NetIQ Client Login Extension 4.6

Administration Guide

June 2023

Legal Notice

Contents

About this Book and the Library

The *Client Login Extension Administrator Guide* provides information about using the Client Login Extension to provide password self-service functionality.

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.

1 System Requirements

This section provides the minimum requirements to install Client Login Extension. Ensure that you review these requirements before installation.

IMPORTANT: In the preceding table, **Certified** includes the versions that are completely tested and supported. Whereas, **Supported** includes the versions that are not tested but are expected to work.

Table 1-1 *System Requirements for Client Login Extension*

Platform	Requirement	
Self Service Password Reset	**Certified:** ◆ Self Service Password Reset 4.5.3	**Supported:** ◆ Self Service Password Reset 4.5
Operating Systems	**Certified:** ◆ Windows 11 ◆ Windows 10 21H2 ◆ Windows Server 2019	**Supported:** ◆ Windows 11 22H2 ◆ Windows 10 Version 1903 ◆ Windows 10 Version 1909 ◆ Windows 10 (All versions) ◆ Windows 8.1 ◆ Windows 7 SP1 Enterprise **NOTE:** Support for Windows 7 SP1 is deprecated in Client Login extension 4.5.1. ◆ Windows Server 2016 R2 ◆ Windows Server 2012 R2 Latest versions of service packs for the certified operating systems.
ZENworks Configuration Management	**Certified:** ◆ ZENworks Configuration Management 20.2	**Supported:** ◆ ZENworks Configuration Management 20.0
Identity Manager	**Certified:** ◆ Identity Manager 4.8	**Supported:** ◆ Identity Manager 4.8
Client Login Programs	**Certified:** ◆ Client for Open Enterprise Server 2 SP5 (IR2)	**Supported:** ◆ Client for Open Enterprise Server 2 SP5 (IR2)

Platform	Requirement	
.NET Framework	**Certified:** ◆ .NET 4.0	**Supported:** ◆ .NET 4.0

2 Preliminary Tasks

Before running the NetIQ Client Login Extension, you must install Self Service Password Reset. For the supported versions of Self Service Password Reset refer the Section 1, “System Requirements,” on page 7. If you are using Identity Manager (IDM) you require a working Identity Manager application (for example, Identity Manager 4.5 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 Setup Guide (https://www.netiq.com/documentation/idm45/setup_guide/data/front.html).

Configuring NetIQ Self Service Password Reset (Self Service Password Reset)

You must configure the following settings in Self Service Password Reset to enable the Challenge Response Force Enrollment and the Password Expiration Notification features.

NOTE: Self Service Password Reset integration features are only supported in the Active Directory environments.

Configuring Self Service Password Reset for the Client Login Extension Integration

Launch Self Service Password Reset, in the Configuration Editor page, click **Settings** > **Web Services** > **REST Services**. For information about configuring the settings for **REST Services**, refer Integrating Self Service Password Reset with Client Login Extension. You must configure all the settings that are available for **REST Services**.

Configuring Self Service Password Reset for Enabling Password Expiration Warning

Launch Self Service Password Reset, in the Configuration Editor page, click **LDAP** > **Active Directory** > **Allow Authentication When Password Expired**.

For more information on how to integrate Self Service Password Reset with Client Login Extension, see, Integrating Self Service Password Reset with Client Login Extension (https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/t42z6iidt663.html).

3 Configuring Client Login Extension Configuration Utility

Using the Client Login Extension Configuration utility, you can configure the Client Login Extension MSI files for installing the Extension. These MSI files are used to install the Client Login Extension on Windows 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 is available in the `<CD_ROOT>/CLE` folder. Here, CD_ROOT refers to the location where the Client Login Extension Installer files are extracted.

To configure the Client Login Extension Configuration Utility:

1. Double-click the `ClientLoginExtensionConfigurationUtility.exe` file, which is provided as part of the Client Login Extension installer, to launch the utility.
2. Read the license agreement and click **I Agree**, if you agree.Then the Client Login Extension Configuration Utility page appears.

   NOTE: The License Agreement page appears only on the first launch of the Configuration Utility. When you launch Configuration Utility for the second time, License agreement page does not appear.

   ---

3. **Path to Installer to Configure**: Shows the path of the Client Login Extension installer file that is being configured.

   Click the **Browse** button and browse to the appropriate location where the Client Login Extension Installer file is present. By default, the **Browse** button opens the `CLE/Installer` sub-folder.

   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.
4. **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 4.3**.
5. **Link URL**: Specify the URL that the Client Login Extension- restricted browser uses to connect to the Self Service Password Reset 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>/Self Service Password Reset/public/
   ForgottenPassword
   ```

IMPORTANT: You must have a valid URL pointing to the Self Service Password Reset'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 "Using Forgotten Password" on page 29.

6 **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 this button in Client for Open Enterprise Server cannot be changed here.

7 (Optional) **Enable Self Service Password Reset Configurations**: This option allows you to enable the configurations for Self Service password Reset and Emergency Access.

If you select this option, **Change Password through Self Service Password Reset**, **Challenge Response**, **Emergency Access** and **EA Custom Message** options are enabled.

NOTE: To enable this feature, you must have already configured Self Service Password Reset, as described in "Configuring Self Service Password Reset for the Client Login Extension Integration" on page 9 and "Configuring Self Service Password Reset for Enabling Password Expiration Warning" on page 9.

8 **REST URI**: Specify the URI that the Client Login Extension- restricted browser uses to connect to the Self Service Password Reset server by using the 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>/Self Service Password Reset/public/rest
```

9 (Optional) **Change Password through Self Service Password Reset**: Select this option to enable users to change the password through Self Service Password Reset. If you do not select this option, the user can change the password through the default Windows password change mechanism.

NOTE: Users can change the password by using Self Service Password Reset or Windows password change mechanism before or after logging in to the computer.

10 **Password Policy Link Text**: Specify the link that the Client Login Extension- restricted browser uses to connect to the Self Service Password Reset Password Policy page. The default text is **Password Policy**.

11 **Challenge Response**: Select the **Force user for challenge response enrollment** option to prompt the users to answer their challenge responses before logging into the computer. However, if you do not select this option, the user can bypass the Force user for challenge responses prompt and proceed to log in. If you do not select this option, they can skip the challenge response prompt and proceed to log in.

NOTE: If **Self Service Password Reset configurations** is enabled for the users who have not yet enrolled in Self Service Password Reset, they will be prompted to answer their challenge questions regardless of the value of this

setting.

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.

12 **Emergency Access**: Select the **Enable Emergency Access** option to enable the users with a temporary access to the desktop when network is not available by providing the challenge responses configured in Self Service Password Reset. You can specify the other details for emergency access after you enable the **Enable Emergency Access** option such as the following:

1. **Maximum Retry Count**: A numerical value that indicates the maximum number of attempts a user is allowed for answering the **challenge-response** questions, before getting locked out. After the maximum number of attempts are exhausted, the Emergency Access feature is not accessible. The default number of attempts are 3.

   If you have configured a higher number of **challenge-response** questions for the user, specify a higher number for the retry attempts. This helps in a situation where the user forgets some of the answers to the **challenge-response** questions.

2. **System Logout Time**: A numerical value that indicates the number of minutes the user is allowed to use the system in the Emergency Access mode. The time allocated for the session should be configured to ensure that the user does not use the system in the emergency access mode for extended durations. The default time allowed is 30 minutes.

   When lockout is imminent, a warning is displayed on the system tray. After the session time is exhausted, the user is automatically locked out of the system

3. **System Logout Warn time**: A numerical value that indicates the number of seconds the

   User gets the warning before session expires. The default time allowed is 30 seconds.

4. **Emergency Access Login Message**: This message is displayed in system tray for the users who logged into desktop.

13 **EA Custom message**: Type a message in the **EA Challenge Response Dialog Message** field. If network is unavailable, the text that you mention in this setting is displayed when you click on Forgotten password. This message gets displayed on all the Emergency Access dialog boxes.

14 **Advance Settings**: In the **CLE/ Proxy settings** option, you can enable the following settings:

- **Enable CLE tile on the logon screen**: You can specify the text that you want to display on the CLE tile and also specify the path of the image that you want to set as a logo for that tile. If you have enabled this setting, then the forgotten password link will be available only on the CLE tile.
- **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. When you do not enable the proxy server, CLE retrieves information directly from Self Service Password Reset server and does not go through the proxy server.

In the **Security Settings** option, you can select the following settings:

- **Allow URL redirection and forwarding:** When you select this setting, the **Configure** button gets enabled and you can add the list of sites that are available for whitelist.

NOTE: You can add only the secured web sites to the list. To configure CLE for the Google captcha, you must update the URL Redirection list to with the URL https://www.google.com.

- **Add site to trusted zone**: When you select this setting, all the sites mentioned in the URL redirection list and the site mentioned in **Link URL** are added to the Internet Explorer trusted zones.
- **Enable TLS 1.2**: This setting is enabled by default.

15 After all of the information is in place, click **Ok** on the **Advance Settings** page.

16 Click **Configure Installer** to write the new configuration settings to the selected Client Login Extension file.

17 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 5 through Step 17.

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 "Localizing Client Login Extension Files for Other Languages" on page 14.

18 Click **Configure Installer**.

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

Enrolling Challenge Responses in Self Service Password Reset

To enroll Challenge Responses in Self Service Password Reset,

1. Login to the Self Service Password Reset server by using the domain username and password.
2. Select **Setup Password Responses** from the main menu and specify the challenge questions.
3. Save the password responses.

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 3-1 *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 3-1 on page 15, 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.

4 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 4-1 *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
Client for Open Enterprise Server CP	Available	Not available	Available
LDAP CP	Available	Available	Available

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

NOTE: In order to configure the password self-service for Client for Open Enterprise Server and SecureLogin, install Client for Open Enterprise Server and SecureLogin before installing Client Login Extension. For other clients, you can follow any installation sequence.

Prerequisites

You must configure Client Login Extension Configuration utility before installing the Client Login Extension. For Steps to configure Client Login Extension Configuration utility, see Chapter 3, “Configuring Client Login Extension Configuration Utility,” on page 11

To install the Client Login Extension:

1. From the `CLE/Installer` directory, run the appropriate windows installer based on platform and language. Inside the folder `CLE/Installer/x64` and `CLE/Installer/x86`, you can find the following installers based on language:
   - `IdentityManagerClientLoginExtension_en` (English--default)
   - `IdentityManagerClientLoginExtension_de` (German)
   - `IdentityManagerClientLoginExtension_es` (Spanish)
   - `IdentityManagerClientLoginExtension_fr` (French)
   - `IdentityManagerClientLoginExtension_it` (Italian)
   - `IdentityManagerClientLoginExtension_ja` (Japanese)
   - `IdentityManagerClientLoginExtension_cs` (Chinese Mandarin)

- `IdentityManagerClientLoginExtension_ct` (Chinese Traditional)
- `IdentityManagerClientLoginExtension_pt` (Brazilian Portuguese)

For instance, if you are using a 64-bit platform in English language, run the windows installer `IdentityManagerClientLoginExtension_en` from the directory `CLE/Installer/x64`.

2. Read the information on the initial wizard pages, then click **Next**.
3. Follow the on-screen prompts to install the Client Login Extension.

5 Using Emergency Access

The Emergency Access feature helps a user who has forgotten the directory password to access the system. If a user forgets the login password to the directory, the Emergency Access feature uses the **challenge-response** information from NetIQ Self Service Password Reset (Self Service Password Reset) to validate, and grant access to the user even if the user is not connected to the network. If the answers to the **challenge-response** are correct, the user is allowed access to the workstation.

To use the Emergency Access feature, the user should be part of an ActiveDirectory domain.

When the user clicks the **Forgotten Password** link, the Credential Provider checks the Self Service Password Reset server availability. If the Self Service Password Reset server is reachable, a Restricted Browser is displayed. If the Self Service Password Reset server is not reachable, a set of challenge-response questions are displayed. When all the questions are answered, the user can login to the workstation for a specific time.

For more information, see Self Service Password Reset documentation (https://www.netiq.com/documentation/self-service-password-reset/).

Prerequisites

- ❒ Ensure that the user is part of Active Directory domain.
- ❒ (Conditional) If you are using SecureLogin, VC++ Redistributable - Install this component if you are on Windows 8 or Windows 2012 server, install. To download, go to Microsoft Download Center (http://www.microsoft.com/en-in/download/details.aspx?id=30679). While downloading, select the executable based on your platform. For instance, for a 64-bit platform select to download `vcredist_x64.exe`.

  NOTE: `vcredist_arm.exe` is not supported on SecureLogin.

- ❒ Ensure that Self Service Password Reset is installed and the security questions information is setup for the user. For information on configuring security questions information, see Configuring the Setup Security Questions Module (https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b14go6pf.html)
- ❒ The user must log in to the online mode at least once before attempting to connect by using the Emergency Access feature.

  Logging in the online mode ensures that any changes to the challenge-response questions are updated in the local cache.

Configuring Emergency Access

1. Login to the Self Service Password Reset server using the domain username and password.
2. Click **Setup Security Questions**.
3. Specify the security questions.
4. Save the password responses.
5. Click your username and click **Configuration Editor**.
6. Specify the configuration password and click **Sign in**.
7. Click **Settings > Web Services > REST Services**.
8. In **Enable Web Services**, select **Enabled (True)**.
9. In **Allow Challenge Services to Read Answers**, select **Enabled (True)**.
10. In **Web Services LDAP Authentication Permissions**, you can query by using **Add Filter** to define the LDAP filter that includes the object class, and by using **Add Group** that includes the LDAP group. Users specified here are permitted to execute REST web services.

Using the Emergency Access Feature

1. Click **Forgotten Password** on the Windows logon page.

   The Credential Provider checks the availability of the Self Service Password Reset server. If the Self Service Password Reset server is reachable, a Restricted Browser window is launched. If the Self Service Password Reset server is not reachable, the challenge-response dialog is displayed.
2. If the challenge questions are answered, the user can log in using Emergency Access feature for a specified time.

   After expiry of the specified duration, the user is logged out automatically.

6 Installing the Client Login Extension MSI File

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

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). You can choose the `IdentityManagerClientLoginExtension_xx.msi` file from the location `CLE\Installer\x64` or `CLE\Installer\x86` based on the platform.

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 "Using the Client Login Extension Installer Command Line Options" on page 21.

   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**.

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+
```

7 Using the Forgotten Password Feature

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

Configuring Self Service Password Reset for Forgotten Password

You can allow users to use challenge response or one time password during forgotten password process. To use any of these verification methods, you need to configure the Self Service Password Reset settings. For more information about configuring forgotten password settings refer, Configuring Forgotten Password Module (https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b1ggnqpg.html).

Client Login Extension now supports more secured hashing methods. The responses are stored in PBKDF2WithHmacSHA512 hashing method. By default, Self Service Password Reset uses the PBKDF2WithHmacSHA512 hashing method.

Accessing the Forgotten Password

You can access the forgotten password link after running the Client Login Extension MSI file on a supported Windows version, or on workstations running the Client for Open Enterprise Server 2 SP4. See Chapter 2, "Preliminary Tasks," on page 9 to ensure that you have all the information in place for Password Self-Service to work.

The users, who have Client for Open Enterprise Server running on their computer, need to perform the following to access the forgotten password:

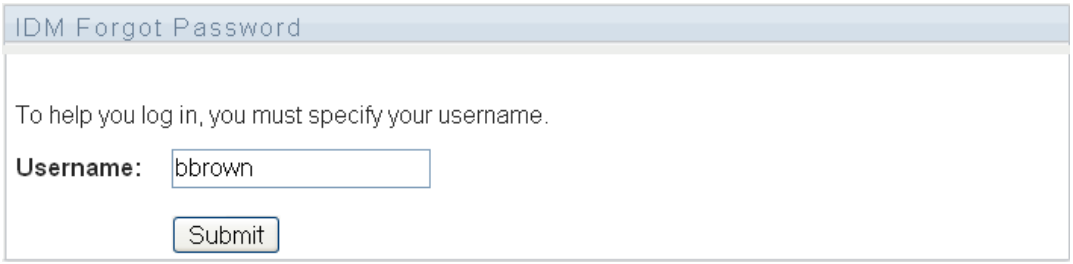
1. If you forget your password, click the **Did you forget your password?** link in Client for Open Enterprise Server.

   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

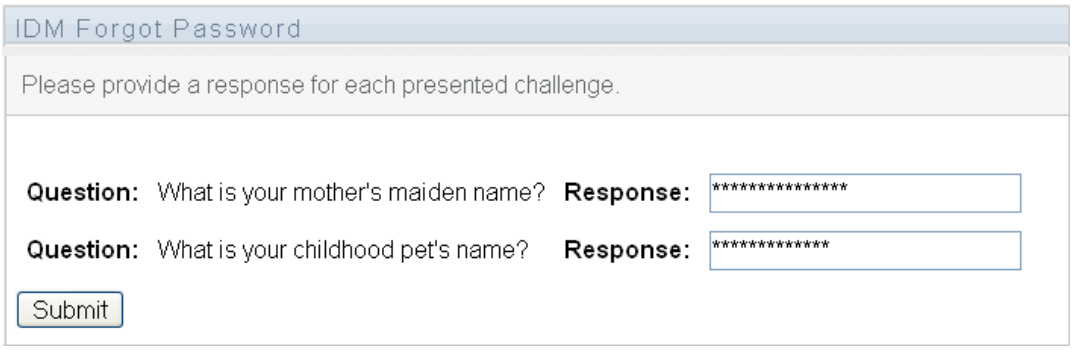
- Disables right-clicking
- Disables ActiveX
- Disables scripts
- Runs on its own process, separate from the Winlogon process.

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**.



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.

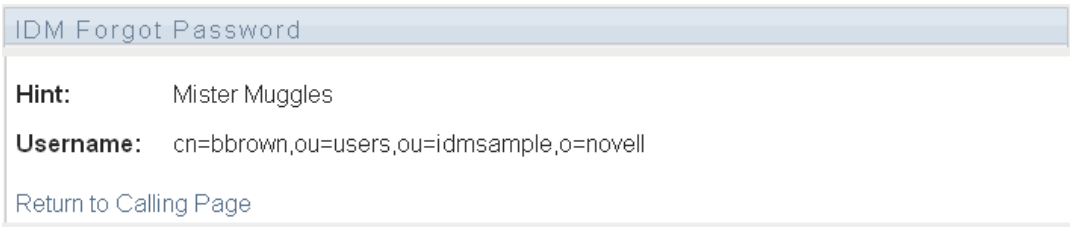


3 Type your response to the questions, then click **Submit**.

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.

The users who do not have Client for Open Enterprise Server running on their computer are redirected directly to the Self Service Password Reset page where they require to answer the challenge responses to retrieve their password. For more information about Forgotten Password feature in Self Service Password Reset refer Configuring Forgotten Password (https://www.netiq.com/documentation/self-service-password-reset-42/sspr-adminguide/data/b1ggnqpg.html) in the Self Service Password Reset Administration guide.

Troubleshooting the Forgotten Password feature

For information about troubleshooting Forgotten Password, see “Using Forgotten Password” on page 29.

Changing Password Through Self Service Password Reset

Client Login Extension facilitates changing the users’ domain passwords through Self Service Password Reset. When a user presses Ctrl-Alt-Del keys, he is presented with the **Change a Password** option using which he can initiate password change.

If the **Change password through Self Service Password Reset** option is enabled in the Client Login Extension Configuration utility, the Client Login Extension routes the password change request to Self Service Password Reset.

8 Upgrading the Client Login Extension

You can upgrade Client Login Extension from the versions 4.3, 4.4, 4.4.1, and 4.5 to 4.5.1. Perform Step 2 before you upgrade Client Login Extension from the versions 3.9 and 3.10 to 4.2.

NOTE: For upgrading from older versions of Client Login Extension, you need to uninstall the older version of Client Login Extension and install Client Login Extension 4.5.

To upgrade Client Login Extension, perform the following:

1. Extract the downloaded Client Login Extension installer file and run the `ClientLoginExtensionConfigurationUtility.exe` executable to launch the Configuration Utility.
2. Configure the required installer using the Client Login Extension Configuration Utility. For more information, refer Chapter 3, “Configuring Client Login Extension Configuration Utility,” on page 11
3. Run the appropriate Client Login Extension Installer based on language and platform from the extracted folder CLE/Installer.
4. Follow the on-screen prompts and install Client Login Extension.

   After installation of Client Login Extension, all the Client Login Extension installer files are replaced with the latest Client Login Extension installer files. However, the older version of Client Login Extension Configuration Utility installer files are not removed. You can remove the older Client Login Configuration Utility installer file from the Control Panel, if required.

9 Troubleshooting

This chapter includes the following sections:

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 Client for Open Enterprise Server and already logged in to the network, if you right-click the tray icon of Client for Open Enterprise Server 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 URL to the Self Service Password Reset 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.

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`
- `CLECredentialProviderdll.log`
- `NclePwmManager.log` (If Self Service Password Reset integration is enabled)
- `eadebug.log` (If EmergencyAccess is enabled)

Enabling Dialog Box On Restricted Browser

From Client Login Extension 4.4, as a security enhancement, all the dialog boxes displaying on the restricted browser are disabled by default. Perform the following steps to enable specific dialog boxes.

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 string value in the **RestrictedBrowser** folder and name the string value as `WhiteListDialogTitle`.

5 Right-click `WhiteListDialogTitle` and select **Modify**. In **Value Data**, specify the dialog box name that you want Client Login Extension to display. You can specify multiple names separated by semi-colon (;).

Customizing the Emergency Access Cache Update

Perform the following steps to customize the Emergency Access cache update.

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\MsPssGina`.

4 Create a new DWORD value and name the DWORD value as `EAMaxCacheRetryCount`.

5 Right-click EAMaxCacheRetryCount and select **Modify**. In **Value Data**, specify the time in minutes.

6 Create a new DWORD value and name the DWORD value as `EACacheRetryTimeout`.

7 Right-click EACacheRetryTimeout and select **Modify**. In **Value Data**, specify the time in minutes.

See the following examples to understand these registry entries.

- **EACacheRetryTimeout = 5** Client Login Extension attempts to update the cache once in five minutes.
- **EAMaxCacheRetryCount = 0** Client Login Extension attempts to update the cache only during login and no attempt after login.
- **EAMaxCacheRetryCount = 5** Client Login Extension attempts five times to update the cache with time interval specified in the EAMaxCacheRetryCount registry.

NOTE: If you do not specify these registries, the following default values are considered for cache update.

`EAMaxCacheRetryCount = 0`

`EACacheRetryTimeout = 5 minutes`

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. You can perform one of the following to overcome this issue:

- Use the keyboard shortcuts ALT+TAB to bring up the browser.
- Keep the restricted browser maximized by updating the registry settings.

  Set the value of DWORD `MaximizeWindow` as `1` at `HKEY_LOCAL_MACHINE\SOFTWARE\NovellRestrictedBrowser` to keep the restricted browser window maximized

Accessing the Windows Input Method Editor on Non-English Computers

Windows Input Method Editor (IME) does not load if you access the Self Service Password Reset 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 Self Service Password Reset 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.

Windows 10 Workstations Does Not Display the Forgotten Password Link

The forgotten password link is not displayed on some Windows 10 workstation. This issue occurs because of the missing visual studio runtime libraries.

To workaround this issue, download the libraries from Microsoft and install the libraries.

For more information on latest supported downloads, see Supported Downloads (https://learn.microsoft.com/en-US/cpp/windows/latest-supported-vc-redist?view=msvc-170).

Forgotten Password Link Does Not Get Triggered after Installing the Latest Advanced Authentication Windows Client

Issue: With CLE 4.6, the `RestrictedBrowserEXE` path is changed while the AA Windows client is expecting the executable to be located in the `Windows\System32` folder.

Workaround 1: Install the newer Advanced Authentication 6.4.2 windows client.

Workaround 2: Perform the following modifications on the workstation:

1. Copy `c:\windows\system32\ncle\restrictedbrowserexe.exe` to `c:\windows\system32`.
2. Copy `c:\windows\system32\ncle\restrictedbrowserexe.dll` to `c:\windows\system32`.
3. Modify the system path to include `c:\windows\system32\ncle`.