



NetIQ® Identity Manager 4.8 Service Pack 6 Release Notes

September 2022

Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal>.

Copyright (C) 2022 NetIQ Corporation. All rights reserved.

Contents

| | |
|---|-----------|
| About this Book | 5 |
| 1 What's New and Changed? | 7 |
| New Features and Enhancements | 7 |
| Platform Support | 7 |
| Angular Update | 7 |
| Third-Party Library Upgrade | 7 |
| Digitally Signed RPMs | 8 |
| Enhancements in Identity Applications | 8 |
| Enhancements in Identity Manager Containers | 9 |
| Component Updates | 9 |
| Identity Manager Component Versions | 9 |
| Updates for Dependent Components | 10 |
| Third-Party Component Versions | 10 |
| Software Fixes | 10 |
| Installation and Upgrade | 11 |
| Identity Manager Engine | 11 |
| Identity Applications | 11 |
| Identity Reporting | 15 |
| Identity Manager Designer | 16 |
| 2 Installing or Updating to This Service Pack | 17 |
| 3 Known Issues | 19 |
| iManager Tomcat Service is Reset to Startup Automatically After Upgrade | 19 |
| Remote Loader Reports Invalid Driver Object Password After Upgrade | 20 |
| .NET Remote Loader Unable to Connect to the MDAD Driver After Upgrade | 20 |
| Unable to Login to the Dxcmd Utility After Upgrade | 20 |
| Unable to Save Responses in SSPR for Identity Manager Standard Edition Deployment on AKS | 20 |
| Number of Open File Handles On the Identity Applications Server Increases Rapidly for Bulk Role and Resource Operations | 21 |
| Error Displayed While Trying to Access SSPR as an Administrator | 22 |
| Error Displayed While Upgrading Standalone SSPR on Linux | 23 |
| Form Renderer Displays a JSON Error When Loading Legacy Forms | 23 |
| User Application Driver Version and Copyright Information is Outdated | 24 |
| Tomcat On RHEL 8.5 and 8.6 Does Not Start After Upgrading Identity Manager to 4.8.6 | 24 |
| Workflow Engine Fails to Start When Upgrading Identity Manager on Oracle Database | 24 |
| Identity Manager Server Edition is Not Displayed in the DirXML Command Line Utility | 25 |
| Enable oidpInstanceData Attribute Clean-up Property is Missing in Designer | 25 |
| Workflow Engine Fails to Start When the Database is on MS SQL Server | 27 |
| Events are Lost Due to Database Transaction Error | 27 |
| Field Values Seen in the Permission Differ From the Values Entered in the Resource Form | 27 |

About this Book

The NetIQ Identity Manager 4.8 Service Pack 6 provides new features, enhancements, improves usability, and resolves several previous issues. 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.

The documentation for this product and the latest release notes are available on the NetIQ Web site on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the [Identity Manager Documentation Website](#).

1 What's New and Changed?

NetIQ Identity Manager 4.8.6 provides the following key features, enhancements, and fixes in this release:

- ♦ [“New Features and Enhancements” on page 7](#)
- ♦ [“Component Updates” on page 9](#)
- ♦ [“Software Fixes” on page 10](#)

New Features and Enhancements

Identity Manager 4.8.6 provides the following key functions and enhancements in this release:

- ♦ [“Platform Support” on page 7](#)
- ♦ [“Angular Update” on page 7](#)
- ♦ [“Third-Party Library Upgrade” on page 7](#)
- ♦ [“Digitally Signed RPMs” on page 8](#)
- ♦ [“Enhancements in Identity Applications” on page 8](#)
- ♦ [“Enhancements in Identity Manager Containers” on page 9](#)

Platform Support

In addition to the existing operating systems (OS), this service pack provides support for the following OS:

- ♦ Red Hat Enterprise Linux (RHEL) 8.6
- ♦ SUSE Linux Enterprise Server SLES15 SP4
- ♦ Open Enterprise Server (OES) 2018 SP3

Angular Update

All components of the Identity Manager have been updated to Angular 13, except for Form Renderer, which continues to use Angular 9. The Identity Manager Dashboard (/idmdash), which was earlier built on Angular JS framework, has been migrated to Angular.

Third-Party Library Upgrade

All third-party libraries have been updated to a newer version. Note that a newer version does not necessarily imply the most recent version. A newer version means a tested version of the library that is claimed to be supported in Identity Manager 4.8.6.

Digitally Signed RPMs

All RPMs in this release are digitally signed. You must verify the RPM signature before installing or upgrading to Identity Manager 4.8.6 version. For more information on how to verify the RPM signature, see [Updating the Identity Manager Components on Linux](#) in the *NetIQ Identity Manager 4.8.6: Installation and Upgrade Guide*.

Enhancements in Identity Applications

Identity Applications includes the following enhancements:

idmdash and idmadmin are Now Combined

Dashboard (`idmdash`) and Identity Applications Administration (`idmadmin`) are now combined into a single application. When accessing the Administration, Configuration, Settings, and other menus in Identity Manager Dashboard, users now interact with `idmdash` instead of `idmadmin`. The following table shows the URL change for one such page:

| Prior to Identity Manager 4.8.6 | Identity Manager 4.8.6 and onward |
|--|---|
| <code>https://<IP_Address>:8543/idmadmin/#/role</code> | <code>https://<IP_Address>:8543/idmdash/#/role</code> |

After upgrading Identity Manager to 4.8.6, any bookmark pointing to the `/idmadmin` pages will no longer be valid. You must add new bookmarks to gain quick access to your favorite pages.

Ability to Monitor Workflow Progress

The Identity Applications user interface includes a new feature, **Workflow Monitoring**, in the **Administration** menu that allows security and provisioning administrators to monitor and manage workflows.

During the workflow execution process, the Workflow Engine performs several activities and logs them as events on the **Workflow Monitoring** page. You can view the comments, reassign activities within the workflow, terminate a workflow, and view the workflow status. This data enables you to make informed decisions, such as reassigning a workflow process if an approval request activity has been left unattended for an extended period. You can also terminate a workflow from this page.

For a detailed information, see [Monitoring Workflows \(https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin_486/data/workflowmonitoring.html\)](https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin_486/data/workflowmonitoring.html) in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Dynamic Workflow Engine IDs

Workflow service offers a unique capability of automatically adding Workflow Engine node in response to workload changes. When a node in a cluster fails, the workflow processes in that node are automatically transferred to another node in the same cluster. It ensures that the Workflow

Engine is always available and there is no downtime in the event of a failure. The node is assigned a unique dynamic Engine ID, which changes with each Tomcat restart. The status and IDs of all nodes are saved in the workflow database.

This feature is enabled by default when you deploy Identity Manager containers on Microsoft Azure.

Enhancements in Identity Manager Containers

Identity Manager Containers has the following enhancements for fresh deployment in Microsoft Azure:

- ◆ Identity Engine will now be managed by AKS ensuring fault tolerance.
- ◆ Identity Engine supports multiple replica deployment with stateful set. The following features are supported:
 - ◆ All Identity Manager Engine replicas would still be deployed in Master-Slave Architecture.
 - ◆ Identity Manager Engine replicas once deployed are ready to load balance the necessary drivers to be run across the replicas.
- ◆ Identity Applications and OSP now supports multiple replica deployment with stateless set. It offers the following advantages:
 - ◆ Zero downtime as all the replicas are managed by AKS.
 - ◆ Load balances the traffic between multiple Identity Applications and OSP replicas.

NOTE: The Identity Manager Engine container and Remote Loader must use the latest Oracle E-Business Suite driver 4.1.2.1 and Managed System Gateway driver 4.2.2.0400. For more information on how to update these drivers on standalone containers, see section [Handling RPM Updates and Third Party Files](#) and section [Handling RPM Updates and Third Party Files for AKS](#) for containers on AKS.

Deployment Using Configuration Templates

This release introduces an alternative method to deploy the infrastructure on Microsoft Azure. You can now use the configuration templates bundled inside the container delivery to customize the deployment without the need for configuration generator image. For more information, see [Infrastructure Deployment on Azure cloud](#) in the *NetIQ Identity Manager 4.8.6: Installation and Upgrade Guide*.

Component Updates

This section provides details on the component updates.

Identity Manager Component Versions

This release adds support for the following components in Identity Manager:

- ◆ Identity Manager Engine 4.8.6
- ◆ Identity Manager Remote Loader 4.8.6

- ♦ Identity Applications 4.8.6
- ♦ Identity Reporting 6.7.2
- ♦ Identity Manager Designer 4.8.6
- ♦ Identity Manager Fan Out Agent 1.2.8

Updates for Dependent Components

This release adds support for the following dependent components:

- ♦ NetIQ eDirectory 9.2.7
- ♦ NetIQ iManager 3.2.6.0200
- ♦ NetIQ Self Service Password Reset (SSPR) 4.6.0.0
- ♦ NetIQ One SSO Provider (OSP) 6.6.1

IMPORTANT: Identity Manager 4.8.6 is only compatible with eDirectory 9.2.7 or later. eDirectory versions older than 9.2.7 are no longer supported by Identity Manager 4.8.6, and vice versa. Make sure that the eDirectory is updated to version 9.2.7.

Third-Party Component Versions

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

- ♦ Azul Zulu 1.8.0_342
- ♦ Apache Tomcat 9.0.65-1
- ♦ PostgreSQL 12.11 (standalone mode only)
- ♦ PostgreSQL 12.12 (containers only)
- ♦ OpenSSL 1.0.2zf
- ♦ Nginx 1.21.6
- ♦ ActiveMQ 5.16.5

Software Fixes

NetIQ Identity Manager includes software fixes for the following components:

- ♦ [“Installation and Upgrade” on page 11](#)
- ♦ [“Identity Manager Engine” on page 11](#)
- ♦ [“Identity Applications” on page 11](#)
- ♦ [“Identity Reporting” on page 15](#)
- ♦ [“Identity Manager Designer” on page 16](#)

Installation and Upgrade

NetIQ Identity Manager includes the following software fixes that resolve several previous issues in installation or upgrade:

java.lang.UnsatisfiedLinkError Resolved Using the Latest Version of JNA Libraries

While updating Identity Manager to 4.8.5, the `msvcr100.dll` file was missing in the Microsoft Visual C++ 2010 Redistributable Package. The latest version of JNA libraries is now bundled with Identity Manager 4.8.6 to remove the dependency on the `msvcr100.dll` file. (Bug 516149)

Identity Manager Engine

NetIQ Identity Manager includes software fixes that resolve several previous issues in the Identity Manager Engine:

The DirXML-PersistentData Attribute No Longer Contains Duplicate Data

The issue wherein the SOAP-drivers added duplicate data to the `DirXML-PersistentData` attribute has been fixed. The exception is no longer seen when iManager loads Dashboard on the Driver Set Overview page. (Bug 383061)

Identity Manager Prints User's DN Correctly for Add, Delete, and Modify Operations in the Publisher Channel

Identity Manager correctly logs user's DN in the DirXML Log event for add, delete, and modify operation in the Publisher Channel. (Bug 383089)

Enabling CEF Auditing Does Not Impact eDirectory Service-related Operations

Regardless of whether CEF Auditing is enabled or disabled on Identity Manager Engine, you can start and stop eDirectory services without causing the `ndsd` processes to crash. (Bug 490076)

Identity Applications

NetIQ Identity Manager includes software fixes that resolve several previous issues in the Identity Applications:

Assigning Roles to Sub-containers Functions as Expected

Administrators can select sub-containers within containers when assigning a role to containers in Dashboard. (Bug 230927)

Delete Action in the Form Builder View Works as Expected

The issue with Form Builder view that caused deleted form fields to reappear after relaunching the form is resolved. When you delete form fields in the Form Builder view, they are removed from the form permanently. (Bug 329644)

The `$requestStatus$` Token in the Role Request Approval Completed Notification Template is Correctly Translated Into Norwegian

All tokens in the Role Request Approval Completed Notification template, including the `$requestStatus$`, are correctly translated into Norwegian. The request status no longer appears in English in the notification email. (Bug 377239)

For more information about using localized email templates, see [Working with Language-Specific Email Templates \(https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin_486/data/t4jt01672k6n.html\)](https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin_486/data/t4jt01672k6n.html).

Recipient Column on the Request History Page Displays the Recipient's Name for All PRDs

When Dashboard makes a REST API call from the Request History page to get the request history of a logged-in user, the API returns the names of all recipients, even if the same PRD is requested for different recipients. (Bug 432030)


Dashboard Displays the Attribute Labels Correctly When Editing a User's Profile

Identity Applications retrieves user attributes from the Directory Abstraction Layer and displays the display label rather than the key value of those attributes on the edit user's profile page. (Bug 432118)

Request Form Correctly Displays the Initiator and Recipient CN for Both Proxy and Original Users

When switching back from proxy to original user, the initiator and recipient fields in the request form are updated with the original user's CN. (Bug 434031)

Added Validation for Invalid Special Characters on Groups Page

When you create a new group, Identity Applications checks the user input in the name and description fields and displays a validation message if you enter invalid characters. For more information about invalid characters, click  on the Dashboard. (Bug 436002)

Workflow Execution Works as Expected When Identity Applications is Installed in a Cluster Environment

Workflows are no longer stuck in the processing state when the activities in the workflow are executed on two different nodes in a clustered environment. (Bug 438003)

Ability to Change the Expiration Date and Resubmit the Request Form After Encountering an Error

Identity Applications now allows you to change the expiration date and resubmit the request form. Prior to Identity Manager 4.8.6, changing the expiration date after receiving the Request(s) failed error was not supported. (Bug 457047)

Simultaneous Requests Have No Effect on the DN Value of a PRD

The issue wherein multiple users requesting the same permission at the same time led to incorrect DN value being passed into the flowdata has now been resolved. (Bug 468018)

Badge Feature Restored on My Approvals Title on the Applications Page

The badge on the My Approvals tile that was missing in previous versions of Identity Manager is now back. It shows how many approval tasks are currently assigned to the logged-in user. (Bug 473013)

HTTP error code 401: Error While Processing the External Application Request is No Longer Seen When the Application Initiates Workflows in Bulk

Identity Applications has updated the way authentication token and refresh token expiration are used to make REST API calls when workflows are initiated in bulk. As a result, the error is no longer seen when Identity Manager initiates a large number of workflows after upgrade. (Bug 478029)

Approval Email Sent to EBA Inbox is Processed Successfully

The issue wherein the User Application stopped checking the EBA incoming mailbox after receiving an email from a user who approved or denied a request via email has been fixed. (Bug 482152)

Changing Views in Form Builder No Longer Cause the Form Fields to Disappear

The issue wherein all fields disappeared from a form after deleting a few form fields is now resolved. Navigating between Form Builder views has no effect on the saved form. (Bug 483079)

REST Activity in a Workflow Returns a Success Message in Response to HTTP 204 No Content Status

Workflows with REST activity no longer fail when a REST service returns an HTTP 204 No Content status response. Identity Applications responds to the status by sending a success message with an empty string. (Bug 492125)

Start Workflow Policy Action Correctly Passes Date to the Workflow Engine

The Start Workflow policy action now passes the date to the Workflow Engine in a proper format, and the workflow is successfully triggered. (Bug 494406)

The Usage of Extended Characters in User Entity's DN Attribute No Longer Results in a Request Form Error

If the DN attribute of a User entity contains Cyrillic or other non-Latin characters (such as Swedish), you can use the `utils.get` function to populate that entity's data in the request form fields without any error. (Bug 505019)

Using IDVault.get() Function to Make a REST Access API call to GET / entities/list Works as Expected

The issue with JSON Forms failing when using the `IDVault.get` function has been resolved. Instead of entity key, Identity Applications uses the LDAP class associated with the entity key as the `objectClass` in an LDAP filter. (Bug 505020)

Roles on the Users Page are Listed in Alphabetical Order

This release includes a fix for an issue in Identity Manager 4.8.5 and 4.8.4 where the Users page lists a user's roles in a non-alphabetical order. (Bug 505021)

Identity Applications Successfully Retrieves the Data Item Value and Data Type From a JSON Response With Java Objects

The logic for assigning values to the objects is now based on data type. As a result, Identity Applications no longer display a null pointer exception when mapping JSON responses with Java objects. (Bug 515049)

Default Location of the User Application Log File Corrected

The property that specifies the default path for creating the `idapps.out` file has been corrected in the `userapp-log4j2.xml` file. (Bug 525093)

Localization Discrepancies in the User Application Driver Base Package Fixed

This release includes a fix for several localization related issues that were seen after upgrading the User Application Driver base package version in Designer. (Bug 543025)

Request to the /IDMProv/rest/access/tasks/workEntries REST Endpoint Returns the expirationTime in a Proper JSON Format

The /tasks/workEntries REST endpoint has been updated to return the response for expirationTime parameter as time for the date type instead of date. (Bug 547086)

Workflows with Integration Activities that Contain the createRoleRequest Operation No Longer Fail After an Upgrade

This release includes a fix for the Identity Manager 4.8.5 Patch 1 that caused workflows with Integration activity containing the createRoleRequest operation to fail after an upgrade. (Bug 553042)

User Application Driver Does Not Hang While Calling the Composer WebService: Execute Operation

This release includes a fix for the Identity Manager 4.8.5 Patch 1 that caused the User Application Driver to hang while calling the Composer WebService: Execute operation after an upgrade. (Bug 562001)

Workflow Process Cache is Cleared at the Set Capacity

The **Process Cache Maximum Capacity** functionality on the Workflow Engine and Cluster Settings page works as expected. If the number of processes in the cache equals or exceeds the configured value, the cache attempts to remove the oldest inactive process from the cache. (Bug 569004)

Identity Reporting

NetIQ Identity Manager includes the following software fixes that resolve several previous issues in Identity Reporting:

Identity Vault Reports Successfully Produce Required Data

When CEF auditing is enabled, and password changes are made by using Identity Manager and SSPR, the report query is modified to handle the user password changes such that the reports can fetch proper data. (Bug 272014)

Placeholder Attribute Populates Entries for Existing Placeholders

Identity Reporting placeholder attribute successfully populates idmrpt_container entry for existing placeholders. (Bug 305081)

Role Owner Management

When the role owner is deleted and then recreated with the same owner, the Identity Reporting successfully updates the identity records with the actual owner of the role. (Bug 368083)

DCS Driver Retry Mechanism for Transient DB Errors

Identity Reporting comes with updated algorithms to deal with transient DB errors such as connection failures, maintenance windows issues, and table space issues. (Bug 502222)

Data Collection Services Overview Page Shows Correct Label

The Identity Manager Data Collection Services Overview page is updated to show the correct label for Data Collection Period. (Bug 515023)

Identity Manager Designer

NetIQ Identity Manager includes software fixes that resolve several previous issues in Designer:

Ability to Handle Sub Element XML Values During Policy Simulation

In addition to the text-based values, the Designer Simulator now supports sub elements such as the XML values under path.xml in the input document. Designer retains these values when editing the output document and toggling between XDS Builder and Source tabs. (Bug 432147)

Ability to Successfully Export a Driver to a File That is Linked to an ECMAScript Object From Another Driver

You can export a driver that contains an ECMAScript object from another driver without any errors. Designer generates the configuration file successfully. (Bug 434055)

Ability to Handle Form Control Events With Expressions Longer Than 64K Characters on a Linux-based Designer

The maximum string length is changed from the default value of 64K characters to a custom value. As a result, you can now define an event with script expression longer than 64K in the Event Action Expression Builder. (Bug 502003)

Pasting Script Text from Clipboard to the Inline ECMAScript Editor Works as Expected

When editing a Provisioning Request Definition in Designer for macOS system, you can copy the script text from one inline ECMAScript Editor to the clipboard and paste it into another. The text copied to the clipboard is not erased when you open the second inline ECMAScript Editor. (Bug 504001)

2 Installing or Updating to This Service Pack

For information on installing or updating to this service pack, see the [NetIQ Identity Manager 4.8.6: Installation and Upgrade Guide](#).

NOTE: if you want to install Identity Manager 4.8 and upgrade to 4.8.6 or later version simultaneously, you must apply the `Identity_Manager_4.8_BundleInstaller_1.0.0.zip` file. For more information, see [NetIQ Identity Manager 4.8 Bundle Installer 1.0 Patch Release Notes](#).

3 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](#).

- ♦ “iManager Tomcat Service is Reset to Startup Automatically After Upgrade” on page 19
- ♦ “Remote Loader Reports Invalid Driver Object Password After Upgrade” on page 20
- ♦ “.NET Remote Loader Unable to Connect to the MDAD Driver After Upgrade” on page 20
- ♦ “Unable to Login to the Dxcmd Utility After Upgrade” on page 20
- ♦ “Unable to Save Responses in SSPR for Identity Manager Standard Edition Deployment on AKS” on page 20
- ♦ “Number of Open File Handles On the Identity Applications Server Increases Rapidly for Bulk Role and Resource Operations” on page 21
- ♦ “Error Displayed While Trying to Access SSPR as an Administrator” on page 22
- ♦ “Error Displayed While Upgrading Standalone SSPR on Linux” on page 23
- ♦ “Form Renderer Displays a JSON Error When Loading Legacy Forms” on page 23
- ♦ “User Application Driver Version and Copyright Information is Outdated” on page 24
- ♦ “Tomcat On RHEL 8.5 and 8.6 Does Not Start After Upgrading Identity Manager to 4.8.6” on page 24
- ♦ “Workflow Engine Fails to Start When Upgrading Identity Manager on Oracle Database” on page 24
- ♦ “Identity Manager Server Edition is Not Displayed in the DirXML Command Line Utility” on page 25
- ♦ “Enable oidpInstanceData Attribute Clean-up Property is Missing in Designer” on page 25
- ♦ “Workflow Engine Fails to Start When the Database is on MS SQL Server” on page 27
- ♦ “Events are Lost Due to Database Transaction Error” on page 27
- ♦ “Field Values Seen in the Permission Differ From the Values Entered in the Resource Form” on page 27

iManager Tomcat Service is Reset to Startup Automatically After Upgrade

Issue: If you set Tomcat startup type to any option other than automatic in the Windows service, it will reset to automatic after upgrading iManager to version 3.2.6.0200. (Bug 586001)

Workaround: After upgrade, go to the service Windows and change the Tomcat startup type to the desired option manually.

Remote Loader Reports Invalid Driver Object Password After Upgrade

Issue: After upgrading Remote Loader to version 4.8.6 on a Windows platform, it is unable to connect to the Active Directory driver using the basic authentication password. (Bug 570031)

Workaround: After upgrading Identity Manager to 4.8.6, 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.

.NET Remote Loader Unable to Connect to the MDAD Driver After Upgrade

Issue: After upgrading Remote Loader to version 4.8.6 on a Windows platform, the .NET Remote Loader service is unable to connect to the Multi-Domain Active Directory (MDAD) driver using the mutual authentication. (Bug 581082)

Workaround: After upgrading Identity Manager to 4.8.6, perform the following steps:

- 1 Stop the Remote Loader instance on the Remote Loader server.
- 2 Start the Remote Loader instance for the Multi-Domain Active Directory driver.
- 3 (Optional) If the issue persists, restart the Multi-Domain Active Directory driver.

Unable to Login to the Dxcmd Utility After Upgrade

Issue: After upgrading Identity Manager to version 4.8.6, the following LDAP exception is displayed when trying to login to Dxcmd command-line utility:

```
I/O Exception on host <hostname>, port 636 (91) Connect Error  
(Bug 580014)
```

Workaround: Sometimes Identity Manager binaries are not available until a new session is started. To resolve this issue, log out of the current session after upgrading all Identity Manager components. Launch a new session, and log in to the server again.

Unable to Save Responses in SSPR for Identity Manager Standard Edition Deployment on AKS

Issue: While trying to save responses in Self Service Password Reset (SSPR), if a user does not have correct permissions, the following error appears in the SSPR log:

```
ERROR, operations.CrService, error saving responses via LDAP, error: 5045
ERROR_WRITING_RESPONSES (permission error writing user responses to ldap
attribute 'pwmResponseSet', user does not appear to have correct
permissions to save responses: javax.naming.NoPermissionException: [LDAP:
error code 50 - NDS error: no access (-672)])
```

This issue is specific to deployment of Identity Manager containers on Azure Kubernetes service.
(Bug 572032)

Workaround: To assign the required permission, add the following `ldif` for the respective container in the `values.yaml` file in the `DATA_CONTAINERS` section:

```
dn: o=data
changetype: modify
add: ACL
ACL: 7#subtree#[This]#pwmResponseSet
-
```

Number of Open File Handles On the Identity Applications Server Increases Rapidly for Bulk Role and Resource Operations

Issue: When a user creates a new role in Identity Manager, the User Application driver sends a REST API request to the `/IDMProv/rest/access/index/permissions` endpoint. A new session between the driver and User Application is created for each request, and the role is added to User Application's permission index. Because the User Application maintains a dedicated LDAP connection to Identity Vault for each session, bulk role or resource operations (for example, creating 10,000 roles in batch) generate a large number of LDAP connections from the User Application to Identity Vault. As a result, the server hosting the Identity Applications runs out of file handles.

The same issue occurs when adding and deleting resources that use the same REST endpoint. (Bug 485070)

Workaround: The number of handles on Linux systems is limited to a soft and hard limit of 4096 and 8192, respectively. A system administrator can resolve this issue by increasing the number of file handles above the default setting of 1024 handles.

IMPORTANT: Increasing the number of handles can have a negative impact on system performance. Your system may not boot the next time you turn it on or restart it. Exercise caution and do not set the number of handles too high.

In addition to increasing the number of file handles, you can manually decrease the LDAP socket cleanup interval. Too many open sessions occupy the LDAP socket objects, resulting in out-of-memory issues. A short interval cleans the memory regularly, reducing the memory footprint of the process.

To decrease the LDAP socket cleanup interval:

- 1 Open the `ism-configuration.properties` file that is located at:

Linux: `/opt/netiq/idm/apps/tomcat/conf/`

Windows: `C:\NetIQ\idm\apps\tomcat\conf`

- 2 Set the `com.novell.idm.ldap.socket.cleanup.interval` property to 10 minutes. Default value is 60 minutes.

For example:

```
com.novell.idm.ldap.socket.cleanup.interval=10
```

- 3 Restart the Identity Applications service.

Linux: `systemctl restart netiq-tomcat.service`


Error Displayed While Trying to Access SSPR as an Administrator

Issue: When you are trying to access SSPR as an Administrator, you might see the following error:

```
2022-01-20T08:01:15Z, FATAL, servlet.AbstractPwmServlet, {19,uaadmin}
unexpected error: 5027 ERROR_UNAUTHORIZED (admin privileges required)
```

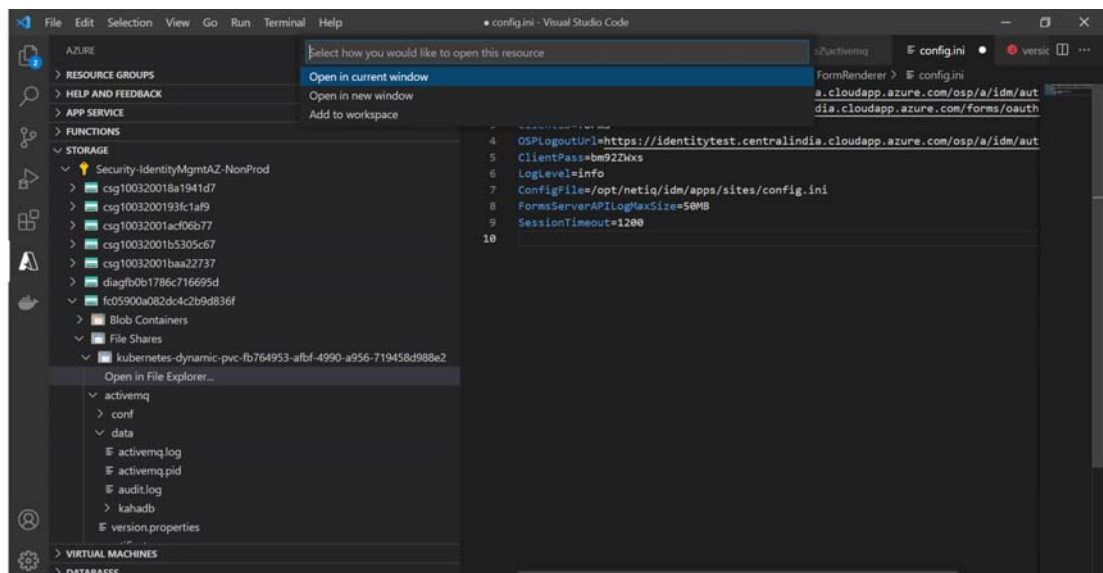
This issue is specific to Identity Manager Docker container deployment on Azure. (Bug 515107)

Workaround: Perform the following steps to resolve this issue:

- 1 Log in to the Visual Studio Code application.
- 2 Click .
- 3 Go to **STORAGE > Security-IdentityMgmtAZ-NonProd > fc05900a082dc4c2b9d836f > File shares > Kubernetes dynamic pvc > Open in File Explorer > Open in current window**. Refer to [Figure 3-1 on page 22](#).

NOTE: In the above navigation path, the **Security-IdentityMgmtAZ-NonProd** and **fc05900a082dc4c2b9d836f** key is mentioned for your reference and would change as per your login credentials.

Figure 3-1 Visual studio code configuration view



4 Click **sspr** > **SSPRConfiguration.xml**.

5 Update the following values under Administrator Permission.

```
<value>{"ldapProfileID":"default","ldapQuery":"(objectClass=*)","ldapBase":"cn=admin,ou=sa,o=system"}</value>
```

```
<value>{"ldapProfileID":"default","ldapQuery":"(objectClass=*)","ldapBase":"cn=uaadmin,ou=sa,o=data"}</value>
```

6 Go to **File** menu, click **Save**.

After saving the changes, the system automatically triggers the deployment of SSPR containers with the updated values.

Error Displayed While Upgrading Standalone SSPR on Linux

Issue: While upgrading SSPR standalone to Identity Manager 4.8.6 on Linux server, it throws the following error:

```
cp: cannot create regular file '/tmp/idm_install/': Not a directory
Could not open the xml file: /tmp/idm_install/SSPRConfiguration.xml
```

This issue happens only when standalone SSPR is upgraded to the latest version. (Bug 581121)

Workaround: Perform the following steps to resolve this issue:

1 Log in to the SSPR server console.

2 Navigate to the following location:

```
/opt/netiq/idm/apps/sspr/sspr_data/
```

3 In the **SSPRConfiguration.xml** file, set **configIsEditable** flag to **true**.

4 Save the changes.

5 Launch SSPR in private mode (<https://<hostname>:<port>/sspr/private/login>).

6 Click **Configuration editor**.

7 Enter the configuration password and click **Sign in**.

8 Under **Settings** > **Security** > **Web Security** go to **Redirect Whitelist**.

9 And add the below settings:

```
https://<OSPHostname>:<OSPPort>/osp/a/idm/auth/app/logout?target=https://SSPRHostname>:<SSPRPort>/sspr
```

10 Click **Save** and click **OK** to save the change.

11 Go back to **SSPRConfiguration.xml** file and set **configIsEditable** flag to **false**.

Form Renderer Displays a JSON Error When Loading Legacy Forms

Issue: While requesting permission on Dashboard, the following error is getting displayed if you select a permission that uses legacy form: A JSONObject text must begin with '{' at character 1

It happens when the form is rendered for the first time. (Bug 580051)

Workaround: Allow pop-ups in the browser, and the form will load on the first click from the second launch.

User Application Driver Version and Copyright Information is Outdated

Issue: The User Application Driver's version and copyright information are out-of-date even after the installer upgrades it to version 4.8.6. Since the driver is updated, you can ignore the issue. (Bug 579078)

Workaround: You can check the rpm version to verify whether the driver has been upgraded. Execute the following command to check: `rpm -q netiq-DXMLuad`

Tomcat On RHEL 8.5 and 8.6 Does Not Start After Upgrading Identity Manager to 4.8.6

Issue: When upgrading Identity Manager to version 4.8.6 on a server running RHEL 8.5 or RHEL 8.6, 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. (Bug 569043)

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

NOTE: Before applying the workaround, we recommend you read 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 on 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`

Workflow Engine Fails to Start When Upgrading Identity Manager on Oracle Database

Issue: When the Workflow Engine starts after upgrading Identity Manager to version 4.8.6, the following error is displayed:


```
09:45:39.291 [main] INFO com.novell.soa.af.impl.core.WorkflowEngineImpl -  
[WORKFLOW] Workflow Engine setState: [STARTING]  
09:45:39.481 [main] ERROR com.sssw.portal.servlet.WorkflowBootServlet -  
[WORKFLOW] Runtime exception initializing.  
...  
Caused by: com.netiq.persist.PersistenceException: ORA-02289: sequence  
does not exist
```

This issue is specific to the Oracle database and is caused by a missing sequence in the Oracle igaworkflowdb schema. (Bug 588018)

This issue will be addressed in a future patch release.

Identity Manager Server Edition is Not Displayed in the DirXML Command Line Utility

Issue: In Identity Manager 4.8.6, the DirXML Command Line (dxcmd) utility does not display whether the installed Identity Manager Server Edition is Advanced or Standard. (Bug 583030)

Workaround: There is no functionality loss.

Enable oidpInstanceData Attribute Clean-up Property is Missing in Designer

Issue: After upgrading User Application Base package to version 4.8.6.20220912161613, the Designer no longer displays the **Enable oidpInstanceData attribute clean-up** property and its sub-parameters in the **Driver Configuration > Driver Parameters** window. It happens because the resource prompt is added to the base package during the upgrade process but not included in the package's initial settings. (Bug 592009)

Workaround: After upgrading the package to version 4.8.6.20220912161613, perform the following steps in Designer:

1. In the Modeler, right-click the User Application driver and select **Driver > Properties**.
2. Select **Driver Configuration** (in the left pane).
3. Click the **Driver Parameters** tab.
4. Click **Edit XML...**
5. In the Driver Parameters XML, insert the following group definitions within the `<configuration-values></configuration-values>` tag:

```

<group>
    <definition critical-change="true" display-
name="Enable oidpInstanceData attribute clean-up"
name="EnableOidpInstanceAttrCleanUp" type="boolean">
        <description>When this setting is enabled,
oidpInstanceData attribute will be set to clean up when it reaches the
size limit of 16kb. Clean up will be performed based on certain
conditions. If the revocation entry is created by browser then based on
the expiration interval entries will be cleaned. For other entries once
it reaches the limit it is removed</description>
        <value>true</value>
    </definition>
    <subordinates active-value="true">
        <definition display-name="Client ID"
name="ClientId" type="string">
            <description>Client ID is used to authenticate
and make rest API calls from Driver. By default, the rest server Client
ID is 'rbpmrest'</description>
            <value xml:space="preserve">rbpmrest</value>
        </definition>
        <definition display-name="Client Password"
name="ClientPassword" type="password-ref">
            <description>Client Password is used to
authenticate and make rest API calls from Driver.</description>
            <value xml:space="preserve">ClientPassword</
value>
        </definition>
        <definition display-name="Specify the OAuth
issuer url (provide complete URL)" name="OauthIssuerUrl" type="string">
            <description>Specify the complete
Authorization provider issuer URL. This will be used to get the Token
and Revocation end points</description>
            <value xml:space="preserve">https://
127.0.0.1:8543/osp/a/idm/auth/oauth2</value>
        </definition>
        <definition display-name="Specify the token entry
expiration time in hours" name="ExpirationInterval" type="integer">
            <description>Specify the token entry
expiration time in hours. Based on this parameter the token entry
created by browser login will be cleared when the odipInstanceData
attribute reaches the size limit</description>
            <value>24</value>
        </definition>
    </subordinates>
</group>

```

6. Click **OK** to save the changes.
7. Click **OK**.
8. Save and deploy the User Application driver to eDirectory.
9. Log in to iManager and restart the User Application driver.

Workflow Engine Fails to Start When the Database is on MS SQL Server

Issue: The following error is displayed while upgrading Identity Manager on Windows:

```
16:23:40.460 [main] ERROR com.sssw.portal.servlet.WorkflowBootServlet -  
[WORKFLOW] Runtime exception initializing.  
com.netiq.common.i18n.LocalizedRuntimeException: Error starting engine.  
....
```

Caused by: com.novell.soa.af.EngineException: Engine Id [engine-3]: Error persisting engine state.

Caused by:

```
com.netiq.persist.PersistenceException: java.lang.IllegalArgumentException:  
id to load is required for loading
```

Caused by: java.lang.IllegalArgumentException: id to load is required for loading

This error happens because the `hibernate-workflow.cfg.xml` file in the `C:\NetIQ\idm\apps\tomcat\conf` folder is not updated correctly during the upgrade. As a result, the Workflow Engine fails to start. It is only observed on the Microsoft SQL Server database when upgrading to Identity Manager version 4.8.6. (Bug 604002)

This issue will be addressed in an upcoming release. For more information, see [KM000012324 \(https://portal.microfocus.com/s/article/KM000012324?language=en_US\)](https://portal.microfocus.com/s/article/KM000012324?language=en_US).

Events are Lost Due to Database Transaction Error

Issue: Due to the DB transaction errors, the events are lost. (Bug 500208)

Workaround: Perform the following steps to resolve this issue:

1. From CEF audit events, for the DCS Driver, search with `Status Error driver_-general` and `CEFReason` value that contains `com.netiq.persist`.
2. From the results, extract the identity information and perform the migration operation of those identities.

Field Values Seen in the Permission Differ From the Values Entered in the Resource Form

Issue: When requesting a permission with a resource form, the values (an integer, string, or list) entered at the time of submission do not match the values entered after the permission is provisioned. (Bug 647026)

Workaround: There is no workaround at this time. The issue is being researched and will be addressed in an upcoming release.

