Client for Open Enterprise Server Release Notes

October 2023

Naming Conventions

Client for Open Enterprise Server refers to the version of the Client for Windows 7, Windows 8, Windows 10, Windows 11, Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Windows Server 2019, and Windows Server 2022.

What's New in Client for Open Enterprise Server

The following changes are included:

What's New in Client for Open Enterprise Server 2 SP7

Micro Focus is now OpenText

For more information, see "Rebranding Changes" on page 6.

NCP Server Side Copy

Beginning with Client for Open Enterprise Server 2 SP7 (IR4) and later, the "OES Copy" functionality will take advantage of Open Enterprise Server capabilities to perform server-side copy operations. This capability will be available only if the source and destination paths specified in the "OES Copy" dialog are within the same volume, or for paths that represent distinct volumes within the same server.

When the supplied paths are determined to qualify for taking advantage of OES server-side copy capabilities, the files will be copied using OES server-side copy NCPs. This will be more efficient than reading and writing the data through the Client for Open Enterprise Server workstation, and can also substantially increase the performance in scenarios where VPN or low-bandwidth networks are involved that would otherwise limit the data transfer rate.

The "OES Copy" feature in the Open Enterprise Server Client is currently the only copy mechanism that can utilize the Open Enterprise Server capabilities to perform server-side copy operations. Further enhancements might include extending this functionality to non-client for Open Enterprise Server copy operations, including paste or drop in Windows File Explorer or third-party applications using the Microsoft CopyFile/CopyFileEx APIs, and so on.

Long Path Support

The Client for Open Enterprise Server 2 SP7 release has eliminated limitations in the kernel-mode drivers which prevented Microsoft Windows file system APIs from working on NCP-based paths which were close to or in excess of the Microsoft Windows "MAX_PATH limit" of around 260 characters. Windows applications specifically designed to take advantage of paths longer than the traditional Microsoft Windows MAX_PATH limit can now successfully specify such paths over NCP. For more information, see Enabling Long Path Support in the Client for Open Enterprise Server Administration Guide.

NCP Encryption TLS 1.3 Support

On Windows 11 and later platforms, the NCP encryption feature now supports using TLS 1.3 when negotiating encryption protocol with the NCP server.

What’s New in Client for Open Enterprise Server 2 SP6

Platform Support

Client for Open Enterprise Server 2 SP6 and later supports Windows 10 update (version 20H2).

Supports Windows 10 Multiple Credential Provider Selection

Client for Open Enterprise Server 2 SP6 optionally supports a Windows 10 credential provider behavior which allows users to select among multiple installed credential providers if necessary easily. When enabled, the Client for Open Enterprise Server credential provider appears in the “Sign-In Options” list along with the other available credential providers for the Windows user accounts.

By default, Client for Open Enterprise Server still operates in the “legacy mode” that presents only the last logged-on user and the “Other User” credential. Starting with Client for Open Enterprise Server 2 SP6, both modes of operation are available to provide whichever behavior would best accommodate the login needs of a workstation.

Custom Re-branding

The Custom Branding feature provides a text-based branding change to customize any string or a specific keyword as per the requirement. The feature also offers multi-language support to customize the strings as per the language preference in which Client for OES was installed.

NCP Encryption and Multi Factor Authentication Enhancement

The Client for Open Enterprise Server 2 SP6 provides support for NCP Encryption and Multi Factor Authentication capability on the volume level as well. Now each volume can be separately configured for encryption or Multi Factor Authentication.

For information on the NCP server side configuration for Volume Encryption, see Managing NCP Security Configurations in the OES 2018 SP3: NCP Server for Linux Administration Guide.

Azure based Active Directory Login Support

The Client for Open Enterprise Server 2 SP6 now provides Azure Active Directory Support. Users can now login to a Microsoft-hosted Azure Active Directory domain using the Client for Open Enterprise Server.

Salvage and Purge Enhancements for Search Filters and Search Subdirectories

The Client for Open Enterprise Server 2 SP6 provides filter options in Salvage and Purge window to help customers navigate the exceedingly long lists of available files. This filter option enables a user to generate and implement an ability to filter the list by different criteria. For example, a specific filename pattern, or a specific date range for the file's deletion timestamp, or a specific date range for the file's creation or modification timestamp.

One can now browse through the deleted subdirectory files from the Salvage/Purge window with the **Include Subdirectory Files** checkbox option.

What’s New in Client for Open Enterprise Server 2 SP5

Platform Support

Client for Open Enterprise Server 2 SP5 (IR2) and later supports Windows 10 update (version 20H2).

NCP Encryption Support

The feature NCP Encryption on OES is a security feature that increases the security of data transmitted across networks between the NCP server and clients.

The Client for Open Enterprise Server 2 SP5 and later provides support for NCP Encryption capability on the OES 2018 SP2 or later server. The following are the new parameters introduced in the Client Properties to support this functionality:

- NCP Encryption
- Cipher Strength

For more information on the parameters, see Advanced Settings in the Client for Open Enterprise Server Administration Guide.

For information on the NCP server side configuration for NCP Encryption, see Managing NCP Security Configurations in the OES 2018 SP3: NCP Server for Linux Administration Guide.

Multi Factor Authentication Enhancement

The Advanced Authentication capability on the Client for Open Enterprise Server 2 SP5 is enhanced to support the Multi Factor Authentication (MFA) on the OES 2018 SP2 server. For more information on the NCP server side configuration for MFA, see Managing NCP Security Configurations in the OES 2018 SP3: NCP Server for Linux Administration Guide.

Server Platform Support

The Client for Open Enterprise Server 2 SP5 supports the Open Enterprise Server (OES) 2018 SP2 release.

Enhanced eDirectory Password Expiration Handling

Previously, the eDirectory password expiry was handled after the execution of the eDirectory login scripts on the user's desktop. Now, the eDirectory password expiration is handled during the login of the user and changing the passwords during the grace login period.

- If the **Password Expiry Warning** option is enabled, the user is alerted to change the password before the actual expiry date.
- If the **Force Grace Login Password Change** option is enabled, the user must change the password before the expiry of the grace login. Else the user will not be able to login.

In cases where the eDirectory account also defines the Windows account, updating the eDirectory password prior to the Windows account improves Domain Services for Windows and other domain account synchronization scenarios.

What's New in Client for Open Enterprise Server 2 SP4

- **LDAP Contextless Login:** Client for Open Enterprise Server 2 SP4 (IR13) and later supports TLS 1.1 and TLS 1.2 encrypted connections only if the LDAP server supports (TLS 1.1 or TLS 1.2) them. This improvement allows connections to avoid the vulnerabilities of TLS 1.0 and earlier versions of the transport layer protocol.
- The Client for Open Enterprise Server 2 SP4 (IR12) and later provides support for the following Advanced Authentication features:
  - **Offline Logon:** Allows to perform an Advanced Authentication logon on a workstation by using the previously cached logon information. This feature can be used in two modes and the Client for Open Enterprise Server credential provider supports both these modes:
    1. Force Offline Login Manually - Provides a check box **Offline logon** during logon. For information on configuring this mode, see Configuring to Force Offline Login Manually in the Advanced Authentication - Windows Client guide.
    2. Enforced Cached Login - An offline logon is always attempted first using the cached logon information and then connects to the Advanced Authentication server in the background. For information on configuring this mode, see Configuring the Enforced Cached Login in the Advanced Authentication - Windows Client guide.

    NOTE: This feature allows the user to logon with Advanced Authentication for Computer Only Logon scenario. It is not possible to perform an offline logon to eDirectory. A network connectivity is always required for an eDirectory login.

  - **Custom Messages:** The Client for Open Enterprise Server credential provider now supports receiving custom messages defined in the Advanced Authentication server policies. For information on configuring Custom Messages, see Custom Messages in the Advanced Authentication - Administration guide.
- **Platform Support:** Client for Open Enterprise Server 2 SP4 (IR12) and later supports Windows Server 2019 and is tested and certified for the latest Windows 10 Update (version 1903).

- **Multi-factor Authentication:** The Client for Open Enterprise Server 2 SP4 (IR11) and later provides an enhanced integration of Client for Open Enterprise Server with Advanced Authentication Client for Windows. The highlights are:
    - The Client for Open Enterprise Server Credential Provider is used as the credential provider to perform both eDirectory and Windows account logon through the Advanced Authentication methods.
    - An option to use the NetIQ Advanced Authentication Credential Provider is also available in Client 2 SP4 (IR11), which was possible in the previous Client releases from Client 2 SP4 (IR6) to Client 2 SP4 (IR10) with Advanced Authentication.
    - A new tab, **Advanced Authentication** is available in the Show Advanced Options dialog during logon to specify the Advanced Authentication logon details.

NOTE: The Client for Open Enterprise Server 2 SP4 (IR11) release is focused only on the enhanced Advanced Authentication integration behavior with the Client, and does not contain any other fixes or changes that are not related to Advanced Authentication.

- **Dependent Products:** The Client for Open Enterprise Server 2 SP4 (IR9) and later includes the following version of the dependent products:
    - NetIQ Modular Authentication Services (NMAS) 9.0.4.1
    - Novell International Cryptographic Infrastructure (NICI) 3.0.3

  For information on installing Client for Open Enterprise Server, see Advanced Installation Options in the Client for Open Enterprise Server Administration Guide.
- **File Compression Configuration:** Beginning with Client for Open Enterprise Server 2 SP4 (IR9), the compression attributes are available for files too. The **Don't Compress** and **Immediate Compression** attributes can now be enabled or disabled on files, directories, and volumes in the **OES Info** tab of the **Properties** window.
- **Platform Support:** Client for Open Enterprise Server 2 SP4 (IR8) and later supports Windows 10 RS4 Update.
- **OES 2018 Support:** With the OES 2018 support, users on Client for Open Enterprise Server 2 SP4 (IR7) and later can perform salvage and purge operations on NSS files having 64-bit ZID numbers using the client.
- **File Caching:** Client for Open Enterprise Server 2 SP4 (IR7) and later supports write caching for network files along with the existing read caching capability. This provides increased efficiency in reading and writing data to network files. For information on the File Caching parameter settings, see Advanced Settings in the Client for Open Enterprise Server Administration Guide.

Client Integration with Advanced Authentication

Client for Open Enterprise Server 2 SP4 (IR6) and later provides optional installation-time integration with the Advanced Authentication Client for Windows, and also optional functionality to require that the Advanced Authentication Client must be used when initiating an eDirectory login. This enables you to perform multi-factor authentication to Windows using Advanced Authentication Client followed by seamless eDirectory login through the Client. For more information on Installing and Configuring Advanced Authentication Client, see Client for Open Enterprise Server Administration Guide.

Further integration capabilities for Client for Open Enterprise Server and Advanced Authentication are being explored and planned to be delivered in the upcoming releases of Client for Open Enterprise Server.

For more information on Advanced Authentication, see Advanced Authentication documentation site.

Client Updated With SHA-2 Certificates

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.

Rebranding Changes

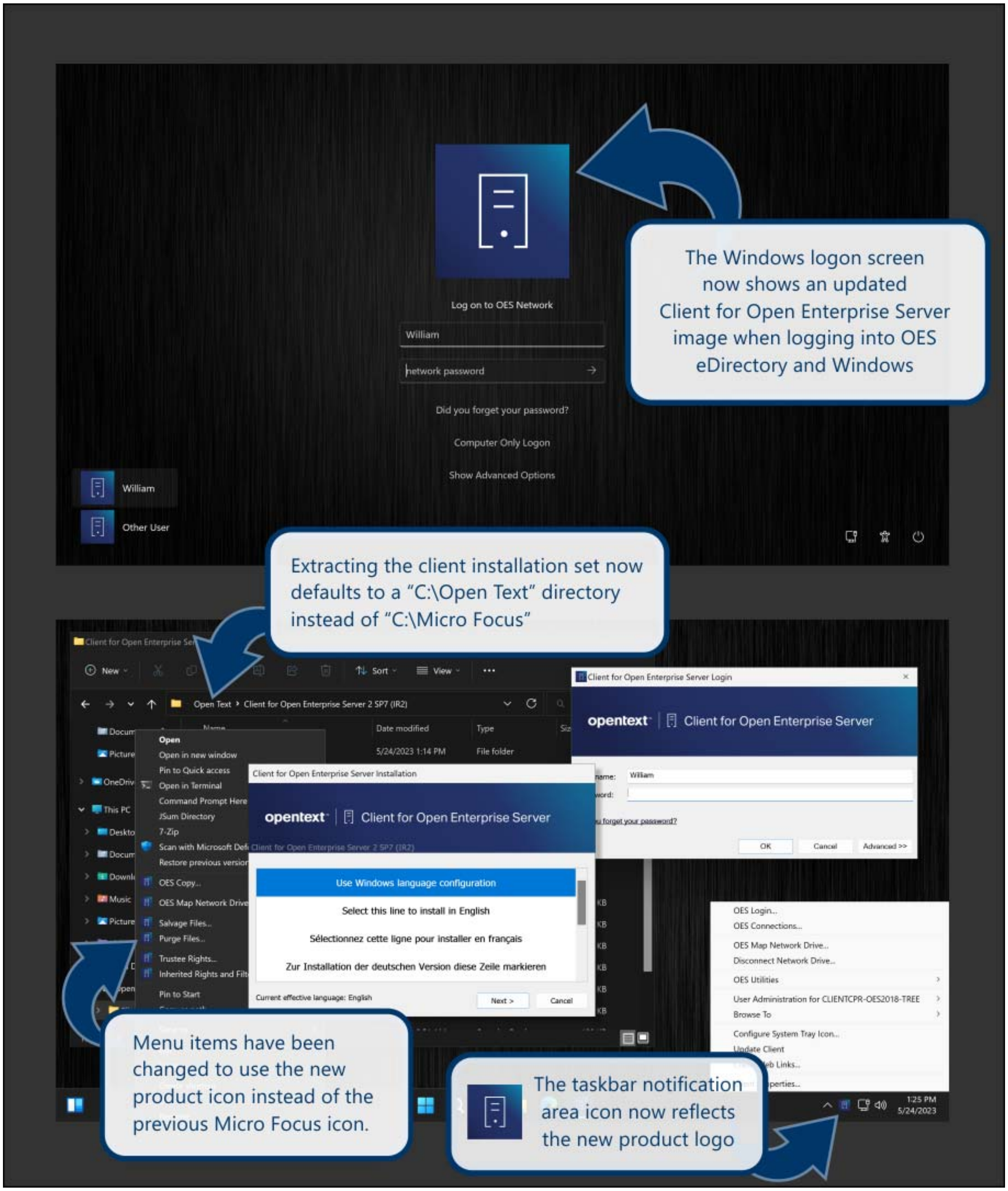
Micro Focus is now part of OpenText. For Client for Open Enterprise Server 2 SP7 (IR2) and later, this branding update is applicable.

Products across the portfolio are now being rebranded to reflect OpenText or a more appropriate name. This corporate change impacts the name of products and components, user interfaces, logos, and so on. The corporate name remains same, "`Client for Open Enterprise Server`".

The documentation update to reflect these changes (such as names and screenshots) is being done in a phased manner.

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 *Overview of Client for Open Enterprise Server*



The Windows logon screen now shows an updated Client for Open Enterprise Server image when logging into OES eDirectory and Windows

Extracting the client installation set now defaults to a “C:\Open Text” directory instead of “C:\Micro Focus”

Menu items have been changed to use the new product icon instead of the previous Micro Focus icon.

The taskbar notification area icon now reflects the new product logo

Log on to OES Network

William

network password

Did you forget your password?

Computer Only Logon

Show Advanced Options

Open Text › Client for Open Enterprise Server 2 SP7 (IR2)

Client for Open Enterprise Server Installation

opentext | Client for Open Enterprise Server

Client for Open Enterprise Server 2 SP7 (IR2)

Use Windows language configuration

Select this line to install in English

Sélectionnez cette ligne pour installer en français

Zur Installation der deutschen Version diese Zeile markieren

Current effective language: English

Client for Open Enterprise Server Login

opentext | Client for Open Enterprise Server

name: William

For more information, see Rebranding Changes in the Client for Open Enterprise Server Administration Guide.

Installation

- “Supported Windows Platforms” on page 8
- “Supported Server Platforms” on page 8
- “Installing the Client for Open Enterprise Server” on page 8

- “Uninstalling a Later Version of Client for Open Enterprise Server to Reinstall a Previous Client Version” on page 9
- “The Total Path to the Installation Set Must Not Exceed 214 Characters.” on page 10

Supported Windows Platforms

The Client for Open Enterprise Server is supported on the following platforms:

- Windows 11 (x64)
- Windows 10 (x86 or x64)

  (Enterprise Edition, Education Edition, or Professional Edition)
- Windows 7 SP1 (x86 or x64)
- Windows 7 (x86 or x64)

  (Ultimate Edition, Enterprise Edition, or Professional Edition)
- Windows Server 2022 (x64)
- Windows Server 2019 (x64)
- Windows Server 2016 (x64)
- Windows Server 2012 R2
- Windows Server 2012 (x64)

The Client for Open Enterprise Server is also supported in Remote Desktop Services and Desktop Virtualization environments.

NOTE

- Ensure Windows 7 and Windows Server 2008 R2 are installed with Microsoft security update KB3033929 to add support for SHA-2 certification.
- The Client for Open Enterprise Server might run but is not supported on Windows Starter, Home Basic, and Home Premium editions.

Supported Server Platforms

The Client for Open Enterprise Server supports Open Enterprise Server (OES) 24.1, OES 23.4, OES 2023, OES 2018, OES 2015 SP1, OES 2015, OES 11 SP2, OES 11 SP1, OES 11, OES 2, and NetWare 6.5.

On Windows Server platforms, the Client for Open Enterprise Server might run but is not supported on Datacenter Edition, Web Server Edition, or on Server Core installations using any edition.

Installing the Client for Open Enterprise Server

To install the Client, run the `setup.exe` file located in the `C:\Open Text\Client for Open Enterprise Server` directory.

Uninstalling a Later Version of Client for Open Enterprise Server to Reinstall a Previous Client Version

The NMAS client installed with Client for Open Enterprise Server includes NICI as a required dependency. Uninstalling the Client automatically uninstalls the NMAS client, but intentionally does not uninstall NICI because other applications on the workstation besides NMAS or the Client may still be using NICI services.

If you uninstall the Client for Open Enterprise Server with the intention of installing a previous version of the Client, it is recommended that you also uninstall NICI (and NICI for Windows x64, if running Windows x64) before re-installing the previous Client.

Attempting to install the initial an earlier Client without first removing NICI can result in one or more of the following issues:

- During installation of the Client on Windows 7 x64, the NMAS Challenge/Response method will report a 1603 error. This is because the NMAS client included in the initial release cannot resolve its required dependencies using the newer version of NICI still present on the machine.
- When starting up, the Windows welcome screen on Windows x64 displays an error, such as `The procedure entry point CCSX_Authenticate could not be located in the dynamic link library ccswx64.dll`.
- The NICI installer of the older NICI version can damage the existing newer NICI installation. For example, attempting to install NICI 2.7.3 or NICI 2.7.4 when NICI 3.0.3 is already present. Subsequent attempts to use NICI can report -1471 0xFFFFFA41 NICI_E_SELF_VERIFICATION errors due to the damaged NICI installation.
- The Client for Open Enterprise Server 2 SP4 (IR9) and later contains NICI 3.0.3. Earlier versions of Client for Open Enterprise Server contains NICI 2.77.3. If you are intending to uninstall NICI 2.77 or later and re-install NICI 2.76, an additional step is necessary. The Novell NICI installer intentionally leaves behind certain NICI files, including `CCSW32.DLL` and `CCSWX64.DLL`. Due to an issue in the NICI 2.76 for Windows x64 installer, re-installing NICI 2.76 on Windows x64 is unable to overwrite the `CCSWX64.DLL` file left behind by the NICI 2.77 or later installers.

  To uninstall a later version of NICI and re-install NICI 2.76 on Windows x64, in addition to uninstalling the NICI product, you will need to rename or delete the `CCSWX64.DLL` from the Windows SYSTEM32 directory.

  IMPORTANT: If you omit this step, NICI 2.76 will still appear to install correctly, but attempting to login to eDirectory using NMAS will fail with a NICI-specific NICI_E_SELF_VERIFICATION (-1471) error. When this issue happens, or before this issue happens, rename or delete the `CCSWX64.DLL` in the Windows SYSTEM32 directory and then run the Novell Client 2 SP2 or earlier installation again to re-install NICI 2.76 successfully.

If you fail to follow these guidelines, features that require NMAS will not function, due to one or all of the above conditions.

These guidelines and issues also apply to installing the Client on a Windows Server 2012 machine where eDirectory 8.8 SP5 or later has already been installed. eDirectory on Windows Server 2008 includes NICI 2.7.6 or later, and installing previous versions of the Client which include NICI 2.7.4 or earlier can cause the NICI installation to become damaged.

The Total Path to the Installation Set Must Not Exceed 214 Characters.

The path to any and all files within a Client for Open Enterprise Server installation set must not exceed 256 characters.

Currently this means the directory path into which you extract the installation set must not exceed 214 characters. This limit is relative to the traditional MAX_PATH or 256-character limit in Windows applications, but also takes into account additional path space that is needed for running the installation.

If the installation set is being accessed from a remote network location, for example \\*servername**volumename*, the length of the network server and volume name also counts against the maximum depth, due to underlying processing that makes use of the *real* path to the installation set. Even if a mapped drive letter and/or the **map root** feature is used for accessing the installation set, the limit is measured as if a UNC path had been used.

Upgrading Client Interim Release

You can download and upgrade to the interim release from Market Place (https://www.microfocus.com/marketplace/appdelivery/content/client-for-open-enterprise-server).

Compatibility with Windows 10 Secure Boot

The Client for Open Enterprise Server 2 SP4 (IR4) and later provides enhanced compatibility with Windows 10 and the UEFI Secure Boot feature. On the Windows 10 July 2016 (build 10493) and later releases, and also on Windows 10 July 2015 (build 10240, before any Windows updates are applied), if the Client for Open Enterprise Server is running on a Windows machine where UEFI Secure Boot is enabled, then the machine fails to boot and instead launches Automatic Repair mode. To avoid this issue, install the Client for Open Enterprise Server 2 SP4 (IR4) on any Windows 10 machine where Secure Boot is enabled, rather than installing any previous version of the Client.

If you have already encountered this issue and your Windows 10 machine is booting into Automatic Repair mode, or if you must continue to use an earlier version of the Client for Open Enterprise Server but still need to avoid this issue, refer to the TID 7017838 (https://www.novell.com/support/kb/doc.php?id=7017838) to resolve the problem.

Known Issues

- "Salvage, Purge and OES Copy Features do not Support Long Paths" on page 11
- "Microsoft SmartScreen Warning when Accessing Some Files on Long Paths" on page 12
- "Earlier Versions of Client for Open Enterprise Server Fail to Load on Windows 11 22H2 and Later" on page 12
- "Newly Added Windows User Does Not Get Default Client Login Option" on page 12
- "Change Password Feature is Not Available when the Workstation is Connected to Azure AD Domain" on page 12
- "The Client on Microsoft Surface Pro 4 or Later Does Not Reconnect After the Workstation Wakes Up" on page 12
- "Additional Advanced Authentication Login is not Prompted for Additional eDirectory Login Attempts Through Login Script" on page 13
- "Client for Open Enterprise Server 2 SP4 (IR11) Does Not Support Authentication Chain" on page 13

Salvage, Purge and OES Copy Features do not Support Long Paths

The Client for Open Enterprise Server shell extension features such as Salvage, Purge and OES Copy do not yet support the longer paths, which can be created and accessed through the Client for Open Enterprise Server 2 SP7 client. These features are not be available for paths which exceed the Microsoft Windows MAX_PATH limit of 260 characters. In addition, the Salvage, Purge and OES Copy features skips processing any enumerated files or subfolders, which cannot be supported within MAX_PATH limits.

Microsoft SmartScreen Warning when Accessing Some Files on Long Paths

It is observed that the Microsoft's SmartScreen filter sometimes present a warning “Windows Security: These files can't be opened. Your Internet Security settings prevented one or more files from being opened.” This happens when using Microsoft's File Explorer to launch an associated application for a file that exists on a long path, which exceeds the Windows MAX_PATH default length of 260 characters. It is currently unclear whether this is a MAX_PATH limitation of SmartScreen itself, and remains under investigation.

Earlier Versions of Client for Open Enterprise Server Fail to Load on Windows 11 22H2 and Later

If the Client for Open Enterprise Server 2 SP6 (IR1) or earlier is available on a machine that is updated to Windows 11 22H2, the login interface reports: “a required network service has not started”. The Windows 11 22H2 release actively blocks the Client 2SP6 (IR1) or earlier kernel-mode drivers, but only on certain hardware platforms. Installing the Client for Open Enterprise Server 2 SP6 (IR2) or later release resolves the issue. For more information, see the Micro Focus Knowledge Base Article (https://portal.microfocus.com/s/article/KM000010710?language=en_US).

Newly Added Windows User Does Not Get Default Client Login Option

When using the “Windows 10 behavior” credential provider mode, Microsoft initially defaults to selecting the Microsoft credential provider for new Windows users. The “Sign-in options” must be used for first-time or newly-created Windows user accounts, to explicitly select the Client for Open Enterprise Server's credential provider. The selection is then expected to remain the default for future logins as this same Windows user account, until the user explicitly uses the “Sign-in options” again to select a different credential provider.

Change Password Feature is Not Available when the Workstation is Connected to Azure AD Domain

- The change password feature in NWTray does not work for Azure Password change. The password change can be done only through Azure Portal. To change the Azure AD password, use **Ctrl+Alt+Del > Change Password** option.
- Ctrl+Alt+Del option in Azure Environment will take the user to the portal to change the password. To change the password of an eDirectory user use NWTray.
- Windows is unable to take either old or new password after the eDirectory password is changed with Zenworks DLU policy applied.

The Client on Microsoft Surface Pro 4 or Later Does Not Reconnect After the Workstation Wakes Up

After the Microsoft Surface Pro 4 or later wakes up from sleep mode, the Client for Open Enterprise Server on it does not reconnect and reports an error. To resolve this issue, create a registry key `NetworkAdapterPowerEventHandling` of type DWORD under `[HKLM\SOFTWARE\Novell\Client\Parameters\NetworkAdapterPowerEventHandling]` and set the value to `0`.

Additional Advanced Authentication Login is not Prompted for Additional eDirectory Login Attempts Through Login Script

Additional eDirectory logins created during eDirectory login script processing does not prompt for additional Advanced Authentication logins. The password of the primary eDirectory login performed with Advanced Authentication is used for the additional eDirectory login attempts as well.

Client for Open Enterprise Server 2 SP4 (IR11) Does Not Support Authentication Chain

The Advanced Authentication feature of selecting which authentication chain should be used during login is currently not supported in Client for Open Enterprise Server.

Deferred Write or Time Stamp Changes Might Not Reflect in Directory Listings

With File Caching configured for Read and Write, if an application performs a directory enumeration before one or more deferred writes or time stamp changes have been committed to the server, the enumerated file information received from the server might not reflect the written file size or time stamp information. This is because the Read and Write caching is still being processed. However, the information is not lost and it will reflect in future directory enumerations after the background writer commits all pending changes.

eDirectory Login Fails After Windows Upgrade to Windows 10 RS3

When you upgrade a device to Windows 10 RS3 (Fall Creators Update) with Client for Open Enterprise Server 2 SP4 (IR6) or earlier already installed, the eDirectory login scripts fail to run and NCP connections fail to establish after Windows logon.

When you upgrade a device to Windows 10 RS3 without Client for Open Enterprise Server, the first login after installing Client for Open Enterprise Server on the upgraded device logs into both eDirectory and Windows successfully. But the issue of eDirectory login scripts failing to run and missing NCP connections is observed on the second and subsequent logins with the same credentials used for first login.

This is because of a new feature introduced in Windows 10 RS3 to automatically reboot the device using the logon information of the user who had logged in last on the device. This feature creates a Windows-only logon session automatically on behalf of previously logged-on user and you are reconnected to this Windows-only logon session even after you provide your credentials to login to eDirectory and Windows again through the interactive credential provider.

To resolve this issue and perform eDirectory login along with Windows logon, disable the existing Windows Update group policy for ‘Automatic Restart Sign On’. The feature can be disabled by creating a registry key `DisableAutomaticRestartsSignOn` of type DWORD under [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System] and set the value to 0x1. Installing or Upgrading to Client for Open Enterprise Server 2 SP4 (IR7) or later by default disables this feature by setting the group policy for Automatic Restart Sign On.

Loss of Client Configuration Settings After Upgrading to Windows 10 RS2

The Windows 10 Creators Update ("1703" or March 2017 release of Windows 10) has introduced a Windows upgrade issue that causes loss of all Client for Open Enterprise Server configuration settings during the Windows upgrade process. For more information on this issue, see TID 7018786.

NOTE: With current preview builds of the upcoming Windows 10 (Fall Creators Update) expected from Microsoft in October 2017, this loss of Client for Open Enterprise Server settings no longer occurs during the Windows 10 upgrade process.

Windows 7 and Windows Server 2008 R2 Displays the Verification Prompt Even if Trusted Software Is Selected

During installations or upgrades of Client for Open Enterprise Server the Microsoft Verification prompt is displayed even if “Always trust software from Micro Focus” is selected or the certificate is installed as a “Trusted Publisher”.

To resolve this issue, apply the Microsoft HotFix KB2921916 in addition to selecting the “Always trust software from Micro Focus” checkbox or pre-installing the Micro Focus SHA-2 certificate as a “Trusted Publisher”.

The 8.3 File Name Support is Unavailable with the Lazy Close Feature

If the Lazy Close feature is set to "ON", the 8.3 (short file name/DOS name) file name support will be unavailable for Client for Open Enterprise Server. For example, a `Dir /x` command will display blank characters instead of the DOS/short file names and will display only the long names for the files in a mapped drive. Also, 16-bit applications will not be able to retrieve the 8.3 file names for the files.

“Login with Third-Party Credential Provider” Feature Not Supported When Microsoft Windows Live ID is Used

"Login with Third-Party Credential Provider" feature is currently not supported when a user tries to login using Microsoft Windows Live ID and Password. Novell plans to fix this in the future release of Novell Client. Also note that "Login with Non-Novell Credential Provider" feature works when PIN-based or Picture Based Login is enabled for the same Microsoft Windows Live ID.

Novell Products Not Supported with the Client for Open Enterprise Server

The NetWare Administrator utility (`nwadmn32.exe`) and ConsoleOne are not supported on Windows or with the Novell Client for Windows, except where explicitly declared by the ConsoleOne release notes.

Welcome Screen Issues

- “One-time Failure to Remember Last Logged-on User When Upgrading to Client for Open Enterprise Server” on page 14
- “After Installing the Client, Local User Tiles Are No Longer Visible During Login” on page 15
- “Welcome Screen Cancel Button” on page 15
- “Fast User Switching/Connecting via Remote Desktop Connection” on page 15

One-time Failure to Remember Last Logged-on User When Upgrading to Client for Open Enterprise Server

After installing Client for Open Enterprise Server on a machine which was previously using Novell Client 2 SP1 or earlier, during the next boot-up the “Username” field will come up blank rather than defaulting to the previous “last logged-on user” info. Once a new login has been performed using the Client for Open Enterprise

Server, future logouts and/or reboots will correctly show the last logged-on user info again. Note that the Client login profile information (the eDirectory tree name, context, and so on.) has not been lost; only a one-time inability to display the last logged-on username.

This issue is not observed when you upgrade to Client for Open Enterprise Server from Novell Client 2 SP3 or SP2.

After Installing the Client, Local User Tiles Are No Longer Visible During Login

If you install the Client on a machine with multiple local users, after rebooting, you are asked to log in to the Client. At this point, there are only two available tiles: one for the local administrator user, and one for the Client for Open Enterprise Server. You will no longer see the individual tiles for the local users.

This is working as designed. The Client for Open Enterprise Server follows Microsoft’s recommendations to filter out the local user accounts after installing the Client. If you install the workstation into a Microsoft Domain, the local user tiles are also filtered out, and the Client follows this behavior.

Welcome Screen Cancel Button

When logging in to eDirectory via the Windows welcome screen, the **Cancel** button that is displayed is not active and therefore cannot be clicked.

Fast User Switching/Connecting via Remote Desktop Connection

When logging in to a Windows workstation using the Client for OES, OES connections made during the login will persist only if the Windows account you specify is not currently logged on to the workstation. If the Windows account specified is already logged in, Windows will reconnect you to that existing session when you log back in to the workstation, regardless of what eDirectory credentials might have been supplied, or whether they're the same as the eDirectory credentials already in use for that running session (if any).

This applies to both Fast User Switching and connecting via Remote Desktop Connection.

Authenticating to a OES Server Through a UNC Path

If you log in to a OES server using a UNC path in Windows Explorer and specify more than just the server and volume, the Windows Explorer window will appear in the foreground and the Results page will appear in the background.

If you specify only the server and volume, authenticating with a UNC path works correctly.

Using Ctrl+Alt+Del to Change Your Password

If you are currently authenticated to eDirectory, after entering your old password and new password, you will see a Change Password dialog box after clicking the **Submit** button. From the Change Password dialog box, you can choose which resources you want the password change to go to.

If you are not currently authenticated to eDirectory, the password change will only be performed for your Windows account.

Mapped Drive Icon Doesn’t Update on Re-Authentication

When you detach from a mapped Network drive, the mapped drive icon displayed in Windows Explorer changes to a red X to indicate that the mapped drive is no longer accessible. If you use the Client Tray icon to re-authenticate to the eDirectory tree (and you selected the **Check to always map this drive letter when you start Windows** option when you originally mapped the drive), the mapped drive icon does not update to show that the drive is accessible again.

LDAP Contextless Login Differences in the Client for Open Enterprise Server

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 Client for Open Enterprise Server welcome screen (the login dialog seen at boot time and when logging out of Windows Vista), the LDAP Contextless Login lookup cannot be triggered when viewing the **eDirectory** tab. If LDAP Contextless Login is enabled, a lookup is performed after the user attempts to log in to eDirectory from the welcome screen.

  This is different from the LDAP Contextless Login behavior when running `LOGINW32.EXE` or selecting the **OES Login** option from the Client tray application 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 eDirectory using information other than a complete username (for example partial usernames using wildcards, or alternate attributes such as phone number or e-mail address) have been disabled in the Client for Open Enterprise Server. Only complete usernames can be used for LDAP Contextless Login.

Login Profiles

Using DHCP in Login Profiles

If **<DHCP>** is chosen as an option in a login profile for Tree, Context, or Server, it cannot be removed by simply editing the field when logging in or by saving the profile on successful login. Any values entered in these fields during login will not be saved when **<DHCP>** is enabled for that field. This is working as designed.

Disabling the Login Profile List

If you set the **Login Profile List** option (available on the Advanced Login tab in the Client Properties dialog box) to **Off** (meaning that the **Login Profile** drop-down list will not be displayed on the Client Login dialog box), your next login will automatically use the last profile you logged in with.

If you want to use the default profile when the **Login Profile List** option is turned off, make sure that you log in using the default before you turn the option off.

Using the Force Grace Login Password Change Option

If you set the **Force Grace Login Password Change** option (available on the Advanced Login tab in the Client Properties dialog box) to **On** (it is Off by default), the OES Login will require a password change on the next-to-last grace login instead of the last grace login.

To work around this issue, use one of the following options:

- Avoid this setting. Users are prompted to change the password on every grace login, but on the last one they have the option of canceling out and potentially getting locked out if they log out one more time without changing the password.
- Add one to the number of grace logins. The message will tell users that they have four, three, then two grace logins, and then they will be required to change the password.
- Suggest that users change their password while they still have two or more grace logins.

File Caching Settings Ignored

The Client for Open Enterprise Server ignores the SET CLIENT FILE CACHING ENABLED parameter on NetWare servers. Caching is on by default. Setting the parameter to `on` or `off` has no effect on the Client behavior. This set parameter does still affect the NCP server's behavior with regard to granting level 1 oplocks when requested.

To disable caching for a client, do the following:

1. Right-click the Client Tray icon in the System Tray.
2. Click **Client Properties**.
3. Select the **Advanced Settings** tab.
4. Select **File Caching** and set it to **off**.

For information on File Caching, see "Advanced Settings" in the administration guide for the client.

Exceeding Disk Quota Is Reported As "Out Of Disk Space" Error

When a user or directory quota has been exceeded, the expected error condition will reflect only "out of disk space," in whatever manner the application chooses to report this error condition. The error status will not differentiate between "the disk is out of total physical space" and "the current user or directory quota has been exceeded".

Login Script Execution Starts Before User's Desktop

When logging in to both eDirectory and Windows through the credential provider of the Client for Open Enterprise Server, the processing of login scripts stored in eDirectory now starts at the same time other login scripts are processed, such as the Windows user login script. This means that eDirectory login script execution will start (but not necessarily finish) before the user's Desktop is built.

In addition, existing Windows policies such as Run logon scripts synchronously now apply to how the Client logon script execution will be handled. This appears to be the default behavior in Windows Server with Terminal Services, but the policy may need to be explicitly set in other Windows configurations.

If you require that logon script processing must finish before the user's desktop is built, you can enable this Windows policy in the Group Policy Editor (GPEDIT.MSC) under **Computer Configuration > Administrative Templates > System > Scripts > Run logon scripts synchronously**. Note the same policy is also available as a User Configuration policy.

Roaming User Profile Paths Saved On Non-Windows Servers

In Windows 2000 SP4 and Windows XP SP1 and later, by default Windows will require that the roaming profile directory successfully pass a test for specific Windows-based permissions. This test fails against OES Network paths since permissions are based on eDirectory permissions instead of Windows permissions, and can fail against Windows- or other non-Windows-based servers as well.

Windows defines a “Do not check for user ownership of Roaming Profile Folders” policy “CompatibleRUPSecurity”) to allow opting out of this security check where necessary. Enabling this policy is required to successfully store roaming profiles on a OES server or other Windows or non-Windows server where the security check cannot succeed.

In the Novell Client for Windows XP/2003, installation of the Client automatically enabled the “CompatibleRUPSecurity” policy by default, regardless of whether it was known that user profiles were being saved to OES Network paths. Administrators who did want to allow the new Microsoft security test to be performed had to override and disable the policy.

Installation of the Client on Windows Vista and later does not enable the “CompatibleRUPSecurity” policy by default. Administrators must enable this policy if they intend to store roaming profiles on OES or non-OES servers that will fail the Microsoft security check.

NOTE: In addition to being able to push this policy setting out with normal Novell ZENworks or Microsoft Group Policy methods, the Client also provides a parameter **Allow Roaming User Profile Paths to non-Windows servers** in **Client Properties**. This parameter can be set during installation through use of a Client Properties File (NCPF), for example `UNATTEND.TXT`.

Windows Program Compatibility Assistant May Be Invoked After Successfully Running NCIMAN.EXE on Windows 7, 8, 10 or Windows Server 2012

After running the Client Installation Manager (`NCIMAN.EXE`) application on Windows 7, 8, 10, or Windows Server 2012, Windows may prompt with the Program Compatibility Assistant as though `NCIMAN.EXE` was an installation program that may not have completed successfully.

`NCIMAN.EXE` is not actually a program that attempts to install or uninstall any part of Client for Open Enterprise Server software, and is just a tool for creating and editing Client Property Files (NCPF), such as an `UNATTEND.TXT` file.

This warning can be ignored by simply selecting the **This program installed correctly** link offered by the Windows Program Compatibility Assistant.

TSClientAutoAdminLogon May Not Use The Profile Specified In DefaultLoginProfile

As part of establishing a TSClientAutoAdminLogon policy, it is required to create a DefaultLoginProfile value to specify which Client login profile should be used for the eDirectory portion of the login.

For Windows Server configurations where only a single Client login profile exists anyway (for example, Default), there is no issue and the single profile will be successfully used. But it has been observed that when more than one login profile is defined, it is possible for the TSClientAutoAdminLogon attempt to use the last-used Client login profile for a user instead of the login profile explicitly specified in the DefaultLoginProfile configuration.

This represents an unintentional behavior, and is being examined for future versions of the Client for Open Enterprise Server. The workaround if this issue is encountered is to define and use just a single Client login profile, at least on Windows Server machines on which Terminal Services and TSClientAutoAdminLogon are expected to be used.

Login From Windows Welcome Screen May Not Use Windows Username From Client Login Profile

In cases where the Client credential provider used by the Windows welcome screen login is switched between “Computer Only Logon” mode and “Network Logon” mode prior to performing a Network Logon login attempt, the Windows account name used during the login attempt might be whatever Windows account name was specified in the **Username** field while the credential provider was in Computer Only Logon mode, instead of the correct Windows account name saved and retrieved from the **Windows** tab of the effective Client login profile.

This represents an unintentional behavior, and is being examined for future versions of the Client. The workaround is to avoid the switch between Computer Only Logon mode and Network Logon mode when possible. And when the issue does occur, provide the correct Windows account credentials in the Windows logon fields that appear after the attempt to use the incorrect Windows account name.

Failures Installing, Uninstalling, and Using the Client for Open Enterprise Server if iPrint is Installed Before the Client

The Novell iPrint 5.32 and iPrint 5.30 clients contain an issue in which incorrect security is established on the [HKEY_LOCAL_MACHINE\Software\Novell] registry key, if and when the Novell iPrint client was the first installed software that needed to create this registry key. This registry security issue is addressed in the Novell iPrint 5.35 client and later.

If the Novell iPrint 5.32 or iPrint 5.30 client is installed prior to the Client for Open Enterprise Server, the security that is established on the [HKEY_LOCAL_MACHINE\Software\Novell] registry key causes incorrect security to be propagated to the Client's own registry sub-keys. In addition, the incorrect registry security can cause the Novell NMAS Challenge Response Method installation to fail with Error 1603, due to incorrect registry security which was propagated to the Novell NMAS Client's registry sub-keys.

The Novell Client 2 SP1 (IR1) contained some mitigation for this issue that could clean-up the incorrect registry security established by Novell iPrint and proceed with a successful Client installation if the Client for Open Enterprise Server or earlier Client installation had not already been attempted and failed after installing the

Novell iPrint client. If a failed Client installation had already been attempted after installing the Novell iPrint client first, the Novell Client 2 SP1 (IR1) installation will still fail due to the improper registry security which has already been established.

The Novell Client 2 SP1 (IR2) contains further mitigation which will actually clean up the registry security issue created by the Novell iPrint client, and furthermore will clean up the incorrect security which may have already been propagated to the Client registry sub-keys and the Novell NMAS Client sub-keys. So on a machine where the Novell iPrint 5.32 or iPrint 5.30 client was installed prior to the Client for Open Enterprise Server, but a Client installation has already subsequently failed, the primary corrective action to perform is to install Novell Client 2 SP1 (IR2) on top of the previously failed Client installation.

There is however one scenario under which even the Novell Client 2 SP1 (IR2) fix will be unable to detect and clean-up registry security problems which still exist due to the Novell iPrint client installation. This problem scenario occurs specifically when *all* of the following conditions are met:

- Novell iPrint 5.32 or iPrint 5.32 was installed before the first Client installation.
- Novell Client 2 SP1 or earlier was installed without NMAS, and with or without NICI.
- Same machine was then upgraded to Novell Client 2 SP1 (IR1); installed with or without NMAS, and with or without NICI.
- Same machine was then upgraded to Novell Client 2 SP1 (IR2); installed with or without NMAS, and with or without NICI.

In this specific sequence where the initial failed Client installation was performed after explicitly deselecting Novell NMAS from being installed with the Client, the subsequent mitigations for the Novell iPrint security issue performed by the Novell Client 2 SP1 (IR1) and Novell Client 2 SP1 (IR2) installations are unable to detect or correct that further clean-up of the Novell iPrint registry security permissions is still necessary.

The symptoms that occur when a machine is still in this broken state include a crash that occurs whenever the Client login dialog would have been presented. For example, when attempting to invoke the “Show Advanced Options” link on the Windows welcome screen, the Windows LogonUI.exe process can crash. When trying to invoke “OES Login” from the client tray menu in the Windows taskbar notification area (systray), the Client NWTRAY.EXE process can crash.

Unfortunately the incorrect permissions established on the registry by Novell iPrint client will also prevent successful un-installation from being performed after the machine is already in this state. This remaining scenario where the Novell iPrint registry permissions are not successfully cleaned up is being examined for additional mitigation in future versions of the Client.

eDirectory AutoAdminLogon Requires Windows AutoAdminLogon

Establishing an eDirectory AutoAdminLogon configuration requires that a Windows AutoAdminLogon configuration is also established. Meaning at minimum an automatic Windows account logon will occur if only a Windows AutoAdminLogon is configured; or both an eDirectory account logon and a Windows account logon will occur if both eDirectory AutoAdminLogon and Windows AutoAdminLogon are configured. Any workstation where only an eDirectory AutoAdminLogon is configured will now have the AutoAdminLogon configuration ignored, instead of experiencing undefined results.

For more information on configuring a Windows AutoAdminLogon policy or both an eDirectory AutoAdminLogon and Windows AutoAdminLogon policy, see Section “Enabling AutoAdminLogon” of the *Client for Open Enterprise Server Administration Guide*.

Client for Open Enterprise Server 802.1x Authentication Not Supported with Microsoft Server 2008 R2-based RADIUS Server

The Client 802.1x Authentication integration does not succeed when Microsoft Server 2008 R2- based RADIUS service is being used for 802.1x authentication.

For more information, see TID 7007679 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7007679&sliceId=1&docTypeID=DT_TID_1_1&dialogID=132236725&stateId=0%200%20280054039) or bug 631640.

Issues in Novell Client 2 SP4 for Windows (IR1) When Windows 7 or 8.1 is Upgraded to Latest Windows 10

If you install the Novell Client 2 SP4 for Windows (IR1) on Windows 7 or 8.1 and then upgrade the Windows to latest Windows 10, the already installed Novell Client 2 SP4 for Windows (IR1) might not work properly. To avoid this issue, ensure that the Novell Client 2 SP4 for Windows (IR1) is newly installed on Windows 10.

This issue is being examined and will be fixed for future versions of the Client.

Unsupported Functionality

Mapping RDN Paths

Relative distinguished name paths are not supported for mapping network drives. For example \\tree\server_volume.context. (note the trailing period) is not supported whereas \\tree\server_volume.context (no trailing period) is.

Fixes Since the Last Release

- Client for Open Enterprise Server 2 SP6 (IR1) and earlier unable to run successfully on Windows 11 Insider Preview 22557 and later, citing “a certificate has been explicitly revoked”.
- If TCP-level VLDB communication is blocked, all VLS connection slots become full after repeated failed attempts to traverse DFS junctions. Once the connection slots are full, even if TCP-level communication to the VLDB is then restored, DFS junctions continue to fail until the workstation is rebooted.
- eDirectory AutoAdminLogon will fail if a clear-text eDirectory AutoAdminLogon password has not been provided, instead of falling back to using the Windows AutoAdminLogon password for the eDirectory AutoAdminLogon. (OCTIM52A507238)
- If NetIQ Advanced Authentication client is installed on a machine where Client for Open Enterprise Server is already installed, the NetIQ credential provider will appear and be used successfully. This continues until someone visits Client Properties and saves any change, at which point the pre-existing Client Properties settings to use Client for Open Enterprise Server credential provider will be re-asserted. Now in SP7, presence of the NetIQ credential provider is recognized as a state to be maintained when visiting Client Properties, until a different credential provider mode is explicitly selected. (OCTIM52A499791)
- NCCredProvider was failing to call ZENworks DLU LocalPreLogonNotify callback if a UPN username had been entered by the user, because the domain value was intentionally blank in this case.
- Provide customer with new “Enforce eDirectory Desktop Login With NetIQ Credential Provider” policy to allow opting-out of Advanced Authentication enforcement for eDirectory-only logins performed from the desktop. (OCTIM52A499791)

- AutoAdminLogon processing could fail to proceed to checking for eDirectory AutoAdminLogon, if and when a Windows domain-involved Windows AutoAdminLogon returns ERROR_TRUSTED_RELATIONSHIP_FAILURE when trying to determine the SID of the Windows AutoAdminLogon user. (OCTIM52A507238)
- Having LDAP Contextless Login caching enabled could create random initial NCP connections. (OCTCR52A414024)
- When AutoAdminQueryNDS is enabled, the ForceLastUserName policy would not be applied. (OCTCR52A397425)
- When AutoAdminQueryNDS is enabled, every Windows account logon uses AutoAdminLogon credentials. (OCTCR52A382073)
- Uninstalling the latest client to re-install an older version could result in files from the latest client being retained. (OCTCR52A380500)
- AutoAdminLogon could fail when the configured Windows user account was an Azure Active Directory account. (OCTIM52A339003)
- LDAP Contextless Login errors could be hidden when logging in with the credential provider. (OCTCR52A333010)
- Deleting a folder could fail if the name of an existing file in that folder exceeded 128 characters. (OCTIM52A229001)
- Potential buffer overrun when the WNetGetUniversalName API is called for path longer than MAX_PATH. (OCTIM52A136048)
- When DontDisplayLockedUserId is enabled, a Change Password with Advanced Authentication enabled can fail. (OCTCR52A131055)
- LDAP Contextless Login could return a context with some Unicode characters still escaped. (OCTCR52A80039)

Documentation

For information on installing, using, and administering the Client for Open Enterprise Server, see https://www.microfocus.com/documentation/client-for-open-enterprise-server/2-sp7/.

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

Legal Notices

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

OpenSLP

“OpenSLP” is copyrighted to Caldera systems. OpenText ships a modified version of OpenSLP for the Client for Open Enterprise Servers. OpenText supports the modified OpenSLP software shipped with the Client for Open Enterprise Server.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Caldera Systems nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CALDERA SYSTEMS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.