NetIQ Client Login Extension 3.7 SP3

Administration Guide

June 2014

Contents

11 Troubleshooting 31

About this Book and the Library

This guide contains information about using the Client Login Extension to provide password self-service functionality in Novell Client and NetIQ SecureLogin 8.0.1. The guide is organized as follows:

- Chapter 1, "What's New," on page 9
- Chapter 2, "Understanding the Client Login Extension," on page 11
- Chapter 3, "System Requirements," on page 13
- Chapter 4, "Preliminary Tasks," on page 15
- Chapter 5, "Installing the Client Login Extension," on page 17
- Chapter 6, "Configuring the Client Login Extension MSI Files," on page 19
- Chapter 7, "Installing the Client Login Extension MSI File," on page 23
- Chapter 8, "Using the Forgotten Password Feature," on page 25
- Chapter 9, "Upgrading the Client Login Extension," on page 27
- Chapter 10, "Uninstalling the Client Login Configuration Utility," on page 29
- Chapter 11, "Troubleshooting," on page 31

Intended Audience

This guide is intended for administrators, consultants, and network engineers who require a high-level introduction to Identity Manager business solutions, technologies, and tools.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

 - Identity & Access Governance
 - Access Management
 - Security Management
 - Systems & Application Management
 - Workload Management
 - Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 What's New

Client Login Extension 3.7 SP3 now provides the following features that work only with NetIQ Self Service Password Reset (SSPR) 3.1.

- ◆ Section 1.1, "Challenge Response Force Enrollment," on page 9
- ◆ Section 1.2, "Password Expiration Warning," on page 9

1.1 Challenge Response Force Enrollment

This release now supports Challenge Response Force Enrollment. Users are prompted to set their challenge responses while logging in, failing which they cannot log in.

This feature ensures that the users set up Challenge Response through Client Login Extension, if they have not already set it up through SSPR.

1.2 Password Expiration Warning

Client Login Extension now displays the number of days before which the password will expire, every time you log in. And if the password has already expired, it displays a warning message. This feature allows you to change the password before it expires or after it has expired. You can choose to change the password using SSPR through the CLE restricted browser.

You can set how many days a user has until their password expires. For example, if you set it to 30 days, the user gets a notification about the impending password expiry starting from 30 days before the password expiry date until the password expires.

2 Understanding the Client Login Extension

The Client Login Extension (CLE) facilitates password self-service by adding a link to the Novell login clients. When users click the *Forgot Password* link in their login client, the CLE launches a restricted browser to access the Password Self-Service feature on the login clients. This feature assists in reducing help desk calls from people who forget their passwords.

Credential Provider Support

Password recovery support is available for graphical authentication interfaces such as Credential Provider for LDAP clients and the Novell Client. In the absence of these clients, the password recovery support is provided by the default Microsoft Credential Provider implemented by the Client Login Extension.

CLE provides a credential provider filter component to filter out any existing credential provider in the user system. If the Novell Client or SecureLogin credential provider is present, then Client Login Extension filters the credential provider provided by the Client Login Extension.

Desktop Automation Services

Password recovery support through the Client Login Extension tool is also available for locked workstations and for workstations in which user operations are controlled by Desktop Automation Services (DAS).

Configuring the Password Self-Service Feature

The Administrator runs the Configuration Utility of Client Login Extension and provides registry entries for the MSI file. The registry entries for the MSI file include a welcome note, text to be shown as a link, URL of the target server, and other required options. The entered values are displayed as fields on the restricted password self-service browser. The user who forgot the password should provide the required values in the self-service browser and retrieve the forgotten password.

The Client Login Extension supports the Self Service Password Reset (SSPR) application. For information on installing and configuring the SSPR application, see NetIQ Self Service Password Reset 3.1 Administration Guide.

Running the Configuration Utility of the Client Login Extension configures the Client Login Extension MSI file, which you then install on client workstations running the Novell Client software, NetIQ SecureLogin 8.0.1 and Microsoft Credential Provider. The Client Login Extension works on Windows 7 workstations.

The Client Login Extension MSI files are available in a number of different languages. You must configure the Client Login Extension file for each language, including English, before it can be used.

The Client Login Extension Configuration utility allows the system administrator to specify the following configuration information for the Client Login Extension MSI file:

◆ You can set the URL for password self-service.
◆ For NetIQ SecureLogin 8.0.1, you can include text (such as "Forgotten Password") for the link to password self-services.

NOTE: The Client Login Extension for NetIQ Identity Manager works with NetIQ SecureLogin 8.0.1 and the Novell Client 4.91 SP3 or later. This utility does not work with any application that alters Microsoft Credential Provider, except the Novell Client 4.91 SP3 or later. The Client Login Extension has been tested for use on licensed NetIQ Identity Manager 3.5 and later systems.

The remaining sections in this guide step you through installing and using the Client Login Extension Configuration utility to configure the Client Login Extension MSI files. The instructions for using the Client Login Extension MSI files are also included.

3 System Requirements

Ensure that the following requirements are met by the system where you will install the Client Login Extension.

3.1 Supported Client Login Programs

The Client Login Extension works with the native Microsoft Credential Provider, and the Novell Client 4.91 SP3 or later. This utility does not work with any application that alters the Microsoft Credential Provider, except the Novell Client 4.91 SP3 or later. The Client Login Extension works with ZCM 11.2.2.

3.2 Supported Windows Versions

You can use the Client Login Extension with the following Windows version:

- Windows 7 (32-bit and 64-bit)
- Windows Vista

  Note that the challenge response force enrollment and password expiration warning features are not supported on Windows Vista.

NOTE: You might encounter some compatibility issues when Client Login Extension is installed on Windows 8.1 and 8.

3.3 Supported Identity Manager Versions

You can use the Client Login Extension with the following Identity Manager versions:

- Identity Manager 3.5 and 3.5.1
- Identity Manager 3.6 and 3.6.1
- Identity Manager 4.0, 4.0.1, and 4.0.2

3.4 Supported .NET Framework Versions

You can use the Client Login Extension with the following .NET Framework versions:

- .NET 2.0
- .NET 3.5

3.5 Supported NetIQ SecureLogin Versions

You can use the Client Login Extension with the following SecureLogin versions:

- Novell SecureLogin 7.0.3 HF6
- NetIQ SecureLogin 8.0.1, 8.0

3.6 Supported NetIQ Self Service Password Reset Versions

You can use the Client Login Extension with the following Self Service Password Reset versions:

- NetIQ Self Service Password Reset 3.1, 3.0

4 Preliminary Tasks

Before running the NetIQ Client Login Extension, you must have a working Identity Manager application (for example, Identity Manager 3.5 or later) system and have the user application configured correctly to enable the Password Self-Service feature. For information on installing Identity Manager and the User Application, see the Identity Manager 4.0.2 Integrated Installation Guide (https://www.netiq.com/documentation/idm402/idm_integrated_install/data/front.html).

4.1 Enabling the Password Self-Service Feature

To enable the Password Self-Service feature, perform the following:

- Enable Universal Password.
- Create a password policy or select an existing password policy.
- Enable and configure the Forgotten Password option.
- Assign the password policy to the appropriate users, groups, or container.
- Enable SSL.

You initially set up the Password Self-Service feature through iManager by using the *Passwords > Password Policies > Forgotten Password* and *Policy Assignment* options. For more information on the Password Self-Service feature, see "Managing Passwords by Using Password Policies" and "Password Self-Service" in the Password Management 3.2 Administration Guide.

Use the Identity Manager User Application to complete the password configuration. For information about configuring Password Self-Service through the Identity Manager User Application, see "Forgot Password Web Service" in the User Application: Administration Guide.

NOTE: After completing the Password Self-Service, restart the operating system in the LDAP CP mode to effect password recovery assistance.

You also need to turn on SSL in JBoss. See "Enabling SSL" in the User Application: Administration Guide. The Client Login Extension does not work without SSL.

You must enable the URL rewriting when the User Application is deployed on the IBM WebSphere Application Server.

1 Log in to the Administration Console.
2 Go to the *Server > Application Servers > Select your server* (for example, server1), then select *Session Management* on the Configuration tab.
3 Select the *Enable URL Rewriting* check box and click *Apply*, then click *Save*.
4 Restart the WebSphere Application Server.

With the Forgotten Password feature enabled and the password policy assigned, you now have a valid HTML link for the restricted browser to use. This link needs to be configured for HTTPS, for example, `https://hostname:8443/IDM/jsps/pwdmgt/ForgotPassword.jsf`. Use this URL when running the Client Login Extension Configuration utility.

4.2 (Optional) Configuring NetIQ Self Service Password Reset (SSPR) 3.1

You must configure the following settings in SSPR 3.1 to enable the Challenge Response Force Enrollment and the Password Expiration Notification features.

4.2.1 Configuring SSPR for Enabling Challenge Response Force Enrollment

Launch SSPR, in the Configuration Editor page, click *Settings > Integration/Developer > Enable External Web Services*.

4.2.2 Configuring SSPR for Enabling Password Expiration Warning

Launch SSPR, in the Configuration Editor page, click *Settings > Active Directory > Allow Authentication When Password Expired*.

5 Installing the Client Login Extension

The NetIQ Client Login Extension interacts with NetIQ Identity Manager and NetIQ SecureLogin applications for the user to log in to all the defined applications, and benefit from the password self-service for the NetIQ, Microsoft, and LDAP clients. The service is also available for DAS-enabled workstations.

However, availability of the service is based on the authentication interface of the clients.

Table 5-1 *Password Self-Service Support for Clients*

Authentication Interface	During Operating System Login	During Operating System Lock	For DAS-Enabled Workstations
Microsoft CP	Available	Available	Available
Novell Client CP	Available	Not available	Available
LDAP CP	Available	Available	Available

You install the Client Login Extension and SecureLogin applications on the systems in which the password self-service feature is required.

NOTE: In order to set up the password self-service for Novell Client, install Novell Client before installing the Client Login Extension. For other clients, you can follow any installation sequence.

The Client Login Extension Configuration utility is available in the `<CD_ROOT>/CLE` folder. Here, CD_ROOT refers to the location where the Identity Manager files are extracted.

To install the Client Login Extension:

1 From the `cle` directory, run `ClientLoginExtensionConfigurationUtilitySetup.msi` to launch the Client Login Extension Configuration Utility installer. Select the executable for your platform. For instance, if you are on a 64-bit platform, select the executable inside the `win64` folder.

   The installer checks to see if .NET platform is installed on the computer. If it is not installed, the installer prompts you for installing it. After the installation is complete, the Client Login Extension Setup Wizard is launched.

2 Read the information on the initial wizard pages, then click *Next*.

3 On the License Agreement page, read the license agreement. If you agree, select *I Agree*, then click *Next*.

4 On the Select Installation Folder page, use the default directory selection or click *Browse* to select a different directory.

   The default directory is `C:\Users\<user>\My Documents\Client Login Extension Configuration Utility Setup 3.7.3.0`.

5 Click *Next*.

6 On the Confirm Installation page, click *Next* to install the Client Login Extension Configuration utility and Client Login Extension files.

7 When the installation completes, click *Close*.

The installation process creates two shortcuts to `ClientLoginExtensionConfigurationUtility.exe`, one for the desktop and one for the *Programs* menu. The process installs the following folders and files in the installation folder:

- `ClientLoginExtensionConfigurationUtility.exe`
- ClientLoginExtensionConfigurationUtility.exe xml configuration file
- `license.rtf`
- `Installer/`
  - `IdentityManagerClientLoginExtension_en.msi` (English--default)
  - `IdentityManagerClientLoginExtension_de.msi` (German)
  - `IdentityManagerClientLoginExtension_es.msi` (Spanish)
  - `IdentityManagerClientLoginExtension_fr.msi` (French)
  - `IdentityManagerClientLoginExtension_it.msi` (Italian)
  - `IdentityManagerClientLoginExtension_ja.msi` (Japanese)
  - `IdentityManagerClientLoginExtension_zh_CN.msi` (Chinese Mandarin)
  - `IdentityManagerClientLoginExtension_zh_TW.msi` (Chinese Traditional)

8 Continue with Chapter 6, "Configuring the Client Login Extension MSI Files," on page 19.

6 Configuring the Client Login Extension MSI Files

Launching the Client Login Extension Configuration utility will configure MSI files for installing the Extension and save them to the local workstation. These MSI files are used to install the Client Login Extension on Windows workstations.

If you have not already installed the utility, see Chapter 5, "Installing the Client Login Extension," on page 17.

The Client Login Extension MSI files are available in a number of different languages. You must configure the Client Login Extension file for each language, including English, before it can be used.

To configure the MSI files:

1 Click the *Client Login Extension Configuration Utility 3.7.3.0* shortcut to launch the Client Login Extension Configuration utility.

or

Double-click the `ClientLoginExtensionConfigurationUtility.exe` file to launch the utility.

The *Path to Installer to Configure* option shows the path to the English version of the Client Login Extension installer file that is being configured. Whenever this text box contains a path to a valid MSI file, the utility automatically opens the file, populates the other controls with the information it contains, and enables the *Configure Installer* button.

If you want to select another language, click the *Browse* button to select the Client Login Extension installer file in a different language. By default, the *Browse* button opens in the `Installer` subfolder in the `installation` folder and displays all files that match with the Client Login Extension Installer pattern.

NOTE: In Windows 7, sometimes the *Path to Installer to Configure* field does not take you to the CLE installer file location. It displays the following error message:

`Location is not available`

To workaround this issue, you must manually browse and select the correct folder. The default location for the installer files is `C:\Users\<user>\My Documents\Client Login Extension Configuration Utility Setup 3.7.3.0`.

2 Welcome Text for Installer: Modify the information in the Welcome text or keep the information as it is presented.

The information in the text box is displayed on the Welcome screen of the Client Login Extension. The string *[ProductName]* displays as *Client Login Extension 3.7.3.0*.

3 Link URL: Specify the URL that the Client Login Extension- restricted browser uses to connect to the User Application Forgotten Password page. You can use either a DNS name or an IP address. An example of a URL using a DNS name that links to the Forgotten Password page is:

`https://<server>:<port>/IDM/jsps/pwdmgt/ForgotPassword.jsp`

This URL can also be configured to access the external password WAR. To do this, see *Installing the User Application on an Application Server* in the *NetIQ Identity Manager Setup Guide* (https://www.netiq.com/documentation/idm402/setup_guide/data/front.html).

IMPORTANT: You must have a valid URL pointing to the User Application's Forgotten Password page; otherwise, the client connection might fail and you might not be able to log in through the workstation. For more information, see Section 11.1, "Using Forgotten Password," on page 31.

---

4 Link Text: Specify the text to be displayed on the link to the restricted browser that the Client Login Extension uses.

The default text is *Forgotten Password*. The text for the button in the Novell Client is provided by the Novell Client and cannot be changed here.

5 (Optional) Enable SSPR Integration: This option allows you to enable the challenge response enrollment and password expiration features.

If you select this option, the *Force user for challenge response enrollment* option and *REST URI* field are enabled.

NOTE: To enable this feature, you must have already configured SSPR, as described in Section 4.2.1, "Configuring SSPR for Enabling Challenge Response Force Enrollment," on page 16 and Section 4.2.2, "Configuring SSPR for Enabling Password Expiration Warning," on page 16.

---

6 (Optional) Force user for challenge response enrollment: Selecting this option enables you to force users to set up their challenge response before logging into the computer. However, if you do not select this option, the user can choose not to set up any challenge response and proceed to log in.

7 Force challenge response enrollment warning message: This option is enabled only if you select *Force user for challenge response enrollment*. Specify the message that you want to display when the user is prompted for force enrollment.

8 REST URI: Specify the URI that the Client Login Extension- restricted browser uses to connect to the SSPR server by using rest calls. You can use either a DNS name or an IP address. An example of a URI using a DNS name is:

```
https://<server>:<port>/sspr/public/rest
```

9 (Optional) Enable Proxy: In an environment where Internet is not directly accessible and the Client Login Extension needs to access it, you need to connect the Client Login Extension to a proxy server. To connect to the proxy server, select the *Enable Proxy* check-box and provide the IP address and the port number of the proxy server in the *Proxy Server* text-box.

10 After all of the information is in place, click *Configure Installer* to write the new configuration settings to the selected Client Login Extension file.

11 Click *OK* to close the confirmation message.

The Client Login Extension Configuration utility remains open, allowing you to configure another Client Login Extension MSI file in a different language. To do so, click the *Browse* button to the right of the *Path to the Installer to Configure* option, select another language, and configure another .msi file by following Step 9 through Step 11.

The localized Client Login Extension MSI files for the more common languages are delivered with the configuration utility in the Installers folder. You must configure each localized installer individually.

To localize the Client Login Extension MSI files for languages other than those delivered with the Client Login Extension, see Section 6.1, "Localizing Client Login Extension Files for Other Languages," on page 21.

12 Click *Configure Installer*.

13 To close the Client Login Extension Configuration utility window, click *Exit*.

6.1 Localizing Client Login Extension Files for Other Languages

To localize the Client Login Extension for languages other than those delivered with the Client Login Extension Configuration utility, you can use Orca to directly edit the content of the MSI database (`IdentityManagerClientLoginExtension.msi`).

Orca (`Orca.exe`) (http://msdn2.microsoft.com/en-us/library/aa370557.aspx) is a database table editor used for creating and editing Windows Installer packages. It is available in the Windows SDK Components for Windows Installer Developers (http://msdn2.microsoft.com/en-us/library/aa370834.aspx).

The text to be localized for `IdentityManagerClientLoginExtension.msi` is located in the following table:

Table 6-1 *Text You Need to Localize*

Table	Column	Comments
Control	Text	
Dialog	Title	
Directory	DefaultDir	Put text after "|".
Launch Condition	Description	
Property	Value	Only ProductName, Manufacturer, ARPCONTACT, and VSDVERSIONMSG.
Radio Button	Text	
Registry	Value	Set LogFile, LinkURL, LinkText, PasswordComplexityText, and LoginExtDesc to the defaults for the configuration utility.
Shortcut	Name	Name
Shortcut	Description	If not Null
UIText	Text	Put text after "|"

WARNING: Translate only the user interface text. For example, do not translate text surrounded by square brackets ([xxxx])or is in mixed case (XxxXxxXxx). Modifying these property names and identifiers breaks the installer.

Use the following procedure to localize the Client Login Extension MSI file to a new language:

1 Copy `IdentityManagerClientLoginExtension.msi` to `IdentityManagerClientLoginExtension_xx.msi`, where *xx* identifies the new language (locale).

2 Open `IdentityManagerClientLoginExtension_xx.msi` in `Orca.exe`, edit the tables and columns to insert the localized text, as listed in Table 6-1 on page 21, then save and close the file.

3 Open `IdentityManagerClientLoginExtension_xx.msi` with the Client Login Extension Configuration utility (`ClientLoginExtensionConfigurationUtility.exe`), review the default values, make any modifications if needed, then click *Configure Installer*.

NOTE: Step 3 is required, even if the default values that you set in the Registry table do not need modification. The Client Login Extension Configuration utility makes additional changes that enable the Client Login Extension MSI file.

---

7 Installing the Client Login Extension MSI File

The following sections provide information to help you distribute the Client Login Extension MSI file to users:

- Section 7.1, "Installing the Extension," on page 23
- Section 7.2, "Using the Client Login Extension Installer Command Line Options," on page 24

7.1 Installing the Extension

With the Client Login Extension MSI file configured, you can distribute the `IdentityManagerClientLoginExtension_xx.msi` file (or its distribution name) to users or to a distribution mechanism. The *xx* identifies the language (locale).

The `IdentityManagerClientLoginExtension_xx.msi` file created by running the Client Login Extension Configuration Utility Setup is located in the `Installer` folder. By default, the Installer folder is located in the `C:\Users\<user>\My Documents\Client Login Extension Configuration Utility Setup 3.7.3.0` folder.

1 Double-click the `IdentityManagerClientLoginExtension_xx.msi` file to launch the Client Login Extension welcome page.

For startup options, you can use when launching the Client Login Extension MSI file, see Section 7.2, "Using the Client Login Extension Installer Command Line Options," on page 24.

The welcome message is the same text that you provided in the Client Login Extension Configuration utility.

2 Click *Next* to start the installation.

3 After the Client Login Extension is installed, click *Close*.

7.1.1 Providing a Custom GINA Name

For branding purpose, you can provide an alternate GINA name.

1 Install the Client Login Extension.

2 Open the Registry editor and navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\MsPssGina` key. This key is created when the Client Login Extension is installed.

3 Create a new string value named `GinaProviderName`. Modify it and enter your GINA name as value data (for example, `MsGina.dll`).

4 Restart the system.

> **NOTE:** You can provide only Microsoft GINA based custom GINAs as value data for the `GinaProviderName` registry entry. Your system might not reboot correctly if you provide any other third-party GINA name.

7.2 Using the Client Login Extension Installer Command Line Options

The Client Login Extension MSI file is a standard MSI installer. It can be used with any of the standard `Msiexec.exe` command line options, which you can find at msdn (http://msdn2.microsoft.com/en-us/library/aa367988.aspx). Some examples are shown below.

To install the Client Login Extension MSI file with no user interface, specify the following at the command line:

`msiexec /i IdentityManagerClientLoginExtension_en.msi /q`

or

`IdentityManagerClientLoginExtension_en.msi /q`

To install with no user interface except for a modal dialog box displayed at the end, specify:

`msiexec /i IdentityManagerClientLoginExtension_en.msi /qn+`

or

`IdentityManagerClientLoginExtension_en.msi /qn+`

To uninstall with no user interface, specify:

`msiexec /x IdentityManagerClientLoginExtension_en.msi /q`

To uninstall with no user interface except for a model dialog box displayed at the end, specify:

`msiexec /x IdentityManagerClientLoginExtension_en.msi /qn+`

Also, see Section 7.1.1, "Providing a Custom GINA Name," on page 23 for information on changing the GINA names.
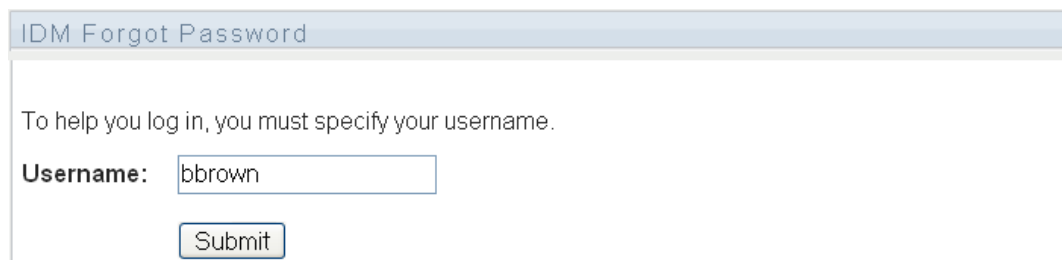
8 Using the Forgotten Password Feature

The following sections explain how to use the Forgotten Password feature in the Novell Client:

8.1 Accessing the Forgotten Password

After you run the Client Login Extension MSI file on workstations running the Novell Client 4.91 SP3 and you have specified a valid HTTPS link, the Password Self-Service feature is ready to use. See Chapter 4, "Preliminary Tasks," on page 15 to ensure that you have all the information in place for Password Self-Service to work.

1 If you forget your password, click the *Did you forget your password?* link in the Novell Client.

Clicking the *Did you forget your password?* link launches a restricted browser that can only go to the URL designated in the Client Login Extension Configuration utility. The restricted browser performs the following tasks:

- Verifies that the protocol is HTTPS
- Validates the hostname
- Verifies that the target Web site is operating in the Internet Explorer restricted sites zone
- Disables hotkeys
- Disables tabs
- Disables right-clicking
- Disables ActiveX
- Disables scripts
- Runs on its own process, separate from the Winlogon process.

2 After the restricted browser connects to the Forgotten Password page, you see the Identity Manager Forgot Password dialog box. Type your login name, then click *Submit*.
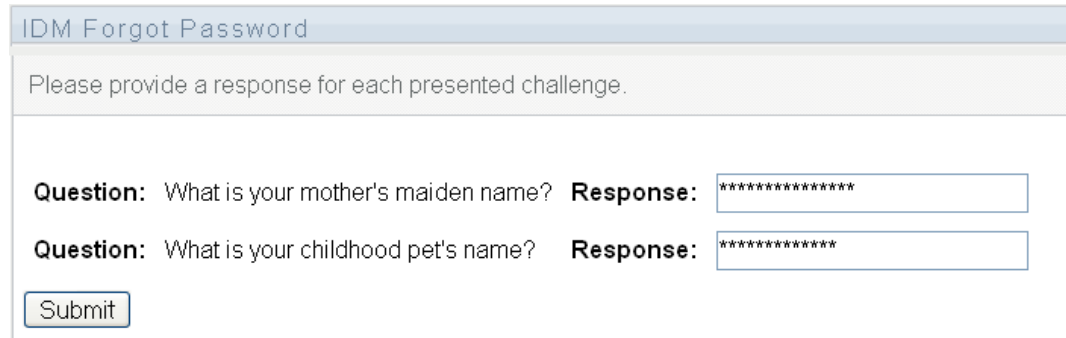

IDM Forgot Password

To help you log in, you must specify your username.

Username: bbrown

Submit

What you see in the Identity Manager Forgot Password dialog box depends on how the system administrator has set up the Forgotten Password option. You can see a hint, have your hint and password sent as an e-mail to you, or you can be allowed to change your password. You can also be provided with challenge questions.

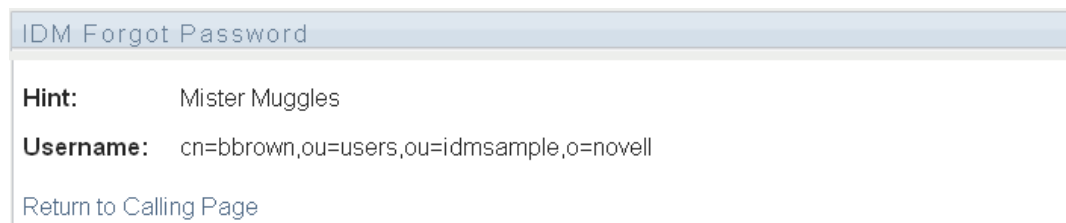For this example, the user is provided with a challenge question and hint.

3 Type your response to the questions, then click *Submit*.

The number of response questions and what they say is configurable by the system administrator.

If you do not answer the questions correctly, you see a *Challenge Response failed* message and are presented with the questions again.

4 After the response questions are answered correctly, you are presented with the password hint, depending on how the system administrator has configured password self-service.

Use the hint to remember your password. If you still cannot remember your password, contact your system administrator.

5 Close the browser window.

8.2 Troubleshooting the Forgotten Password feature

For information about troubleshooting Forgotten Password, see Section 11.1, "Using Forgotten Password," on page 31.

9 Upgrading the Client Login Extension

There is no version upgrade supported for CLE. You need to uninstall the existing version before installing a newer version of it. If you try to install a new version on top of an existing version, you are presented with an option of repairing or removing the existing version. The *Repair* option is same as the Microsoft Windows *Repair* option. If you select it, it troubleshoots the installation issues, such as missing file or configuration issues. You can use the *Repair* option to return to the normal state. The *Remove* option uninstalls the existing version of CLE.

If you make changes to the MSI installation file, remove the existing version of CLE before running the MSI install program again.

10 Uninstalling the Client Login Configuration Utility

Refer to the following sections to uninstall the configuration utility:

10.1 Using Add or Remove Programs to Uninstall the Configuration Utility

1 Open the Add or Remove Programs dialog box in the Control Panel, select *Client Login Extension Configuration Utility Setup 3.7.3.0*, then click *Remove*.

10.2 Using the Setup Wizard to Uninstall the Configuration Utility

1 Re-run `ClientLoginExtensionConfigurationUtilitySetup.msi` to relaunch the Client Login Extension Setup Wizard.

2 Select the option *Remove Client Login Extension 3.7.3.0*, then click *Finish*.

11 **Troubleshooting**

This chapter includes the following sections:

11.1 Using Forgotten Password

Keep in mind the following information as you use the Forgotten Password feature:

- If your system administrator allows you to change your password through this process, it can take up to 15 minutes or longer before all changes are in place throughout the network. Be patient before contacting your system administrator.
- For those using the Novell Client and already logged in to the network, if you right-click the red N in the taskbar, select *NetWare Login*, then select the *Did you forget your password?* link, the restricted browser is not launched. The Client Login Extension applies only when you have not logged in.
- If the server running the Identity Manager User Application is down and you select the *Did you forget your password?* link, you receive the message *An error has occurred* in red on the initial page of the restricted browser. Contact your system administrator.
- If the server running the Identity Manager external WAR is down and you select the *Did you forget your password?* link, you receive the message *Page Not Found* on the initial page of the restricted browser. Contact your system administrator.
- If the URL to the Identity Manager Forgot Password page is incorrectly configured and you select the *Did you forget your password?* link, you receive the message *Page Not Found* on the initial page of the restricted browser. Contact your system administrator.

11.2 Generating Log Files

1. On the Windows *Start* menu, click *Start > Run* to display the Run dialog box.
2. Type regedit, then click *OK* to open the Registry Editor.
3. Browse to the HKEY_LOCAL_MACHINE\SOFTWARE\Novell.
4. Create a new key PSS.
5. Create a new string value in the PSS folder and name the string value as LogDir.

6 Right-click LogDir and select *Modify*. The Edit String dialog box appears.

   Value Data: Enter the directory name in which you want the log files to be created.

   Example: C:\

7 Exit the Registry Editor.

8 The following log files will be generated in the specified directory:

   ◆ `RestrictedBrowserDLL.log`

   ◆ `RestrictedBrowserEXE.log`

11.3 Connecting to the Internet on Windows 7 (32-bit) Through a Proxy Server

When you attempt to connect to the Internet on Windows 7 (32-bit) through a proxy server, you are prompted for a security certificate. This is because Client Login Extension uses System profile along with the Winlogon service. For more information about this issue, see (http://support.microsoft.com/kb/2623724).

11.4 Logging into the Computer if Restricted Browser is Minimized

If an instance of a restricted browser is running and minimized, you may not be able to login to the computer. Use the keyboard shortcuts ALT+TAB to bring up the browser.

11.5 Accessing the Windows Input Method Editor on Non-English Computers

Windows Input Method Editor (IME) does not load if you access the SSPR Forgotten Password page through Client Login Extension on a non-English computer. Without IME, you cannot enter text in other languages except English. However, IME loads without errors when you access the SSPR Forgotten Password page directly using the Web browser.

To workaround this issue, use the keyboard shortcuts ALT+SHIFT key to change the language when the IME fails to load, and then press ALT+TILDE (~) to select any language.