

Client for Open Enterprise Server 25.2 Release Notes

May 2025

- ♦ “Introduction” on page 1
- ♦ “What’s New” on page 1
- ♦ “Installation and Upgrade” on page 1
- ♦ “Fixed Issues” on page 2
- ♦ “Documentation” on page 2
- ♦ “Legal Notices” on page 2

Introduction

Client for Open Enterprise Server 25.2 is an update to Client for Open Enterprise Server 24.4. This release includes integration with Advanced Authentication version 6.4.3.3, providing improved security and compatibility enhancements.

What’s New

Advanced Authentication Upgrade

This release integrates Advanced Authentication 6.4 Service Pack 3 Patch 3.

For more information, see [Advanced Authentication Release Notes \(https://www.netiq.com/documentation/advanced-authentication-64/advanced-authentication-releasenotes-6433/data/advanced-authentication-releasenotes-6433.html\)](https://www.netiq.com/documentation/advanced-authentication-64/advanced-authentication-releasenotes-6433/data/advanced-authentication-releasenotes-6433.html).

Improved TLS Version Handling

In earlier versions, the Client for Open Enterprise Server needed to programmatically set the TLS version in the existing SDK. Upgrading to Advanced Authentication SDK version 6.4.3.3 removes this limitation and provides additional security.

Installation and Upgrade

For information on installing the Client on a single workstation, see [Client for Open Enterprise Server Installation Quick Start](#).

For advanced installation options and procedures, see [Client for Open Enterprise Server Administration Guide](#).

Fixed Issues

- ◆ **AutoAdminLogon now supports empty passwords**

In earlier versions, when AutoAdminLogon was enabled and Client for OES was set as the primary credential provider, a non-empty Windows password was required.

In this release, the client removes this requirement to align with Microsoft behavior, which allows AutoAdminLogon with an empty password.

- ◆ **Compatibility with NetIQ AAF 6.4.3.3**

Installing NetIQ Advanced Authentication Framework (AAF) version 6.4.3 previously prevented Client for OES from functioning as the primary credential provider.

This issue has been resolved in NetIQ AAF 6.4.3.3. OpenText recommends using AAF 6.4.3.3 in conjunction with Client for OES 25.2 to ensure proper credential provider integration.

- ◆ **Updated "Save As" functionality in folders with delete inhibit attribute**

In earlier versions, performing a **Save As** operation was not possible in folders with the **Delete Inhibit** attribute set.

In this release, file creation is now prevented if **ERASE** rights are lacking and the application (e.g., Notepad, Word) requests **DELETE** access during file creation.

The **Delete Inhibit** attribute is no longer considered during the file creation process.

- ◆ **Accurate display of MFA method descriptions**

In earlier versions, the graphical user interface displayed incorrect labels for selected multi-factor authentication (MFA) methods when Advanced Authentication (AAF) was enabled. For example, TOTP was incorrectly shown as "password."

In this release, the issue has been resolved when used with NetIQ AAF 6.4.3.3. MFA methods are now accurately labeled in the user interface.

Documentation

For Client for Open Enterprise Server documentation, see [Client for Open Enterprise Server website \(https://www.microfocus.com/documentation/client-for-open-enterprise-server/\)](https://www.microfocus.com/documentation/client-for-open-enterprise-server/).

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

Legal Notices

Copyright 2022 - 2025 Open Text.

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.

Copyright © 2000 Caldera Systems, Inc

All rights reserved.

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.

