ◆ Section 2.6.3, "Expiration of the Micro Focus Certificate," on page 31
 ◆ Section 2.6.4, "Effects of the Micro Focus Certificate Expiration," on page 32

2.6.1 Signing Requirements on Windows 10 Platforms

Starting with the Client for Open Enterprise Server 2 SP4 (IR4) and later, on Windows 10 platforms the Client has been signed using a Microsoft certificate instead of a Micro Focus certificate. This Microsoft signature is only valid for Windows 10 platforms, which includes the Windows Server 2016 and Windows Server 2019 platforms.

For these Windows 10 platforms, there will not be any Micro Focus publisher verification prompt presented by Windows during installation of the Client driver software. This is because Windows already considers the Microsoft signature to be part of the **Trusted Publishers** on a Windows machine.

Therefore, it is neither possible nor necessary to import or pre-distribute the Micro Focus certificate as a **Trusted Publishers** certificate on Windows 10 platforms. Windows does not evaluate the Micro Focus certificate during driver installation, nor does Windows present the **Always trust software from Micro Focus** option during installation on these Windows 10 platforms.

For Windows 10 platforms, all discussion of importing or pre-installing the Micro Focus certificate as a **Trusted Publishers** certificate can be ignored. The Microsoft certificate needed to pre-approve installation as a Trusted Publisher is already part of the Windows installation.

For all Windows 8.1 and earlier platforms, including Windows Server 2012 R2 and earlier, the Client remains signed with a Micro Focus certificate. For these Windows 8.1 and earlier platforms, Windows will prompt for publisher verification, and will present the **Always trust software from Micro Focus** option during installation.

Therefore, the remaining sections in this documentation which describe how to import and pre-distribute the Micro Focus certificate only apply to these Windows 8.1 and earlier platforms.

2.6.2 Pre-distributing a Trusted Publisher Certificate for the Client Installation

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

An **Always trust software from Micro Focus** option is also available. If you select this option, Windows adds the Micro Focus 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 Micro Focus certificate, Windows proceeds with installation rather than prompting you again for confirmation.

If you want to prevent Windows from presenting this publisher approval prompt as part of the Client installation, you can pre-distribute the Micro Focus certificate used to sign the Client installation set. Pre-distributing and pre-importing this Micro Focus certificate into the Windows machines' **Trusted Publishers** certificate list will prevent Windows from prompting for verification during installation of any driver software signed with this certificate.

NOTE: Pre-distributing the Micro Focus certificate as a Trusted Publishers certificate on the workstation only eliminates the Microsoft publisher verification prompt that Windows presents during Client for Open Enterprise Server installation. To eliminate other confirmation prompts presented by the Client installation program, see the INSTALL.INI settings in Section 2.3, "Using the Install.ini File," on page 25. Configuring the INSTALL.INI settings is required for an installation to be initiated without any prompts through Client Update Agent or another software distribution mechanism like Novell ZENworks Configuration Management.

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

NOTE: The exact name on the Micro Focus certificate may be "Micro Focus International plc" or may be "Micro Focus (US), Inc", depending upon which release of the Client software is being installed. Whichever one of these is correct for the version of the Client being installed, this is the certificate being referred to in documentation as "the Micro Focus certificate."

The exported certificate can be used to pre-distribute Micro Focus certificate 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* (Authenticode.doc, http://www.microsoft.com/whdc/driver/install/authenticode.mspx), and the Microsoft Windows Group Policy documentation.

2.6.3 Expiration of the Micro Focus Certificate

Certificates have a start date and an expiration date, and the certificate a software publisher uses to digitally sign their release will eventually change as the current certificate reaches expiration and a new certificate is obtained.

For example, the Micro Focus certificate used to sign the Client for Open Enterprise Server 2 SP4 (IR9) release was valid from March 2016 to August 2018, so pre-distributing this certificate will work for automatically approving any of the Novell Client software releases that occurred in this time period.

The next Client for Open Enterprise Server releases after August 2018, such as the Client for Open Enterprise Server 2 SP5, were signed with a new Micro Focus certificate which is valid from July 2018 to July 2021. Because this is a different certificate than the releases prior to August 2018, the

certificate installed as a **Trusted Publishers** certificate for the previous releases does not continue to work for suppressing the Windows publisher approval prompt when installing releases after August 2018.

Customers who want to pre-distribute the Micro Focus certificate necessary to install Client releases that occurred during the time period of August 2018 to July 2021 must obtain the updated certificate from one of the post August 2018 releases, and then distribute this updated Micro Focus certificate as a Trusted Publisher on the workstations. Each time the certificate expires and is replaced with a new certificate in future releases, the certificate pre-installed on the workstations must be updated.

2.6.4 Effects of the Micro Focus Certificate Expiration

Expiration of the Micro Focus certificate does not mean that the Client for Open Enterprise Server will cease functioning, nor does it mean that installation of the Client for Open Enterprise Server will fail. When the existing Micro Focus certificate expires, workstations where this Micro Focus certificate was pre-distributed as a **Trusted Publishers** certificate will no longer be able to automatically approve the publisher verification prompt Windows presents during installation of future Client software.

However, Client software that was signed using a Micro Focus certificate which expired in August 2018 can continue being successfully installed and used even after August 2018. This is an intentional aspect of the Microsoft Authenticode signing behavior, which permits a signed file to also be given an independent time stamp signature. The time stamp signature allows Windows to validate that the signing certificate was valid at the time the files were signed, even if the signing certificate has subsequently expired.

Expiration of the Micro Focus certificate does not mean that the Client for Open Enterprise Server will cease functioning, nor does it mean that installation of the Client for Open Enterprise Server will fail after the expiration date. It also does not mean that the expired Micro Focus certificate should necessarily be removed from the **Trusted Publishers** store on the workstation.

Expiration of the existing Micro Focus certificate simply means that no future releases of the Client software will be signed with this same certificate. The next Client release after the expiration date will be signed with a different Micro Focus certificate, with a new start date and a new expiration date.

Windows continues to consider the expired Micro Focus certificate as valid. That is, Windows will continue being able to successfully verify software that had been signed with this certificate during the time period when the certificate was not yet expired.

For example, the Client for Open Enterprise Server 2 SP4 (IR9) release which was signed with the Micro Focus certificate valid from March 2016 to August 2018, Windows will continue verifying and allowing this software to install and run even after August 2018.

This also means that if you have the Micro Focus certificate valid from March 2016 to August 2018 installed as a **Trusted Publishers** certificate on the workstation, this certificate need to remain in the **Trusted Publishers** certificate store even after August 2018, to permit Windows to continue pre-approving the trusted publisher prompt that will occur when installing Client for Open Enterprise Server 2 SP4 (IR9) or any previous releases that were signed with this certificate; even though this certificate is now expired.

Having only the latest Micro Focus certificate installed in the **Trusted Publishers** certificate store does not guarantee pre-approval of the publisher verification prompt that Windows presents during Client for Open Enterprise Server installation. More specifically, you must install the certificate that was used to sign the particular release of the Client being installed.

This might be the latest Micro Focus certificate, or it might be a previous Micro Focus certificate which is now expired, depending upon when the particular Client release was made. Windows supports importing or maintaining multiple versions of the Micro Focus certificate (both expired and non-expired) concurrently, as needed to have the certificate necessary for the version(s) of Client being installed.

2.6.5 Importing the Micro Focus Certificate as a Trusted Publisher on a Single Machine

As described earlier, the easiest method for installing the Micro Focus certificate used to sign a particular Client release as a **Trusted Publishers** certificate for Windows is to use the **Always trust software from Micro Focus** option presented on the Windows publisher verification dialog during driver installation.

Should you want to import the Micro Focus certificate onto a single machine using the Microsoft Certificate Management Console (certmgr.msc), an important aspect will be to import the Micro Focus certificate into the **Trusted Publishers** certificate list that will be available to the Windows machine during driver installation, as opposed to the per-user **Trusted Publishers** certificate list that is specific to the current logged-on user.

For example, on Windows 7 the following steps can be used to import the certificate as a **Trusted Publishers** certificate available to the Windows driver installation process, such that a publisher verification dialog would not be presented when installing the Client:

1 Run CERTMGR.MSC (normally; do not have to force elevation via "Run as Administrator").

2 From the View menu, select Options and enable "Physical certificate stores".

3 Expand "Trusted Publishers" and select/highlight the "Local Computer" store.

4 Right-click on the "Local Computer" store, and from "All Tasks" choose "Import".

5 Browse to the Micro Focus certificate which had been exported from a different Windows machine, and on the "Certificate Store" page of the import wizard, ensure "Trusted Publishers\Local Computer" is selected.

6 Complete the Import wizard, and ensure the Micro Focus certificate shows under "Trusted Publishers\Local Computer" in the CERTMGR.MSC console.

   The selection of the Local Computer certificate store during the certificate import process is what ensures the Micro Focus certificate is being imported in a way that will be available as a **Trusted Publisher** to the Windows driver installation process. This is exactly what happens automatically when using the **Always trust software from Micro Focus** option during an interactive Client installation.

For additional information on the Trusted Publishers certificate store and the Local Computer certificate store, see Trusted Publishers Certificate Store and Local Computer and Current User Certificate Stores.

2.6.6 Requirement of SHA-2 Certificates for Client for Open Enterprise Server

Client for Open Enterprise Sever 2 SP4 (IR3) and later is signed using a new Micro Focus SHA-2 certificate, due to Windows' deprecation of SHA-1 certificates.

For successful installation of Client on Windows 7 and Windows Server 2008 R2, ensure to install the Microsoft Security Update KB3033929 to add support for SHA-2 certification.

2.7 Installing and Configuring Advanced Authentication Client

Client for open Enterprise Server supports Advanced Authentication to log in to Windows and eDirectory. If you want to use Advanced Authentication for log in, you must download the Advanced Authentication product and install it along with Client for Open Enterprise Server. If you are already using Advanced Authentication for Windows logon and now want to extend its functionality to Client for Open Enterprise Server, you can do so by enabling Advanced Authentication integration functionality when installing Client for Open Enterprise Server.

- Section 2.7.1, "Installing Advanced Authentication Client with Client for Open Enterprise Server," on page 34
- Section 2.7.2, "Enabling Advanced Authentication Integration Functionality," on page 35
- Section 2.7.3, "Advanced Authentication Settings in Install.ini," on page 36

2.7.1 Installing Advanced Authentication Client with Client for Open Enterprise Server

1 Extract the Client for Open Enterprise Server installation set.
2 Copy or move the subdirectory `Windows-components` from the Advanced Authentication product download to Client for Open Enterprise Server installation set.
3 (Optional) To configure the default settings, modify the `install.ini` file located in the root directory of the client build (For example, `C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR11)`). For more information on the settings, see Section 2.7.3, "Advanced Authentication Settings in Install.ini," on page 36.
4 Run the `setup.exe` file for Client for Open Enterprise Server and select **Custom Installation**, then click **Next**.
5 Select **Advanced Authentication Client**, then click **Next**.
6 The Advanced Authentication installation options are displayed.

Client for Open Enterprise Server Installation

6a Select the Credential Provider you want to use for logging in to the workstation from the **Login experience for Advanced Authentication support:** list.

6b (Optional) Specify the DNS name or IP address of the Advanced Authentication Server in **Advanced Authentication Server (optional):**.

6c (Optional) Specify an alternate Advanced Authentication event name for non-domain Windows logon in **Advanced Authentication Event Name (optional):**, then click **Next** to complete the Client for Open Enterprise Server installation.

After successful installation of the Advanced Authentication Client and Client for Open Enterprise Server, a new parameter **Advanced Authentication** is listed in **Client Properties** > **Advanced Login** tab > **Parameter group** list and is set to **Enabled** by default. This setting enables the Client to use Advanced Authentication when performing an eDirectory login.

NOTE: Installing Advanced Authentication Client during the installation of Client for Open Enterprise Server versions between 2 SP4 (IR6) and 2 SP4 (IR10) sets the Advanced Authentication parameter to **On** and sets the existing parameter **Login With Third-Party Credential Provider** to **On**. This setting enables the eDirectory login attempt using the Windows credentials after the Windows-only logon performed by Advanced Authentication credential provider. For more information on Advanced Authentication credential provider login mechanism, see Section 3.6, "Advanced Authentication Credential Provider," on page 62.

2.7.2   Enabling Advanced Authentication Integration Functionality

The integration of Advanced Authentication and Client for Open Enterprise Server on the workstations already using Advanced Authentication for Windows logon can be achieved by enabling Advanced Authentication-specific behaviors in Client. This does not need any installation or upgrade of Advanced Authentication Client components.

1 Extract the Client for Open Enterprise Server installation set.

2 Set `InstallAdvancedAuthentication=yes` in the install.ini file located in the root directory of the client build (For example, `C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR6)`). For more information on the setting, see Section 2.7.3, "Advanced Authentication Settings in Install.ini," on page 36.

3 (Optional) To configure the default settings for
`AdvancedAuthenticationClientDiscoveryHost` and
`AdvancedAuthenticationClientEventName` parameters, modify the `install.ini` file.
For more information on the settings, see Section 2.7.3, "Advanced Authentication Settings in
Install.ini," on page 36.

4 Run the `setup.exe` file for Client for Open Enterprise Server and select the installation option
desired, then click **Next** to complete the Client for Open Enterprise Server installation.

If `setup.exe` detects that the Advanced Authentication Client is already installed on the
workstation, even though the Advanced Authentication Client is not installed along with Client for
Open Enterprise Server, the parameters **Advanced Authentication** is set to **Enabled** by default in
Client Properties. This is because, the parameter `InstallAdvancedAuthentication` is set to `Yes`
in the `install.ini` file.

NOTE: If the Client for Open Enterprise Server version is between 2 SP4 (IR6) and 2 SP4 (IR10), the
parameters **Advanced Authentication** and **Login With Third-Party Credential Provider** is set to **On** by
default in **Client Properties**.

If `AdvancedAuthenticationClientDiscoveryHost` and
`AdvancedAuthenticationEventName` parameters are configured in the `install.ini`, they are
added to the Advanced Authentication `config.properties` file when `setup.exe` detects the
Advanced Authentication Client already installed on the workstation.

2.7.3 Advanced Authentication Settings in Install.ini

- `InstallAdvancedAuthentication=[Yes/No]`

  Controls the installation of Advanced Authentication Client during the Client installation if the
  Advanced Authentication install packages are available in the Client installation set. If this
  option is set to Yes, the Advanced Authentication Client check box is selected by default during
  Custom Installation. For Express Installation, this option controls whether Advanced
  Authentication Client has to be installed in addition to the Client for Open Enterprise Server.

- `InstallAdvancedAuthenticationDeviceServices=[Yes/No]`

  This option is valid when `InstallAdvancedAuthenticationClient` is set to `Yes` because,
  Device Services cannot be installed without installing Advanced Authentication Client. This
  option controls the installation of Advanced Authentication Device Services during the Client
  installation if the Advanced Authentication install packages are available in the Client
  installation set. If this option is set to Yes, the Advanced Authentication Device Services check
  box is selected by default during Custom Installation. For Express Installation, this option
  controls whether Advanced Authentication Device Services has to be installed in addition to the
  Client for Open Enterprise Server and Advanced Authentication Client.

- `AdvancedAuthenticationClientDiscoveryHost=[blank/DNS name/IP address]`

  Configures the Advanced Authentication Client to use a specific Advanced Authentication
  server with the DNS name or IP address specified. If left blank, the Advanced Authentication
  Client attempts to automatically discover Advanced Authentication Servers using DNS. The DNS
  name or IP address specified is used as the value for `discovery.host` parameter in the
  Advanced Authentication Client's `config.properties` file. For more information on
  preliminary configuration on Advanced Authentication Client, see Advanced Authentication -
  Windows Client Installation Guide.

- **AdvancedAuthenticationClientEventName=[blank/*Event name*]**

    Configures the Advanced Authentication Client to use an event created on the Advanced Authentication for the logon process. If left blank, Windows logon is used as default event. The Event name specified is used as the value for event_name: parameter in the Advanced Authentication Client's config.properties file. For more information on preliminary configuration on Advanced Authentication Client, see Advanced Authentication - Windows Client Installation Guide.

- **AdvancedAuthenticationLogonExperience=[Keep/NetIQ/OES]**

    Controls the mode in which the Client for Open Enterprise Server supports Advanced Authentication. If this option is set to Keep, The logon experince to the users continues to be same as it is currently.

    If this option is set to NetIQ, the NetIQ Advanced Authentication credential provider is used to provide the primary logon experience to the users. A password based eDirectory only login is attempted using the Login with Third-Party Credential Provider feature of the Client after the Windows-only logon.

    If this option is set to OES, the Client for Open Enterprise Server credential provider is used to provide the primary logon experience to the users. The Advanced Authentication logon, eDirectory login, and Windows account logon are all performed using the Client credential provider.

2.8 Customizing the Brand as Per Client Requirement

Client for Open Enterprise Server supports company-specific name, text changes for modules and features in multiple languages. The strings present on the Login page, System Tray menu, Dialog boxes, Specific keyword within a string can be modified as per the client requirement. To apply the branding changes you have to modify the strings in `NC_Strings.xml` file.

NOTE: All the strings that can be custom branded are available in the NC_Strings.xml file.

Example to apply custom branding for the Client for Open Enterprise Server login page

Figure 2-5   Default Client for Open Enterprise Server Login Page
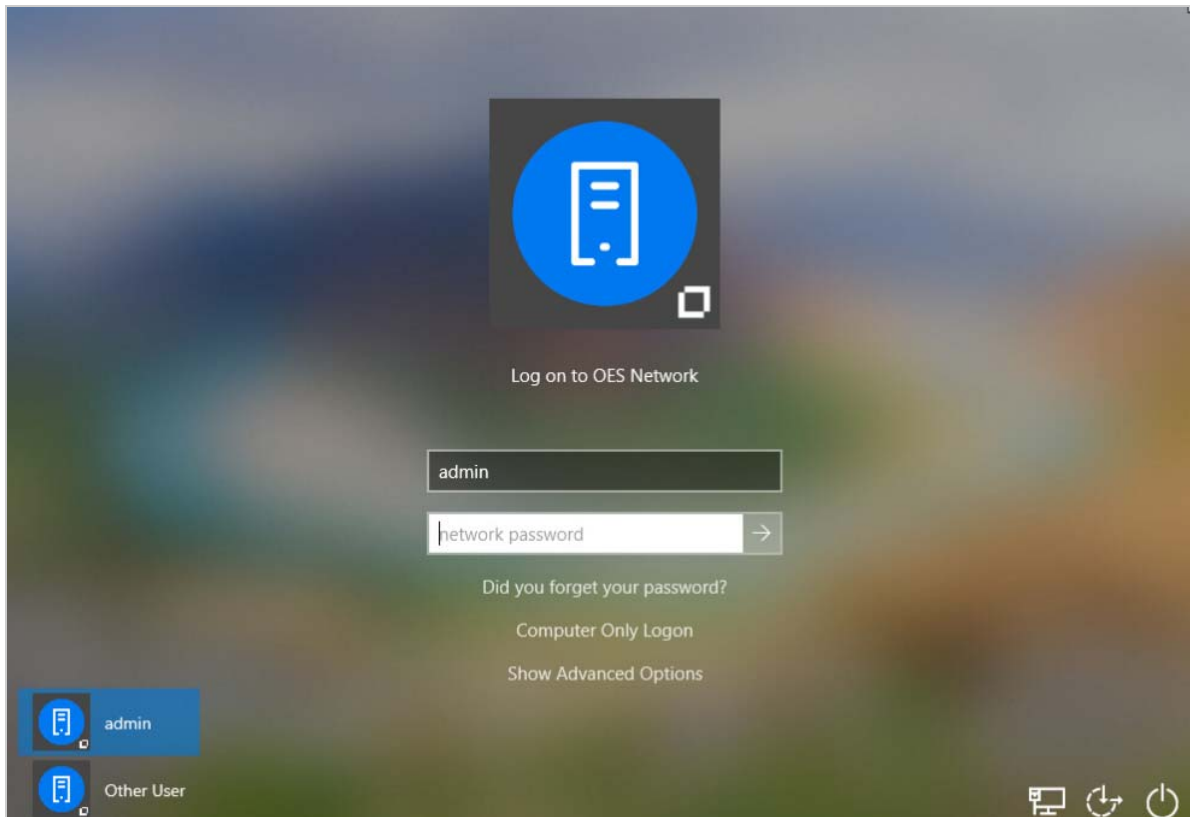
To apply branding changes on the login page modify the tags in `NC_Strings.xml` file as shown below:

```
<credprovider>
    <ui_string>
    <id>104</id>
     <text>Log on to OES Network</text>
     <description/>
     <en>Log on to XYZ Network</en>
     <de></de>
     <es></es>
    </ui_string>
    <ui_string>
    <id>202</id>
     <text>Did you forget your password?</text>
     <description></description>
    <en>Password Recovery</en>
    <de></de>
    <es></es>
    </ui_string>
    <ui_string>
    <id>107</id>
       <text>Computer only Logon</text>
```

```
        <description/>
        <en>XYZ Workstation Login</en>
        <de></de>
        <es></es>
      </ui_string>
      <ui_string>
      <id>108</id>
        <text>Show Advanced Options</text>
        <description/>
        <en>Look for Advanced Options</en>
        <de></de>
        <es></es>
      </ui_string>
     </credprovider>
```

After applying the custom branding and relaunching the login page, you can see the modified Login page as below.

Figure 2-6 *Custom Branding Applied Client for Open Enterprise Server Login Page*
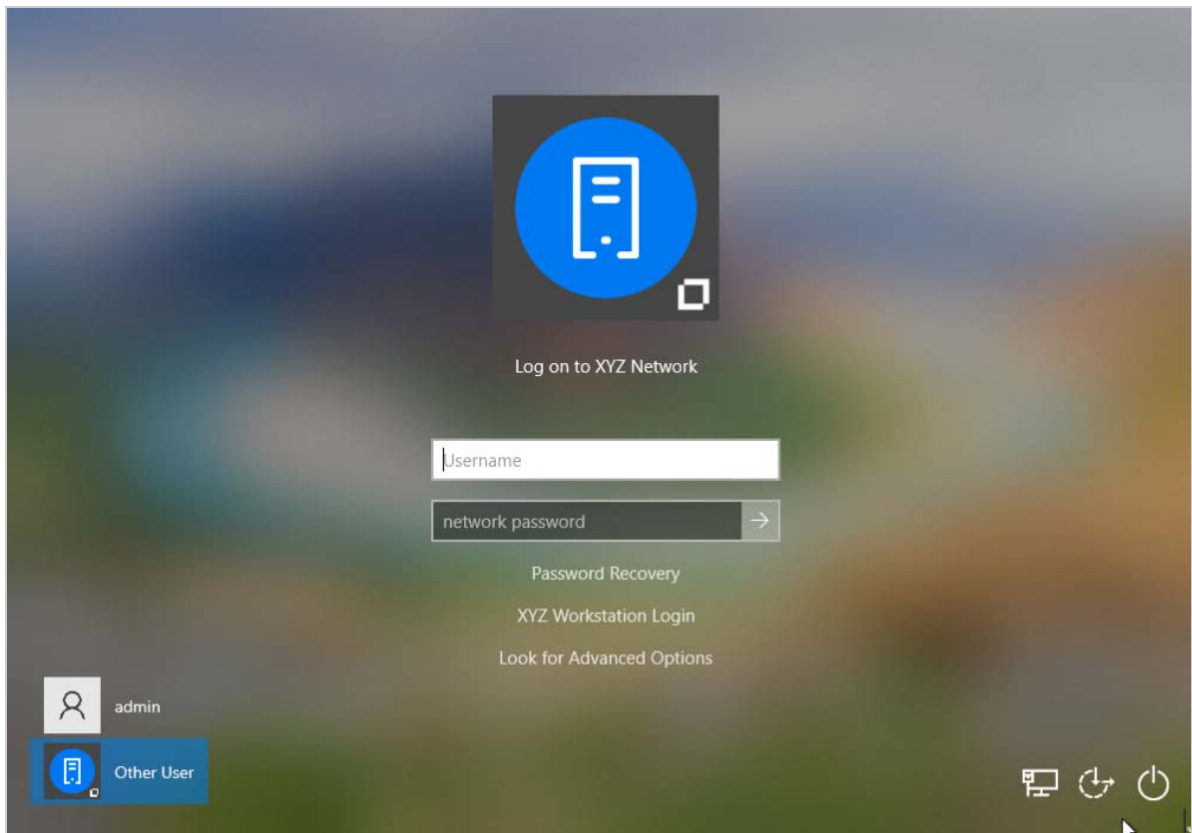
Example to apply custom branding for System Tray Menu and String Name

Figure 2-7 *Default System Tray Menu and String Names*
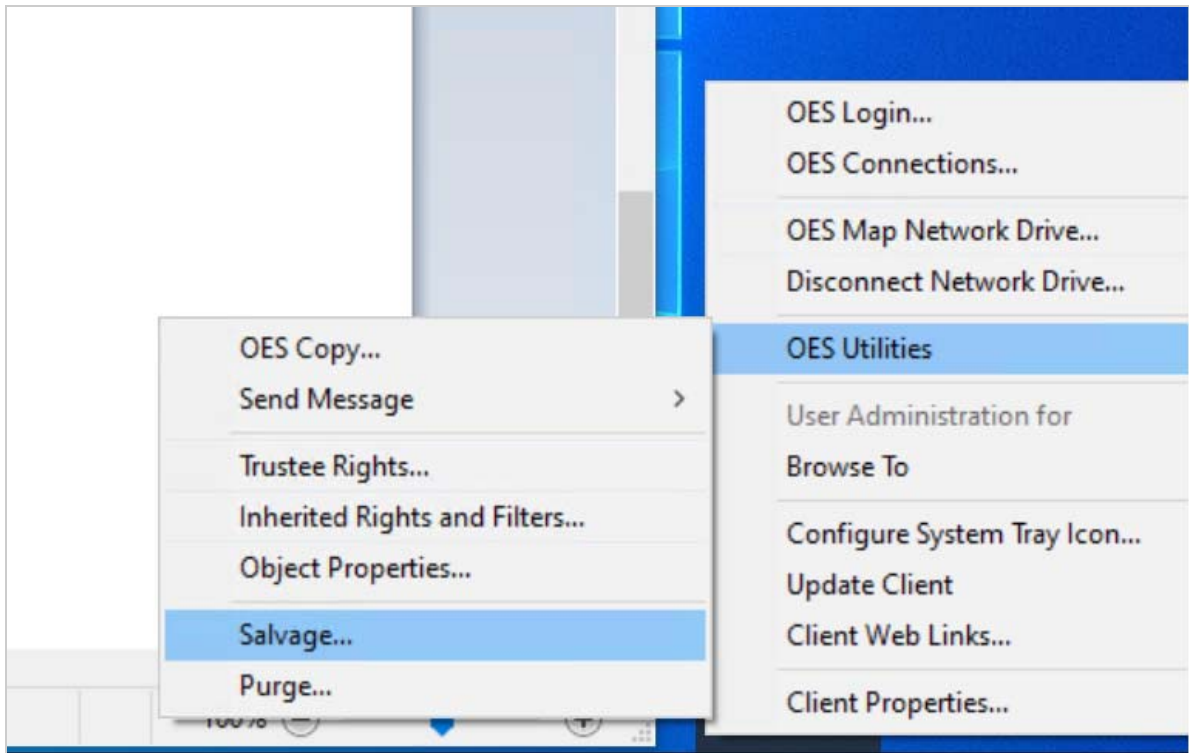
To apply the branding changes for the System Tray menu and Strings, modify the tags in
`NC_Strings.xml` file as shown below:

```
<netprovider>
    <ui_string>
     <id>549</id>
     <text>Salvage...</text>
     <description></description>
     <en>Files Recover</en>
     <de></de>...
 ...</ui_string>
</netprovider>

<replacestrings>
   <ui_string>
    <en>OES</en>
    <en_replace>XYZ!</en_replace>
   </ui_string>
    <ui_string>
    <en></en>
    <en_replace></en_replace>
    </ui_string>
</replacestrings>
```

After applying the custom branding and relaunching you can see the modified System Tray Menu
and String Names as below.

Figure 2-8 *Custom Branding Applied System Tray Menu and String Names*

Example to apply custom branding for the Title Name in NW Tray login page

Figure 2-9 *Default Title Name in NW Tray Login Page*
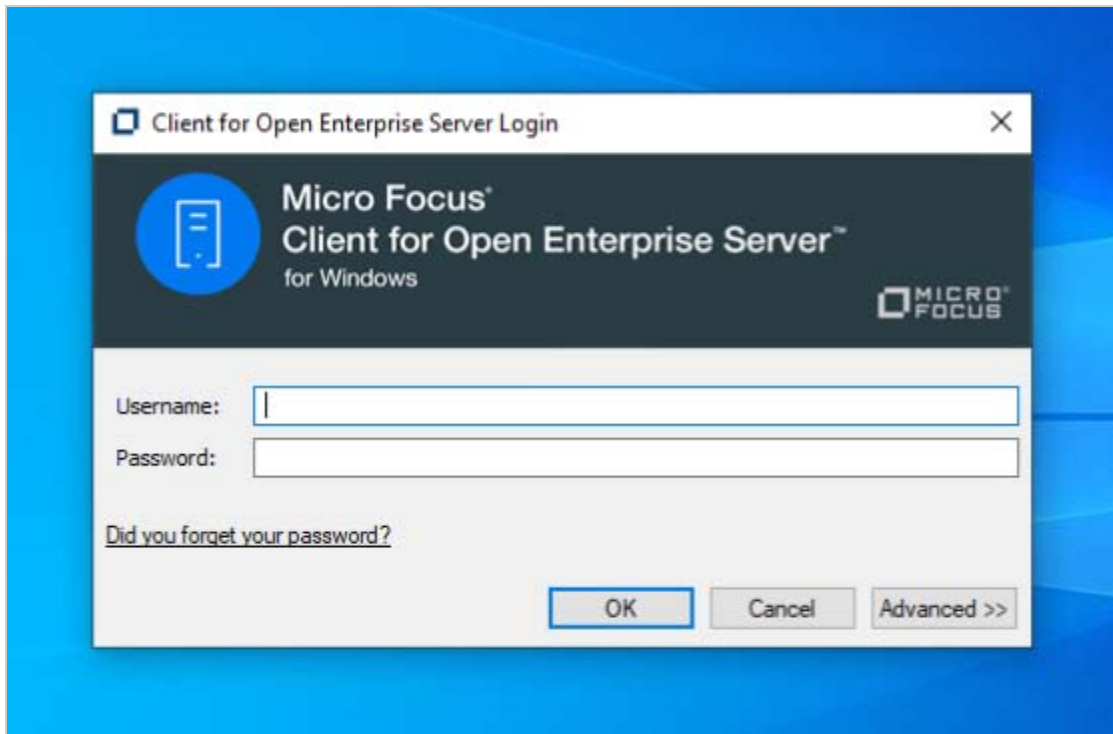
To apply the branding changes for the Title name in NW tray login page, modify the tags in `NC_Strings.xml` file as shown below.

```
<ncloginui>
   <ui_string>
     <id>20</id>
     <text>Client for Open Enterprise Server Login</text>
     <description></description>
     <en>XYZ user's login</en>
     <de></de>
     <es></es>
   </ui_string>
</ncloginui>
```
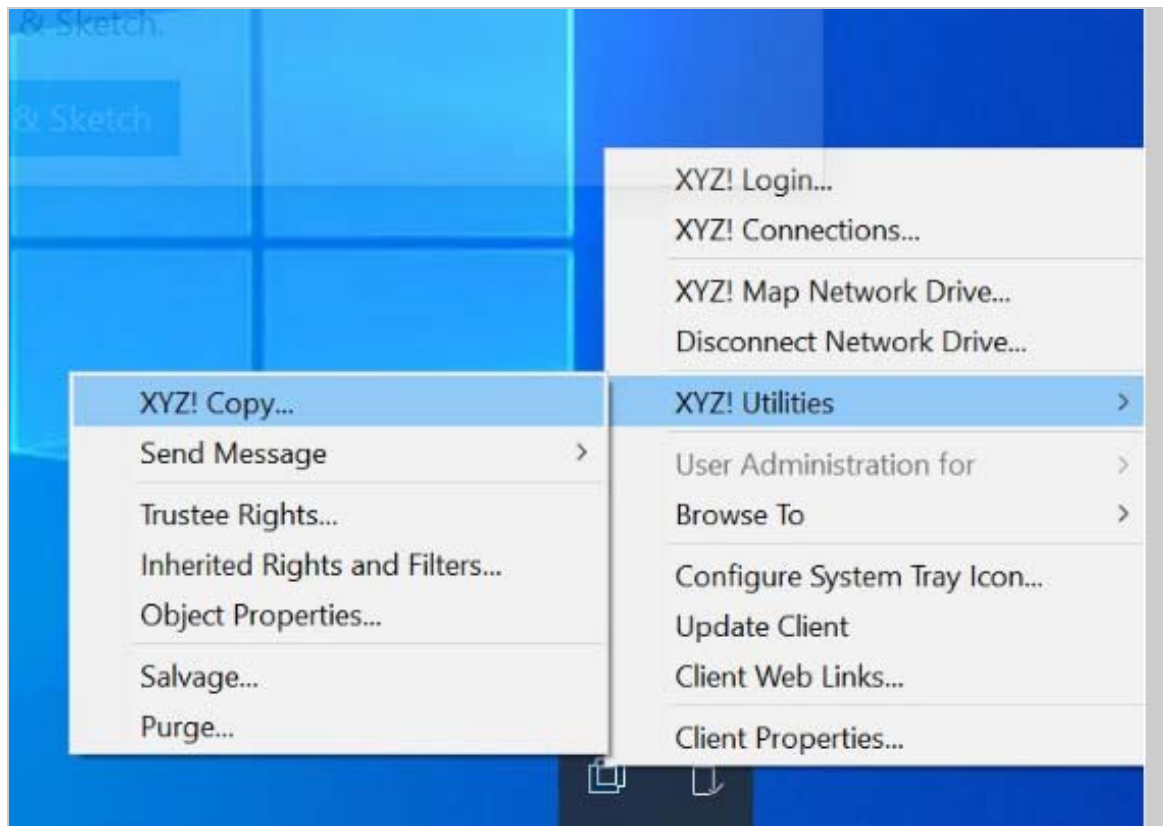
After applying the custom branding and relaunching you can see the modified NW Tray Title Name as below.

Figure 2-10 *Custom Branding Applied NW Tray Title Name*
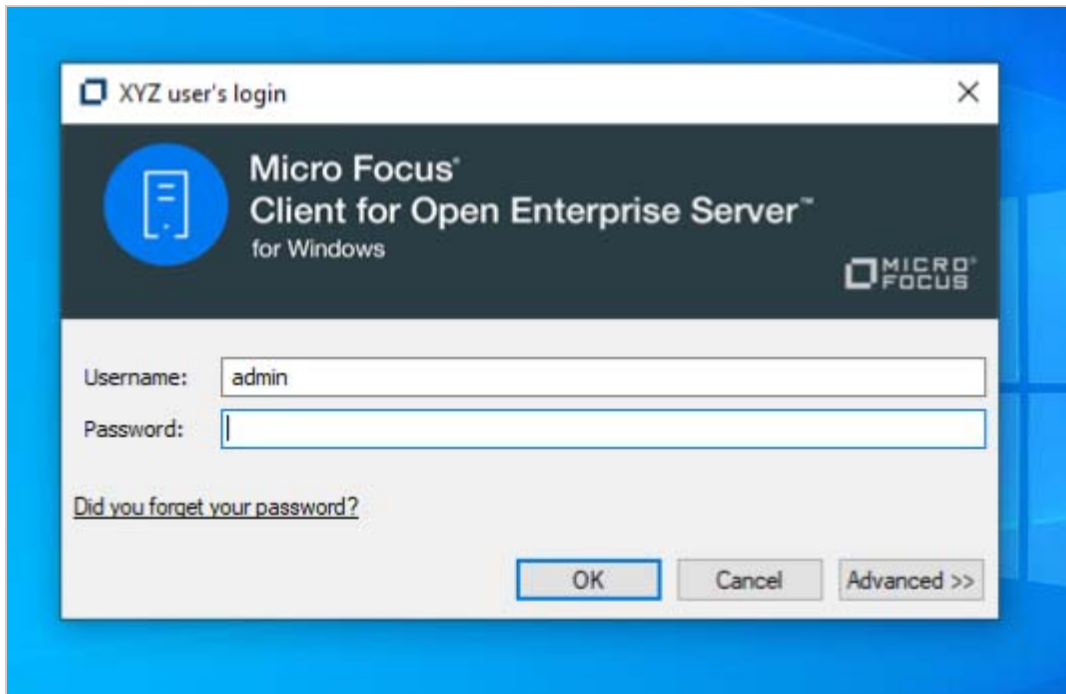
2.8.1 Adding Custom Branding in Client for Open Enterprise Server

1. Run the Client for Open Enterprise Server installation set.

   The WinZip Self Extractor to extract installation files appears.

2. Clear the checkbox **When done unzipping open: .\setup.exe** and click **Unzip**.

   The files get extracted in the default location, C:\Micro Focus\Client for Open Enterprise Server 2 SP6.

3. Edit the strings in `NC_Strings.xml` file located in, `C:\Micro Focus\Client for Open Enterprise Server 2 SP6\Install`.

4. Set `CustomStrings=yes` in the `install.ini` file located in the root directory of the client build, `C:\Micro Focus\Client for Open Enterprise Server 2 SP6`.

5. Run the `setup.exe` extracted in the location, `C:\Micro Focus\Client for Open Enterprise Server 2 SP6`.

6. Depending on your locality select the Language you want to use for the installation.

7. Select **I Accept the Client License Agreement**, then click **Next**.

8. Select one of the following installation options, then click **Install** or **Next**.

   Express Installation: Installs the Client with the default configuration.

   Custom Installation: Lets you customize the installation.

9. When the installation is complete, reboot the workstation.

2.8.2 Disabling the Custom Branding Feature

To disable the custom branding feature, in the Registry Entry
`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Client\Parameters` change the
`CustomStrings REG_DWORD` value to `0 (zero).`

3 Authenticating to a OES Network

This section describes the methods used on Windows 11, Windows 10, Windows 8, Windows 7, Windows Server 2012, Windows Server 2016, Windows Server 2019, and Windows Server 2022 to authenticate to a OES 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 Windows 11, Windows 10, Windows 8, Windows 7, Windows Server 2012, Windows Server 2016, Windows Server 2019 platforms, and Windows Server 2022, having been replaced by a new method of collecting logon credentials called Credential Providers.

3.1 Windows 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 Welcome Screen*

In Windows 11, Windows 10, Windows 8, Windows 7, Windows Server 2012, Windows Server 2016, Windows Server 2019, and Windows Server 2022 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.

3.1.1   Windows Live ID Based Credential Authentication

The Microsoft Windows Live ID based login is supported. To use this feature, ensure that your administrator has added your Windows Live ID to your PC. For more information on adding a Live ID to a Windows PC, refer the Microsoft article on Your life, connected and to create a Live ID, refer How do I sign up for a Microsoft account?

Logging on to Your PC Using Windows Live ID

Once your Live ID is added to the PC and after a successful Network login, in the Log on to this computer screen, enter your Live ID username and password.

Figure 3-2 *Windows Live ID Login Screen*
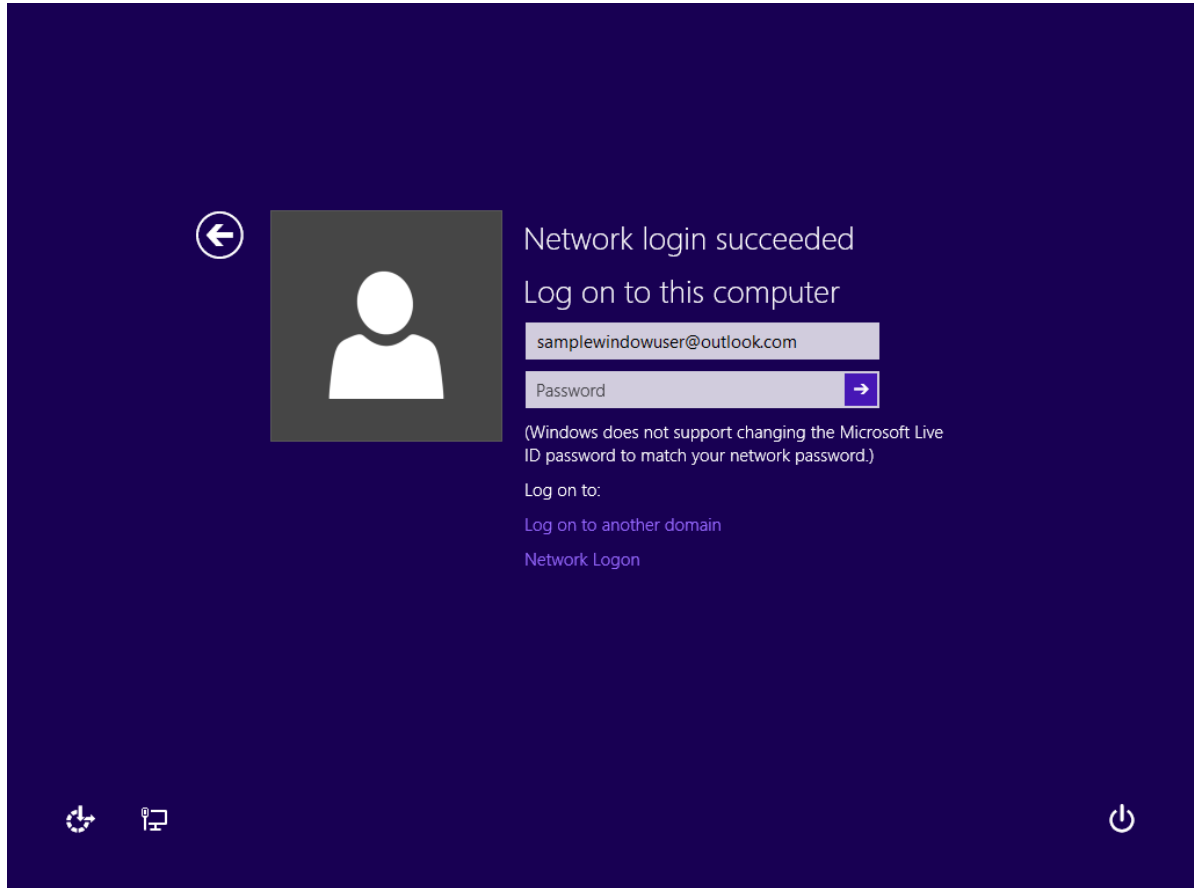
In the Client for OES, users are expected to authenticate to the network first using the Client for OES Credential Provider and then to their PC using Live ID. Or, you can combine your network login and your Windows Live ID login in the Network login screen.

To combine your network and Windows Live ID login:

1 In the **Network Login** screen, click **Show Advanced Options**.

2 In the **Login** dialog, on the **Windows** tab, type the Windows Live ID in the **Local username** text box and then click **Apply**.

NOTE: Ignore the **From:** list box for now. It will be disabled in case of a Windows Live ID login.

Figure 3-3 *Network Login with Windows Live ID*
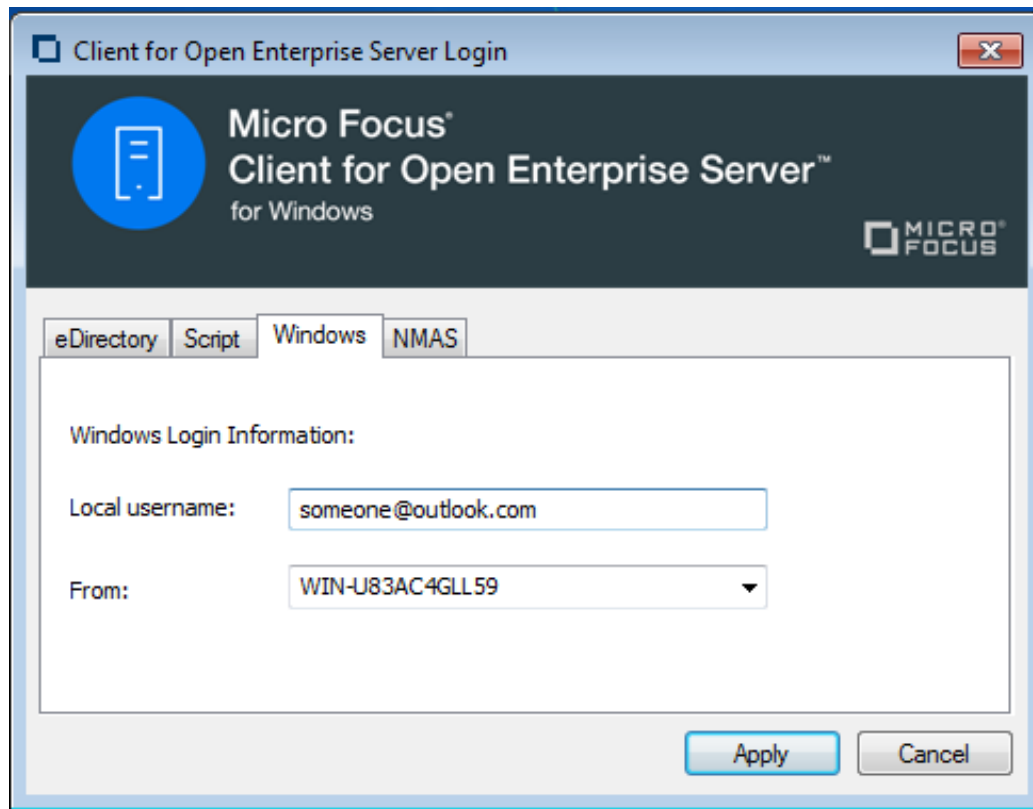
Limitations of Windows Live ID Based Login

The Client for OES password sync feature that is used to synchronize your Windows password to that of the eDirectory does not work in case of a Windows Live ID based login.

Figure 3-4 *The Unsupported Password Sync Feature*
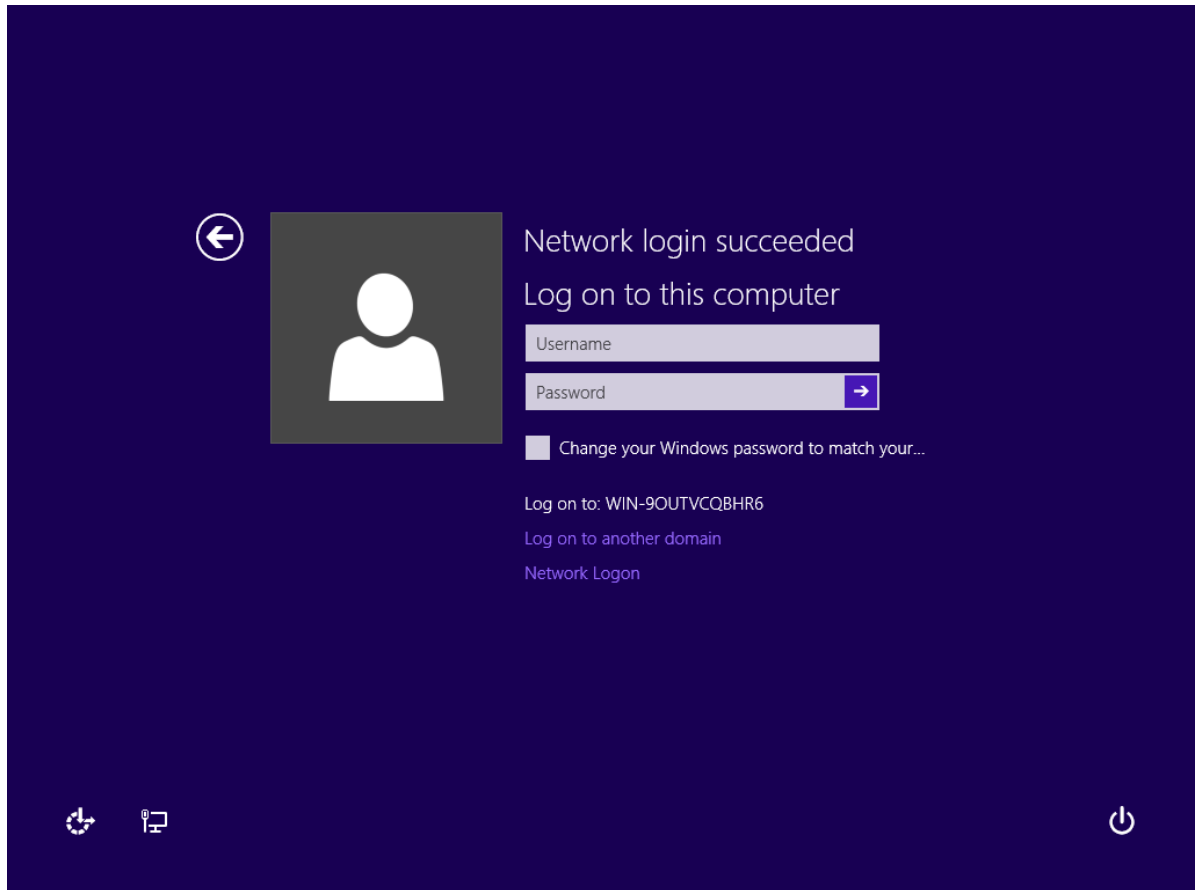
Also, the change password feature is not supported by Client for OES when Windows Live ID is used for computer log in.

Figure 3-5 *The Unsupported Client Change Password Feature*

3.2   Client for OES Credential Provider

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

3.2.1   Logon

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

Figure 3-6 *Windows Welcome Screen When the 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 3-7 *Network 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 Network logon tile also provides a link (**Show Advanced Options**) that allows users to interact with the Advanced Options dialog box, which lets users specify the eDirectory tree, context, and server they want to log in to.

Figure 3-8 *Advanced Options Dialog Box*
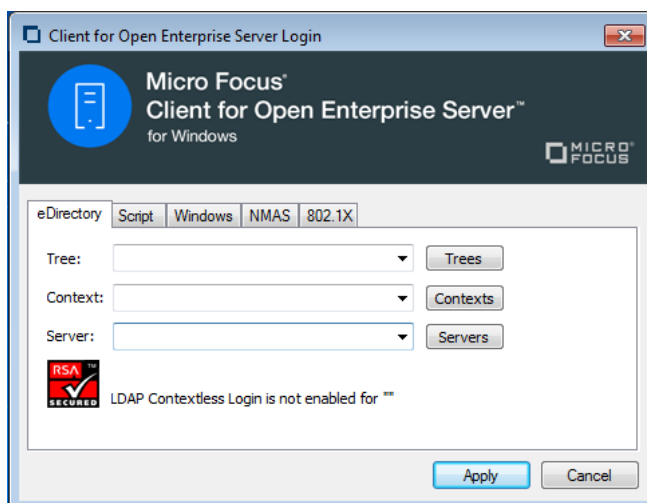
3.2.2 Logon With Advanced Authentication

When the Client for Open Enterprise Server is enabled with Advanced Authentication, the Client for OES Credential Provider provides the logon tile to allow the user to log on interactively by simply entering the eDirectory user name.
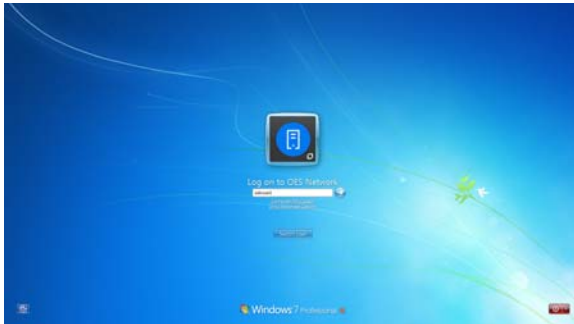
The logon tile provides an option Computer Only Logon to log in only to the local machine and bypasses the network logon. It also provides a link, **Show Advanced Options** that allows users to interact with the Advanced Options dialog box. The **Advanced Authentication** tab in the dialog box allows the user to specify the Advanced Authentication username, Repository, and server information.

Next, the Credential Provider provides an interface to specify the information for Advanced Authentication logon based on the authentication method configured for the user.

Upon successful Advanced Authentication logon, the eDirectory and Windows logon proceeds transparently.

If the eDirectory password or the Windows account name or password stored by Advanced Authentication is no longer correct or if it has never been stored, the user will be prompted to provide the current credentials.
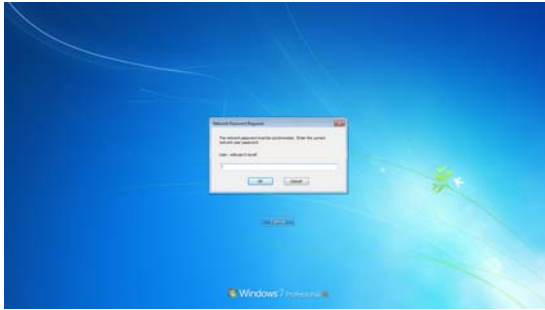
NOTE: If you want to use Advanced Authentication Credential Provider instead of using Client for OES Credential Provider for the logon experience, you must change the following parameters in the **Client Properties** > **Advanced Login**.

- **Client Logon:** Set this parameter to **Off**.
- **Login With Third-Party Credential Provider:** Set this parameter to **On**.

3.2.3 Locking and Unlocking the Workstation

The Credential Provider supports locking and unlocking the Windows 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 3-9 *Unlock Computer Screen*
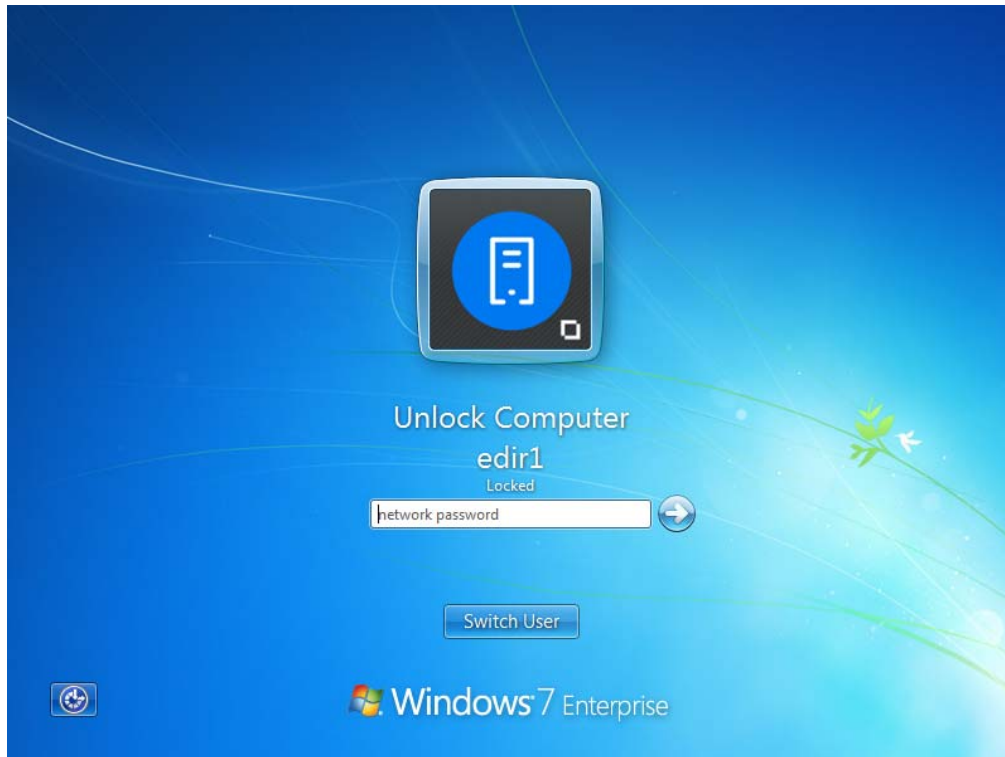
If the Client for Open Enterprise Server is enabled with Advanced Authentication, the locked user account is represented by a logon tile. To unlock, the user is required to perform the Advanced Authentication logon based on the Advanced Authentication method configured. An Advanced Authentication logon proceeds using the same Advanced Authentication user which logged this user into eDirectory and the workstation will be unlocked using the Windows account credentials retrieved from that successful Advanced Authentication logon.

3.2.4 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 Network Logon tile that allows a new user to log on interactively.

Figure 3-10 *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 Network Login 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 workstation using the Client for OES Credential Provider, OES connections made during the login will persist only if you are not currently logged in to the workstation. If your Windows 7 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.

3.2.5   Logon Using Windows Server 2012 Terminal Services

On Windows Server 2012, 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 2012.

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 2012 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 3-11   *Client for OES Credential Provider with Terminal Services Enabled*

3.3 Downloading Client for Open Enterprise Server

You can download Client for Open Enterprise Server from the following places:

◆ Micro Focus Customer Center (SLD)

◆ Marketplace

3.4 Logging in When eDirectory and Windows Credentials Are Not Synchronized

If your eDirectory account password is not in sync with the Windows account password when logging in through the Client for OES Credential Provider, you will see a screen confirming that the network login succeeded and letting you enter the Windows account password.

Figure 3-12   Windows Account Logon Screen

If you specify the correct Windows account password and continue with the login, the 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 Network password after a successful login** checkbox will syncronize the account passwords after the correct credentials have been provided.

3.5 Changing Passwords

The Client for OES Credential Provider lets you change a network password as well as a Windows password.

3.5.1 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 network 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 Network Change Password dialog box opens.

5 Select which resources you want the password change to go to.
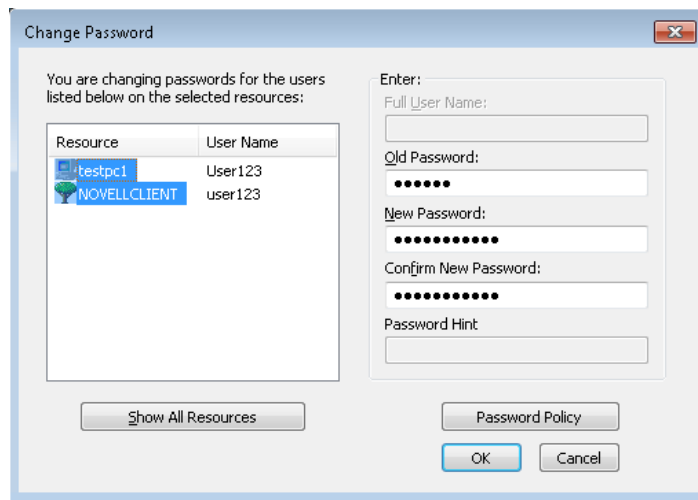
For example, you can change your Network password and your Windows password, or you can change only your Network password.

6 Click **OK**.

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

7 Click **OK** to close the message.

3.5.2 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.

3.5.3 Changing Your Password When Advanced Authentication is Enabled

1 Press Ctrl+Alt+Delete, then click **Change a password**.

2 Press Enter to begin the password change process for the displayed eDirectory user.

3 Perform the Advanced Authentication logon based on the method configured.

4 Select the resources for which you want to change the password.

Type your current network 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.

5 Click **OK**.

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

6 Click **OK** to close the message.

3.6 Advanced Authentication Credential Provider

After successful installation of Client for Open Enterprise Server 2 SP4 (IR6) or later and Advanced Authentication Client, to perform the Windows logon followed by automatic eDirectory login using the Advanced Authentication credential provider, the following requirements must be met:

- The existing Advanced Authentication credential provider obtains its configuration from the `config.properties` file setting, or performs DNS discovery if the `config.properties` is not configured.

- The Windows account password is set the same as user's eDirectory account password for an automatic and transparent eDirectory login to be successful.

- In avoid not being prompted for eDirectory information, the user would need to have logged into eDirectory successfully before using Advanced Authentication. So that the eDirectory tree name, eDirectory context, and other login profile information for Client for Open Enterprise Server is populated during the login process. Otherwise, the user will be prompted to provide and save these details during their first login.

- To use the Advanced Authentication Credential Provider in the Client for Open Enterprise Server 2 SP4 (IR11) and later, in the **Advanced Login** tab of Client Properties, the parameter **Client Logon** must be set to **Off** and the parameter **Login with Third-Party Credential Provider** must be set to **On**.

To log in to Windows, on the Advanced Authentication login page, the user must provide the user credential in the format *Advanced Authentication user repository\username*. Further login requirements are based on the enrolled methods that are required by Advanced Authentication for the Windows user login. For more information on configuring Advanced Authentication methods, see Advanced Authentication Administration Guide.

NOTE: For a non-domain joined Windows workstation, when logging in with Advanced Authentication for the first time, the Advanced Authentication credential provider prompts for additional Windows account credentials. This information is used to map the local account to the domain account of the user.

After the user has successfully completed the required Advanced Authentication methods and before the Windows user desktop is displayed, the Login with Third-Party Credential Provider functionality of Client for Open Enterprise Server performs the eDirectory login.

If the user has not logged into eDirectory before from this workstation, or if the eDirectory tree name, eDirectory context, or eDirectory password are incorrect, then the Client for Open Enterprise Server prompts the user to provide correct eDirectory information to complete the eDirectory login. The information thus provided for the first time the user logs into eDirectory successfully is saved for future logins.

When the Windows user desktop is displayed after successful login, the user is logged in to both Windows and eDirectory.

If the user disconnects their NCP connections or logs out of eDirectory, the Client for Open Enterprise Server requires the user to perform the Advanced Authentication log in again to access eDirectory.

4 Setting Client Properties

You can optimize the Client for your network by using property pages to configure the 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:

- Section 4.1, "Setting Properties During Installation," on page 65
- Section 4.2, "Setting Properties on a Single Workstation after Installation," on page 66
- Section 4.3, "Setting Properties on Multiple Workstations after Installation," on page 84

4.1 Setting Properties During Installation

Use the 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 Client Install Manager (`nciman.exe`) located in the `C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)\Admin` folder (created when you unzipped the downloaded file).
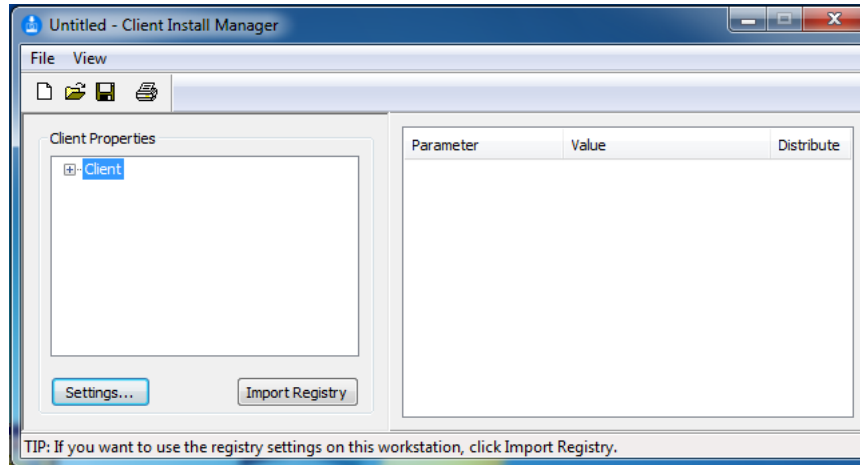
2 Click **Settings**.
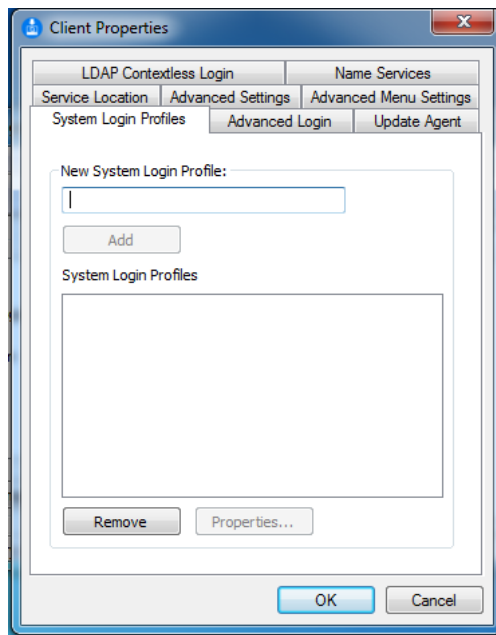
3 Modify the parameters you want, then click **OK**.

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

For more detailed information on these options, see Section 4.2, "Setting Properties on a Single Workstation after Installation," on page 66.

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 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 Install Manager.

4.2 Setting Properties on a Single Workstation after Installation

1 At the user's workstation, right-click the ▫ icon in the notification area of the taskbar.

2 Click **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 to view which version of the Client you are running.

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

Figure 4-1 *Client Property Page*
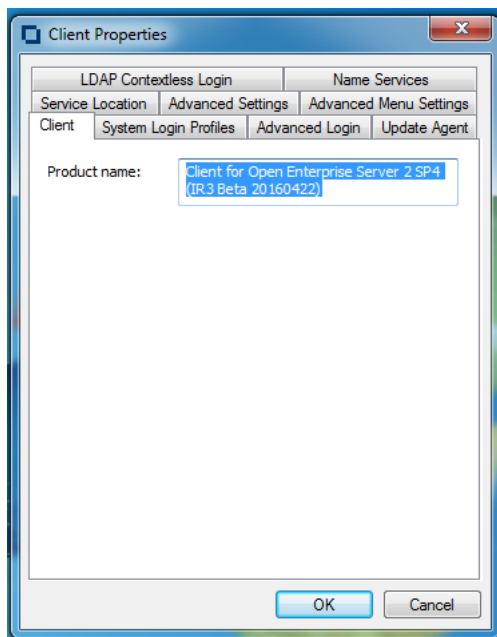
4.2.2 Login Profiles Settings

Use the System Login Profiles property page in the 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 8.7, "Setting Up Login Profiles," on page 115.

Figure 4-2 *System Login Profiles Property Page*
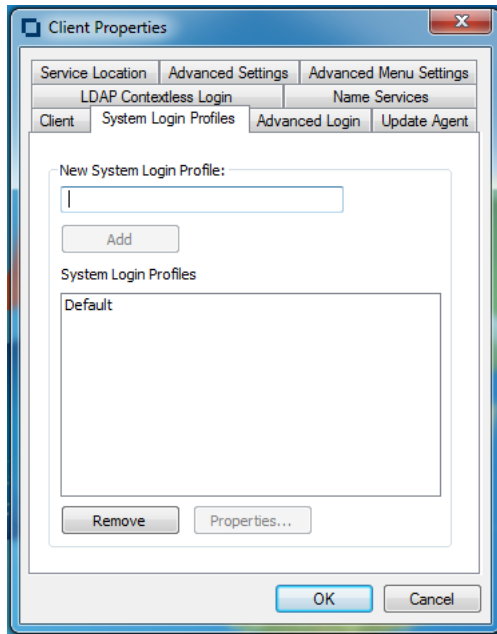
- ◆ "Adding a System Login Profile" on page 68
- ◆ "Viewing or Editing a System Login Profile's Properties" on page 68
- ◆ "Removing a System Login Profile" on page 69

Adding a System Login Profile

1 Right-click the ⬜ icon in the notification area of the taskbar.

2 Click **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 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 Login dialog box, then click **OK** to close the Client Properties dialog box.

Viewing or Editing a System Login Profile's Properties

1 Right-click the ⬜ icon in the notification area of the taskbar.

2 Click **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 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 Login dialog box, then click **OK** to close the Client Properties dialog box.

Removing a System Login Profile

1 Right-click the ☐ icon in the notification area of the taskbar.

2 Click **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 Client Properties dialog box.

4.2.3   Advanced Login Settings

Use the Advanced Login property page to configure user login settings.

Figure 4-3   *Advanced Login Property Page*
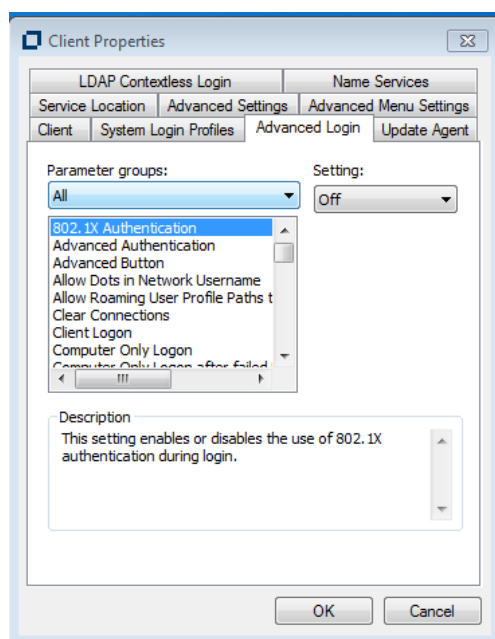
Use the **Parameter groups** drop-down list to display all the advanced login parameters or to sort the parameters by function (**Execution Options**, **Password**, and **Shown on Login**). Select the parameter you want, then use the **Setting** option to configure the parameter. For most parameters, 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 8.9, "Configuring 802.1X Authentication," on page 132.

- ◆ **Advanced Authentication:** Enables or disables the use of Advanced Authentication when performing eDirectory login.

  NOTE: On a fresh install of Advanced Authentication Client and Client for Open Enterprise Server 2 SP4 (IR 11) or later, the default option is **Enabled**.

For more information, see Section 2.7, "Installing and Configuring Advanced Authentication Client," on page 34

◆ **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 Network Username:** If this setting is On, any periods entered in the network user name are treated as part of the name, rather than as eDirectory 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 user name such as John.Smith to both OES and Windows.

◆ **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 an Open Enterprise Server (OES) volume or other non-Windows-compatible resource. Setting this parameter to On allows roaming profile paths to OES volumes and other non-Windows server by disabling this Windows-specific security check. Note this policy is defined and controlled by Windows and not the Client for Open Enterprise Server, 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.

◆ **Client Logon:** Enables the Client Logon option to provide Open Enterprise Server logon options when logging into Windows on this computer. When it is set to On, Client for Open Enterprise Server Credential Provider provides the logon experience.

◆ **Computer Only Logon:** Specifies whether the Computer Only Logon option is shown when the Network 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 Open Enterprise Server network.

◆ **Computer Only Logon after failed Network Logon:** Determines whether or not Computer Only Logon is offered when a Network Logon attempt fails. Automatic means a Computer Only Logon will be offered unless the administrator has hidden the 'Computer Only Logon' option. Always and Never indicate how the Computer Only Logon should be offered regardless of whether the Computer Only Logon option is hidden.

◆ **Computer Only Logon Default:** Determines whether the Client will default to the Computer Only Logon mode. Automatic means the Client will remember when Computer Only Logon was the mode previously selected, and will continue defaulting to Computer Only Logon until Logon mode is interactively selected again. Always means the Computer Only Logon will always be the default mode presented, even if Network Logon was the previous mode used. Never means that 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 Client Login dialog:** Specifies the path and filename for a bitmap that will be used on the Client Login dialog in place of the default Client bitmap. Custom bitmap sizes can be used, but will affect the overall size of the Client 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.

◆ **Enable Sigle Sign-On:** Enables use of NMAS-based Single Sign-On for automatically providing the Windows account password during an otherwise non-password-based NetIQ eDirectory login using NMAS. This setting is only available on machines where the installed version of the NMAS client supports Single Sign-On capabilities. For more details on SSO, see Section 8.12, "Setting Up Single Sign-On (SSO)," on page 139.

◆ **Force Early Password Expiration Period:** Specifies the number of days by which the password expiration mechanism is preempted, before the actual eDirectory password expiration occurs. For example, if the eDirectory password expiration is set to occur in 5 days, and "Force Early Password Expiration Period" is set to 5, Client will preempt the password expiration process 5 days in advance.

NOTE: This setting takes effect only when the "Password Expiry Warning" setting is also enabled.

This parameter is set to 0 by default and has a valid range of 0 to 120 days.

◆ **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 96 for more information.

◆ **Last Logged On User:** Specifies whether the last logged on user is displayed along with the Network 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 2012 when Terminal Services are installed.

◆ **Last Logged On User Default User:** Forces the "Last Logged On User" presented by Client to always be the user that is specified, regardless of which user has logged in last. If no value is specified, the default behavior is to specify the previously logged in user. The default value of this parameter is blank.

◆ **Last Logged On User Default Profile:** Indicates which Client Login Profile should be used in conjunction with the "Last Logged On User Default User". If no value is specified, the default behavior is to use the Client Login Profile that was previously selected for the user, if more than one Client Login Profile is available.

For example, when configuring a specific "Last Logged On User Default User" that should always be shown by default, it might be desirable to configure "Last Logged On User Default Profile" as "Default" (or a different Client Login Profile name that has been created) so that a specific Client Login Profile will always be selected by default.

◆ **Login Profile List:** Specifies whether the Login Profiles drop-down list on the Client 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 Network password functionality that occurs during login to both eDirectory and Windows when the password 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 Third-Party Credential Provider:** This setting controls whether an OES login will still be attempted after the Windows logon, in cases where the Client's credential provider was not used during the Windows logon.

◆ **Make Script Tab Read Only During Login:** Disables all the fields in the Script tab during login to prevent users from overriding any of the Script tab settings.

◆ **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.

◆ **Password Expiry Warning:** Enables or disables the presentation of password expiration alerts before the actual password expiration occurs. When disabled, no alerts are presented until the password expiration occurs, and the user must change their password before exhausting the available grace logins. This is the normal eDirectory password expiration behavior.

When enabled, the Client will begin presenting expiration alerts before the password expiration occurs, allowing the user to change their password before expiration or grace logins occur. This is similar to the Windows password expiration behavior.

◆ **Password Expiry Warning Period:** Specifies the number of days before the password expiration that the user starts receiving password expiration alerts. If the number of days is set to "0", Client will default to using the number of days specified by the Microsoft-defined "Prompt user to change password before expiration" policy, such that both Windows and Client will begin prompting at the same number of days before expiration. This parameter is set to 0 by default and has a valid range of 0 to 120 days.

◆ **Prompt for Network login during Windows AutoAdminLogon:** If the Client Login parameter is enabled, and Windows is configured to perform a Windows-only AutoAdminLogon as a specific user account, enabling this setting causes a Client 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 Network password option is shown when logging in to both eDirectory and Windows when the passwords are not already synchronized.

◆ **Show Suppress Single Sign-On checkbox:** Specifies whether the "Suppress Single Sign-On for this login" check box appears in the "Windows" tab of the Show Advanced Options dialog. This setting to optionally show the suppression check box is only available when the "Enable Single Sign-On" setting is enabled. Selecting this check box during a logon attempt allows you to disable the use of Single Sign-On for the current login attempt only; the check box will automatically reset back to the de-selected state for the next login attempt. For more details on SSO, see Section 8.12, "Setting Up Single Sign-On (SSO)," on page 139 .

◆ **Suppress NMAS ID Plugin support:** When enabled, the Client will suppress the features provided by an NMAS Identity Plug-In (ID Plug-In), even though the ID Plug-In is registered and configured for use with NMAS. This option is intended for use by an administrator who needs to temporarily suppress the ID Plug-In related behaviors in the course of setup or troubleshooting.

ID Plug-Ins provide various NMAS method-specific behaviors such as certificate lookup in eDirectory for certificates found on a smart card or token device, automatic entry of the Novell eDirectory identity in the Client login interface, user interface overrides such as hiding the 'Username' and 'Password' fields, or other behaviors which are specific to the NMAS method or hardware device being used.

◆ **Suppress NMAS Support for Computer Only Logon:** When enabled, the Client will suppress the features related to performing Computer Only Logon using NMAS, even though the required NMAS components and configuration may be available on the local machine. This option is intended for use by an administrator who needs to temporarily suppress this NMAS behavior in the course of setup or troubleshooting. This setting will not be available on machines where the required NMAS components and configuration are not present. For more information, see Section 8.13, "Setting Up NMAS Based Windows Logon," on page 146.

◆ **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.

◆ **Unlock Workstation Credentials:** Specifies the types of credentials that are accepted during workstation unlock, terminal session reconnect, and switch user operations. The Automatic option allows the user to provide either eDirectory or Windows credentials. The eDirectory if available option defines that eDirectory credentials are required if the logged-on user session is logged into eDirectory. The Windows only option defines that Windows credentials must always be used. The eDirectory only option defines that only eDirectory credentials are permitted, and unlock will not be allowed to use any other credential type.

◆ **Use NMAS for Windows Logon Default:** Determines the initial state of the 'Use NMAS for Windows Logon' check box. 'Automatic' means the Client will select this check box by default if the NMAS has been configured to enforce use of NMAS for Windows logons. If NESCM is not configured to be enforced, the behavior of 'Automatic' will be the same as 'Last Used'. 'Last Used' means the Client will remember the previously used state of the 'Use NMAS for Windows Logon' check box. 'Never' means the 'Use NMAS for Windows Logon' check box will be initially de-selected by default. 'Always' means the 'Use NMAS for Windows Logon' check box will be initially selected by default. For more information, see Section 8.13, "Setting Up NMAS Based Windows Logon," on page 146.

◆ **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 Network 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 Client Update Agent provides a workstation-initiated (manual or automatic) update of the Client software. It launches `acu.exe` from a specified location. Update Agent can be run manually from the Client Application Tray 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 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 Client Update Agent.

Figure 4-4   *Update Agent Property Page*
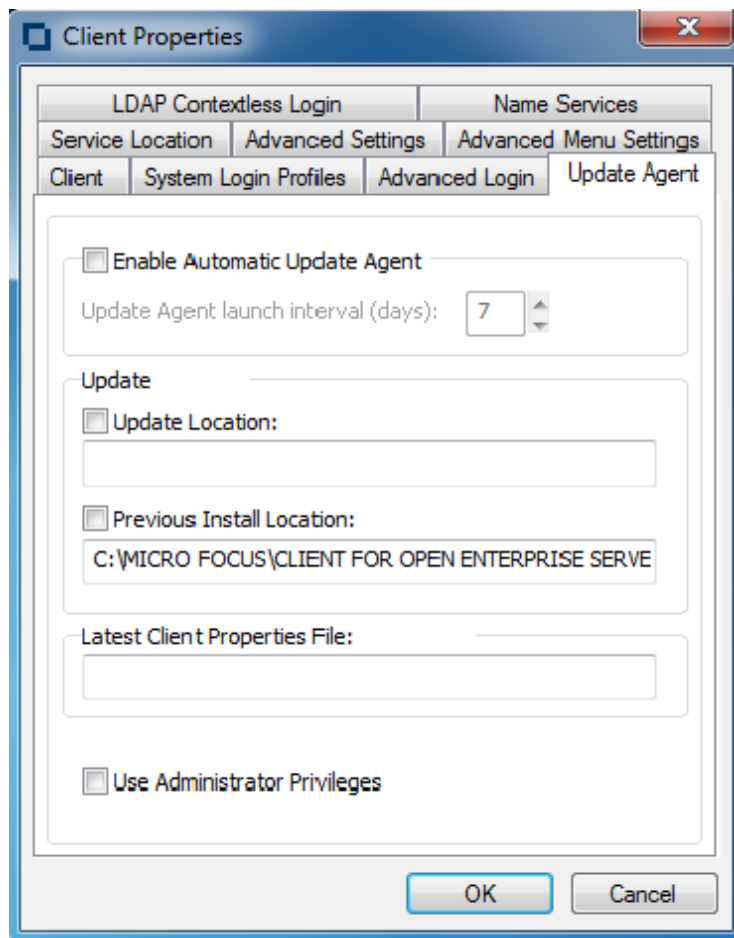
- **Enable Automatic Update Agent:** Select this check box to enable the automatic update agent, then use the Update Agent launch interval option to set the interval (in days) that the Client Update Agent will check for a new version of the Client for Open Enterprise Server.

- **Update Source(s):** Select the Update Location check box to enable the Client Update Agent to look for a new version of the 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 that you have the latest Client installation files in the first location that the Update Agent searches.

- **Latest Client Properties File:** Displays the name, date, and time of the most recent Client properties file used to apply Client settings on this workstation. For more information, see Section 2.2.1, "Creating the Client Properties File," on page 24.

- **Use Administrator Privileges:** If this option is selected, the Update Agent uses the 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 Client 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*
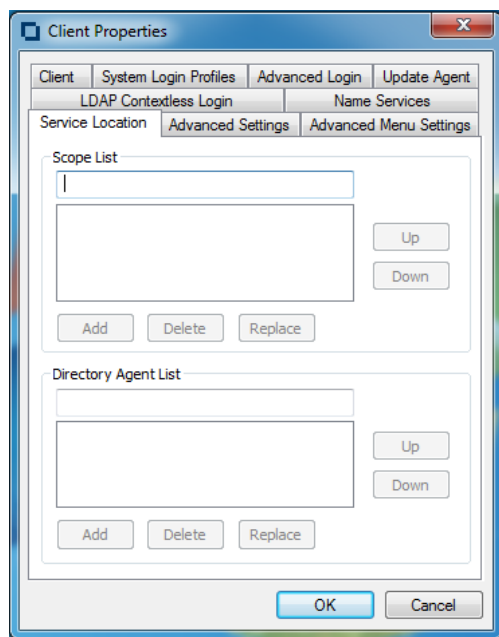
◆ **Scope List:** A list of scope names to be reported to SLP applications on a workstation. Multiple scope names are allowed. The list order reflects the preference order. Scopes can also be configured via DHCP or discovered dynamically from Directory Agents.

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.
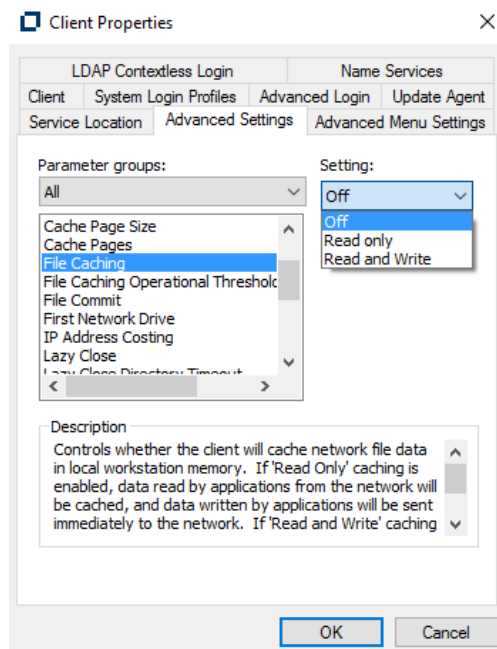
4.2.6 Advanced Settings

Use the Advanced Settings property page in the Client 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 Client auto reconnect.

- **Auto Reconnect Interval:** Specifies the delay in seconds between Client reconnect attempts.

- **Bad Address Cache:** Enables or disables use of the Bad Address Cache. You can set this value to "ON" or "OFF" to enable or disable Bad Address Cache. This parameter is set to "ON" by default.

- **Bad Address Cache Timeout:** Determines the number of seconds a Bad Address will remain in the Bad Address Cache. If the Client is unable to establish a TCP-level connection to a particular IP address, it stores that address in the Bad Address Cache for the number of seconds specified in this parameter. The timeout can be set from 30 to 21600 seconds and the default value is set to 300 seconds.

- **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.

- **Cipher Strength:** Specifies the strength of cipher suites that is used in establishing an encrypted connection between the server and the client. This setting is related to NCP encryption feature and it determines the strength of the algorithm used for encryption and decryption between the server and the client. You can set this value to "Low", "Medium", or "High". This parameter is set to "Medium" by default.

- **File Caching:** Controls whether the Client caches files locally or not. Setting this value to Read only caches the data read by the applications from the network and the data written by the applications is sent to the network immediately. Setting this value to Read and Write returns the control to the application during data write and the data is written to the network in the background.

- **File Caching Operational Threshold:** Establishes the threshold, in kilobytes, for which application read and write requests should be cached. Application read and write requests which are smaller than this value will be cached. Typically it is more efficient to send applications that read or write a large amount of data as a single request directly to the network, rather than utilizing the cache. Recommended and default value is 128KB.

- **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:** Defines which Windows drive letter the Client will start with in response to eDirectory login script commands such as "MAP *1" and "MAP NEXT", which are expecting to utilize drive letters relative to a First Network Drive setting which may be unique to each machine where the eDirectory login script executes.

The First Network Drive setting only applies to these "relative" drive mapping commands. The First Network Drive setting does not force or prevent attempts to map using an explicit drive letter reference (such as "MAP E:"), nor does the First Network Drive setting affect or prevent drive selection in the "OES Map Network Drive" feature available in the Client Application tray menu.

By default, the First Network Drive parameter is set to "Automatic". This means that the Windows drive letter will be determined and selected automatically based on the local virtual and physical drives present at the time the map command is executed. Starting with drive "A:", the Client will skip past any removable media, hard disk drives, optical drives and RAM disks and will select the first available Windows drive letter after these local drives. For example, if drive letters "A:" through "P:" are already assigned to local drives on the current Windows machine, having the Client "First Network Drive" parameter set to "Automatic" will choose "Q:" as the effective First Network Drive letter during the map command.

For more information regarding the MAP command and syntax, see the Client Login Script Commands and Variables documentation (http://www.novell.com/documentation/linux_client/login/data/hb3rxdni.html).

NOTE: After mapping a network drive using a script, if you change the eDirectory tree context, the same drive letter is used for mapping. You might loose all the unsaved changes that are associated with the previous eDirectory tree context.

 ◆ **Lazy Close:** Delays the file close on the network, allowing the file to be reopened without accessing the network. This parameter is turned "OFF" by default.

 ◆ **Lazy Close Directory Timeout:** Determines the time, in milliseconds, that Lazy Close will delay before closing a directory or volume handle.This parameter is set by default to 2000 milliseconds and has a valid range of 100-15000 milliseconds.

 ◆ **Lazy Close File Timeout:** Determines the time, in milliseconds, that Lazy Close will delay before closing a file handle.This parameter is set by default to 500 milliseconds and has a valid range of 100-15000 milliseconds.

NOTE: The Lazy Close File and Directory timeouts can be configured according to file access patterns to maximize performance improvements. Client workstations that predominantly access files exclusively can benefit from higher lazy close timeout values. On the other hand, client workstations with predominantly running applications that frequently access files shared for concurrent use by other workstations should consider lowering the timeout values or turning the Lazy Close feature OFF altogether.

 ◆ **Maximum Delayed Writes:** Controls the maximum amount of data, in megabytes, that will be allowed to queue for background writing when File Caching parameter is set to Read and Write. It is recommended to use a smaller value because setting larger values may impact available Windows kernel mode memory. Default value is set as 4MB.

 ◆ **NCP Encryption:** Determines the encryption capabilities between the server and the client. If this parameter is set to "Encryption preferred" and connected OES server supports encryption, then the Client establishes an encrypted connection with the OES server for all communications. If this parameter is set to "Non-encryption preferred", then the Client establishes a non-encrypted connection with the OES server for all its file communications unless the OES Server enforces encryption to all connected clients.

- **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).

- **Server Time Zone Configuration Cache Timeout:** Determines the time interval (in minutes) for which Client will cache the server time zone configuration for an NCP connection. After this time interval is over, Client queries the server again to determine the current time zone configuration. This refresh of the server's time zone configuration helps the Client workstation respond to Daylight Savings Time events or other time zone configuration changes that occur on the server. This parameter is set by default to 60 minutes and has a valid range of 1 to 720 minutes.

- **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 Client to determine if the server name is known to be a OES resource. If it is determined to be a OES 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 OES resources as though it might be a Windows server.
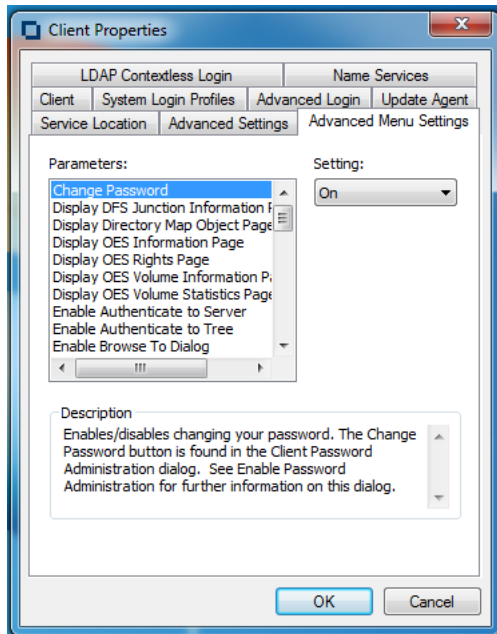
4.2.7 Advanced Menu Settings

Use the Advanced Menu Settings property page in the Client for Windows Properties dialog box to determine which options are available to users on the Client Application Tray menu when they right-click the ▢ 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 Client 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 OES 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 OES Information Page:** Display or hide the **OES Information** tab. The **OES Information** tab is found by selecting **Properties** from the context menu of a volume, directory, or file on a OES server.

- **Display OES Rights Page:** Display or hide the **OES Rights** tab. The **OES Rights** tab is found by selecting **Properties** from the context menu of a volume, directory, or file on a OES server.

- **Display OES Volume Information Page:** Display or hide the **OES Volume Information** tab. The **OES Volume Information** tab is found by selecting **Properties** from the context menu of a volume.

- **Display OES Volume Statistics Page:** Display or hide the **OES Volume Statistics** tab. The **OES 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 Client Tray 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 98.

◆ **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 *Client for Open Enterprise Server 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 **OES Utilities** menu item in the Client Application Tray 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 *Client for Open Enterprise Server 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 Client Tray 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 OES 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 OES 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 *Client for Open Enterprise Server 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 *Client for Open Enterprise Server 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 *Client for Open Enterprise Server User Guide* for more information on this menu.

◆ **Enable Client Help:** Enable or disables the Client help. This menu item is displayed in the context menu of the Client Tray icon.

◆ **Enable Client Properties:** Enables or disables viewing the Client property pages. This menu item is displayed in the context menu of the Client Tray icon.

- **Enable OES Connections Dialog:** Enables or disables the OES Connections dialog box. This menu item is displayed in the context menu of the Client Tray 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 OES Utilities:** Enables or disables the OES Utilities. This menu item is displayed in the context menu of the Client Tray icon.

- **Enable Object Properties Dialog:** Enables or disables the Object Properties dialog box. This menu item is displayed in the OES Utilities menu. See "Using OES Utilities" in the *Client for Open Enterprise Server 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 Client Application Tray 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 OES Utilities submenu on the Client Tray icon.

- **Enable Update Client:** Enables or disables the Update Client menu item. This menu item is displayed in the context menu of the Client Tray 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 OES 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 *Client for Open Enterprise Server User Guide* for more information on this menu.

- **Show Client System Tray Icon:** If this parameter is enabled, the Client Tray icon appears in the notification area of the taskbar, located in the bottom right portion of the Windows screen. Right-click the Client Tray icon to select from a list of 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 Client Properties dialog box to let users log in to the network without specifying a tree name or context For more detailed information, see Section 8.8, "Setting Up LDAP Contextless Login and LDAP Treeless Login," on page 124.

Figure 4-8 *LDAP Contextless Login Property Page*
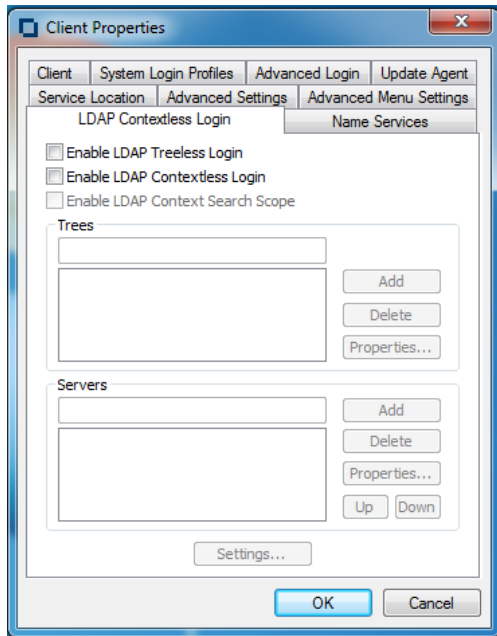

This page contains the following options:

- **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 Client Properties dialog box to specify which name service protocols are used to attempt to resolve names.

***Figure 4-9***   *Name Services Property Page*
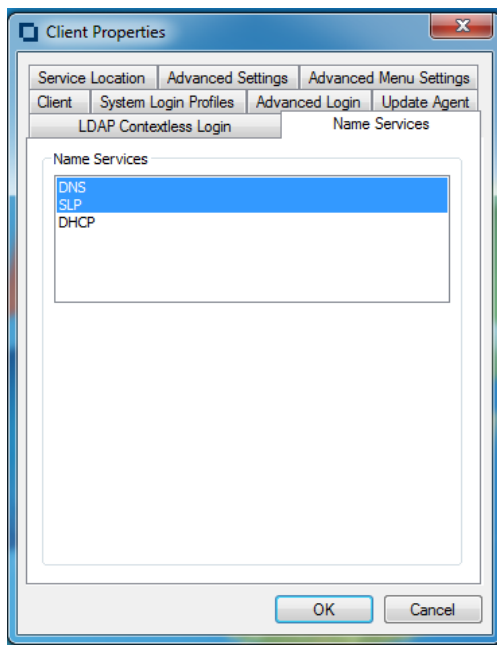
All configured name service providers are queried asynchronously in order to resolve the name to an address. They are first queried with a cache flag that allows name service providers (NSP) who maintain a cache to attempt to resolve the name. If no NSP resolves the name then they are queried again without the cache flag, allowing all NSPs to attempt to resolve the name. Service Location Protocol queries SLP for eDirectory and Bindery names.

4.3 Setting Properties on Multiple Workstations after Installation

You can use the 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 Client Properties dialog box (right-click the ▢ icon in the notification area of the taskbar > **Client Properties** > **Update Agent**).
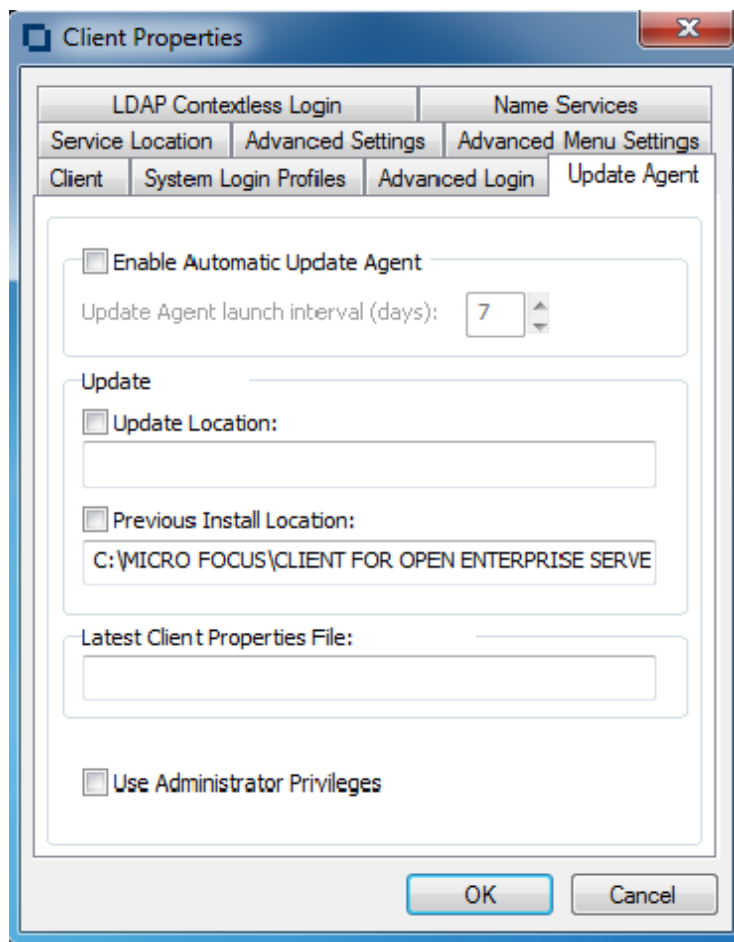
The Update Agent can be configured during installation or after installation by enabling it on each workstation.

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

See Section 2.2.1, "Creating the Client Properties File," on page 24 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 Client properties file is displayed in the **Last Client Properties File** field on the Update Agent property page.

5 Managing File Security

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 OES 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 *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 88. 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 87)
- Changing Trustee Rights (page 88)
- Combining Multiple Trustees (page 90)

5.1 Checking File or Folder Rights

1 In Windows explorer, right-click a OES file system directory or file.

2 Click **Properties**.

3 Click the **OES Rights** tab.
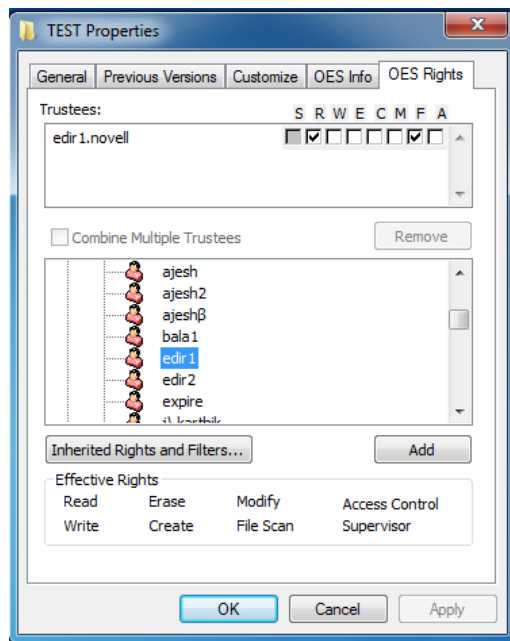
4 View the information.

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 (https://www.netiq.com/documentation/edir88/edir88/data/fbachifb.html) in the *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 appropriate right to change trustee assignments.

1 In Windows Explorer, right-click a OES file system directory or file.

2 Click **Properties**.

3 Click the OES 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.

  This right does not allow to add or remove the Supervisor right. Also, it does not allow to remove the trustee with the Supervisor right.

- **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 OES 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 file or directory that you want to add a trustee to.

2 Click Properties.

3 Click the OES 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.

  This right does not allow to add or remove the Supervisor right. Also, it does not allow to remove the trustee with the Supervisor right.

- **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 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 file or directory whose trustee you want to remove.

2 Click **Properties**.

3 Click the **OES 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 OES 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 files or directories that you want to combine rights for.
2 Right-click the files or directories, then click **Properties**.
3 Click the **OES Rights** tab.
4 Click **Combine Multiple Trustees**, then click **OK**.

6 Managing Passwords

Starting with NetWare 6.5 and eDirectory 8.7.3, Client 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) and "Managing Passwords by Using Password Policies" (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 Client for Open Enterprise Server 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) 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) 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) 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.

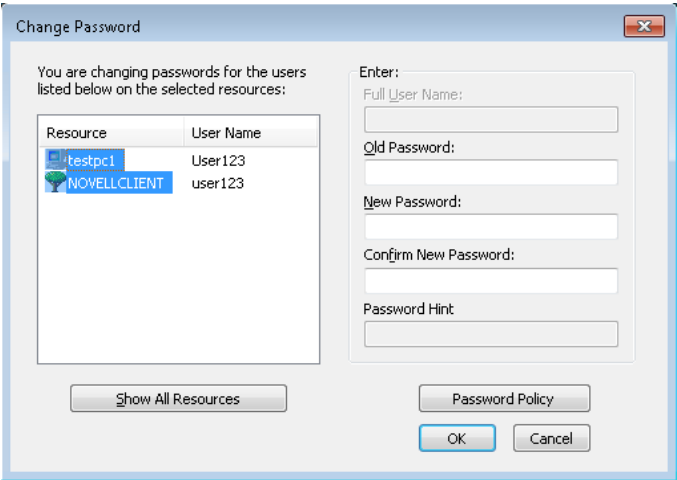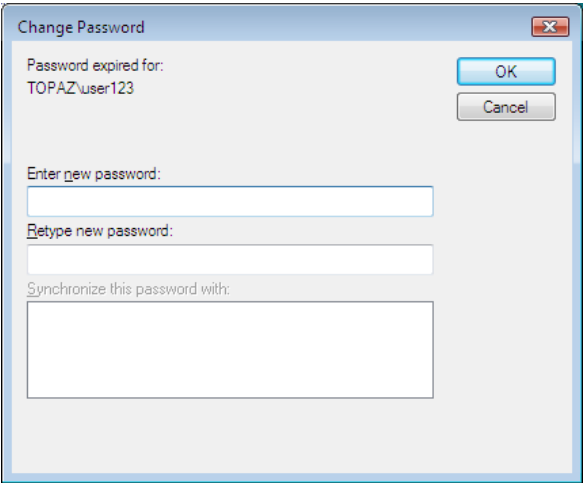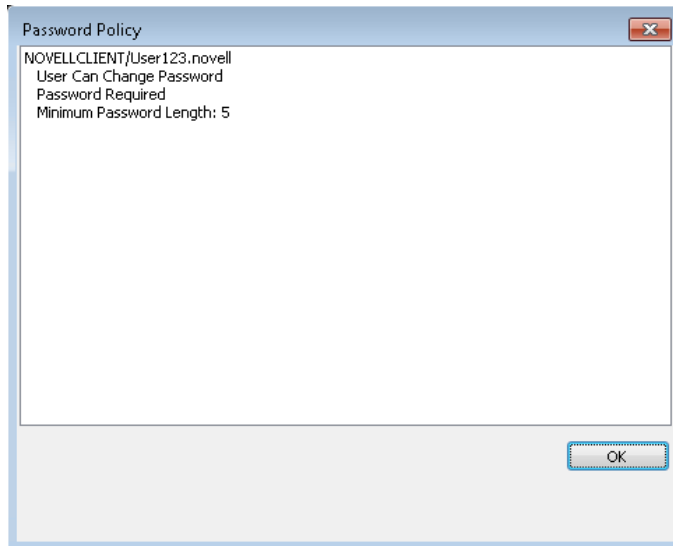*Figure 6-1* *Change Password Dialog Box*

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 *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 96
- "Using Hints for Remembering Passwords" on page 100

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) 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 Login dialog box, the system invokes the Forgotten Password Policy specific to the user. The following three options are supported by the Client:

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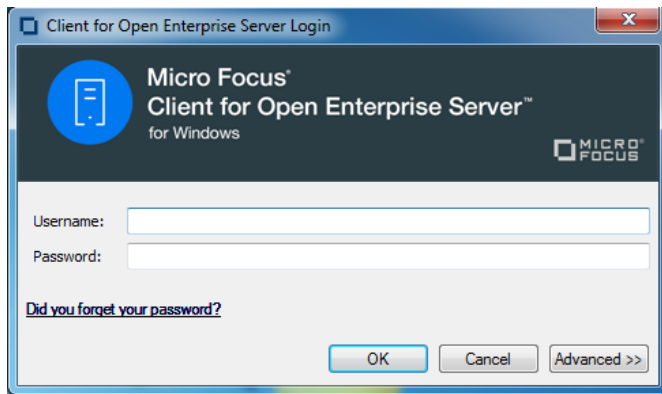- Authenticate via Challenge/Response and reset the password.

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

Figure 6-4 *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 Login dialog box.

1 Right-click the Client Tray icon, then click **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 97

❒ "Configuring Challenge/Response Settings" on page 98

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 Client at this time, including e-mailing passwords and hints.
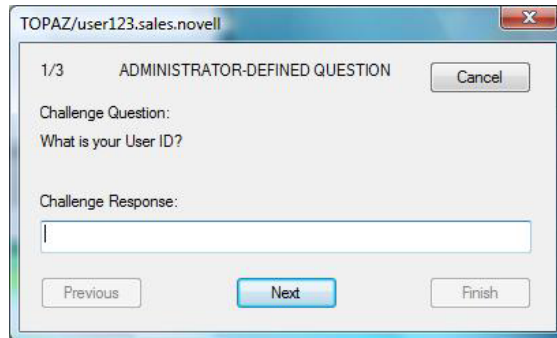
Configuring Password Self-Service

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 Client Tray icon (▢), 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 Client does provide a way to reset the answers. Right-click □, 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
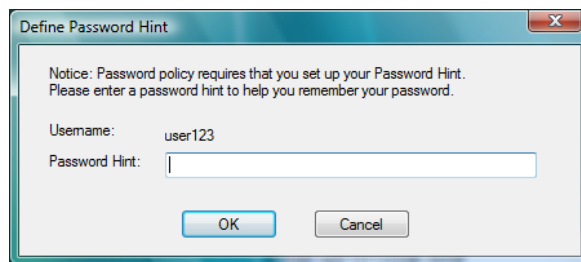
If a user clicks the **Did you forget your password?** link in the Login dialog box, the user is asked to answer their challenge questions. When the series of challenge questions is answered correctly, a dialog box containing the password hint is displayed.

Figure 6-8   Forgotten Password Hint Dialog Box
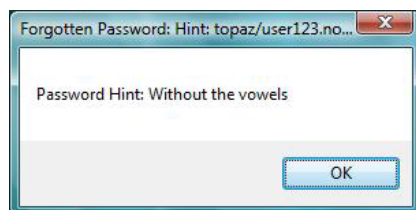
If a user enters an erroneous password, the login program displays a message with a prompt to retype the password or click the **Did you forget your password?** link.

Figure 6-9 *Password Error Dialog Box*
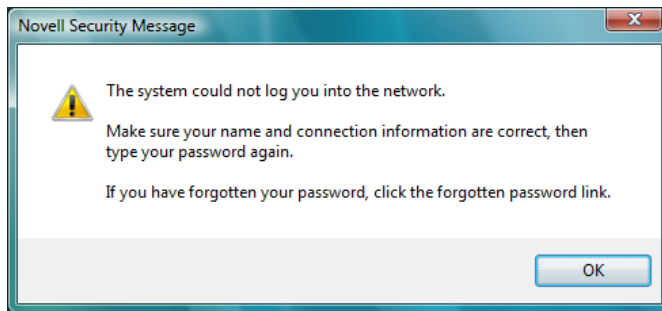
If the policy action is to show a hint but the user did not enter a hint for the current password, an error message is displayed telling the user to contact the system administrator to reset the password and to enter a hint the next time the password is set.

Figure 6-10 *Forgotten Password Error Dialog Box*
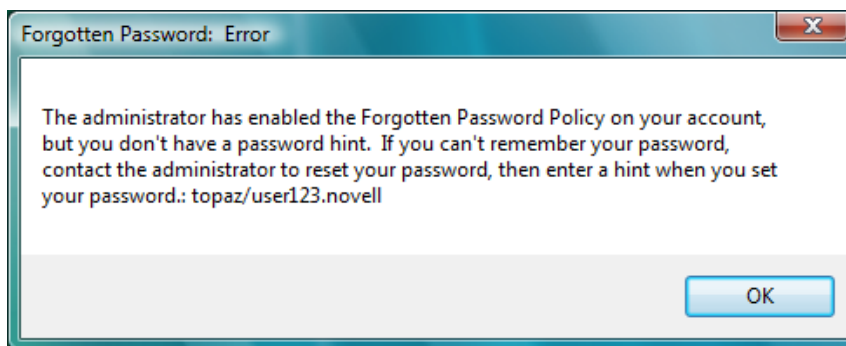
Users can also create a hint at any time using the Change Password window available at login, or by pressing Ctrl+Alt+Delete, then clicking **Change Password**.

Figure 6-11 *Change Password Dialog Box*
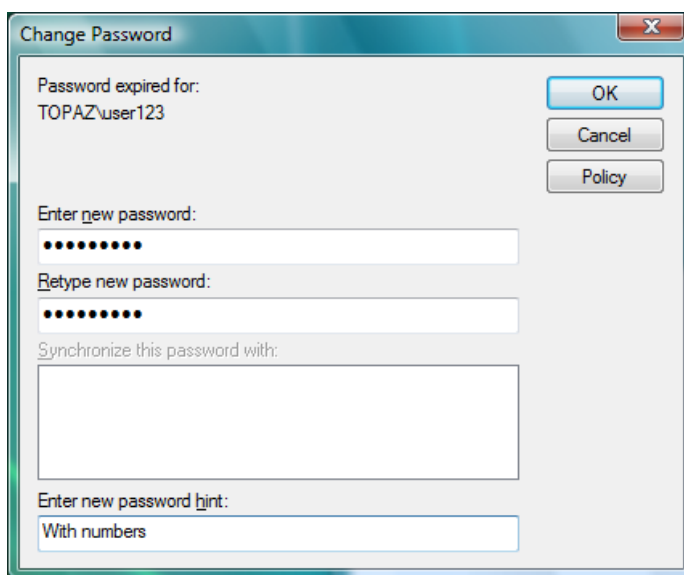
6.4 Setting Up Passwords in Windows

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

7 Security Considerations

This section contains the following topics:.

7.1 Security Features

The following table contains a summary of the Client for Open Enterprise Server security features:

Table 7-1 *Client 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.

Feature	Yes/No	Details
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 Client, 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

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.

8 Managing Login

You can customize the Client login environment to suit your network and have greater control over what users can access during login.

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 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 93.

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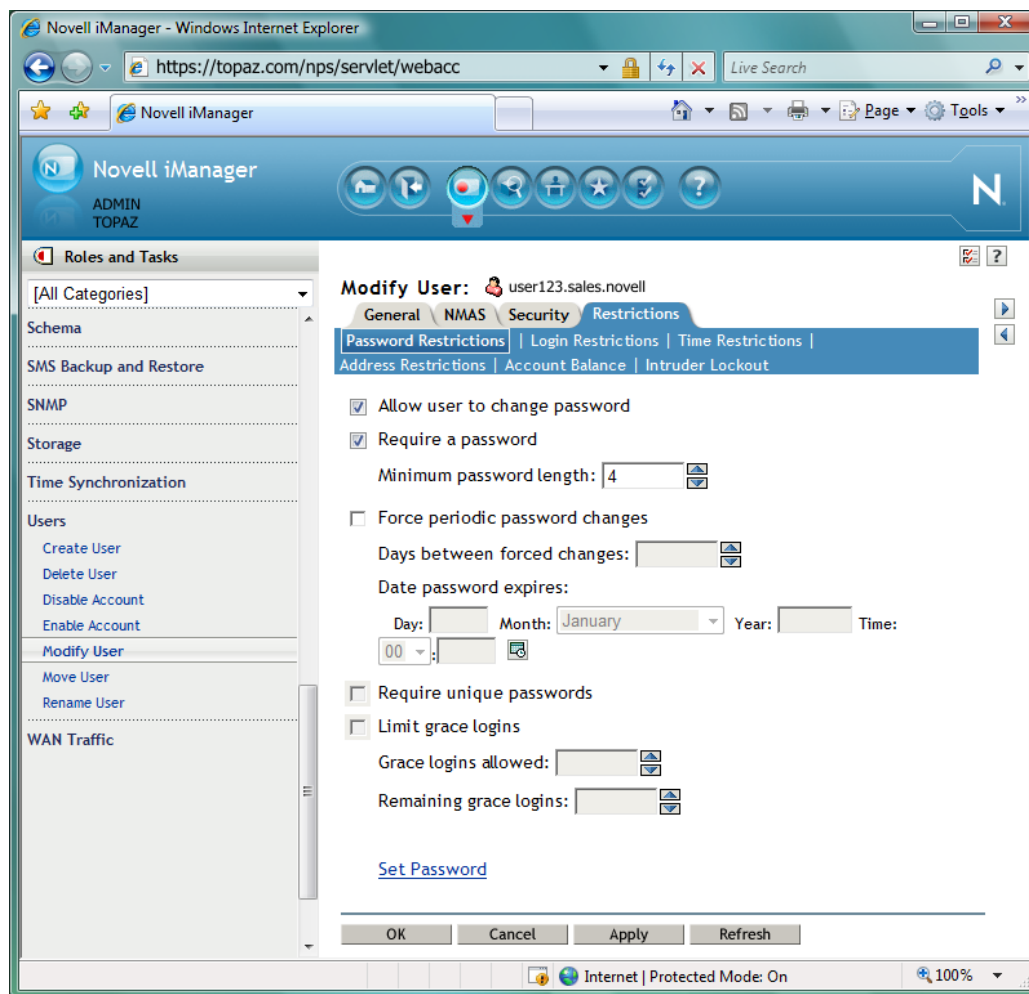
The following options appear. They open pages that display various properties:

- 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 Client Login

The 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 25 for more information.

- 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 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 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 96 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 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 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 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 Client Tray icon (⬛) in the notification area of the taskbar, then click **Client Properties**.

2 Click **Advanced Login**.

3 Select **Show on Login** in the **Parameter groups** drop-down list.
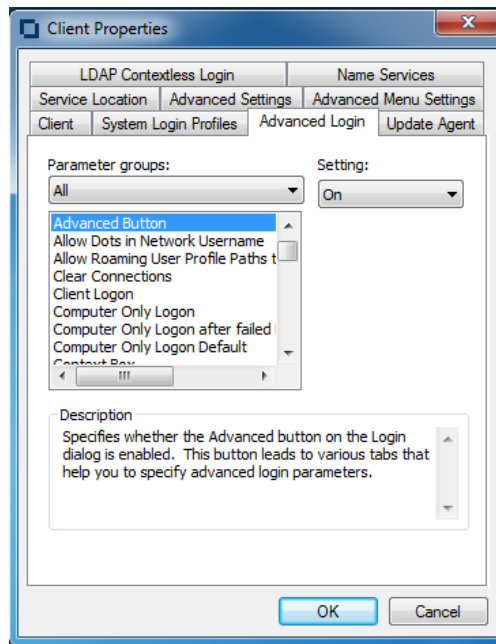
4 Select the parameter you want, then select **On** or **Off** in the **Setting** drop-down list.

   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 69.

5 Click **OK**.

8.4 Setting Up the Computer Only Logon If Not Connected Feature

This feature allows the Client to automatically select performing a **Computer Only Logon** when the available network connectivity fails to meet specific criteria, or when simply no network connectivity is available at all.

The **Workstation Only If Not Connected** option in the Novell Client for Windows XP/2003 functioned purely on "Does Windows know of one or more active network interfaces?" to decide whether or not to automatically select the **Workstation Only** login option. While this approach was useful in many cases, scenarios where the workstation was still connected to a network over which the eDirectory servers were not accessible (such as a home broadband network) could prevent the feature from engaging. The fact this feature decided to enable or disable the **Workstation Only** option before any logon attempt occurred could also be a limitation, if Windows was still in the process of starting up and more Windows network interfaces arrived after **Workstation Only if Not Connected** had already made its decision.

The Client for Windows **Computer Only Logon If Not Connected** feature, when enabled, improves upon both of these points. Instead of any Windows network interface, it is now possible to specify specific Windows network categories (for example, Work, Home, and Public) for which a **Computer Only Logon** is preferred. Additionally, specific names assigned to Windows networks (for example, Network 1, Network 2, My Office, and so on) can be specified for more granular control.

Finally, the **Computer Only Logon If Not Connected** feature does not make its decision about whether to proceed with a Logon or automatically switch to **Computer Only Logon** until the user actually initiates a logon attempt. Thereby permitting the maximum time possible for additional network interfaces to arrive or be detected before the feature makes its decision.

The **Computer Only Logon If Not Connected** feature, when enabled, also maintains the basic "if no Windows network interfaces are available, perform a Computer Only Logon instead of Logon" functionality. This functionality can be used even without having to specify any Windows network names or categories.

At the next available opportunity, the Client will add configuration of the **Computer Only Logon If Not Connected** feature into the Client Properties configuration interface. Until then, this feature can be enabled by directly editing the described registry configuration.

8.4.1 Enabling the Computer Only Logon If Not Connected Feature

1. Log on to the Windows machine with administrative privileges.

2. Edit the registry and navigate to the existing
   `\HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login\` key.

3. Create a subkey named **Computer Only Logon If Not Connected**, such that a key path of
   `\HKEY_LOCAL_MACHINE\Software\Novell\Login\Computer Only Logon If Not Connected\` now exists.

4. Under the **Computer Only Logon If Not Connected** key, create the following entries:

   - A DWORD (32-bit) value named **Enable**. If the value of this entry is set to 1, the **Computer Only Logon If Not Connected** feature is enabled. If this value does not exist or is set to 0 (zero), the feature is disabled.

   - Optionally, create a Multi-String (not String) value named **Network Category List**. This Multi-String can be set to one or more of the following values, which correspond to the names Windows uses to describe network categories: **Home**, **Work** and **Public**.

   - Optionally, create a Multi-String named **Network Name List**. This Multi-String can contain a list of one or more names that have been assigned to networks identified by Windows. For example, **Network 1**, **Network 2**, **My-Residence**, **My-Office** and so on.

   - Optionally, create a DWORD(32 bit) value named **Use Lists for Novell Logon**. If the value of this entry is set to 1, the **Network Catrgory List** and **Network Name List** values will be interpreted as criteria for networks which CAN access eDirectory servers, and when networks matching these criteria are present the Client should attempt a normal Logon. If the Use Lists for Novell Logon value does not exist or is set to 0 (zero), the **Network Category List** and **Network Name List** values will be interpreted as criteria for networks which CAN NOT access eDirectory servers, and if all connected networks match this criteria the Client should skip the eDirectory login attempt and proceed immediately with a Computer Only Logon instead. Continue reading the description below of the **Network Category List** and **Network Name List** values for additional explanation.

The **Computer Only Logon If Not Connected** feature takes effect when the **Enable** value is set to 1, even if the **Network Category List** or **Network Name List** values are not defined. When the **Computer Only Logon If Not Connected** feature is enabled, at minimum the Client will automatically perform a Computer Only Logon instead of a Logon if Windows reports there are not any active network interfaces when the logon attempt is initiated.

If the **Network Category List** is defined, the Client will query Windows to determine what category each identified network belongs to (**Work**, **Home**, or **Public**). When the **Use Lists for Novell Logon** value does not exist or is set to 0 (zero), the **Network Category List** names which Windows network categories the **Computer Only Logon If Not Connected** feature should assume CAN NOT access eDirectory servers, and assumes any non-matching connected networks CAN access eDirectory servers. When the **Use Lists for Novell Logon** value is set to 1, the N**etwork Category List** names which Windows network categories the **Computer Only Logon If Not Connected** feature should assume CAN access eDirectory servers, and assumes any non-matching connected networks CAN NOT access eDirectory servers.

If the **Network Name List** is defined, the Client first performs the **Network Category List** processing described above if the **Network Category List** is defined. After matching the active network categories against the **Network Category List**, the Client will additionally match the network names against the **Network Category List**. When the **Use Lists for Novell Logon** value does not exist or is set to 0 (zero), the **Network Category List** names individual Windows networks the **Computer Only Logon If Not Connected** feature should assume CAN NOT access eDirectory servers, regardless of what Windows network category the named networks belong to. When the **Use Lists for Novell Logon** value is set to 1, the **Network Category List** names individual Windows networks the **Computer Only Logon If Not Connected** feature should assume CAN access eDirectory servers, regardless of what Windows network category the named networks belong to.

After completing both the **Network Category List** processing (if defined) and the **Network Name List** processing (if defined), and after considering the meaning of those lists in relation to the **Use Lists for Novell Logon** value (if defined), if the **Computer Only Logon If Not Connected** feature has ultimately

determined there is ONE OR MORE connected networks which CAN access eDirectory servers, a Logon attempt will be permitted to proceed normally and attempt an eDirectory login. If the **Computer Only Logon If Not Connected** feature ultimately determined that ALL of the connected networks CAN NOT access eDirectory servers, a Logon attempt will skip the eDirectory login attempt and proceed immediately with a Computer Only Logon instead.

For example, assume the **Network Category List** has been configured with **Home** and **Public**, and the **Network Name List** has been configured with **RemoteOffice**, and the **Use Lists for Novell Logon** value does not exist or is set to 0 (zero). During the next logon attempt, Windows reports a **Public** network and also a **Work** network named **RemoteOffice**. Even though based on the **Network Category List** alone a Logon would have been permitted to attempt eDirectory login due to presence of the **Work** category network, because the **Work** network is named **RemoteOffice** and this network name appears in the **Network Name List**, the Client will actually consider that none of the active networks detected by Windows can access eDirectory servers. Attempting a Logon would result in the Client skipping the eDirectory login attempt and would proceed with a Computer Only Logon instead.

8.4.2 Using the Computer Only Logon If Not Connected Feature

1. Logout of Windows, or reboot the machine.

2. Select the **Logon** link on the Windows logon page, if the Client login is not already in **Logon** mode. If **Computer Only Logon** mode is explicitly selected, the **Computer Only Logon If Not Connected** feature does not need to engage.

   NOTE: By default, the Client remembers whether **Logon** or **Computer Only Logon** was last used, and will default to that mode during the next logon. If you want the Client to always come up in **Logon** mode and then just let the **Computer Only Logon If Not Connected** automatically decide whether a Logon attempt is actually appropriate, change the **Computer Only Logon Default** setting from **Automatic** to **Never** in the **Advanced Login** tab of the Client Properties.

   ---

3. Now attempt to logon in Logon mode. Once you enter your password and click **Submit**, the Client will begin the **Computer Only Logon If Not Connected** processing of querying Windows for connected network names and categories, and matching those names and categories again any configured **Network Category List** and **Network Name List** values.

4. If the Client determines there are one or more active Windows networks present over which a Logon attempt will be appropriate, the Client will simply proceed with normal Logon processing of attempting to login to both eDirectory and the Windows account.

5. If the Client determines that all of the active Windows networks match criteria indicating that cannot access eDirectory servers, or if Windows reports there simply are not any active Windows networks, even though the Client was in Logon mode when the logon attempt was initiated, the eDirectory login will be transparently skipped, and only the Windows account logon attempt will be made.

6. Note in cases where the Windows account password is not the same as the eDirectory account password – for example, because the Windows account password was normally supplied from a Novell ZENworks Dynamic Local User (DLU) policy, or the password was expected to be

retrieved by NMAS-based Single Sign-On – the Windows-only account logon attempted by **Computer Only Logon If Not Connected** will not be able to succeed using the eDirectory password.

In this case, the Client will still skip the eDirectory logon attempt and will perform just a Computer Only Logon, but the user will have to manually enter their Windows account password. This is only an issue in cases which otherwise would have retrieved their Windows account passed from eDirectory-based sources.

8.5 Logging In to the Network

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

* Right-click the Client Tray icon (▢) in the notification area of the taskbar, then click **OES Login**.
* In the Network folder, double-click the desired tree or server.
* In the Network folder, right-click the desired 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 startup folder.

    This causes the Client Login to run automatically at workstation startup and shows the Login screen when Windows first opens.

8.6 Logging Out of the Network

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

If you want to log out of both the Windows workstation and server, 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 Client Tray menu, click **OES Connections**, select the server or tree, and then click **Detach**.

8.7 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.

System Login Profiles and User Login Profiles

The Client supports "system login profiles", which are created and managed by an administrator. System login profiles allow an administrator to provide the defaults for login even to new users who have never logged on from the current Windows machine. System login profiles may also be created by an administrator using the Client Install Manager (NCIMAN.EXE) so that they will be created automatically during the Client installation. For more information, see Section 8.7.2, "Creating a System Login Profile for Use on Multiple Workstations," on page 120".

The Client also supports "user login profiles", which can be created and managed by the user. In many cases, a user login profile is created automatically for the user in response to the **Save profile after successful login** setting in a system login profile. The user can also directly create and edit their user login profiles from the **Login Profile Administration** option in the Client Tray menu. For more information, see "Managing Your Login Profiles" in the Client for Open Enterprise Server User Guide.

When a login profile exists both as a system login profile and also as a user login profile, the user login profile takes precedence so that any user-specific details necessary for the user to successfully login will be used. For example, the administrator may have created a system login profile named "Default" that specifies the eDirectory tree name and a specific default eDirectory context. But the user may need to specify a more specific eDirectory context in order to successfully log on to eDirectory, different from the eDirectory context that the administrator specified in the system login profile.

The user's eDirectory context selection will be saved as part of a user login profile named "Default". Such that now a user login profile named "Default" exists for this user, in addition to the system login profile named "Default" created by the administrator. As the user login profile takes precedence, during future Client logins the eDirectory context and other login defaults will be correctly remembered for the user. As the user login profiles specific to this user, it will be loaded as soon as their username is entered into the "Username" field of the Client login.

If a user chooses to delete their user login profile, and a system login profile exists with the same name, the login profile will revert to the administrator-defined system login profile settings. Only an administrator can delete or change the properties of a system login profile. The user can only create and manage their own user login profile of the same name (which was initially based on the administrator defined system login profile), or the user can create their own additional login profiles completely independent of any system login profile.

You can edit system profiles (and only system profiles) on the **System Login Profiles** tab in the Client Properties dialog box (right-click the Client Tray icon in the notification area of the taskbar, click **Client Properties**, then click the **System Login Profiles** tab).

Figure 8-1 *System Login Profiles*
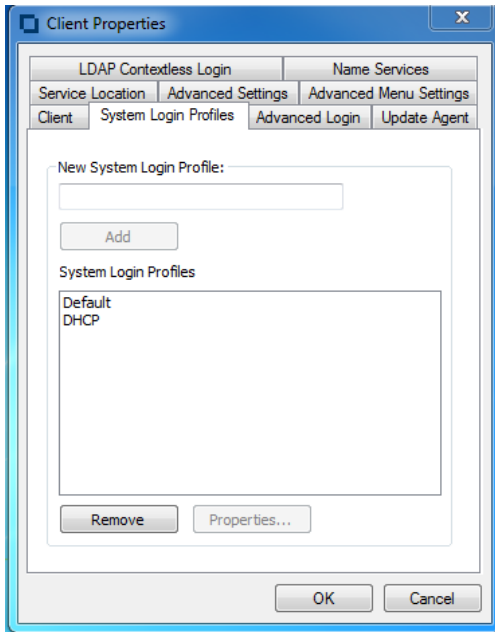
When you edit user profiles (right-click the Client Tray icon in the notification area of the taskbar, click **User Administration for**, then click **Login Profile Administration**), you will see both system profiles and user profiles in the list of profiles. Whether a profile name listed in the Login Profile Administration list happens to be a system login profile or user login profile should not be important. Both the Login Profile Administration list and the "Login Profile" selection list (if any) on the Client login dialog simply intends to present the list of selectable login profile names, regardless of whether they happen to be system login profiles or user login profiles.

Figure 8-2 *User Login Profiles*
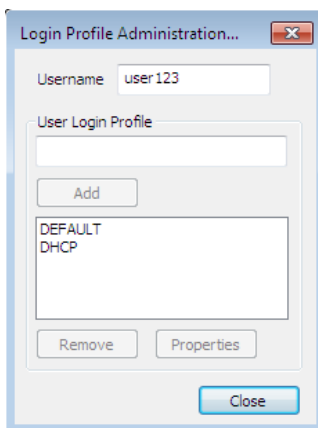

You can initiate editing any profile presented in the Login Profile Administration list regardless of whether it happens to be a system login profile or a user login profile. Editing a user login profile will modify the profile directly, whereas if the profile selected for editing happens to be a system profile, any changes made during editing will be saved as a user login profile.

Using Login Profiles During Login

When users log in using the 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 Client Properties dialog box to specify if the Login Profile drop-down list is available or not.

By default the Client displays the Login Profile list "automatically", which means that the Login Profile list is automatically enabled whenever there is more than one login profile the user might potentially be able to choose. If there is only one login profile available, then the Login Profile list will not be shown since no alternate login profile selection can be made.

Figure 8-3 *Login Dialog Box with the "office" Login Profile Selected*
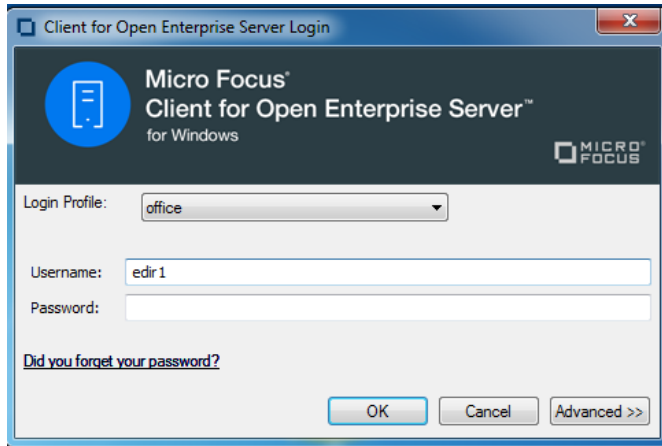

If you login with a system login profile which has the "Save profile on successful login" enabled, or if you explicitly attempt to edit the system login profile from the Login Profile Administration dialog, a user login profile is automatically created with the same name as the system login profile. During future logins or login profile editing actions, this user login profile will take precedence and be used or edited instead of the system login profile.

- Section 8.7.1, "Creating a System Login Profile," on page 118
- Section 8.7.2, "Creating a System Login Profile for Use on Multiple Workstations," on page 120
- Section 8.7.3, "Viewing or Editing a System Login Profile's Properties," on page 122
- Section 8.7.4, "Removing a System Login Profile," on page 122
- Section 8.7.5, "Enabling the Use of DHCP In a System Login Profile," on page 122

For information on creating and editing user login profiles, see "Managing Your Login Profiles" in the *Client for Open Enterprise Server User Guide.*

8.7.1   Creating a System Login Profile

1 Right-click the Client Tray icon (▢) in the notification area of the taskbar.

2 Click **Client Properties**, then click the **System Login Profiles** tab.
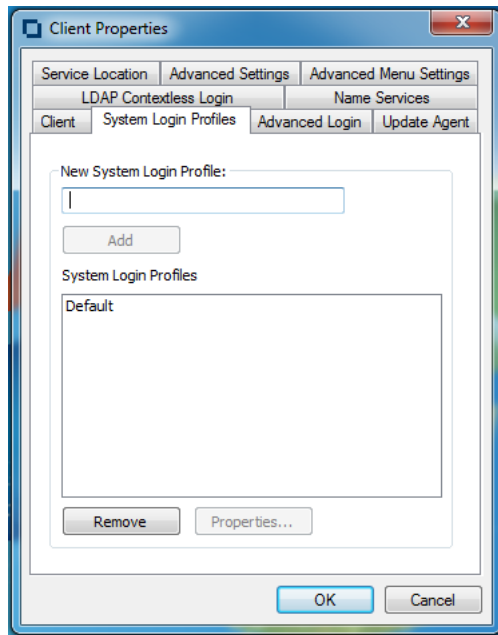
3 Type the name of the profile you want to add in the **New System Login Profile** text box, then click **Add**.

You can give a system login profile the same name as a user login profile, but be aware that during login if a user already has a user login profile with the name, the user login profile will be used because user profiles always supersede system profiles when they have the same name.

4 In the Login dialog box, specify the login information you want for this profile, such as a tree, context, and server.
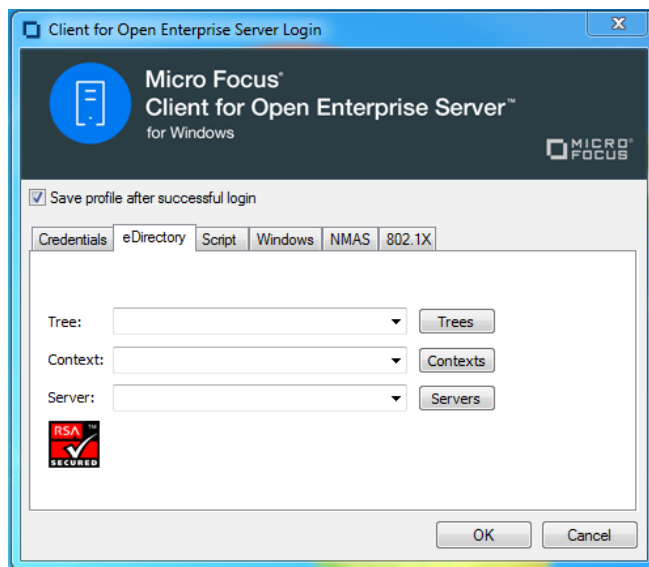
5 Click **OK** to close the Login dialog box, then click **OK** to close the Client Properties dialog box.

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

Figure 8-4   *Login Dialog Box with a System Login Profile Selected*
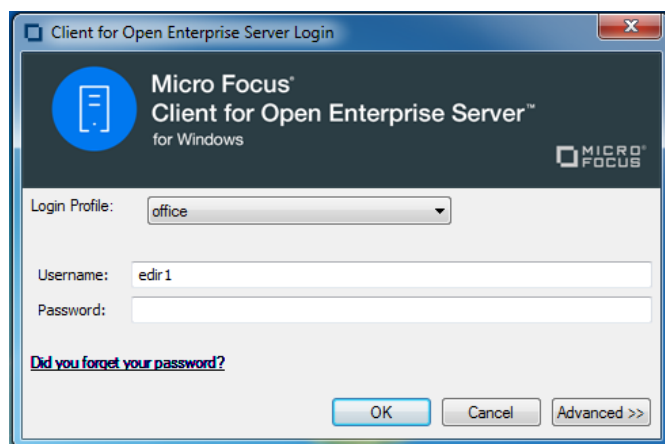
8.7.2   Creating a System Login Profile for Use on Multiple Workstations

Login Profiles are one of many settings that can be predefined by using a Client properties file that is applied during installation of the Client. For more information, see "Creating the Client Properties File" on page 24.

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

1 Start the Client Install Manager (`nciman.exe`), located in the `C:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)\Admin` folder.

2 In the **Client for Windows Properties** box, double-click **Client** to open the 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**.
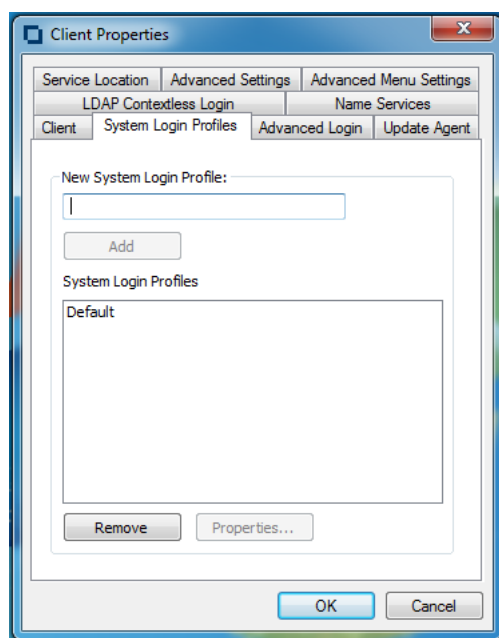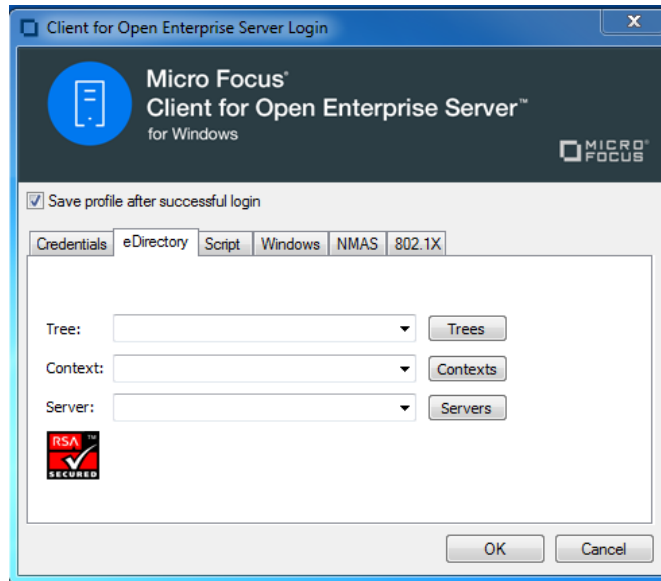
To create the Default system profile, enter `Default` as the new profile name.

4 In the 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 Login dialog box, then click **OK** to close the Client Properties dialog box.

A parameter for the login profile you just created appears in the **Parameter** list in the Client Install Manager.
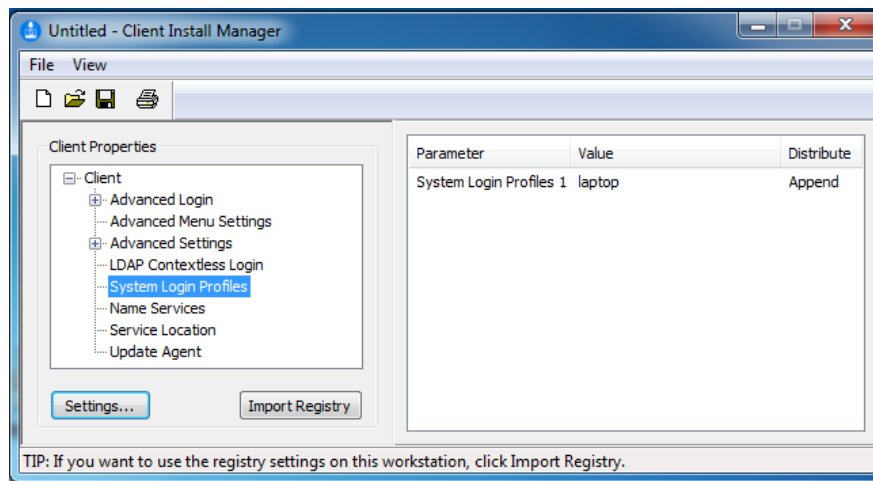
6 Right-click the system login profile parameter, then click **Distribute (Append)**.

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 Client Properties File" on page 24.

9 Click **File > Save**, then specify a name for the 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:\Micro Focus\Client for Open Enterprise Server 2 SP4 (IR3)`).

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 19.

8.7.3 Viewing or Editing a System Login Profile's Properties

1 Right-click the ⬜ icon in the notification area of the taskbar.

2 Click **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 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 Login dialog box, then click **OK** to close the Client Properties dialog box.

8.7.4 Removing a System Login Profile

1 Right-click the ⬜ icon in the notification area of the taskbar.

2 Click **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 Client Properties dialog box.

8.7.5 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 Client of network-specific configuration information.

You can easily configure OES 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_dnsdhcp_lx/?page=/documentation/oes2/ntwk_dnsdhcp_lx/data/bookinfo.html#bookinfo) 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 Client Properties dialog box. Using information from DHCP in the Client 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 ◻ icon in the notification area of the taskbar.

2 Click **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 Client Tray menu. See "Enabling the Use of DHCP In a Personal Login Profile" in the *Client for Windows 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.
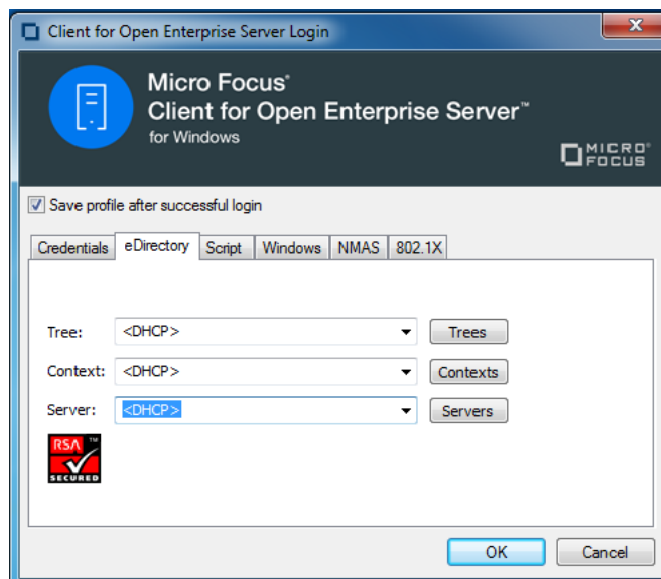
5 Click **OK** twice.

The next time a user opens the 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 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 fo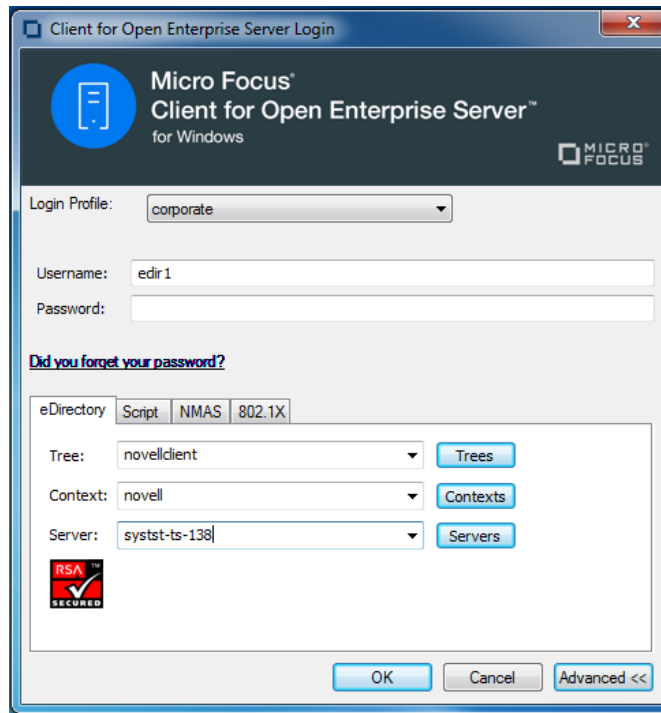r Tree, Context, or Server, it cannot be removed by simply editing the field when logging in or by saving the profile on successful login. Any values entered in these fields during login are not saved when **<DHCP>** is enabled for that field. If users want to permanently change the values in that field, they must edit the login profile using either the System Profile Manager (**System Login Profiles** tab on the Client Properties dialog box) or the User Profile Manager (**Login Profile Administration** option on the Client Tray menu).

8.8 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 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 eDirectory is a server application that lets LDAP clients access information stored in eDirectory.

If your network has LDAP Services for eDirectory set up on your eDirectory tree and you are running 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 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.

Generally, when a user connects to the network using LDAP, the connection is made through an LDAP client. Now, the Client Login acts as an LDAP client and connects to the network. All LDAP clients bind (connect) to 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 eDirectory, see "Understanding How LDAP Works with eDirectory" (https://www.netiq.com/documentation/edir88/edir88/data/h0000007.html) in the *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 LDAP Services for eDirectory.

  See "Setting Up LDAP Services for eDirectory" on page 126.

2 Do one of the following:

- If you are installing Client software on a few workstations, install the software and then configure the 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 129.

- If you are installing 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 131). Then install the Client software.

3 Inform users about contextless login.

See "Logging In Using LDAP Contextless Login" on page 131.

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.

8.8.1 Setting Up LDAP Services for eDirectory

Before users can take advantage of LDAP Contextless Login, the network must be running 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 eDirectory" (https://www.netiq.com/documentation/edir88/edir88/data/a4wyf4a.html) and "Configuring LDAP Services for eDirectory" (https://www.netiq.com/documentation/edir88/edir88/data/ahlmb7h.html) in the *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 126.

- Create a Proxy User Object that has the correct rights. See "Connecting As a Proxy User" on page 127.

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 127.

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" (https://www.netiq.com/documentation/edir88/edir88/data/agq8auc.html) in the *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**.

8.8.2   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 131.

1 At the user's workstation, right-click the Client Tray icon (▢) in the notification area of the taskbar, then click **Client Properties**.

2 Click the **LDAP Contextless Login** tab.
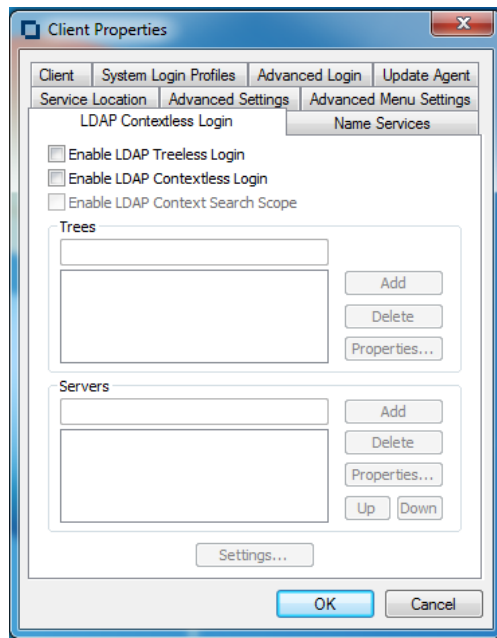
3 Do one of the following:

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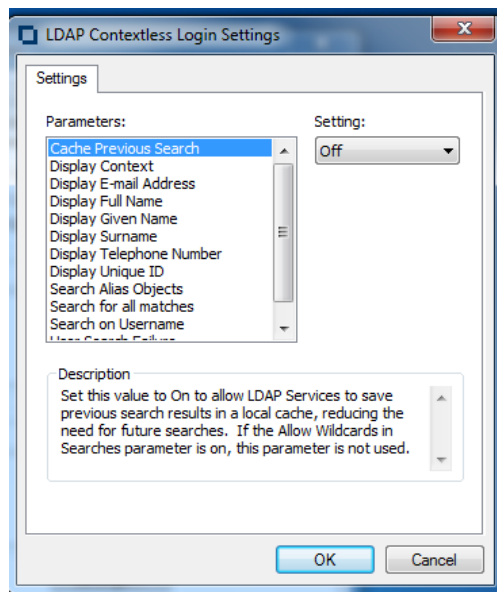
Select the parameter you want, then use the **Setting** drop-down menu to turn the parameter On or Off. A short description of each parameter is available in the **Description** field when you select the parameter.

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

8.8.3 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 65 and Section 4.3, "Setting Properties on Multiple Workstations after Installation," on page 84.

8.8.4 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 Login dialog box when the username is found.

The 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 Client has been enabled, either in a treeless or tree-specific mode.

8.8.5 LDAP Contextless Login Differences between Client for Open Enterprise Server and Novell Client for Windows XP/2003

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

 ◆ When invoking **Show Advanced Options** from the credential provider (the login dialog box seen at boot time and when logging out of Windows), 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 **Login** option from the Client Tray 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 Client for Open Enterprise Server release.

 ◆ Wildcard based search is disabled in Client for Open Enterprise.

8.9 Configuring 802.1X Authentication

The Client includes an Extensible Authentication Protocol (EAP) plug-in to the Microsoft Windows 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 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 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 Client 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 Client-specific EAP support is required.

The ability to browse for trees and servers in the 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 8.9.1, "Enabling 802.1X Authentication," on page 132
- Section 8.9.2, "Enabling Wired 802.1X Authentication on Windows10, Windows 8, and Windows 7," on page 134

8.9.1 Enabling 802.1X Authentication

1 Right-click the Client Tray icon () in the notification area of the taskbar, then click **Client Properties**.

2 In the 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**.
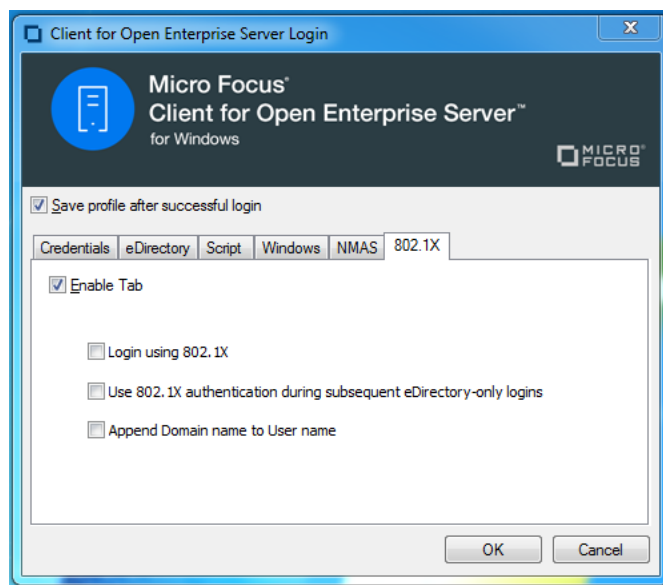
6 Select **Login using 802.1X**.

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 Client Tray icon, 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.
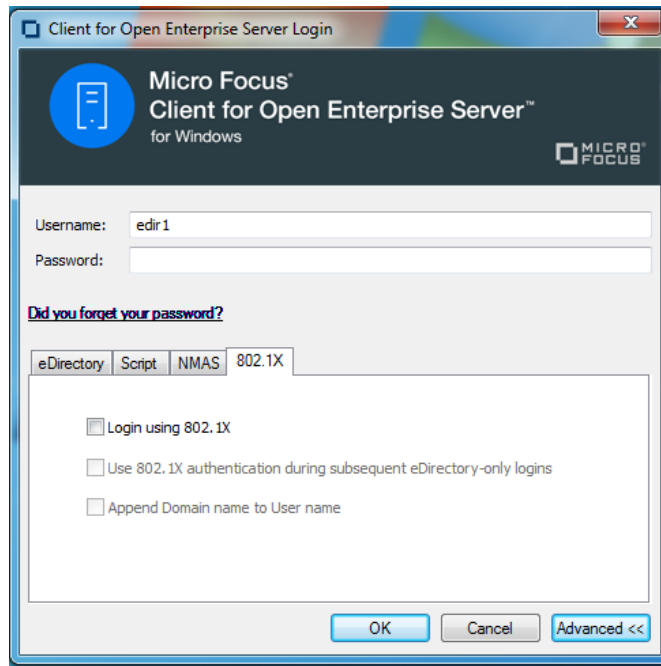
NOTE: Contextless login runs after you click **OK**.

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 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.


8.9.2 Enabling Wired 802.1X Authentication on Windows10, Windows 8, and Windows 7

To enabled wired 802.1x authentication on Windows, 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 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**.
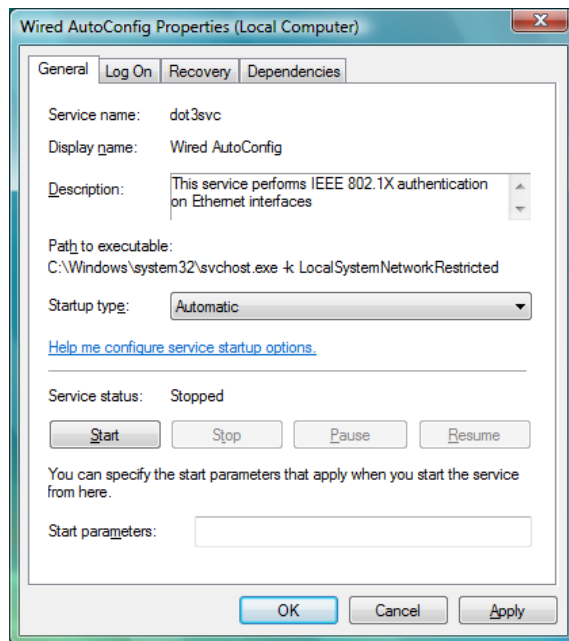
5 Click the **Start** button under **Service status**, then click **OK**.

6 Close the **Services** and **Administrative Tools** windows.

7 In the Windows 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.
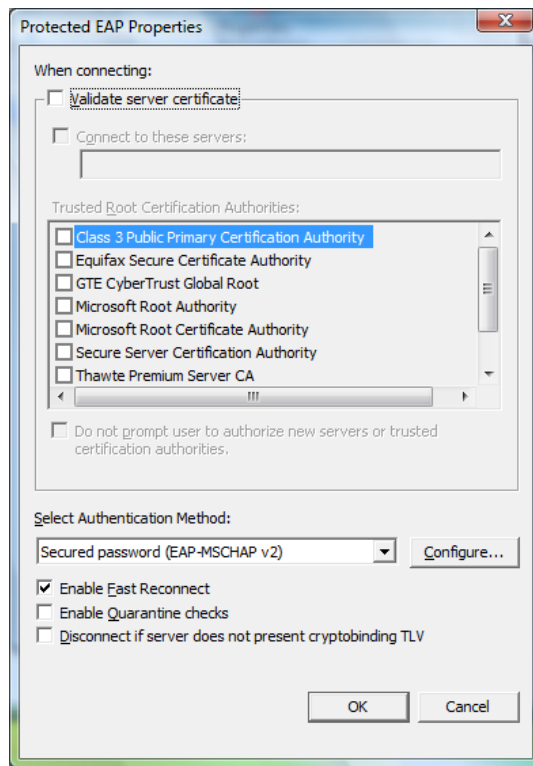
12 Click **OK** twice.

13 Close the Network Connections window.

8.10 Enabling AutoAdminLogon

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

8.10.1 Enabling a Windows-Only AutoAdminLogon

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**.
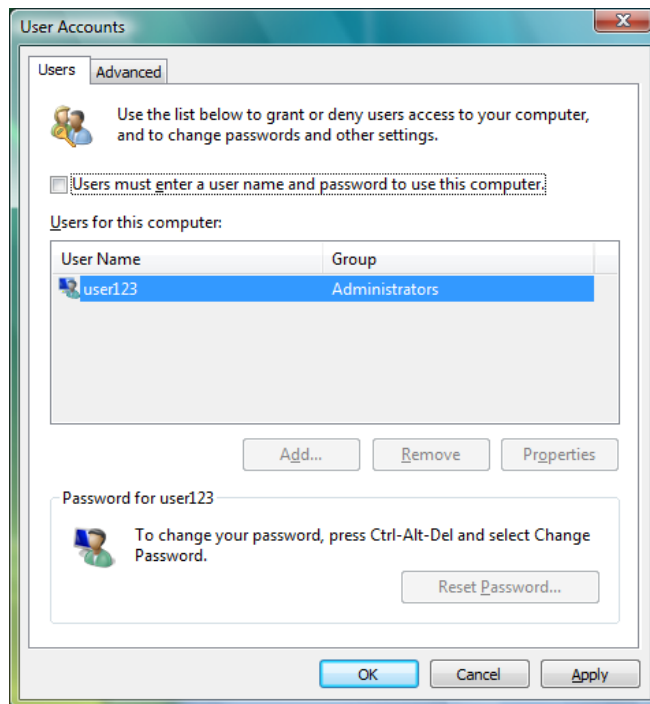
5 Click **OK**.

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.

8.10.2 Configuring Windows-Only AutoAdminLogon Through Registry

The autoadminlogon configuration information can also be added/modified by writing directly to the registry.

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\Microsoft\Windows NT\CurrentVersion\Winlogon`, then modify or add the following parameters:

```
Value Type=REG_SZ, Name=DefaultUserName, Data=User Name
Value Type=REG_SZ, Name=DefaultPassword, Data=user Password
Value Type=REG_SZ, Name=DefaultDomainName, Data=DomainName (Optional)
```

NOTE

- If you do not specify a domain name, Client attempts to log on to the Local Machine.

- Manually writing DefaultPassword key into the registry makes it visible to all users who have registry access.

8.10.3   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=DefaultLoginProfile, Data=`*`name of profile to use`*

  if you need the same login profile for both eDirectory AutoAdminLogon and TSClientAutoAdminLogon.

  or

  `Value Type=REG_SZ, Name=AutoAdminDefaultLoginProfile, Data=`*`name of profile to use`*

  if you need to specify a unique profile name for eDirectory AutoAdminLogon, which is different from the TSClientAutoAdminLogon default profile name.

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

NOTE:

- If either DefaultLoginProfile or AutoAdminDefaultLoginProfie is not provided, the Default profile for the eDirectory username is used for the eDirectory AutoAdminLogon.

- 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.

- Once Windows AutoAdminlogon is configured, it will work with or without having the eDirectory AutoAdminLogon configured or enabled.

- eDirectory AutoAdminLogon, even if configured, will work only if Windows AutoAdminlogon is configured and enabled.

---

4 Close the Registry Editor.

8.11   Enabling TSClientAutoAdminLogon

Normally, without the Client 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 Client 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 Windows account logon using these credentials provided from the terminal client, the Windows account username and Windows account password will "merged" with a specified 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 2012 Terminal Services coniigurations, the TSClientAutoAdminLogon policy also has the same operational behavior for Remote Desktop usage on Windows 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 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.

8.11.1 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`*

   if you need the same login profile for both eDirectory AutoAdminLogon and TSClientAutoAdminLogon.

   or

   `Value Type=REG_SZ, Name=TSClientDefaultLoginProfile, Data=`*`name of profile to use`*

   if you need to specify a unique default profile name for TSClientAutoAdminLogon, which is different from the eDirectory AutoAdminLogon default profile name.

NOTE: If either DefaultLoginProfile or TSClientDefaultloginProfile is not provided, the Default profile for the eDirectory username is used for the TSClientAutoAdminLogon.

---

4 Close the Registry Editor.

8.12 Setting Up Single Sign-On (SSO)

The SSO feature provides a method by which the Windows account password can be automatically saved and retrieved during a login to both eDirectory and Windows. This enables the user to achieve a transparent single sign-on to both eDirectory and Windows even in cases where a non-password-based Novell NMAS authentication method is being used for the eDirectory login, such as the Novell

Enhanced Smart Card Method (NESCM). Without the SSO feature, even though a non-password-based login to eDirectory could be performed, the user would still be prompted to perform a password-based Windows account login.

To enable the SSO feature, you must first enable the SSO functionality in the Client Properties. Once enabled, SSO will be attempted during every login to both eDirectory and Windows. Note that the Client SSO functionality is only available in cases where an eDirectory login is being performed in addition to the Windows account login.

The SSO feature is provided through capabilities of the Novell NMAS client, and is only available when the NMAS Client 3.5.0 or later is installed.

TIP: To create a new Windows user, go to the user's Windows 7 workstation, log in as an administrator, then create a new Windows user with a password. For more information on creating users in Windows 7, see Create a user account (http://windows.microsoft.com/en-IN/windows7/Create-a-user-account).

- Section 8.12.1, "Enabling SSO," on page 140
- Section 8.12.2, "Enrolling the Windows User for SSO," on page 141
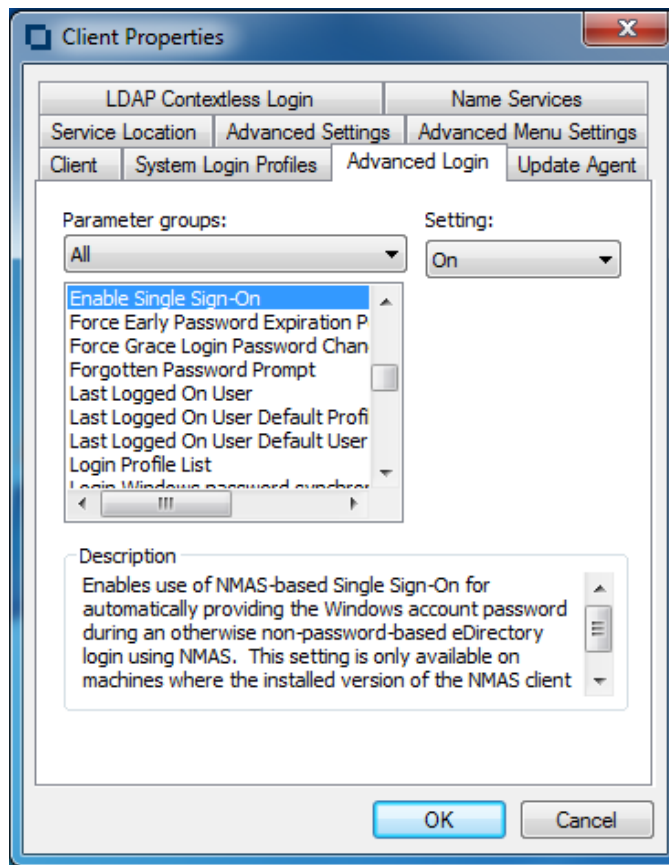- Section 8.12.3, "Enabling the Suppress Single Sign-On Option," on page 144

8.12.1 Enabling SSO

1 At the user's Windows 7 workstation, right-click the ▢ icon in the notification area.
2 Click **Client Properties**.
3 On the **Advanced Login** tab, select **Enable Single Sign-On**, then select **On** in the **Setting** list.

**NOTE:** By default, the value of **Settings** is set to Off.

---

4 Click **OK**, then log out of the workstation.

You have successfully enabled SSO.

## 8.12.2 Enrolling the Windows User for SSO

1 On the Windows 7 login page, click **OES Logon**, then enter the eDirectory user credentials that you want to link to the Windows user.

2 Click **Show Advanced Options** to display the **Login** dialog box.

3 On the **eDirectory** tab, specify the tree name, tree context, and the server name.
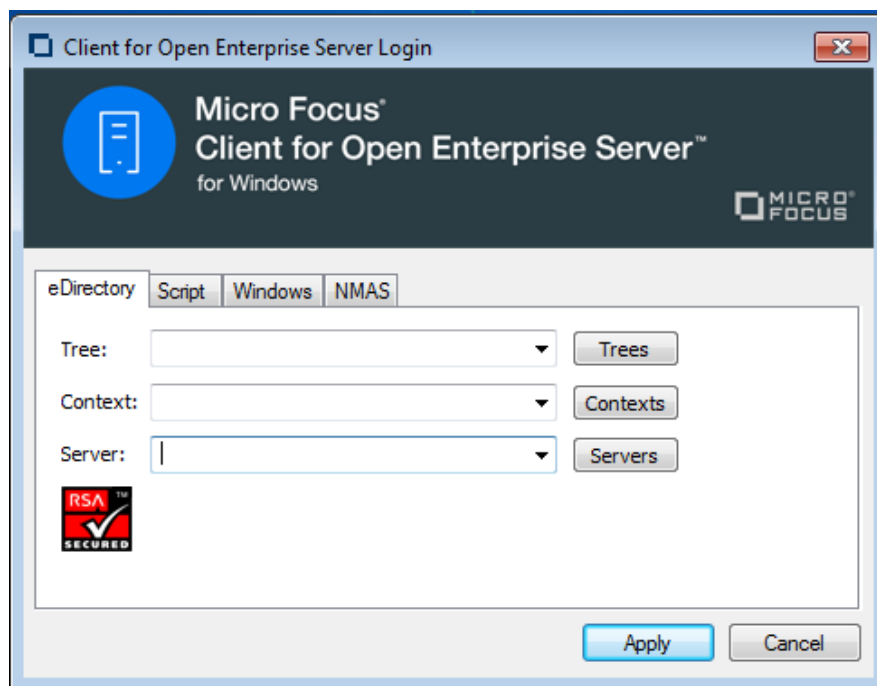
4 On the **Windows** tab, specify the Windows user name that you want to enroll, then click **Apply**.
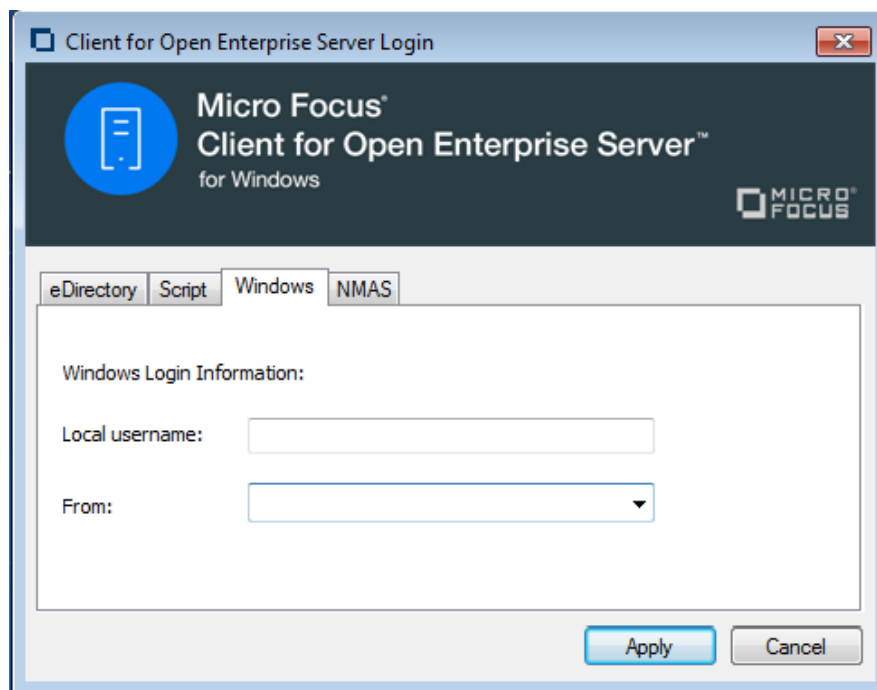
5 Click the icon.

You are logged in to the network through the eDirectory credentials.

6 On the **Log on to this Computer** page, specify the Windows user credentials, then click the icon.

You are logged on to the workstation through the Windows credentials.

7 Log out of the workstation.

For subsequent logins, it's enough to provide the eDirectory credentials, and you are automatically logged on to the workstation through the enrolled Windows credentials.

NOTE: You can link any number of Windows users to a single eDirectory user.
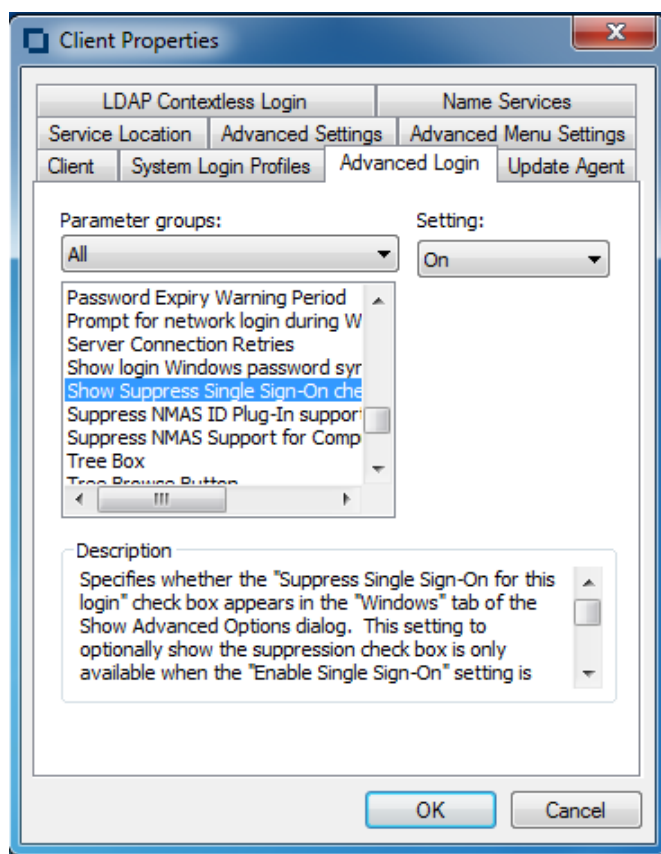

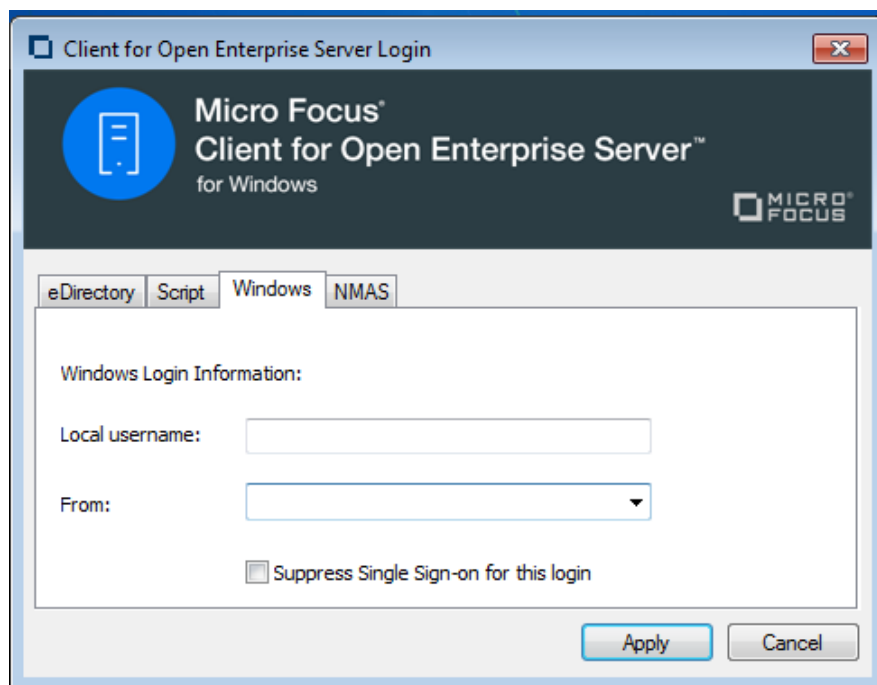
8.12.3   Enabling the Suppress Single Sign-On Option

1 Right-click the ◻ icon in the notification area.

2 Click **Client Properties**.

3 On the **Advanced Login** tab, select **Show Suppress Single Sign-On check box**, then select **On** in the **Setting** list.

By default, the value of **Settings** is set to **Off**.

You have successfully enabled the Suppress SSO option for all users of the workstation. For the next login attempt, the check box appears in the Login dialog box under the **Windows** tab.

NOTE: Selecting the Suppress Single Sign-on for this login check box suppresses SSO only for the particular login attempt.

8.13 Setting Up NMAS Based Windows Logon

The NMAS for Windows Logon support allows the smart card to be used for a workstation login when eDirectory is not available or eDirectory login is not desired. This is useful in situations where network connectivity is not always available, such as for laptop users.

To enable the NMAS for Windows Logon feature:

◆ Install IAS (Identity Assurance Client) 3.0.8. IAS installation triggers Novell Client 2 SP3 for Windows (IR2a) and NESCM 3.0.8 (Novell Enhanced Smart Card Method) installation. For more information on the IAS installation, see Novell Enhanced Smart Card Method Installation in the Novell Enhanced Smart Card Method Installation and Administration Guide.

NOTE: NMAS Client 3.5.1 or later is required for NMAS Based Windows Logon to work. NMAS Client 3.5.1 gets installed by default along with Novell Client 2 SP3 for Windows (IR2a).

◆ Select the Use Smart Card for Workstation Only Login and Require Smart Card for Workstation only Login check boxes as per the security requirement of the organization during the NESCM installation. For more information, see Novell Enhanced Smart Card Method Installation in the Novell Enhanced Smart Card Method Installation and Administration Guide.

◆ Enroll the workstation users with the eDirectory user.

After enabling NMAS for Windows Logon feature, you can disable it for a specific workstation as well as exempt some users from using it.

After a successful eDirectory plus workstation login (enrollment), the NMAS for Windows Logon functionality encrypts and stores the credentials for future computer only logins. This means that a successful enrollment must have occurred before NMAS for Windows Logon functionality is available.

8.13.1 Enrolling Users for "NMAS for Windows Logon"

1 Insert the smart card that is configured in the eDirectory. For more information, see Configuring the Server in the Novell Enhanced Smart Card Method Installation and Administration Guide.

2 On the Log on to OES Network page, enter the eDirectory username and pin.

3 Click **Show Advanced Options** to display the **Login** dialog box.

4 On the **eDirectory** tab, specify the tree name, tree context, and the server name.
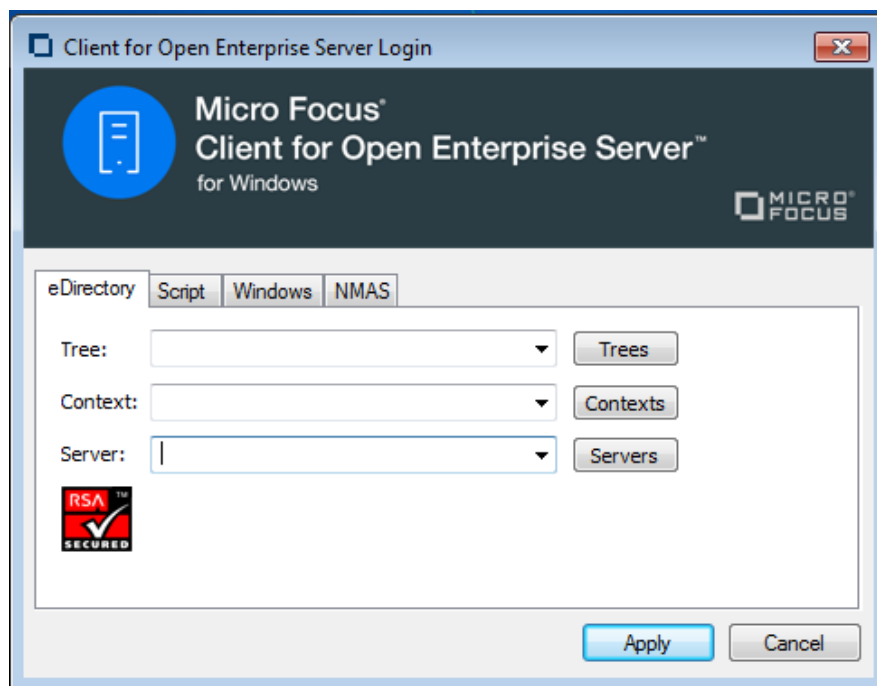
5 On the **NMAS** tab, select the sequence as **Enhanced Smart Card**, then click **Apply**.
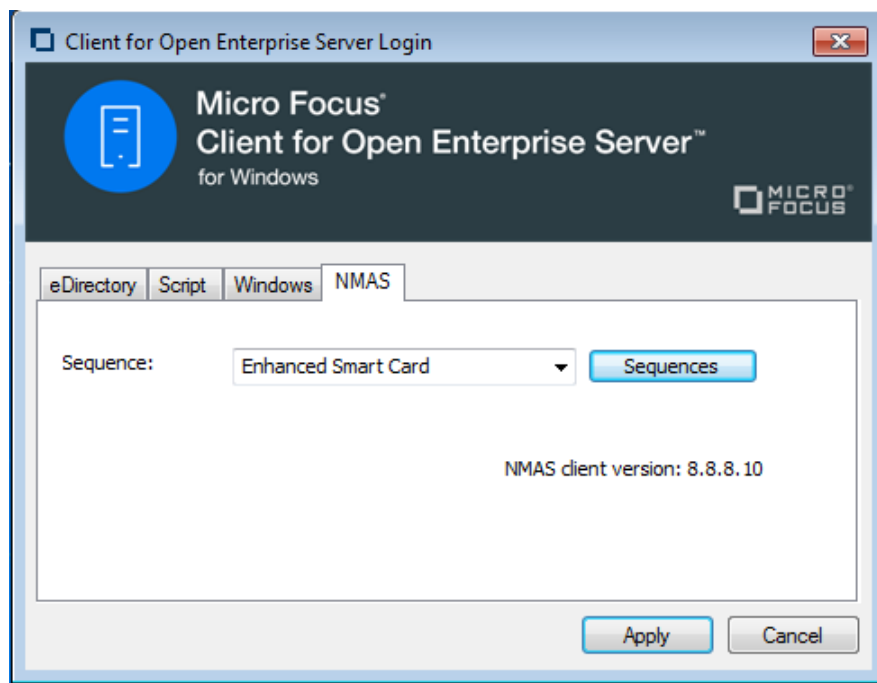
6 Click the ➡ icon.

You are logged in to the network through the eDirectory credentials.

7 On the **Log on to this Computer** page, specify the Windows user credentials (username and password), then click the login icon.

You are logged on to the workstation through the Windows credentials.

8 Log out of the workstation.

For subsequent logins, it's enough to provide the enrolled local user name, the smart card and the smart card pin, and you are seamlessly logged on to the workstation.

8.13.2 Performing an NMAS Based Windows Logon

1 Insert the smart card that is configured in the eDirectory.

2 On the Windows 10/ Windows 8/ Windows 7/ Windows 2012 credential provider page, click **Computer Only Logon**, to display the Log on to this computer screen.

3 Select **Use NMAS for Windows Logon** check box, enter the enrolled local username, and the smart card pin.

> **NOTE:** You can also login using your password if Require Smart Card for Workstation Only Login is not enabled at the time of IAS client installation. For more information, refer <IAS Section>. Deselect the Use NMAS for Windows Logon check box for a Windows password based login. It is recommended to remove the smart card from the smart card reader during this login.

4 Click the ![icon] icon and you are logged on to the workstation.
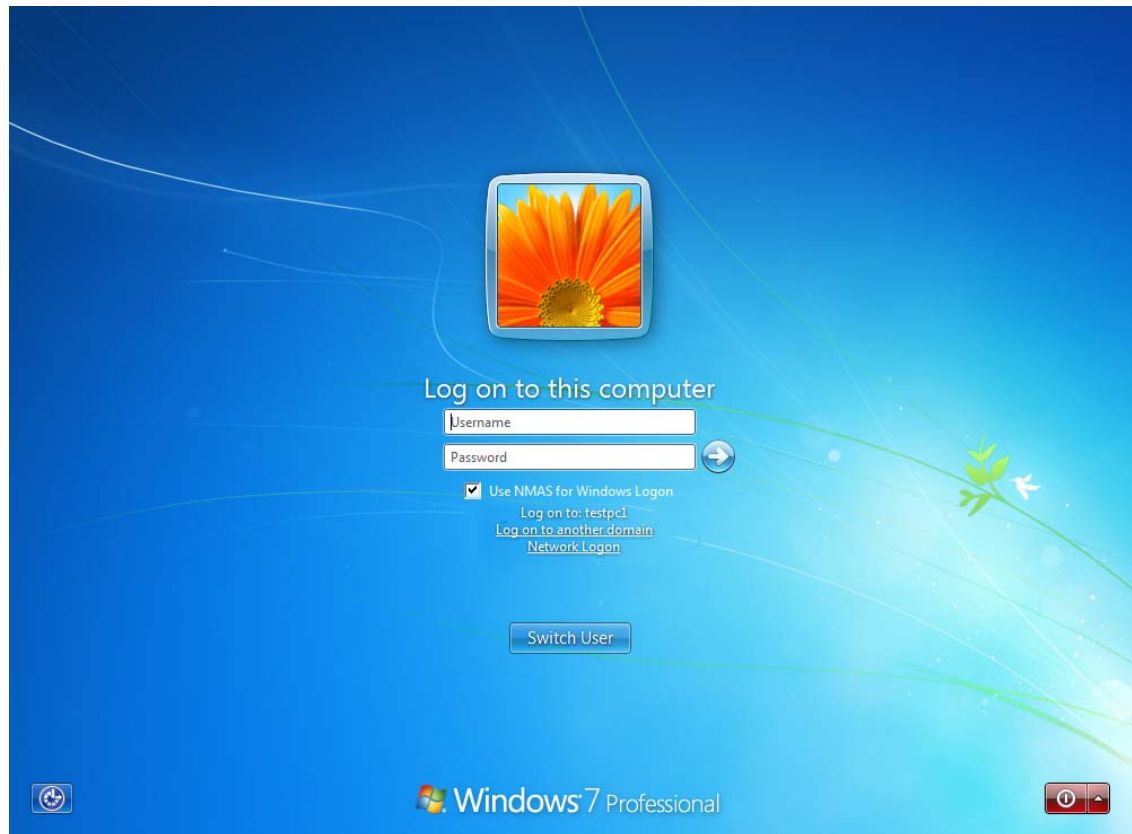
8.13.3 Creating an Exception List

Exception List is used to exempt some users from using NMAS based Windows Logon. This can be used only when the **Require Smart Card for Workstation Only Login** check box is enabled at the time of IAS client installation.

1 Open Windows registry editor.

2 Create a key named **Disconnected Login** under **HKEY_LOCAL_MACHINE > SOFTWARE > NOVELL > Login**.

3 Right-click to create a value named **Enforcement Exception List** of type multi-string value.

4 Open the **Enforcement Exception List** entry, add usernames that have to be exempted from NMAS based Windows Logon, then click **OK**.

Separate each username with a Return Key press.

NOTE: The usernames can be in any of the following formats: simple user names such as john, user names preceded by domain names (for example, domainname\john), and UPN format user names such as john@domainname.com.

---

5 Close the registry.

You have successfully created an exception list. Users in this list can login using their password after deselecting the **Use NMAS for Windows Login** check box in the **Windows Log on to this computer** page.

8.13.4 Suppressing the NMAS Support for Computer Only Logon

1 Right-click the ▢ icon in the notification area.

2 Click **Client Properties**.

3 On the **Advanced Login** tab, select **Suppress NMAS Support for Computer Only Logon**, then select **On** in the **Setting** list.

By default, the value of Settings is set to Off.

You have successfully suppressed the NMAS support for computer only logon for this workstation. In the consecutive login attempts, you can log on to the workstation using password.

8.14 Troubleshooting Service Location Protocol (SLP) Configuration

This section contains troubleshooting information related to SLP configuration.

◆ Section 8.14.1, "Client Service Location Diagnostic Utility (SLPINFO)," on page 151

8.14.1 Client Service Location Diagnostic Utility (SLPINFO)

The Client now includes an `SLPINFO` utility intended to help with the troubleshooting and verification of SLP-related workstation behavior. The `SLPINFO.EXE` program is installed by the Client into the Windows `SYSTEM32` directory, and therefore the `SLPINFO` command should be available in any Windows command prompt.

The `SLPINFO` output available in the Client for Open Enterprise Server is different from the `SLPINFO` output presented by previous platforms such as the Novell Client for Windows XP/2003. Most of these differences relate to the level of information that is available through existing standards-based OpenSLP user agent APIs, versus the information which had been exposed by the proprietary `SRVLOC.SYS` user agent used earlier Client platforms.

The intention of the `SLPINFO` tool remains unchanged, and that is to provide information which can help verify or diagnose SLP-related behavior from the client machine's perspective. As improvements are made to the OpenSLP user agent APIs, additional information can also be presented by the Client for Windows SLPINFO utility.

The Client for Windows SLPINFO utility supports the following options:

◆ **/D** - Displays the SLP Directory Agent (DA) resources and associated SLP scopes that can be located in the environment via the Client Properties **Service Location** tab configuration, via DHCP Inform options 78 and 79, and via multicast solicitation.

> **NOTE:** This discovery is being performed using an instance of the OpenSLP user agent running on the `SLPINFO.EXE` process itself, and is not the same OpenSLP user agent instance actually being used by the Client for name resolution. As such it is possible that firewall policies or other user program restrictions could prevent the `SLPINFO` utility from discovering some SLP DAs which are actually available in the environment, even though these same SLP DAs actually can be successfully discovered and used from the OpenSLP user agent instance running on the Client XTSVCMGR service.

  ◆ **/T** - Displays the eDirectory tree (ndap.novell) resources visible to the Client via SLP, as well as their associated IPv4 addresses.

  ◆ **/S** - Displays the NCP server (bindery.novell) resources visible to the Client via SLP, as well as their associated IPv4 addresses.

    For both the `/T` and `/S` displays, the `SLPINFO` tool is actually receiving this information from the Client itself. Meaning any eDirectory tree and NCP server listed is by definition visible to the Client's own name resolution processing which occurs on the `XTSVCMGR` service, and is not potentially limited by firewall or other restriction policies that apply to the `SLPINFO.EXE` tool being executed by the user. So unlike the `/D` display, an eDirectory tree or NCP server name which isn't listed in `/T` or `/S` means the Client itself cannot see that name either, and is not potentially just a limitation applying to the `SLPINFO` utility itself.

  ◆ **/A** - Displays all of the SLP DAs, SLP scopes, eDirectory trees and NCP servers. Same as specifying `SLPINFO /D /T /S`.

  ◆ **/H or /?** - Displays the help screen for SLPINFO.

8.15   Setting up Service Account eDirectory Login

For more information on setting up a service account eDirectory Login, see Configure a Windows (Vista/7/2008/R2) service for authentication to eDirectory (http://www.novell.com/support/kb/doc.php?id=7008266).

A   Documentation Updates

The *Client for Open Enterprise Server Administration Guide* has been updated as shown below.

May 2016

Section	Change
All	The guide is updated for rebranding changes. Novell Client is rebranded to Client for Open Enterprise Server. This rebranding change do not cause any impact on the product functionality.

September 30 2015

Section	Change
All	Updated guide content to reflect the added support for Windows 10 in the SP4 IR1 release.

January 30 2012

Section	Change
All	Updated guide content to reflect the added support for Windows 8 and Windows Server 2012 in the SP3 release.