

OpenText™ Identity Manager CE 24.4 (v4.10) Release Notes

January 2025

OpenText Identity Manager 24.4 (v4.10) includes new features and enhancements, improves usability, and resolves several previous issues. The updates in this release are cumulative. They include software fixes and enhancements in the current version, as well as all previously released fixes from the service packs, patches, and hotfixes. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the [Identity Manager Community Forums \(https://community.opentext.com/cyberres/iga/idm\)](https://community.opentext.com/cyberres/iga/idm) on OpenText Forums, our online community that also includes product information, blogs, and links to helpful resources.

For information about what's new in previous releases, see the "Previous Releases" section on the [OpenText Identity Manager documentation website \(https://www.netiq.com/documentation/identity-manager-4.10/\)](https://www.netiq.com/documentation/identity-manager-4.10/).

For more information about this release and the latest release notes, see the [Documentation \(https://www.netiq.com/documentation/identity-manager-4.10/\)](https://www.netiq.com/documentation/identity-manager-4.10/) page.

To download this product, see the [Software License and Download \(https://sld.microfocus.com\)](https://sld.microfocus.com) portal.

- ♦ "What's New?" on page 1
- ♦ "Deprecated Functionality" on page 3
- ♦ "Supported Component Versions" on page 3
- ♦ "System Requirements" on page 5
- ♦ "Resolved Issues" on page 5
- ♦ "Installing OpenText Identity Manager 24.4 (v4.10)" on page 6
- ♦ "Upgrading to OpenText Identity Manager 24.4 (v4.10)" on page 9
- ♦ "Known Issues" on page 12
- ♦ "Contacting OpenText" on page 21
- ♦ "Legal Notice" on page 22

What's New?

This release includes the following enhancements:

- ♦ "Operating System Support" on page 2
- ♦ "Branding Updates" on page 2

- ♦ [“Support for OpenSSL 3.0.15 with TLSv1.3” on page 2](#)
- ♦ [“Installer Enhancements” on page 2](#)
- ♦ [“Identity Applications Enhancements: Viewing Task History” on page 3](#)

For more information about the new features in OpenText Identity Manager 24.4 (v4.10) Designer, see [OpenText™ Identity Manager CE 24.4 \(v4.10\) Designer Release Notes](#).

Operating System Support

This release adds support for the Red Hat Enterprise Linux (RHEL) 9.4 platform. For a complete list of supported operating systems, see the [System Requirements for OpenText™ Identity Manager CE 24.4 \(v4.10\)](#) page.

For information about the components packaged, databases, and browsers supported with this release, see [“Supported Component Versions” on page 3](#).

Branding Updates

Micro Focus is now part of OpenText. To adhere to the OpenText brand, the name of the product, its components and user interfaces, logos, company name references, and documentation are updated. The OpenText versioning mechanism uses the CY.Q (Calendar Year.Quarter) format. Starting from the 4.10 release, Identity Manager adheres to the OpenText versioning convention. Identity Manager 4.10 is known as OpenText Identity Manager 24.4 (v4.10).

Support for OpenSSL 3.0.15 with TLSv1.3

Starting from this release, OpenText Identity Manager uses OpenSSL 3.0.15. When you install the product, the new version of OpenSSL is implemented, and TLSv1.3 is used for communication among its components.

If you upgrade from version 4.7.5, 4.8.x or 4.9.x to 24.4 (v4.10), support for TLSv1.2 will remain available. To enable TLSv1.3, you must manually configure TLSv1.3 for all components. For more information, see [Configuring TLSv1.3 for Tomcat Services](#).

IMPORTANT: The TLS version specified in the Tomcat server .xml file supersedes the TLS version set in the components.

Installer Enhancements

This release incorporates the following enhancements to the installer:

- ♦ A new prompt for master keystore password during Identity applications and Identity Reporting configuration and upgrade.
- ♦ Automated prompts for typical configuration of OpenText Identity Console.
- ♦ The addition of the SAP HANA driver in the OpenText Identity Manager 24.4 (v4.10) driver deliverables.

Identity Applications Enhancements: Viewing Task History

Now, users can view the status of all their past actions in one place. The **Task History** option under the **Task** menu lists all tasks a user performed, including permission requests that were approved or denied. This feature tracks users' workflow executions and makes it easy to review their past actions. Users with appropriate roles, like Provisioning Administrator, can also see the task history of others. For more information, click the help icon on the Dashboard.

NOTE: In this release, adding a new widget to your Dashboard does not include the **Task History** option in the **IDM** category.

Deprecated Functionality

The following features have either been removed or have been deprecated and will be removed in a future release:

Configuring OSP to Use Advanced Authentication for Two-Factor Authentication is Deprecated

Starting with this release, configuring OSP to use Advanced Authentication for two-factor authentication is deprecated. Instead, you can use SAML authentication from Advanced Authentication. Advanced Authentication also provides many other authentication methods such as Card, OATH OTP, and Facial Recognition during the login process.

Specifying IP Address for Hostname is Deprecated

When configuring the hostname for OpenText Identity Manager components, use the server's Fully Qualified Domain Name (FQDN). Prior to this release, both IP address and FQDN were allowed, but from this release onward, only FQDNs are supported. This change does not impact Identity Reporting, which continues to accept either IP address or FQDN for configuration.

Supported Component Versions

This section provides information about the supported versions of the components.

- ♦ [“OpenText Identity Manager Component Versions” on page 3](#)
- ♦ [“Third-Party Component Versions” on page 4](#)
- ♦ [“Database” on page 4](#)
- ♦ [“Web Browser” on page 4](#)

OpenText Identity Manager Component Versions

This release bundles the following components:

- ♦ OpenText™ eDirectory 24.4 (v9.3)
- ♦ OpenText™ Identity Console 24.4 (v1.9)
- ♦ Identity Manager Engine 4.10

- ♦ Identity Manager Remote Loader 4.10
- ♦ Identity Manager Fan Out Agent 4.10
- ♦ Designer for OpenText™ Identity Manager 24.4 (v4.10)
- ♦ Identity Applications 24.4 (v4.10)
- ♦ One SSO Provider (OSP) 6.7.7
- ♦ Self Service Password Reset (SSPR) 4.8.0.1
- ♦ Identity Manager Identity Reporting 24.4 (v7.4)
- ♦ Sentinel Log Management for IGA 8.7.0.0 (for event auditing)
- ♦ OpenText™ Identity Manager drivers

NOTE:

- ♦ OpenText Identity Manager 24.4 (v4.10) is only compatible with OpenText™ eDirectory™ 24.4 (v9.3) or later.
 - ♦ OpenText Identity Manager 24.4 (v4.10) contains the latest versions of supported drivers. For more information, see **Version Shipped with 24.4 (v4.10)** on the [OpenText Identity Manager Drivers \(https://www.netiq.com/documentation/identity-manager-4.10-drivers/\)](https://www.netiq.com/documentation/identity-manager-4.10-drivers/) page.
-

Third-Party Component Versions

This release adds support for the following third-party components:

- ♦ Zulu 11.76+21-CA
- ♦ Apache Tomcat 9.0.96
- ♦ PostgreSQL 14.14 (standalone and containers)
- ♦ OpenSSL 3.0.15
- ♦ Nginx 1.24.0-1
- ♦ ActiveMQ 5.18.4

Database

All product components, including Identity Applications, are compatible with Oracle 21c. However, Identity Reporting 24.4 (v7.4) continues to support Oracle 19c and 18c.

Web Browser

Any of the following browsers, at a minimum:

- ♦ Google Chrome 131.0.6778.85/86
- ♦ Mozilla Firefox 132.0.2
- ♦ Apple Safari 17.4.1
- ♦ Microsoft Edge 131.0.2903.63

System Requirements

For information about hardware requirements and supported operating systems, see the [System Requirements for OpenText™ Identity Manager CE 24.4 \(v4.10\)](#) page.

Resolved Issues

This release includes the following software fixes:

Component	Global ID	Description
Identity Applications	OCTCR56A582892	Roles and Resource Service Driver does not process groups, roles, or resources consistently.
	OCTCR56A583444	When searching for roles, combining multiple search criteria produces irrelevant results.
	OCTCR56A583741	When creating a user account entitlement in Active Directory, the dashboard fails to display an AD entitlement value even when using the asterisk (*) as a wildcard for searching.
	OCTCR56A583753	The Edit Dashboard option in Access Settings is not working properly. Even when a specific user or role is specified as a trustee for dashboard editing, the Edit My Dashboard option remains available to all users.
	OCTCR56A583970	Users with the provisioning manager role cannot see the Others option in Access > Permissions on the dashboard.
	OCTCR56A584665	The User Application Driver's Enable oidpInstanceData attribute clean-up property is failing. As a result, users cannot log in when the oidpInstanceData attribute reaches its limit.
	OCTCR56A584708	When the Enable multi-threaded Role and Resource driver setting is set to true, the Roles and Resource Service Driver stops tracing its own log and instead records everything in the driverset . log file located at/var/log/idm/driverset . log.
	OCTCR56A584712	The Password Sync Status option is not displayed on the Users page, even if a user, group, role, or container is designated as a trustee to view this option from the Access Settings page.
	OCTCR56A584753	Editing a boolean attribute for a user entity on the My Profile page does not save correctly.
	OCTCR56A584827	If a workflow with a nested flow data structure contains many whitespace, the application does not ignore it and prints them in the workflow comments section.
	OCTCR56A584956	The nrfAllowAprOveride attribute is not working properly. When a resource that requires approval is mapped to a role and a user requests that role, the resource is assigned without triggering the approval process.
	OCTCR56A585003	The member count for Role Assignments and Resource Assignments displays incorrect values when it exceeds the maximum display limit set in the property.

Component	Global ID	Description
Installation and Upgrade	OCTCR56A585485	When a role is revoked, the Role and Resource Service Driver recalculates the roles for all users in a container, including inherited ones. This process can cause performance delays depending on the number of recalculations required. To optionally disable the recalculation operations during role revoke or assign actions, set the skip-processing attribute to true and create a custom event transformation policy. NOTE: Skipping recalculations may result in the role not being fully revoked, leaving its status as “running.” Be sure to set skip-processing back to false post revocation.
	OCTCR56A585680	Single-valued attributes for a user entity are not editable, even if they are set as Editable Attributes in the Customization Settings .
	OCTCR56A587004	The Permission of Other’s page does not display the Expiration date in the role details window.
	OCTCR56A627092	Identity Manager cannot send emails when policies include the <do-send-email-from-template> or <do-send-email> action with customer notification set as HTML in the message field within <use-html> tags.
	OCTCR56A627201	Audit events from Identity Applications cannot be sent to Sentinel due to a connection issue.
	OCTCR56A639081	The DirXML-PasswordSyncStatus attribute of a user changes from 0004: SUCCESS to 0005: PENDING when users are added to eDirectory in bulk.
	OCTCR56A646136	The Form builder does not work without Internet access.
	OCTCR56A647072	Single-valued attributes for custom entities are not editable.
	OCTCR56A674108	The Identity Manager 4.9 containers don’t handle time zones correctly, resulting in logs and traces displaying timestamps in UTC instead of local time.

Installing OpenText Identity Manager 24.4 (v4.10)

This release includes Advanced Edition and Standard Edition in a single ISO file. Before downloading the installation files, you must understand the features available with each edition and the options for downloading the product’s components. For information about the features supported by each edition, what features are contained in each edition, see [OpenText™ Identity Manager CE 24.4 \(v4.10\) Overview and Planning Guide](#).

- ♦ [“Downloading OpenText Identity Manager” on page 7](#)
- ♦ [“Locating the Executables and Default Installation Paths” on page 7](#)
- ♦ [“Installing the Product” on page 9](#)

Downloading OpenText Identity Manager

After purchasing OpenText Identity Manager 24.4 (v4.10), log in to the [Software License and Download portal \(https://sld.microfocus.com/mysoftware/index\)](https://sld.microfocus.com/mysoftware/index) and follow the link that allows you to download the software. The following files contain the OpenText Identity Manager components:

File Name	Description
Identity_Manager_4.10.0_Linux.iso	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, OpenText Identity Console), Identity Applications, and Identity Reporting.
Identity_Manager_4.10.0_RL_Linux.iso	Contains the Identity Manager Remote Loader for Linux.
Identity_Manager_4.10.0_Containers.tar.gz	Contains individual container images for Identity Manager Engine, Remote Loader, Fanout Agent, ActiveMQ, PostgreSQL, Form Renderer, OSP, Identity Applications, Identity Reporting, SSPR, and OpenText Identity Console.
Identity_Manager_4.10.0_Windows.iso	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, and Identity Console), Identity Applications, and Identity Reporting.
Identity_Manager_4.10.0_RL_Windows.iso	Contains the 64-bit and .NET Remote Loader for Windows.
Identity_Manager_4.10.0_Designer_Linux.tar.gz	Contains Designer for Linux platforms.
Identity_Manager_4.10.0_Designer_Windows.zip	Contains Designer for Windows platforms.
Identity_Manager_4.10.0_Designer_MacOSX.dmg	Contains Designer files for macOS Sonoma.
SentinelLogManagementForIGA8.7.0.0.tar.gz	Contains Sentinel Log Management for Identity Governance and Administration (IGA). This installation is supported only on Linux.
acdi_v24.4.zip	Contains Audit, Compliance & Data Intelligence (includes ACDI driver, ACDI Monitor packages, and ACDI Workflow Monitor package).

IMPORTANT:

- ♦ The product no longer compiles the 32-bit version of the Remote Loader and is available with .NET and 64-bit versions.
- ♦ The Analyzer tool is not included in the installer. If Analyzer is already installed, ensure that you update it to version 4.8.5 and use it with OpenText Identity Manager 24.4 (v4.10). For installing and upgrading Analyzer, see [OpenText™ Identity Manager CE 24.4 \(v4.10\) Install and Upgrade Guide for Linux](#) or [OpenText™ Identity Manager CE 24.4 \(v4.10\) Install and Upgrade Guide for Windows](#).

Locating the Executables and Default Installation Paths

- ♦ [“Executables and Default Installation Paths on Linux” on page 8](#)
- ♦ [“Executables and Default Installation Paths on Windows” on page 8](#)

Executables and Default Installation Paths on Linux

OpenText Identity Manager Component	Location of the Executable within ISO	Default Installation Path
Identity Manager Server (Contains Identity Manager Engine, Remote Loader, Fan-Out Agent, OpenText Identity Console)	install.sh in the mounted location	♦ Engine: /opt/novell/eDirectory/lib/dirxml ♦ Remote Loader: /opt/novell/dirxml/bin/x86_64 ♦ Fanout Agent: /opt/novell/dirxml/fanoutagent ♦ OpenText Identity Console: /opt/novell/eDirAPI/sbin/
Identity Applications (Identity Manager Dashboard and Administration Interface, User Application, Role and Resource Service driver, User Application driver, Configuration Update Utility, One SSO Provider, Self Service Password Reset)	install.sh in the mounted location	♦ Identity Applications: /opt/netiq/idm/apps ♦ User Application: /opt/netiq/idm/apps/UserApplication ♦ Configuration Update Utility: /opt/netiq/idm/apps/configupdate ♦ Form Renderer: /opt/netiq/idm/apps/sites ♦ NGINX: /opt/netiq/common/nginx
Designer for OpenText Identity Manager	/designer/packages	/root/designer
Identity Reporting	install.sh in the mounted location	/opt/netiq/idm/apps/IDMReporting
Password Management Component	./install.sh in the /sspr directory from the mounted location	/opt/netiq/idm/apps/sspr
Sentinel Log Management for IGA	./install.sh in the /SentinelLogManagementForIGA directory of the SentinelLogManagementForIGA8.7.0.0.tar.gz file	/opt/novell/sentinel

Executables and Default Installation Paths on Windows

Identity Manager Component	Location of the Executable within ISO	Default Installation Path
Identity Manager Server (Contains Identity Manager Engine, Remote Loader, Fan-Out Agent)	install.exe located in \<iso mounted location>\IdentityManagerServer\	♦ Engine: C:\netiq\idm ♦ Remote Loader: C:\netiq\idm\RemoteLoader ♦ Fanout Agent: C:\netiq\idm\FanoutAgent

Identity Manager Component	Location of the Executable within ISO	Default Installation Path
Identity Applications (Identity Manager Dashboard and Administration Interface, User Application, Role and Resource Service driver, User Application driver, Configuration Update Utility, One SSO Provider, Self Service Password Reset)	install.exe located in \<iso mounted location>\IdentityApplications\	♦ Identity Applications: C:\netiq\idm\apps\ ♦ User Application: C:\netiq\idm\apps\UserApplication ♦ Configuration Update Utility: C:\netiq\idm\apps\configupdate ♦ Form Renderer: C:\netiq\idm\apps\sites ♦ NGINX: C:\netiq\common\nginx
Designer for OpenText Identity Manager	install.exe located in \designer_install\ folder of the Identity_Manager_4.10.0_Designer_Windows.zip file	C:\netiq\
Identity Reporting	install.exe located in \<iso mounted location>\IdentityReporting\	C:\netiq\idm\apps\IdentityReporting
Password Management Component	install.exe located in the <iso mounted location>\common\sspr	C:\netiq\idm\apps\common\sspr

Installing the Product

Depending on the edition you are installing, review the information from one of the following resources:

- ♦ Advanced Edition: [OpenText™ Identity Manager CE 24.4 \(v4.10\) Install and Upgrade Guide for Linux](#) or [OpenText™ Identity Manager CE 24.4 \(v4.10\) Install and Upgrade Guide for Windows](#)
- ♦ Standard Edition: [Quick Start Guide for Installing and Upgrading OpenText™ Identity Manager CE 24.4 \(v4.10\) Standard Edition](#)

Upgrading to OpenText Identity Manager 24.4 (v4.10)

You can directly upgrade to OpenText Identity Manager 24.4 (v4.10) from Identity Manager 4.7.5, 4.8.x (where x is 0, 1, 2, 3, 4, 5, 6, and 7) and 4.9.x versions.

Before starting the upgrade, review the information from the release notes for your current version.

- ♦ [“Upgrading from Identity Manager 4.9.x, 4.8.x, and 4.7.5 Versions” on page 10](#)
- ♦ [“Upgrading to Advanced Edition” on page 11](#)
- ♦ [“Upgrading to Standard Edition” on page 12](#)

For more information about upgrading OpenText Identity Manager, see “[Upgrading OpenText Identity Manager](#)” in the *OpenText™ Identity Manager CE 24.4 (v4.10) Install and Upgrade Guide for Linux* or *Upgrading OpenText Identity Manager* in *OpenText™ Identity Manager CE 24.4 (v4.10) Install and Upgrade Guide for Windows*.

Upgrading from Identity Manager 4.9.x, 4.8.x, and 4.7.5 Versions

The following table lists the component-wise upgrade paths for Identity Manager 4.9.x, 4.8.x, and 4.7.5 versions:

Component	Base Version	Upgraded Version
Identity Manager Engine	4.9.x, 4.8.x, 4.7.5	1. Upgrade the operating system to a supported version. 2. Upgrade Identity Vault to 24.4 (v9.3). 3. Upgrade Identity Manager Engine to 4.10.
Remote Loader/Fanout Agent	4.9.x, 4.8.x, 4.7.5	Upgrade to 4.10 Remote Loader/Fanout Agent.
Designer		Install Designer 24.4 (v4.10).
Identity Applications	4.9.x, 4.8.x, 4.7.5	Before you upgrade Identity Applications, ensure that the Identity Vault and Identity Manager engine are upgraded to 24.4 (v9.3) and 4.10 respectively. 1. Upgrade the operating system to a supported version. 2. Stop Tomcat. 3. Upgrade the database to a supported version. For the supported database versions, see System Requirements for OpenText™ Identity Manager CE 24.4 (v4.10). 4. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.8.0.1 version. 5. Update the User Application driver and Roles and Resources driver packages using Designer. 6. Upgrade Identity Applications to 24.4 (v4.10). 7. Start Tomcat.

Component	Base Version	Upgraded Version
Identity Reporting	4.9.x, 4.8.x, 4.7.5	Before you upgrade Identity Reporting, ensure that the Identity Vault, Identity Manager engine, and Identity Applications are upgraded to 24.4 (v9.3), 4.10, and 24.4 (v4.10), respectively. 1. Upgrade the operating system to a supported version. 2. Upgrade the database to a supported version. For more information about the supported database versions, see System Requirements for OpenText™ Identity Manager CE 24.4 (v4.10). 3. Upgrade SLM for IGA to a supported version. 4. Update the Data Collection Services and Managed Services Gateway driver packages. 5. Upgrade Identity Reporting to 24.4 (v7.4). 6. (Conditional) Create a data synchronization policy from the Identity Manager Data Collection Services page. 7. Start Tomcat.

Before starting the upgrade, review the information from the release notes for your version from the [Documentation \(https://www.netiq.com/documentation/identity-manager-4.10/\)](https://www.netiq.com/documentation/identity-manager-4.10/) page.

Upgrading to Advanced Edition

OpenText provides the following upgrade paths for upgrading to OpenText Identity Manager 24.4 (v4.10) Advanced Edition from a prior Advanced Edition or Standard Edition:

- ♦ Identity Manager 4.7.5, 4.8.x, and 4.9.x Advanced Edition to 24.4 (v4.10) Advanced Edition
- ♦ Identity Manager 4.7.5, 4.8.x, and 4.9.x Standard Edition to 24.4 (v4.10) Advanced Edition, in one of the following ways:
 - ♦ From Identity Manager 4.7.5, 4.8.x, and 4.9.x Standard Edition to 24.4 (v4.10) Standard Edition and then to 24.4 (v4.10) Advanced Edition
 - ♦ From Identity Manager 4.7.5, 4.8.x, and 4.9.x Standard Edition to 24.4 (v4.10) Advanced Edition and then to 24.4 (v4.10) Advanced Edition

Upgrading to Standard Edition

You can upgrade to OpenText Identity Manager 24.4 (v4.10) Standard Edition from Identity Manager 4.7.5, 4.8.x, and 4.9.x Standard Edition. For upgrade instructions, see [Quick Start Guide for Installing and Upgrading OpenText™ Identity Manager CE 24.4 \(v4.10\) Standard Edition](#).

The OpenText Identity Manager 24.4 (v4.10) Standard Edition continues to provide support for the following reports:

- ♦ Authentication by user
- ♦ Authentication by server
- ♦ Database statistics
- ♦ Self-password changes
- ♦ Password resets
- ♦ Identity Vault Driver Associations Report Current State
- ♦ Identity Vault User Report Current State
- ♦ User Password Change Events Summary

For more information, see [OpenText™ Identity Manager CE 24.4 \(v4.10\) Administrator's Guide to Identity Reporting](#).

IMPORTANT: To use reports, import the latest report definitions into Identity Reporting. Log in to the Reporting application and use the **Download** page within the application to download the reports.

Known Issues

OpenText strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact [Technical Support \(https://www.opentext.com/products/identity-access-management\)](https://www.opentext.com/products/identity-access-management).

For the list of known issues in Designer, see the [OpenText™ Identity Manager CE 24.4 \(v4.10\) Designer Release Notes](#).

- ♦ [“Issue with the Ellucian Banner Driver After Upgrade” on page 13](#)
- ♦ [“Failed to load class “org.slf4j.impl.StaticLoggerBinder” Error” on page 13](#)
- ♦ [“Set SSO Credential Action Displays an Error” on page 13](#)
- ♦ [“Appender Error is Seen in Catalina Logs for WFCEF” on page 14](#)
- ♦ [“Authentication Reports Not Generated on Sentinel After Upgrade” on page 14](#)
- ♦ [“An Error Reported in the OpenText eDirectory Log File After Upgrade” on page 15](#)
- ♦ [“An Error During Non-root Installation of Engine” on page 15](#)
- ♦ [“An Error Reported in the PostgreSQL Startup Log” on page 15](#)
- ♦ [“An Error Reported in the Upgrade Log File” on page 16](#)
- ♦ [“An Error Reported in the Catalina Log File” on page 16](#)
- ♦ [“The DirXML Command-Line Utility Displays an Error After Upgrade” on page 17](#)
- ♦ [“An Error While Upgrading SSPR with Identity Applications” on page 17](#)
- ♦ [“Invalid Keystore Format: An Error During Upgrade” on page 17](#)

- ♦ “An Error Displayed During Identity Manager Engine Upgrade” on page 17
- ♦ “The Windows Installer Displays an Error” on page 18
- ♦ “The dirxml_remote and RLConsole Properties Display the Outdated Product Version” on page 18
- ♦ “OpenText Identity Manager Does Not Reflect Changes Made to the Use SMTP TLS Option in OpenText Identity Console” on page 18
- ♦ “Organization Chart Buttons for a Level 2 or Higher Relationship Hierarchy Is Missing” on page 19
- ♦ “Remote Loader Reports Invalid Driver Object Password After Upgrade” on page 19
- ♦ “Observing Error: StatusLogger Reconfiguration Failed in Catalina Log File” on page 19
- ♦ “Form Builder Issues” on page 19

Issue with the Ellucian Banner Driver After Upgrade

Issue: The Integration Module for Banner by Ellucian fails due to incompatibility with Jetty libraries shipped with OpenText Identity Manager 24.4 (v4.10).

Workaround: If you have installed the driver, we recommend to use with Remote Loader 4.9.

Failed to load class “org.slf4j.impl.StaticLoggerBinder” Error

Issue: During the configuration of Identity Applications, the Linux installation program generates a new master key. However, you may encounter the error “SLF4J: Failed to load class 'org.slf4j.impl.StaticLoggerBinder'” during this process or while updating the master key. [Issue: OCTCR56A701128]

Workaround: The error does not affect any functionality. You can ignore it.

Set SSO Credential Action Displays an Error

Issue: After upgrading to version 24.4 (v4.10), the do-set-sso-credential action in the Credential Provisioning policy displays an error. This issue occurs specifically when credential provisioning is implemented with SecureLogin. [Issue: OCTCR56A675056]

Workaround: Perform the following steps to resolve this issue:

- 1 Log in to the Identity Manager Engine server.
- 2 Download and extract Java SSO SDK zip from the following location: <https://www.netiq.com/documentation/securelogin-88/references/Java%20SSO%20SDK-8.8.0-0.zip> (<https://www.netiq.com/documentation/securelogin-88/references/Java%20SSO%20SDK-8.8.0-0.zip>).
- 3 Rename the JAR files as follows:
 - ♦ Change jssoapi-prov-8.8.0-0-SNAPSHOT.jar to jsso-prov.jar
 - ♦ Change jssoapi-cmd-8.8.0-0-20191207.071450-46.jar to jsso-cmd.jar
- 4 Navigate to /opt/novell/eDirectory/lib/dirxml/classes and replace jsso-prov.jar with the JAR file you renamed in [Step 3](#). Also, add jsso-cmd.jar to the same directory.
- 5 Restart the server.

Appender Error is Seen in Catalina Logs for WFCEF

Issue: While upgrading Identity Application to 4.10, you might see similar appender error in the catalina logs.

```
com.netiq.logging.log4j2.Log4jLogger.addAppender Error adding Appender WFCEF to
Logger com.microfocus
```

```
com.netiq.logging.log4j2.Log4jLogger.addAppender Error adding Appender WFCEF to
Logger com.sssw
```

```
com.netiq.logging.log4j2.Log4jLogger.addAppender Error adding Appender WFCEF to
Logger com.novell
```

```
com.netiq.logging.log4j2.Log4jLogger.addAppender Error adding Appender WFCEF to
Logger workflow.log
```

```
com.netiq.logging.log4j2.Log4jLogger.addAppender Error adding Appender WFCEF to
Logger com.netiq
```

This happens when you configure auditing prior to upgrading the Identity Applications.

[OCTCR56A679501]

Workaround:

1 Navigate to the following directories:

- ♦ Linux: /opt/netiq/idm/apps/tomcat/conf
- ♦ Windows: C:\NetIQ\IDM\apps\tomcat\conf

Comment the following entries from the `ism-configuration.properties` file:

```
workflow.logging.wfs.definition.workflow.log =
{"name\":"workflow.log\","level\":"INFO\","additivity\:true,\"appenderRe
fs\":[\"WFCEF\"]}
```

```
workflow.logging.wfs.definition.com.novell =
{"name\":"com.novell\","level\":"INFO\","additivity\:true,\"appenderRefs
\":[\"WFCEF\"]}
```

```
workflow.logging.wfs.definition.com.netiq =
{"name\":"com.netiq\","level\":"INFO\","additivity\:true,\"appenderRefs\
\":[\"WFCEF\"]}
```

```
workflow.logging.wfs.definition.com.sssw =
{"name\":"com.sssw\","level\":"INFO\","additivity\:true,\"appenderRefs\
\":[\"WFCEF\"]}
```

```
workflow.logging.wfs.definition.com.microfocus =
{"name\":"com.microfocus\","level\":"INFO\","additivity\:true,\"appender
Refs\":[\"WFCEF\"]}
```

2 Restart Tomcat services.

Authentication Reports Not Generated on Sentinel After Upgrade

Issue: Following the upgrade of OpenText Identity Manager to version 24.4 (v4.10), the *Authentication by User* and *Authentication by server* reports are not generated on Sentinel. This issue is observed on SUSE Linux Enterprise Server 15 SP5.

[OCTCR56A655281]

Workaround: Delete the existing data synchronization policy in Identity Manager Data Collection Service (idmdcs) and Sentinel Log Management for IGA, then create a new one. For more information about how to create a data synchronization policy, see [Administrator Guide to Identity Reporting \(https://www.netiq.com/documentation/identity-manager-4.10/report_setup/data/dcs-settings.html#t44exgvft7eh\)](https://www.netiq.com/documentation/identity-manager-4.10/report_setup/data/dcs-settings.html#t44exgvft7eh).

An Error Reported in the OpenText eDirectory Log File After Upgrade

Issue: After upgrading OpenText Identity Manager from version 4.9 to 24.4 (v4.10), users may encounter the following error in the ndsd.log file:

```
Loader Failed:for lib/opt/novell/eDirectory/lib64/nds-modules/
libdxevent.so.3.so,error lib/opt/novell/eDirectory/lib64/nds-modules/
libdxevent.so.3.so: cannot open shared object file: No such file or
directory,errno 2
```

This issue is observed in the *All-in-One* server setup for OpenText Identity Manager on Linux.
[OCTCR56A639009]

Workaround: The error does not affect any functionality. You can ignore it.

An Error During Non-root Installation of Engine

Issue: When installing the OpenText Identity Manager engine, non-root users may encounter the following error in the idminstall.log file:

```
novell-edirectory-xdaslog-9.3.0.0000-1error: lsetfilecon: (/opt/novell,
system_u:object_r:usr_t:s0) Operation not permitted
error: Plugin selinux: hook fsm_file_prepare failed
#####
error: unpacking of archive failed on file /opt/novell: cpio: (error 0x2)
error: novell-edirectory-xdaslog-9.3.0.0000-169.x86_64: install failed
```

This occurs when unpacking the novell-edirectory-xdaslog-<version> RPM at /opt/novell location fails because a non-root user does not have the required access to this directory.[OCTCR56A647216]

Workaround: The error does not affect any functionality. You can ignore it.

An Error Reported in the PostgreSQL Startup Log

Issue: When configuring Identity Applications and Identity Reporting components on PostgreSQL database, users may encounter the following errors in the startup logs:

```

[16154] ERROR: relation "databasechangelog" does not exist at character 13
[16154] STATEMENT: insert into databasechangelog(id, author, filename, dateexecuted, orderexecuted, exectype,
description, comments, liquibase) values('410', 'IDMRBPM', 'ProvisioningViewValueConstraint45.xml', now(),
796, 'EXECUTED', 'sql', 'Dummy RECORD - TEMP SOLUTION', '3.2.2')
[16220] ERROR: relation "public.databasechangeloglock" does not exist at character 22
[16220] STATEMENT: SELECT COUNT(*) FROM public.databasechangeloglock
[16249] ERROR: relation "public.databasechangeloglock" does not exist at character 22
[16249] STATEMENT: SELECT COUNT(*) FROM public.databasechangeloglock
[15803] LOG: received fast shutdown request
[15803] LOG: aborting any active transactions
[15803] LOG: background worker "logical replication launcher" (PID 15810) exited with exit code 1
[15805] LOG: shutting down
[15803] LOG: database system is shut down
[1389] LOG: starting PostgreSQL 14.13 on x86_64-pc-linux-gnu, compiled by gcc (SUSE Linux) 7.4.1 20190424
[gcc-7-branch revision 270538], 64-bit
[1389] LOG: listening on IPv4 address "0.0.0.0", port 5432
[1389] LOG: listening on IPv6 address ":::", port 5432
[1389] LOG: listening on Unix socket "/tmp/.s.PGSQL.5432"
[1389] LOG: could not open configuration file "/opt/netiq/idm/postgres/data/pg_hba.conf": Permission denied
[1389] FATAL: could not load pg_hba.conf
[1389] LOG: database system is shut down
[1473] LOG: starting PostgreSQL 14.13 on x86_64-pc-linux-gnu, compiled by gcc (SUSE Linux) 7.4.1 20190424
[gcc-7-branch revision 270538], 64-bit
[1473] LOG: listening on IPv4 address "0.0.0.0", port 5432
[1473] LOG: listening on IPv6 address ":::", port 5432
[1473] LOG: listening on Unix socket "/tmp/.s.PGSQL.5432"
[1474] LOG: database system was shut down at 2024-10-05 07:39:04 IST
[1473] LOG: database system is ready to accept connections
[1679] ERROR: relation "idm_rpt_data.databasechangeloglock" does not exist at character 22
[1679] STATEMENT: select count(*) from idm_rpt_data.databasechangeloglock
[1733] ERROR: relation "idm_rpt_cfg.databasechangeloglock" does not exist at character 22
[1733] STATEMENT: select count(*) from idm_rpt_cfg.databasechangeloglock

```

[OCTCR56A662182]

Workaround: The error does not affect any functionality. You can ignore it.

An Error Reported in the Upgrade Log File

Issue: After upgrading OpenText Identity Manager to 24.4 (v4.10), users may encounter the following SSPR-related errors in the `idmupgrade.log` file:

```

ERROR password.pwm.util.cli.MainClass - 5083 ERROR_ENVIRONMENT_ERROR (unable to
establish operating environment: file for option 'outputFile' at '/opt/netiq/idm/
apps/sspr/sspr_data/SSPRConfiguration.xml' already exists)

```

[OCTCR56A662286]

Workaround: These error does not affect any SSPR functionality. You can ignore it.

An Error Reported in the Catalina Log File

Issue: After installing or upgrading to OpenText Identity Manager 24.4 (v4.10), users may encounter an error when starting Tomcat. The error is reported in the `catalina.out` log file.

[RPT-CORE] Error validating report configuration schema.

```

com.netiq.persist.PersistenceException: java.lang.RuntimeException: Cannot use
default schema name idm_rpt_cfg on Microsoft SQL Server because the login schema of
the current user (dbo) is different and MSSQL does not support setting the default
schema per session.

```

This issue occurs when the Identity Manager engine and Identity Reporting are configured in a distributed server setup on the MS SQL 2019 database. [OCTCR56A667011]

Workaround: The error does not affect any functionality. You can ignore it.

The DirXML Command-Line Utility Displays an Error After Upgrade

Issue: After upgrading OpenText Identity Manager to version 24.4 (v4.10), users may encounter the following LDAP error when launching the DirXML command-line utility:

Connection lost waiting for results from 10.71.142.57:636 (91) Connect Error

```
javax.net.ssl.SSLException: Unexpected error:
java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must
be non-emp
```

This issue occurs when OpenText Identity Manager is configured to operate in the FIPS-enabled mode.

[Issue: OCTCR56A669101]

Workaround: The error does not affect any functionality. You can ignore it.

An Error While Upgrading SSPR with Identity Applications

Issue: If Identity Applications and Self-Service Password Reset (SSPR) are on the same server, users may encounter an IO operation error during the upgrade of the SSPR service. This error can occur while upgrading from version 4.8.x to 24.4 (v4.10) on Linux. [OCTCR56A670098]

Workaround: The error does not affect any functionality. You can ignore it.

Invalid Keystore Format: An Error During Upgrade

Issue: While upgrading OpenText Identity Manager in the FIPS-enabled mode, users may encounter the following error while importing the reCAPTCHA public key certificate into the keystore:

keytool error: java.io.IOException: Invalid keystore format

[Issue: OCTCR56A671139]

Workaround: Import the public key certificate from the cacerts file into the idm.bcfks keystore by using the following command:

```
keytool -importkeystore -srckeystore /opt/netiq/common/jre/lib/security/cacerts -
srcstorepass changeit -srcstoretype BCFKS -destkeystore /opt/netiq/idm/apps/
tomcat/conf/idm.bcfks -deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath $CLASSPATH
--noprompt
```

An Error Displayed During Identity Manager Engine Upgrade

Issue: While upgrading OpenText Identity Manager Engine in FIPS-enabled mode, users might encounter the following exception on Linux and Windows:

LDAPException: Error configuring LDAP SSL/TLS. (82) Local Error

java.security.KeyStoreException: BCFKS not found

[Issue: OCTCR56A670109]

Workaround: The error does not affect any functionality. You can ignore it.

The Windows Installer Displays an Error

Issue: After installing OpenText Identity Manager 24.4 (v4.10) components, the following error is displayed on starting Tomcat: SEVERE [main]
org.apache.catalina.util.LifecycleBase.handleSubClassException Failed to start component [Connector["ajp-nio-<IP_address>-8010"]]

This issue occurs during a fresh installation and after upgrading to OpenText Identity Manager 24.4 (v4.10).
[Issue: OCTCR56A607041]

Workaround: It does not cause any functionality loss. However, if you want to resolve the issue, delete the following line in the server.xml file:

```
<Connector port="8010" protocol="AJP/1.3" redirectPort="8543"/>
```

The server.xml file is available in C:\NetIQ\idm\apps\tomcat\conf

The dirxml_remote and RLConsole Properties Display the Outdated Product Version

Issue: When you install or upgrade Remote Loader through the Identity_Manager_4.10.0_RL_Windows.iso or Identity_Manager_4.10.0_RL_Linux.iso, you might notice that the **Product version** does not change in the **dirxml_remote Properties** window. It still shows **4.8.0.0**. The same issue is seen in **RLConsole** properties. [Issue: OCTCR56A608072]

Workaround: It does not impact the Remote Loader functionality. You can check the **File Version** in the same window to confirm whether Remote Loader is installed successfully.

OpenText Identity Manager Does Not Reflect Changes Made to the Use SMTP TLS Option in OpenText Identity Console

Issue: While setting up an email server in OpenText Identity Console, if you enable or disable the notSMTPUseTLS attribute for the default notification template in the Tree View, the same value might not be available on the Email Based Approval page in OpenText Identity Manager. However, the selection is saved, and the email server is updated based on your preference.

This discrepancy happens because the notfSMTPUseTLS LDAP attribute is updated differently in Identity Applications and OpenText Identity Console. When you make the change in OpenText Identity Console, the attribute is updated directly. However, changing the **Use SMTP TLS** value in **Outgoing Email Settings** of OpenText Identity Manager's Email Based Approval page, it updates the com.netiq.rbpm.smtp.tls property in the ism-configuration.properties file. But, the value you select in OpenText Identity Console is still applied, even if it does not appear on the Email Based Approval page in OpenText Identity Manager. [Issue: OCTCR56A585739]

Workaround: To ensure consistent behavior, you can modify the **Use SMTP TLS** value in the **Outgoing Email Settings** option on Identity Manager's Email Based Approval page based on the value you select in Identity Console.

Organization Chart Buttons for a Level 2 or Higher Relationship Hierarchy Is Missing

Issue: For a level 2 or higher relationship, the organization chart does not show the options to choose a relationship for viewing, navigate to the next level in the relationship hierarchy, send emails, and view more information about that entity. This issue is seen when the hierarchical depth in the **General Settings** is set to a level 2 (or higher). [Issue: OCTCR56A585426]

Workaround: To view the organization chart buttons for the level 2 (or higher) relationship, search for the level 2 user/entity in the organization chart.

Remote Loader Reports Invalid Driver Object Password After Upgrade

Issue: After upgrading Remote Loader to version 24.4 (v4.10) on Windows, it is unable to connect to the Active Directory driver using the basic authentication password. [Issue: OCTCR56A584022]

Workaround: After upgrading Identity Manager to 24.4 (v4.10), perform the following steps:

- 1 Stop the Remote Loader instance on the Remote Loader server.
- 2 Reset the driver object password and the Remote Loader password.
- 3 Start the Remote Loader instance for the Active Directory driver.

Observing Error: StatusLogger Reconfiguration Failed in Catalina Log File

Issue: After installing OpenText Identity Manager 24.4 (v4.10) on Windows, you might encounter the following error in catalina.out logs:

```
ERROR StatusLogger Reconfiguration failed: No configuration found for '<xxxxxxx>' at 'null' in 'null'
```

[Issue: OCTCR56A584800]

Workaround: The error does not affect any functionality. You can ignore it.

Form Builder Issues

You might encounter the following issues while working with JSON forms in Form Builder:

- ♦ [“Field Validation Messages Lack Clarity” on page 19](#)
- ♦ [“Form Builder Hangs While Scrolling” on page 20](#)
- ♦ [“The Button Component Does Not Work” on page 20](#)
- ♦ [“Tree Component Issues” on page 21](#)

Field Validation Messages Lack Clarity

Issue: Form field validation messages notify users when they enter an invalid or unacceptable value into a field. These messages typically consist of a key-value pair, with the value intended for user display. However, in this release, the form fields display keys rather than the corresponding values. For example, entering an invalid email address presents `invalid_email` instead of `Email must be a valid email`.

[Issue: OCTCR56A598009]

Workaround: To add the messages in English:

1. Launch Form Builder.
2. Click the  **Localization** icon.
3. Click **English** to expand.
4. Add a trailing comma and the key-value pairs for the messages to the last line.

For example,

```
{
  "Submit": "",
  "error": "Please fix the following errors before submitting.",
  "invalid_date": "{{field}} is not a valid date.",
  "invalid_email": "{{field}} must be a valid email.",
  "invalid_regex": "{{field}} does not match the pattern {{regex}}.",
  "mask": "{{field}} does not match the mask.",
  "max": "{{field}} cannot be greater than {{max}}.",
  "maxLength": "{{field}} must be shorter than {{length}} characters.",
  "min": "{{field}} cannot be less than {{min}}.",
  "minLength": "{{field}} must be longer than {{length}} characters.",
  "next": "Next",
  "pattern": "{{field}} does not match the pattern {{pattern}}",
  "previous": "Previous",
  "required": "{{field}} is required"
}
```

5. Click **Save**.

Form Builder Hangs While Scrolling

Issue: The form builder occasionally freezes while scrolling through the JSON forms in **Form JSON** and **JS Editor** views. This issue is observed in two scenarios:

- ♦ While working with a JSON form that contains many functions and methods.
- ♦ When your screen resolution differs from the system-recommended value.

[Issue: OCTCR56A602415]

Workaround: There is no workaround is available. You can relaunch Form Builder.

The Button Component Does Not Work

Issue: After upgrading to Designer 4.9, the Button component in JSON forms does not work for approve and request actions. [Issue: OCTCR56A604329]

Workaround: Perform the following steps:

- 1 Go to the Button component's **Display** tab.
- 2 Copy the logic specified in the **Button Request Logic** or **Button Approve Logic** fields.
- 3 Change the **Action** to custom.
- 4 Specify the logic copied from [Step 2](#).
- 5 Click **Save**.

Tree Component Issues

You might encounter the following issues with the Tree component in Form Builder:

- ♦ The fields display a nonarray validation error in the form **Preview**. This error occurs when the Tree component is set to display a default value. You cannot submit the form until you resolve the validation error. [Issue: OCTCR56A585664]

To resolve the error, change the default value with ID of that field in the **Form JSON** view.

- ♦ The expand functionality of a Tree component does not work as expected. The **Preview** form does not allow you to expand or select a sub-container.
- ♦ When you select a container or sub-container, the field displays the dn value instead of name.

The following **Data Source Raw JSON** is a sample data from the Tree component:

```
{
  "dn": "unique id",
  "name": "container data",
  "data": "any meta-data attached with the container",
  "subContainers": [
    {
      "dn": "id1",
      "name": "container data1",
      "icon": "glyphicon glyphicon-cloud"
    },
    {
      "dn": "id2",
      "name": "container data2",
      "data": "any meta-data attached with the container",
      "subContainers": [
        {
          "dn": "id3",
          "name": "container data3",
          "icon": "glyphicon glyphicon-cloud"
        }
      ]
    }
  ]
}
```

When you select the **container data** option in the **Preview**, the field displays the unique id instead of the container data. [Issue: OCTCR56A603396]

Contacting OpenText

For specific product issues, contact OpenText Support at <https://www.microfocus.com/support-and-services/>.

Additional technical information or advice is available from several sources:

- ♦ Product documentation, Knowledge Base articles, and videos: <https://www.microfocus.com/support-and-services/>
- ♦ The OpenText Community pages: <https://www.microfocus.com/communities/> (<https://www.microfocus.com/communities/>)

Legal Notice

Copyright 2009 - 2024 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.