

NetIQ Identity Manager 4.9

Release Notes

May 2024

NetIQ Identity Manager 4.9 provides new features, 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](#) on NetIQ Communities, 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 [Identity Manager Documentation Website \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/).

For more information about this release and for the latest release notes, see the [Documentation \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/) page. To download this product, see the [Software Licenses and Downloads \(https://sld.microfocus.com\)](https://sld.microfocus.com) portal.

- ♦ "What's New?" on page 2
- ♦ "Significant Changes in Behavior or Usage" on page 6
- ♦ "Deprecated Functionality" on page 6
- ♦ "Supported Component Versions" on page 6
- ♦ "System Requirements" on page 8
- ♦ "Resolved Security Vulnerability" on page 8
- ♦ "Resolved Issues" on page 8
- ♦ "Installing NetIQ Identity Manager 4.9" on page 12
- ♦ "Upgrading to NetIQ Identity Manager 4.9" on page 15
- ♦ "Known Issues" on page 19
- ♦ "Contacting Micro Focus" on page 30
- ♦ "Legal Notice" on page 30

What's New?

Identity Manager 4.9 provides the following new features and enhancements:

- ♦ [“Operating System Support” on page 2](#)
- ♦ [“NetIQ Audit, Compliance & Data Intelligence” on page 2](#)
- ♦ [“Identity Manager Drivers Now Supports Java 11” on page 2](#)
- ♦ [“Support for Modern Authentication” on page 4](#)
- ♦ [“Ability to Configure Identity Manager in FIPS Mode” on page 4](#)
- ♦ [“Integration of Workflow Service into the Monitoring Framework” on page 4](#)
- ♦ [“Identity Applications Enhancements” on page 4](#)
- ♦ [“Installer Enhancements” on page 5](#)
- ♦ [“Reporting Enhancements” on page 5](#)

For information about the new features in NetIQ Identity Manager Designer 4.9, see [NetIQ Identity Manager Designer 4.9 Release Notes](#).

Operating System Support

This release adds support for the following platforms:

- ♦ Red Hat Enterprise Linux (RHEL) 9.3, 9.2, 8.9, and 8.8
- ♦ Open Enterprise Server (OES) 24.2
- ♦ For Identity Manager Designer
 - ♦ Red Hat Enterprise Linux (RHEL) 9.2, 9.1, 8.9, 8.8, and 8.7
 - ♦ SUSE Linux Enterprise Server (SLES) 15 SP5
 - ♦ Windows 11 (Desktop)
 - ♦ macOS Sonoma

For a complete list of supported operating systems, see the [System Requirements for Identity Manager 4.9](#) page. For information about the components packaged, databases, and browsers supported with this release, see [“Supported Component Versions” on page 6](#).

NetIQ Audit, Compliance & Data Intelligence

Identity Manager introduces Audit, Compliance & Data Intelligence (ACDI), a new tool to provide visual analytics for identity-related data. The tool collects all identity-related data from Identity Manager sources, process it, and offers reporting and monitoring capabilities on the ACDI dashboard. For more information about this tool, see [NetIQ Audit, Compliance and Data Intelligence for Identity Manager](#).

ACDI is available as an add-on along with Identity Manager 4.9. You can download it from the [Software License and Download portal \(https://sld.microfocus.com/mysoftware/index\)](#). The tool is available only for the Identity Manager 4.9 off-cloud solution and not for the on-cloud deployment.

Identity Manager Drivers Now Supports Java 11

This release adds Java 11 support for Identity Manager 4.9 drivers. The following is a list of updated drivers.

Table 1 Identity Manager 4.9 drivers and their functional equivalent version in 4.8.x

Driver	Version Shipped with 4.9	Base Version (Identity Manager 4.8.x)
Azure Active Directory (AD)	5.2.0.0000	5.1.7.0200
Bidirectional eDirectory	4.1.0.0000	4.0.8.0300
REST	1.3.0.0000	1.2.0.0000
Delimited Text	4.1.0.0000	4.0.2.0200
GroupWise (REST-based)	4.1.0.0000	4.0.1.1
Identity Gateway Integration Module	1.1.0.0000	1.0.1.0300
JDBC	4.3.0.0000	4.2.2.0400
JDBC Fanout	1.3.0.0000	1.2.8
JMS	4.1.0.0000	4.0.0
LDAP	4.3.0.0000	4.2.0.0200
Lotus Notes	4.2.0.0000	4.1.2.0100
Manual Task Service	4.2.0.0000	4.1.0
Oracle E-Business Suite HR	4.2.0.0000	4.1.2.1
Oracle E-Business Suite TCA	4.2.0.0000	4.1.2.1
Oracle E-Business Suite User Management	4.2.0.0000	4.1.2.0101
PeopleSoft	5.3.0.0000	5.2.4.0
Entitlements Service (Role-based Entitlements)	4.1.0.0000	4.0.1.0
Salesforce	4.2.0.0000	4.1.0.1
SAP HR	4.1.0.0000	4.0.4.1
SAP Portal	4.1.0.0000	4.0.2.0100
SAP User Management	4.1.0.0000	4.0.4.1
SCIM	1.1.0.0000	1.0.1.0300
ServiceNow	1.1.0.0000	1.0.0
SOAP	4.2.0.0000	4.1.0.1
WorkOrder	4.1.0.0000	4.0.0.0100
Workday	1.4.0.0000	1.3.0.0200
Identity Tracking for Sentinel	4.1.0.0000	4.0.2
ID Provider	4.1.0.0000	4.0.0.0

There are no new features except the updated Java class file. For more information, see **Version Shipped with 4.9** on the [NetIQ Identity Manager Drivers \(https://www.netiq.com/documentation/identity-manager-49-drivers/\)](https://www.netiq.com/documentation/identity-manager-49-drivers/) page.

Support for Modern Authentication

In addition to basic authentication, Identity Applications support modern authentication in the incoming and outgoing email settings for email-based approval. Modern authentication provides more secure user authentication and access authorization.

Additionally, modern authentication is integrated with the Identity Manager Engine to [authenticate job notifications](#) and [template-based emails](#) deliver during policy execution.

NOTE: This release supports modern authentication only using the Office 365 OAuth authentication service provided by Azure Active Directory (Azure AD) for Microsoft Outlook.

Ability to Configure Identity Manager in FIPS Mode

You can now configure Identity Manager components in FIPS mode. For more information, see [Configuring Identity Manager in FIPS Mode](#) in *NetIQ Identity Manager Install and Upgrade Guide for Linux* or *Installing and Configuring Identity Manager Components* in *NetIQ Identity Manager Install and Upgrade Guide for Windows*.

Integration of Workflow Service into the Monitoring Framework

You can now use the existing LDAP search method to retrieve monitoring data for the Workflow Service component in your environment. You can do this by issuing a search request with a search base of `cn=idm,cn=monitor` on the Identity Vault. With this enhancement, you can monitor the status of Workflow Service using various statistics, such as total workflows, workflows in progress, completed workflows, new requests in the last 10, 60, and 300 seconds, and so forth.

In addition, this release adds more `jvm_stats` data to the existing statistics for User Application. For more information about these enhancements, see [Monitoring Identity Manager](#).

Identity Applications Enhancements

This release introduces the following Identity Applications enhancements:

Enhanced Version of Identity Applications Tools

NetIQ Identity Manager 4.9 has been updated with an enhanced version of the Identity Applications tool. The tool now supports the Java 11 platform. This enhancement includes the following utilities:

- ♦ [Workflow migration utility](#)
- ♦ [Workflow migration API utility](#)
- ♦ [Client settings migration utility](#)

For more information about how to use each of these utilities, click the link in the list.

A New Property to Change the Default Workflow Logging Behavior

The [Guidelines for Enabling Workflow Logging](#) have been updated. Starting with this release, the log level specified in the `workflow_logging.xml` file for an individual package takes precedence by default. For example, if the log level for the `com.novell.soa.af.impl.timers` package is set to `DEBUG` and the log level for the Workflow Engine (at a global level) is set to `INFO`, then the application will log `DEBUG` information for the selected package only. All other packages and loggers will be logged at the `INFO` log level.

In addition, a new property called `com.microfocus.workflow.engine.logging` has been introduced if you want to revert to the old behavior. You can add the `com.microfocus.workflow.engine.logging` property to the `ism-configuration.properties` file and set it to `true` if you want the log level set for the Workflow Engine to take precedence over the package log level. For more information about this property, see [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#).

Changes in the `IDVault.get()` Function

The `IDMProv/rest/access/entities/list` access API has been updated to include a new query parameter called `lookupAttr`. By default, `lookupAttr` is set to `false`. When set to `true`, the API will return the **Lookup Attributes** specified in the **DNLookup** definition of the attribute sent in the `filterAttr` parameter. `filterAttr` is another query parameter used in this API.

For example, if you want to retrieve a user entity's direct reports from the Identity Vault using the `IDVault.get` function, the method signature would be as follows:

```
IDVault.get('IDM', '/rest/access/entities/list', data.manager, 'user',  
["directReports"], true)
```

Where `directReports` is sent as the `filterAttr` and `true` is the `lookupAttr` value.

In the **DNLookup** definition of `directReports`, the **Lookup Attributes** for the **User Lookup** entity are Last Name, First Name, and Initials. When you add the `true` attribute to the function, the Identity Application returns the last name, first name, and initials of direct reports in response. If the **Lookup Attribute** is not configured, no **Lookup Attribute** value will be returned in response.

Installer Enhancements

This release incorporates the following enhancements to the installer:

- ♦ Integration of Identity Console within the Identity Manager Linux installer.
- ♦ Introduction of a new `ism-sensitive.properties` file, which securely stores the keypass and master storepass utilized for encrypting all passwords.

Reporting Enhancements

This release introduces the following Identity Reporting enhancement:

Default Reports that Use New Font set. Replace or Update Installed Reports

We have discontinued use of monotype fonts and all defaults reports have been converted to OT-Report-Font-Set.

Starting with Reporting 7.4, the Arial font is no longer included. For first time users, no additional steps are required as there will not be any report definition on the Repository page.

For those who are upgrading:

- ♦ If the report definition was originally installed using the Download feature in Reporting, reinstall the latest version of the report from the Download page.
- ♦ If the custom report definition was provided by Professional Services, please contact them for a new version.
- ♦ If the custom report definition was provided by a Partner, please contact them for a new version.
- ♦ If you created the custom report, replace Arial with OT-Report-Font-Set throughout the report definition, repackage, and then import the report definition.

If the report definition is not updated, it will fail at runtime with the following error: An error was detected while running report '%name%': Font "Arial" is not available to the JVM. See the Javadoc for more details.

Significant Changes in Behavior or Usage

Identity Manager 4.9 introduces changes in this release that might affect the behavior of its existing applications or features.

- ♦ The server's fully qualified distinguished name (FQDN) or short name is required instead of an IP address while configuring Identity Manager components on Linux and Windows platforms.
- ♦ Configuration utility (`configupdate.sh`) now prompts to enter a password before launching.
- ♦ If you are configuring the Workday driver on Identity Manager 4.9 on a Windows server and want to access the sample style sheet, you can find it in the following location within the Identity Manager 4.9 Windows ISO:
`\IdentityManagerServer\products\IDM\windows\setup\utilities\workday\transformation_style_sheets`

Deprecated Functionality

Starting with this release, the support for NetIQ SecretStore will be deprecated. Going forward, the account passwords will be saved in a new attribute called `notfSMTPMailPassword`. This attribute belongs to the `notfTemplateCollection` class and is included in the User Application Driver (UAD) package `NOVLUABASE_4.8.8.20240401125038`. When you install Identity Manager 4.9, this UAD package gets installed automatically. However, if you are upgrading from an earlier version, you will need to update the package manually.

After you upgrade to the latest UAD package and restart Tomcat, the existing email account passwords in the NetIQ SecretStore repository will automatically migrate to the `notfSMTPMailPassword` attribute. This password migration process is controlled by the `com.netiq.idm.migrate.secretstore` property, which is available in the `ism-configuration.properties` file. By default, this property is set to `true`. After the migration is complete, the property will automatically set back to `false` and will remain in this state.

Supported Component Versions

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

- ♦ [“Identity Manager Component Versions” on page 7](#)
- ♦ [“Third-Party Component Versions” on page 7](#)

- ♦ [“Database” on page 7](#)
- ♦ [“Web Browser” on page 8](#)

Identity Manager Component Versions

Identity Manager 4.9 bundles the following components:

- ♦ NetIQ eDirectory 9.2.9
- ♦ NetIQ Identity Console 1.7.2
- ♦ NetIQ Identity Manager Engine 4.9
- ♦ NetIQ Identity Manager Remote Loader 4.9
- ♦ NetIQ Identity Manager Fan Out Agent 1.3
- ♦ NetIQ Designer for Identity Manager 4.9
- ♦ NetIQ Identity Applications 4.9
- ♦ NetIQ One SSO Provider (OSP) 6.7.0
- ♦ NetIQ Self Service Password Reset (SSPR) 4.7.0.1
- ♦ NetIQ Identity Manager Identity Reporting 7.4.0
- ♦ NetIQ Sentinel Log Management for IGA 8.6.1.0 (for event auditing)
- ♦ NetIQ Identity Manager drivers

NOTE:

- ♦ Identity Manager 4.9 is also compatible with eDirectory 9.2.8.
 - ♦ Identity Manager 4.9 contains the latest version of a supported driver. For more information, see **Version Shipped with 4.9** on the [NetIQ Identity Manager Drivers \(https://www.netiq.com/documentation/identity-manager-49-drivers/\)](https://www.netiq.com/documentation/identity-manager-49-drivers/) page.
-

Third-Party Component Versions

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

- ♦ Zulu 11.70+15-CA
- ♦ Apache Tomcat 9.0.85-1
- ♦ PostgreSQL 12.18 (standalone and containers)
- ♦ OpenSSL 1.0.2zg-0
- ♦ Nginx 1.24.0-1
- ♦ ActiveMQ 5.18.3-1

Database

All Identity Manager 4.9 components, including NetIQ Identity Applications, are compatible with Oracle 21c, except for Identity Reporting. Identity Reporting 7.4.0 will continue the support on Oracle19c and 18c databases.

Web Browser

Any of the following browsers, at a minimum:

- ♦ Google Chrome 126.0.6478.8
- ♦ Mozilla Firefox 126.0
- ♦ Apple Safari 17.5
- ♦ Microsoft Edge 124.0.2478.109

System Requirements

For information about hardware requirements and supported operating systems, see the [Identity Manager System Requirements for Identity Manager 4.9](#) page.

Resolved Security Vulnerability

This version of Identity Manager resolves the following Common Vulnerabilities and Exposures (CVE): CVE-2024-4191.

Resolved Issues

This release includes the following software fixes:

Component	Global ID	Description
Installation and Upgrade	OCTCR56A583299	The Workflow Engine does not start if the database is maintained on Microsoft SQL Server.
Identity Manager Engine	OCTCR56A580623	The SOAP driver adds duplicate data to the DirXML - PersistentData attribute, causing an exception while iManager loads Dashboard on the Driver Set Overview page.
	OCTCR56A584222	Connection to the User Application server hangs when using the do- invoke-rest-endpoint action to make a REST request to an endpoint.
Identity Reporting	OCTCR56A580314	While clearing the reporting database on MS SQL, it displays the following error message: Incorrect syntax near the keyword 'CASCADE'.
	OCTCR56A581810	Driver Health job event (event-id: query-driver-ident) generates the following warning message: Recovered from unexpected condition: @cached-time no available.
	OCTCR56A585188	A REST API DELETE request to the /IDMDCS-CORE/rpt/ collectors/{identifier}/trust endpoint does not remove the trusted certificate from the collect_cert field of the data collector record.
Identity Applications	OCTCR56A572998	The field validation and value refresh form builder functionalities do not work in asynchronous scenarios.
	OCTCR56A573780	Sentinel Universal Collector fails to parse the message field in the CEF Event: 3152C- User Message.

Component	Global ID	Description
	OCTCR56A580840	Form fields based on Dynamic Entity component display square brackets as default values in the drop-down list.
	OCTCR56A580876	When you use the <code>RoleVault.getRolesUserIn</code> function to make a REST API call to the <code>/rest/access/assignments/role/list</code> endpoint, it retrieves only ten role assignment permissions for a given user. After upgrading to Identity Manager 4.9, you can retrieve information about all roles by adding the <code>true</code> attribute to the same function. Syntax: Here is the method signature: <pre>RoleVault.getRolesUserIn('IDM', '/rest/access/assignments/role/list', userDN, true)</pre>
	OCTCR56A581016	Form fields disappear on saving after switching between different Form Builder views.
	OCTCR56A581716	Workflow Engine logging is not working after upgrading to Identity Manager 4.8.4.
	OCTCR56A581762	The Select component includes an extra <code>_regex</code> string when querying an external web source for data.
	OCTCR56A581978	When using the Dynamic Entity component in a multi-tab form, the display name of the selected user changes when returning to the tab using the Back button.
	OCTCR56A582360	A JSON form does not display an error if the validation checks on a dynamic form field fails.
	OCTCR56A582959	When you use the <code>RoleVault.getRoleAssignmentCause</code> function to make a REST API call to <code>/rest/access/assignments/list/v2</code> endpoint, it retrieves role assignment cause for only ten roles by default. After upgrading to Identity Manager 4.9, you can retrieve the assignment cause for all roles by adding the <code>true</code> attribute to the same function. Syntax: Here is the method signature: <pre>RoleVault.getRoleAssignmentCause('IDM', '/rest/access/assignments/list/v2', identityDn, roleDn, true)</pre>
	OCTCR56A583294	Adding a group to the Requesters field fails while trying to modify an existing team.
	OCTCR56A583369	The Refresh On functionality does not work if the form fields are inside a Data Grid component.
	OCTCR56A583373	A Day field does not validate data correctly for non-English languages.
	OCTCR56A583421	Adding a comment with a single quotation mark (') in the Custom Default Value function corrupts the form.
	OCTCR56A583440	When using the <code>setFieldValue()</code> function to set a Custom Default Value, the validation process runs infinitely.

Component	Global ID	Description
	OCTCR56A583441	The Request History page on the Dashboard displays an error message if a requested permission is mapped to a resource with controlled access.
	OCTCR56A583590	Identity Manager allows any authenticated user to change another user's preferred locale.
	OCTCR56A583609	The Request State on the Request History page displays as "provisioned" even after denying the task.
	OCTCR56A583692	While editing the HelpDesk Ticket tile or any other PRD/form attached as a tile on the Manage Applications page, errors are displayed in the browser console logs.
	OCTCR56A583714	Duplicate delegations are created when you click the Create button on the Create Delegate Assignment page more than once.
	OCTCR56A583722	When reviewing the details of a request on the Request History page, the log activity's author and the corresponding comment are not separated by a space.
	OCTCR56A583747	When you use an <code>alert()</code> form action method in the Javascript code, the JS Editor and Form JSON stop working.
	OCTCR56A583754	Any custom functions saved in the JS Editor disappear if you modify the form again in Form Builder.
	OCTCR56A584217	The form rendered on the Identity Manager Dashboard is different from the form displayed in the Form Builder preview mode.
	OCTCR56A584275	A Select component with Enable Static Search set to <code>true</code> cannot search for values longer than 50 characters. The Select component will now allow you to search values up to 1000 characters in length.
	OCTCR56A584283	When defining a logic for any component, it is not possible to select a property for an action triggered by an event.
	OCTCR56A584291	When the Select and Radio component's Label Position is set to <code>Left (Right-aligned)</code> , the options displayed are not properly aligned.
	OCTCR56A584322	The Custom Default Value function of a Checkbox component does not execute on initial form load, nor when triggered by a change or an explicit <code>triggerChange()</code> execution.
	OCTCR56A584373	The Tasks page on the Dashboard does not refresh automatically. Even after a task is approved using the approval form, it still appears on the list.
	OCTCR56A584374	The Permissions page on Dashboard no longer lists permissions with square or curly brackets in the search results.
	OCTCR56A584399	Attributes set as Editable Attributes in Settings are not editable on My Profile and Users pages.
	OCTCR56A584489	When requesting a PRD, the New Request page shows fields for entering the Effective Date and Expiration Date .

Component	Global ID	Description
	OCTCR56A584625	Field labels are missing in localized forms.
	OCTCR56A584638	A Dynamic Entity Component set with a display limit (the maximum number of items to request or view) does not list all matching entities in search results.
	OCTCR56A584639	After enabling the ONLINE mode and then going OFFLINE and back to ONLINE mode, Form Builder does not allow logging in with a different credential after the first login.
	OCTCR56A584666	The Users List Container option in Settings > Customization is not used to list users on the New Request for Others page.
	OCTCR56A585183	The Applications page on Identity Manager Dashboard displays category headings with no permitted items within them.
	OCTCR56A585185	The time input element is missing from a Date/Time component that is set to display both the calendar and time elements.
	OCTCR56A585231	The telephone number entered in the Telephone Number attribute on the My Profile page cannot be edited or deleted.
	OCTCR56A585264	Form Builder executes the Custom Default Value function every time a user switches between Form Builder views.
	OCTCR56A585443	The procedure for reassigning tasks to other team members does not work as documented.
	OCTCR56A585477	The Signature attribute on the user profile page displays a text value instead of the signature image.
	OCTCR56A585503	Form Builder does not load properly when launched from Designer on a Windows system without an Internet connection.
	OCTCR56A585527	After upgrading to Identity Manager 4.8.7, the counter for permissions on the Permission of Other's page is not correctly positioned in the supported locales (excluding English and Portuguese).
	OCTCR56A585557	The DN Display component of Form Builder shows an error message when conditions are set.
	OCTCR56A585618	Unable to access User Application and SSPR after an upgrade. Restarting the ndsd service on eDirectory and Tomcat on the Identity Applications server temporarily resolves the problem, but the components become inaccessible again after some time.
	OCTCR56A585698	The My Profile page displays incorrect attributes when Identity Manager is configured to manage multiple clients.
	♦ OCTCR56A584920 ♦ OCTCR56A585772	The Card View of a user and the attributes on the Users page of the Identity Manager Dashboard display attributes that differ from those configured in the client customization settings.

Installing NetIQ Identity Manager 4.9

Identity Manager 4.9 provides Advanced Edition and Standard Edition in a single ISO file. Before downloading the installation files, you must understand what features are contained in each edition and the options for downloading the Identity Manager components.

- ♦ [“Features Supported with Identity Manager Advanced and Standard Editions” on page 12](#)
- ♦ [“Downloading Identity Manager” on page 12](#)
- ♦ [“Locating the Executables and Default Installation Paths” on page 13](#)
- ♦ [“Installing NetIQ Identity Manager 4.9” on page 15](#)

Features Supported with Identity Manager Advanced and Standard Editions

To meet different customer needs, the Identity Manager functionality is delivered in two product groups:

- ♦ Identity Manager Advanced Edition
- ♦ Identity Manager Standard Edition

Identity Manager features provided with Identity Manager Standard Edition are also included in Identity Manager Advanced Edition, along with additional features. The following table provides a comparison of features available in Identity Manager Advanced and Standard Editions:

Feature	Advanced Edition	Standard Edition
Rule-based automated user provisioning	Yes	Yes
Real-time identity synchronization	Yes	Yes
Password management and password self-service	Yes	Yes
Uniform identity information tool (Analyzer)	Yes	Yes
REST APIs and single sign-on support	Yes	Yes (limited support)
Current state reporting	Yes	Yes
Role-based enterprise-level provisioning	Yes	No
Automated approval workflows for business policy enforcement	Yes	No
Advanced self-service in identity applications	Yes	No
Resource model and catalog for easy resource provisioning	Yes	No
Historical state reporting	Yes	No
Connected systems reporting	Yes	No
Role and resource administration	Yes	No

Downloading Identity Manager

After purchasing Identity Manager 4.9, 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 Identity Manager components:

IMPORTANT: We have refreshed the Identity Manager 4.9 deliverables for Linux, Windows, and Containers in December 2024. The updated deliverables now includes the latest versions of the Identity Manager Reporting and Data Collection Service driver. The new version is available on the [Software License and Download portal \(https://sld.microfocus.com/mysoftware/index\)](https://sld.microfocus.com/mysoftware/index).

File Name	Description
Identity_Manager_4.9_Linux.iso	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, Identity Console), Identity Applications, and Identity Reporting.
Identity_Manager_4.9_RL_Linux.iso	Contains the Identity Manager Remote Loader for Linux.
Identity_Manager_4.9_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 Identity Console.
Identity_Manager_4.9_Windows.iso	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent), Identity Applications, and Identity Reporting.
Identity_Manager_4.9_RL_Windows.iso	Contains the 64-bit and .NET Remote Loader for Windows.
Identity_Manager_4.9_Designer_Linux.tar.gz	Contains Designer for Linux platforms.
Identity_Manager_4.9_Designer_Windows.zip	Contains Designer for Windows platforms.
Identity_Manager_4.9_Designer_MacOSX.dmg	Contains Designer files for macOS Sonoma.
SentinelLogManagementForIGA8.6.1.0.tar.gz	Contains Sentinel Log Management for Identity Governance and Administration (IGA).
This installation is supported only on Linux.	

IMPORTANT: The Analyzer tool is not included in the Identity Manager 4.9 ISO. If Analyzer is already installed, ensure that you update it to version 4.8.5 and use it with Identity Manager 4.9. For installing and upgrading Analyzer, see [NetIQ Identity Manager Install and Upgrade Guide for Linux](#) or [NetIQ Identity Manager Install and Upgrade Guide for Windows](#).

Locating the Executables and Default Installation Paths

- ♦ [“Executables and Default Installation Paths on Linux” on page 14](#)
- ♦ [“Executables and Default Installation Paths on Windows” on page 14](#)

Executables and Default Installation Paths on Linux

Identity Manager Component	Location of the Executable within ISO	Default Installation Path
Identity Manager Server (Contains Identity Manager Engine, Remote Loader, Fan-Out Agent, 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 ♦ 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 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 SentinelLogManagementForIGA8.6.1.0.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 Identity Manager	install.exe located in \designer_install\ folder of the Identity_Manager_4.8_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 the <iso mounted location>\common\sspr	C:\netiq\idm\apps\common\sspr

Installing NetIQ Identity Manager 4.9

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

- ♦ Advanced Edition: [NetIQ Identity Manager Install and Upgrade Guide for Linux](#) or [NetIQ Identity Manager Install and Upgrade Guide for Windows](#)
- ♦ Standard Edition: [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.9 Standard Edition](#)

Upgrading to NetIQ Identity Manager 4.9

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

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

- ♦ [“Upgrading from Identity Manager 4.8.x Versions” on page 16](#)
- ♦ [“Upgrading from Identity Manager 4.7.x Versions” on page 17](#)
- ♦ [“Upgrading to Advanced Edition” on page 18](#)
- ♦ [“Upgrading to Standard Edition” on page 19](#)

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

Upgrading from Identity Manager 4.8.x Versions

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

Component	Base Version	Upgraded Version
Identity Manager Engine	4.8.x	1. Upgrade the operating system to a supported version. 2. Upgrade Identity Vault to 9.2.9. 3. Upgrade Identity Manager Engine to 4.9.
Remote Loader/Fanout Agent	4.8.x	Upgrade to 4.9 Remote Loader/Fanout Agent.
Designer		Install Designer 4.9.
Identity Applications	4.8.x	Before you upgrade Identity Applications, ensure that the Identity Vault and Identity Manager engine are upgraded to 9.2.9 and 4.9, 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 the NetIQ Identity Manager Technical Information Website. 4. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.9 version. 5. Update the User Application driver and Roles and Resources driver packages using Designer. 6. Upgrade Identity Applications to 4.9. 7. Start Tomcat.

Component	Base Version	Upgraded Version
Identity Reporting	4.8.x	Before you upgrade Identity Reporting, ensure that the Identity Vault, Identity Manager engine, and Identity Applications are upgraded to 9.2.9, 4.9, and 4.9, 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 the NetIQ Identity Manager Technical Information Website. 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 7.4.0. 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 [NetIQ documentation \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/) page.

Upgrading from Identity Manager 4.7.x Versions

The following table lists component-wise upgrade paths for Identity Manager 4.7.x versions:

Component	Base Version	Upgraded Version
Identity Manager Engine	4.7.5	1. Upgrade the operating system to a supported version. 2. Upgrade Identity Vault to 9.2.9. 3. Upgrade Identity Manager Engine to 4.9.
Remote Loader/ Fanout Agent	4.7.5	Upgrade to 4.9 Remote Loader/Fanout Agent.
Designer		Install Designer 4.9.

Component	Base Version	Upgraded Version
Identity Applications	4.7.5	Before you upgrade Identity Applications, ensure that Identity Vault and Identity Manager engine are upgraded to 9.2.9 and 4.9 versions, respectively. 1. Upgrade the operating system to a supported version. 2. Stop Tomcat. 3. Update the User Application driver and Roles and Resources driver packages. 4. Upgrade the database to a supported version. For the supported database versions, see the NetIQ Identity Manager Technical Information Website. 5. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.9. 6. Upgrade Identity Applications to 4.9. 7. Start Tomcat.
Identity Reporting	4.7.5	Before you upgrade Identity Reporting, ensure that the Identity Vault, Identity Manager engine, and Identity Applications are upgraded to 9.2.9, 4.9, and 4.9, 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 the NetIQ Identity Manager Technical Information Website. 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 7.4.0. 6. Start Tomcat.

Before starting the upgrade, review the information from the release notes for your version from the [NetIQ documentation \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/) page.

Upgrading to Advanced Edition

NetIQ provides the following upgrade paths for upgrading to Identity Manager 4.9 Advanced Edition from a prior Advanced Edition or Standard Edition:

- ◆ Identity Manager 4.8 Advanced Edition to 4.9 Advanced Edition
- ◆ Identity Manager 4.8 Standard Edition to 4.9 Advanced Edition, in one of the following ways:
 - ◆ From Identity Manager 4.8 Standard Edition to 4.9 Standard Edition and then to 4.9 Advanced Edition
 - ◆ From Identity Manager 4.8 Standard Edition to 4.8 Advanced Edition and then to 4.9 Advanced Edition
- ◆ Identity Manager 4.7.5 Advanced Edition to 4.9 Advanced Edition

- ♦ Identity Manager 4.7.5 Standard Edition to 4.9 Advanced Edition, in one of the following ways:
 - ♦ From Identity Manager 4.7.5 Standard Edition to 4.9 Standard Edition and then to 4.9 Advanced Edition
 - ♦ From Identity Manager 4.7.5 Standard Edition to 4.7.5 Advanced Edition and then to 4.9 Advanced Edition

Upgrading to Standard Edition

You can upgrade to Identity Manager 4.9 Standard Edition from Identity Manager 4.8 Standard Edition. For upgrade instructions, see [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.9 Standard Edition](#).

The Identity Manager 4.9 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 [Administrator Guide to NetIQ Identity Reporting](#).

IMPORTANT: To use the 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

NetIQ 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](#). For the list of known issues in Designer, see the [NetIQ Identity Manager Designer 4.9 Release Notes](#).

- ♦ [“Sending HTML-based Emails Through the Driver Policy Fails” on page 20](#)
- ♦ [“Set SSO Credential Action Displays an Error” on page 20](#)
- ♦ [“Windows Installer Displays an Exception” on page 21](#)
- ♦ [“An Error Occurs While Logging in to Identity Manager When Using Two-Factor Authentication” on page 21](#)
- ♦ [“The dirxml_remote and RLConsole Properties Displays Outdated Product Version” on page 21](#)
- ♦ [“Installer Generates Empty Database Schema SQL Files” on page 21](#)
- ♦ [“Some Reports Do Not Fetch Any Data While Using MS SQL Database” on page 22](#)
- ♦ [“Error Reported in the Upgrade Log File” on page 25](#)
- ♦ [“Identity Manager Does Not Reflect Changes Made to the Use SMTP TLS Option in Identity Console” on page 25](#)

- ♦ “On Linux, iManager Displays a Blank Page After Upgrade” on page 25
- ♦ “Warning: Illegal Reflective Access Operation Has Occurred” on page 26
- ♦ “Tomcat Does Not Start on RHEL 8.x and 9.x After Upgrading Identity Manager to 4.9” on page 26
- ♦ “Organization Chart Buttons for a Level 2 or Higher Relationship Hierarchy Is Missing” on page 26
- ♦ “Remote Loader Reports Invalid Driver Object Password After Upgrade” on page 27
- ♦ “Observing Error: StatusLogger Reconfiguration Failed in Catalina Log File” on page 27
- ♦ “Form Builder Issues” on page 27

Sending HTML-based Emails Through the Driver Policy Fails

Issue: After upgrading Identity Manager to version 4.9, sending HTML-based emails through policies that use the <do-send-email-from-template> action fails. The following error message is displayed:

```
Couldn't send email: java.lang.NoSuchMethodError: 'int
com.sun.mail.util.QEncoderStream.encodedLength(byte[], boolean)'
```

Version 4.9 includes two libraries: `angus-mail-1.0.0.jar` and `jakarta.mail-2.0.1.jar`. Both libraries provide the `com.sun.mail.util.QEncoderStream` class. However, the `angus-mail-1.0.0.jar` library does not define the `encodedLength` method in the `QEncoderStream` class. As a result, when the engine runs the policy, if `angus-mail-1.0.0.jar` is loaded first, the email is sent, but it does not go through. Not all HTML email templates are impacted by this issue.

[Issue: OCTCR56A627092]

Workaround: To provide the email functionality, only the `jakarta.mail-2.0.1.jar` library is required. Therefore, delete the `angus-mail-1.0.0.jar` and `jakarta.mail-api-2.1.2.jar` files from the `/opt/novell/eDirectory/lib/dirxml/classes` directory, and restart eDirectory to apply the changes. For more information, see [KM000033855 \(https://portal.microfocus.com/s/article/KM000033855?language=en_US\)](https://portal.microfocus.com/s/article/KM000033855?language=en_US).

Set SSO Credential Action Displays an Error

Issue: After upgrading to version 4.9, 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.

Windows Installer Displays an Exception

Issue: Starting Tomcat after installing Identity Manager 4.9 components displays the following exception:
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 Identity Manager 4.9. [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 located at `C:\NetIQ\idm\apps\tomcat\conf`

An Error Occurs While Logging in to Identity Manager When Using Two-Factor Authentication

Issue: Users might encounter login failures if NetIQ One SSO Provider (OSP) on the Identity Manager server is configured with NetIQ Advanced Authentication for two-factor authentication. The OSP log file displays the following error: Unexpected error while searching:
`internal.atlaslite.jcce.exception.CoreInitializationException: No administrator password is configured.`

[Issue: OCTCR56A603388]

Workaround: No workaround is available.

The `dirxml_remote` and `RLConsole` Properties Displays Outdated Product Version

Issue: When you install or upgrade Remote Loader through the `Identity_Manager_4.9_RL_Windows.iso` or `Identity_Manager_4.9_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.

Installer Generates Empty Database Schema SQL Files

Issue: During the Identity Applications component upgrade, if you choose the `write to file` option for creating database schema, the installer creates empty `databaseschema.sql` and `wfatabaseschema.sql` files. Because these files are empty, you cannot use them to create database schema after the upgrade is complete. [Issue: OCTCR56A586043]

Workaround: Download the appropriate database jar file on your application server from a third-party website for your Identity Applications database. Install it on a separate system or a server along with Identity Applications.

When the installer prompts you to enter the **Identity Applications and Workflow Engine database JDBC jar file** path during Identity Applications update, specify the location of the installed database jar file.

Some Reports Do Not Fetch Any Data While Using MS SQL Database

Issue: If you are using MS SQL as the Identity Reporting database, the [Access Requests by Recipient](#), [Access Requests by Requester](#), and [Access Requests by Resource](#) reports do not return any data.

[Issue: OCTCR56A604404]

Workaround: To fetch the data for the above reports, perform the following steps:

- 1 Log in to the server where Identity Reporting is installed.
- 2 Open a database administrator tool such as SQL Server Management Studio.
- 3 Run the following query:

NOTE: Specify the appropriate Identity Reporting database name in the <identity reporting database name> field.

```
USE [<identity reporting database name>]
GO

/***** Object: UserDefinedFunction [IDM_RPT_DATA].[get_formatted_user_dn]
Script Date: 5/9/2020 7:03:55 PM *****/
DROP FUNCTION [IDM_RPT_DATA].[get_formatted_user_dn]
GO

/***** Object: UserDefinedFunction [IDM_RPT_DATA].[get_formatted_user_dn]
Script Date: 5/9/2020 7:03:55 PM *****/
SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO

CREATE FUNCTION [IDM_RPT_DATA].[get_formatted_user_dn]
(
    -- Add the parameters for the function here
    @user_path nvarchar(max)
    , @user_name nvarchar(200)
)
RETURNS nvarchar(max)
AS
BEGIN
    DECLARE
        @new_path          nvarchar(200),
        @new_path_2        nvarchar(max),
        @l_user_path       nvarchar(max),
        @l_old_delimiter   nvarchar(1) = '\\',
        @l_new_delimiter   nvarchar(1) = '.',
        @MyCursor CURSOR,
        @MyField nvarchar(max);

    if @user_path is not null
    BEGIN
        SET @l_user_path = SUBSTRING(@user_path , 2 , (LEN(@user_path)-1));
        SET @MyCursor = CURSOR FOR
            SELECT value FROM STRING_SPLIT( @l_user_path ,
```

```

@l_old_delimiter )
OPEN @MyCursor
FETCH NEXT FROM @MyCursor
INTO @MyField
WHILE @@FETCH_STATUS = 0
BEGIN
    if @MyField is not null
    BEGIN
        SET @new_path = @l_new_delimiter + @MyField;
    END
    if @new_path_2 is not null
    BEGIN
        SET @new_path = @new_path + @new_path_2;
    END
    SET @new_path_2 = @new_path;
    FETCH NEXT FROM @MyCursor
    INTO @MyField
END
CLOSE @MyCursor
DEALLOCATE @MyCursor

if @new_path is not null
BEGIN
    SET @new_path = @user_name + @new_path;
END
else
BEGIN
    SET @new_path = @user_name;
END
END
return LTRIM(RTRIM(@new_path));
END;

GO

CREATE FUNCTION [IDM_RPT_DATA].[patternReplace]
(
    @InputString VARCHAR(4000),
    @Pattern VARCHAR(100),
    @ReplaceText VARCHAR(4000)
)
RETURNS VARCHAR(4000)
AS
BEGIN
    DECLARE @Result VARCHAR(4000) SET @Result = ''
    -- First character in a match
    DECLARE @First INT
    -- Next character to start search on
    DECLARE @Next INT SET @Next = 1
    -- Length of the total string -- 8001 if @InputString is NULL
    DECLARE @Len INT SET @Len = COALESCE(LEN(@InputString), 8001)
    -- End of a pattern
    DECLARE @EndPattern INT

```

```

        WHILE (@Next <= @Len)
        BEGIN
            SET @First = PATINDEX('%' + @Pattern + '%', SUBSTRING(@InputString, @Next,
@Len))
            IF COALESCE(@First, 0) = 0 --no match - return
            BEGIN
                SET @Result = @Result +
                CASE --return NULL, just like REPLACE, if inputs are NULL
                WHEN @InputString IS NULL
                OR @Pattern IS NULL
                OR @ReplaceText IS NULL THEN NULL
                ELSE SUBSTRING(@InputString, @Next, @Len)
            END
            BREAK
        END
        ELSE
        BEGIN
            -- Concatenate characters before the match to the result
            SET @Result = @Result + SUBSTRING(@InputString, @Next, @First - 1)
            SET @Next = @Next + @First - 1

            SET @EndPattern = 1
            -- Find start of end pattern range
            WHILE PATINDEX(@Pattern, SUBSTRING(@InputString, @Next, @EndPattern)) = 0
                SET @EndPattern = @EndPattern + 1
            -- Find end of pattern range
            WHILE PATINDEX(@Pattern, SUBSTRING(@InputString, @Next, @EndPattern)) > 0
                AND @Len >= (@Next + @EndPattern - 1)
                SET @EndPattern = @EndPattern + 1

            --Either at the end of the pattern or @Next + @EndPattern = @Len
            SET @Result = @Result + @ReplaceText
            SET @Next = @Next + @EndPattern - 1
        END
        END
        RETURN(@Result)
    END;

```

GO

- 4 Navigate to the [CDN](#) website.
- 5 Click the **Access Requests by Recipient** report.
- 6 Download the .rpz and .zip files for the **Access-Requests-by-Recipient** report.
- 7 Perform steps [Step 5](#) and [Step 6](#) for the **Access Requests by Requester**, and **Access Requests by Resource** reports.

Error Reported in the Upgrade Log File

Issue: After upgrading Identity Manager to 4.9, users may encounter the following SQL exceptions in the `idmupgrade.log` file:

Unexpected error running Liquidbase Error: cannot drop view idmrpt_identity_cs_v.

Unexpected error running Liquidbase Error: idmrpt_identity_v already exists.

This issue occurs after you upgrade the reporting component from Identity Manager 4.8.7 to 4.9[OCTCR56A677245].

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

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

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

This happens because the `notfSMTPUseTLS` LDAP attribute is updated differently in Identity Applications and Identity Console. When you make the change in Identity Console, the attribute is updated directly. Whereas, when you change the **Use SMTP TLS** value in **Outgoing Email Settings** of 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 Identity Console is still applied, even if it does not appear on the Email Based Approval page in 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.

On Linux, iManager Displays a Blank Page After Upgrade

Issue: After upgrading Identity Manager to 4.9, iManager no longer works if installed with other components. When you try to launch a previously installed version, iManager displays a blank page.

Workaround: Install and use Identity Console in place of iManager. However, if you want to continue using iManager after upgrading Identity Manager to version 4.9, ensure that:

- ♦ iManager is installed on a standalone server.
- ♦ The server has a supported version of Java. For example, iManager 3.2.6.0200 on Java JDK 1.0.8 Update 342 in Identity Manager 4.8.6

Perform the following steps to reuse the old Java files:

1. Create a new directory using the following command:

```
mkdir -p /opt/novell/iManager/java_iman
```

2. Copy the existing Java files of iManager to the new directory:

```
cp -r /opt/netiq/common/jre/ /opt/novell/iManager/java_iman
```

3. To change the ownership to the new directory, run the following command:

```
chown -R novlwww:novlwww /opt/novell/iManager/java_iman
```

4. Navigate to `/etc/opt/novell/tomcat9/` and update the `JAVA_HOME` and `JRE_HOME` with the new Java path in the `tomcat9.conf` file.
5. Restart Tomcat using the following comment:

```
rcnovell-tomcat9 restart
```

Warning: Illegal Reflective Access Operation Has Occurred

Issue: When configuring Identity Applications, you might encounter the following message:

Warning: An illegal reflective access operation has occurred

This occurs because the current version of Identity Applications uses Java 11. [Issue: OCTCR56A583685]

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

Tomcat Does Not Start on RHEL 8.x and 9.x After Upgrading Identity Manager to 4.9

Issue: When upgrading Identity Manager to version 4.9 on a server running RHEL 8.x or RHEL 9.x (where x is the version supported in 4.9), OSP fails to start due to a database connection issue. It typically happens when the random key generation process takes longer than expected while the OSP is getting deployed. As a result, Tomcat services also fail to start. [Issue: OCTCR56A584564]

Workaround: Modify the following lines in the `java.security` file at the `/opt/netiq/common/jre/conf/security` location and restart Tomcat:

NOTE: Before applying the workaround, refer to the [RHEL documentation \(https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-encryption-using_the_random_number_generator\)](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-encryption-using_the_random_number_generator) for more information about random number generators.

- ♦ Replace `securerandom.source=file:/dev/random`
with
`securerandom.source=file:/dev/./urandom`
- ♦ Replace `securerandom.strongAlgorithms=NativePRNGBlocking:SUN`
with
`securerandom.strongAlgorithms=SHA1PRNG:SUN`

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 4.9 on a Windows platform, it is unable to connect to the Active Directory driver using the basic authentication password. [Issue: OCTCR56A584022]

Workaround: After upgrading Identity Manager to 4.9, 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 Identity Manager 4.9 on a Windows platform, you might encounter the following error message 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 when you are working with JSON forms in Form Builder.

- ♦ [“Field Validation Messages Do Not Convey the Message Clearly” on page 27](#)
- ♦ [“Form Field Displays Non Array Validation Error After Upgrading Designer to Version 4.9” on page 28](#)
- ♦ [“Form Builder Hangs While Scrolling” on page 28](#)
- ♦ [“Button Action Is Not Working” on page 28](#)
- ♦ [“Tree Component Issues” on page 29](#)

Field Validation Messages Do Not Convey the Message Clearly

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 are displaying 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 for English language:

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 Field Displays Non Array Validation Error After Upgrading Designer to Version 4.9

Issue: If a single-valued form field contains multiple values, the Form Builder will now display a non-array validation error. This validation check has been added in the latest version of Form Builder. Therefore, when you upgrade Designer to version 4.9, this issue will occur in exiting forms. [Issue: OCTCR56A586045]

Workaround: To fix the error, perform one of the following options:

- ♦ Open the form in Form Builder and select the **Multiple Values** check box in the affected form field. This will add an **Add Another** button to the field, allowing users to enter more values.
- ♦ Modify the Custom Default Value function in the affected field to display only the first value returned in an array, even if the array has a single value.

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.

Button Action Is Not Working

Issue: After upgrading to Designer 4.9, the Button component in JSON forms is not working 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 will not be able to 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 is not working as expected. The **Preview** form does not allow you to expand or select a subcontainer.
- ♦ 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 Micro Focus

For specific product issues, contact Micro Focus 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 Micro Focus Community pages: <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.

For additional information, such as certification-related notices and trademarks, see <http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>).