NetIQ® Identity Manager

NetIQ Identity Manager 4.8 SP2 Release Notes

October 2020

Legal Notice

Contents

About this Book

NetIQ Identity Manager 4.8 Service Pack 2 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?

Identity Manager 4.8.2 provides the following key features, enhancements, and fixes in this release:

New Features and Enhancements

Identity Manager 4.8.2 provides the following key functions and enhancements in this release:

Platform Support

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

- SUSE Linux Enterprise Server (SLES) 15 SP2
- Red Hat Enterprise Linux (RHEL) 7.8 and 8.2

New Features in Identity Applications

Identity Applications component includes the following new features:

Enabling Separation of Duties Constraint for Inherited Roles

A new property `com.microfocus.idm.sod.inheritedroles` has been included in Identity Manager 4.8.2 version that enables detection of Separation of Duties violation for inherited roles, where a user cannot be assigned a parent role if the SoD Constraint defined at the child role level is violated by the current role of the user.

Displaying SoD violation for inherited roles is disabled by default; however, an administrator can enable it by adding the `com.microfocus.idm.sod.inheritedroles=true` property in the `ism-configuration.properties` file located at `/opt/netiq/idm/apps/tomcat/conf/` directory.

New Features in Identity Reporting

Identity Reporting component includes the following new features:

Ability to Handle Role and Resource Assignment Changes Efficiently in Identity Reporting

This release enables reports to retrieve resource assignment details from the Role and Resources Service Driver (RRSD) through DCS driver. The Roles and Resources Driver is updated to pass on the audit details on a resource modification to Access Request Reports. Identity Reporting now displays the requester details in reports when a resource is assigned or revoked. In order to achieve this, you must update Roles and Resources Service Driver prior to running reports in Identity Reporting.

To update the Role and Resources Service Driver, perform the steps mentioned in Role and Resource Service Driver 4.8.2 Release Notes.

To run a report and view its details, perform the following steps:

1. Enable auditing in User Applications. For more information, see Configuring Identity Applications in the *NetIQ Identity Manager - Configuring Auditing in Identity Manager*.
2. To start data collection services:
   - **2a** Log in to Identity Reporting Data Collection Services.
   - **2b** Navigate to **Settings** > **Data Sync Policy**.
   - **2c** Click add icon, specify the server and database details, and then click **Create**.
   - **2d** Navigate to **General Settings** and click **Start Data Collection**.
3. Download Access Requests reports from https://nu.novell.com/designer/rpt660/idm/
4. Log in to database and run the respective `idmrpt_events_v2.sql` and `idmrpt_trustview_v.sql views`.
5. Tor run and view the downloaded report:
   - **5a** Log in to Identity Reporting.
   - **5b** Navigate to **Import** > **Import Report Definitions**, click **Select File** and import `rpz` file of the report.
   - **5c** Navigate to **Repository** and click **Run Now** on the imported report.
   - **5d** Navigate to **Reports** and click **View** of the report.

What's Changed?

In this release, new REST APIs for **Get All Processes**, **Get Process details**, and **Get Tasks details** have been added to the `IDMProv.war` to match the APIs that were provided by `RIS.war`. The REST APIs and the corresponding documentation are available in the `idmappsdoc.war` file. You can also refer to the REST API Documentation available at the Identity Manager Developer website.

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 4.8.2
- Identity Manager Remote Loader 4.8.2
- Identity Applications 4.8.2
- Identity Reporting 6.6.1
- Identity Manager Designer 4.8.2
- Identity Manager Fanout Agent 1.2.4

Updates for Dependent Components

This release adds support for the following dependent components:

- NetIQ eDirectory 9.2.3

  For considerations about upgrading eDirectory, see "Supported Update Paths" on page 19.
- NetIQ iManager 3.2.3

  You must install iManager 3.2.3 to support eDirectory 9.2.3. Ensure that you update your existing plug-ins to the latest versions for the iManager version you are using.
- NetIQ Self Service Password Reset (SSPR) 4.5.0.2
- NetIQ One SSO Provider (OSP) 6.4.1
- Sentinel Log Management for IGA 8.3.0

Third-Party Component Versions

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

- Azul Zulu 1.8.0_265
- Apache Tomcat 9.0.37-1
- ActiveMQ 5.15.13
- Nginx 1.17.9
- NetIQ Universal CEF Collector 2011.1r5

Software Fixes

NetIQ Identity Manager includes software fixes for the following components:

Identity Manager Engine

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

Memory to Accommodate Driver ID is Increased to Start the eDirectory Successfully

The enhanced buffer size limit for zoomdb file name enables the Rest driver to successfully start eDirectory. (Bug 232094)

Ability to Run the Extensive do-for-each Loop Successfully

Identity Engine is enhanced to process the extensive do-for-each loop on server without any contexts. (Bug 232093)

Ability to Delay Loading of Identity Manager Engine While Initializing the eDirectory

Identity Manager introduces a new configurable environment variable that defers the loading of Identity Manager Engine during eDirectory initialization. For more information on configuring environment variable, see the Troubleshooting Identity Manager Engine in NetIQ Identity Manager Setup Guide for Linux and Troubleshooting Identity Manager Engine in NetIQ Identity Manager Setup Guide for Windows sections. (Bug 232013)

CPRS Successfully Sends the Destination Domain Information for MDAD Driver to Query

The Identity Manager Engine UI now enables CPRS to select logical domain even when there is only a single domain configured. (Bug 231491)

Identity Plugins

NetIQ Identity Manager includes software fix that resolve previous issues in the Identity Plugins:

Duplicate Header Names are Not Created in GCV After a Driver Import

Identity Manager is updated to avoid inclusion of duplicate header names in to the GCV after importing the driver. (Bug 230482)

Identity Manager Plugins Correctly Display the Check Password Status of a User After a Successful Upgrade

After successfully upgrading the Identity Manager Plugins from 4.8.0 version to 4.8.1 version, the iManager displays details of connected system for the selected user. (Bug 232130)

Identity Applications

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

Ability to Handle Extended characters in a Workflow

On Windows platform, the entities in Identity Applications now displays the German umlauts ö, ä, and ü (extended characters) correctly on the Identity Manager Dashboard. (Bug 232122)

Ability to Successfully View Workflow Details Through Workflow Administrator

Catalina.out file no longer displays any exceptions when you access the details of a listed workflow in iManager. (Bug 231621)

REST API Call Fail Always Display Appropriate Error Logs

Identity Applications correctly logs error messages in the catalina.out file, when a REST API fails. (Bug 230808)

User Search Functionality Successfully Retrieves the List of Users

Identity Manager Dashboard lists the users when a requester searches for user, without displaying any error. (Bug 232125)

Dashboard Tasks Page Correctly Displays Localized Recipient Value

Identity Manager Dashboard displays the Tasks' page localized strings in the defined browser locale. (Bug 229917)

Ability to Depict the Display Name of a Custom Workflow in Appropriate Locale

Designer is updated to show the selected custom workflow display name in the respective locale. (Bug 230490)

Provision to Accommodate More Characters for Role Description in a New Request Form

This release enhances the size limit of role description to 200 characters for a New Request Form. (Bug 231503)

Any Modification to Logged In User Tasks Dynamically Updates the Task Count

Enhanced Client settings notifies the logged in user with task count update. (Bug 230750)

Custom Role Approval Correctly Retrieves and Show the Appropriate Display Name

On selection of Custom Role Approval, its respective srvprvLocalizedNames value for the locale is displayed. (Bug 231042)

Enhanced UI Successfully Displays Request History Records as per the Configured Limit.

Identity Dashboard now allows you to enhance the limit of comments to display in Request History page. (Bug 231438)

Ability to View User Details from the Edit Group Page

You can now click group members link to view the respective user details in a pop-up window. (Bug 232075)

Any Modification in a Role or Resource with Custom Approval Always Retains its Respective nrfapprover Attribute

You can view the assigned nrfapprover attribute in NDS iMonitor even after updating a role or resource. (Bug 231443)

Identity Manager Administrator UI Supports Special Characters with Role and Resource Name

Special Characters > and & are no longer restricted to be used in role and resource name. (Bug 229894)

Allows You to View List of Administrator Assignments When System Role is Mapped as a Child Role to a User

Identity Manager Administrator API is enhanced to display administration assignments with a child role assignment. (Bug 232127)

Permissions Successfully Display All the Roles Assigned Through Groups

Permissions page settings are updated to list all the direct and indirect assignments. (Bug 230781)

Added Information About OSP OAuth 2.0 Token Endpoint

The NetIQ Identity Applications REST API documentation is updated with token endpoint details. (Bug 230977)

Application Item gets Displayed only when a Client with Appropriate Trustee Settings Logs in to Dashboard

Client assigned as a trustee to the application item can view it after accessing the Identity Manager Dashboard. (Bug 231490)

Request History Form Successfully Displays the Resource Expiration Date

The Identity Application is updated to display resource expiration date correctly on Request History form. (Bug 232066)

With Time Input Option Enabled the Request Form Calendar Works as Expected

When the Enable Time Input option is set, click the Esc or Tab button to close the calendar in the new Request Form. (Bug 230698)

Request, Approve, Deny, and Claim Options are Added to the Form Builder

New options in the Form Builder now enables you to perform custom action in the Workflow. (Bug 230847)

Addition of a Component to New Form Allows Performing All the Actions Available in the Form

Form builder is updated to execute all the action functionalities as expected for form components. (Bug 230817)

Selection of Change Language Option in the Form Builder Settings Results in Custom Localization

With an update to Formio.js, the Preview tab displays all the form fields as per custom localization. (Bug 231338)

SOD Conflict in a Multilevel Parent Child Mapping Results in Conflict Detection for Inherited Roles

You can now view inherited role conflicts when its respective group has a conflict. (Bug 231551)

Data Item Mapping Allows Transfer of Values from a Workflow to Data Grid Component

Workflow is enhanced to successfully set values in the Data Grid Component and display them in the Form Renderer. (Bug 231575)

Dashboard Displays Complete Workflow Comments in History and Task Pages

You can now view complete comments for a specific workflow in the Comments column. (Bug 233689)

Workflow Scripts Successfully Accomplish Mapping Activity

An upgrade to the Rhino JS engine successfully runs the workflow scripts. (Bug 234051)

Delegated Resource Admin with Bind Entitlement Permissions for a Driver can Successfully Create a Resource with Entitlement

With authorization check introduced in this release, a delegated resource admin can create a resource with entitlement. (Bug 231244)

All the Menu Options gets Listed for Users with a Role Not Assigned as Trustee

Non-admin user with a role unassigned as trustee can now view all the menu options. (Bug 232126)

Form Builder Successfully Translates Labels in JSON Based Forms to Defined Locale

All labels in the form are displayed in configured locale set in the Localization tab. (Bug 231344)

Role Search Process Correctly Displays the Search Results Irrespective of the Locale

The Search Role functionality performs correctly when you use Swedish as the locale to search roles. (Bug 231614)

Identity Applications Performs the Open and Submission Tasks on Legacy and New Forms as Expected

Identity Application now enables you to open and submit a PRD without displaying any error. (Bug 231595)

Successfully Deploys IDMProv After an Upgrade

The updated Identity Manager Application now successfully deploys IDMProv.war file. (Bug 232139)

Ability to Access Entities Page Successfully as a Custom Client

You can now successfully access the entities page when logged in as a non-default client. (Bug 231629)

Identity Reporting

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

Expiration Time in Reporting Database is Correctly Updated After a Role Gets Revoked

Identity Reporting database displays the date when a role gets revoked as new expiration time. (Bug 230843)

Identity Reporting Efficiently Handles the Roles and Resources Filter in Reports

Identity Reporting no longer utilizes resources filter in Identity Vault Users with Permissions to Managed Systems report. You can now filter the data by roles and resources in Available Permissions and Available Permissions Current State reports. (Bug 229386)

Ability to Display Correct Records in Authentication by Server Report

Sentinel is updated and the CEF log now displays sentinel_events tables' valid columns (xdastaxname and xdasoutcomename) with appropriate values to generate reports. (Bug 230958)

Designer

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

Displays Only Single Weights per Policy Even When the Migrate Linkages Option is Run Multiple Times

Designer no longer displays duplicate weights for a policy when you run migrate linkages on package catalog. (Bug 230878)

Retains All the Associated PRDs in SVN Whenever a PRD is Updated and Committed to SVN

An update and commit of a PRD in a package to SVN does not delete the rest of the PRDs in the package. (Bug 230970)

Introduces an Option to Skip the Re-import Process of All Such Policies that are Already Imported

Designer now enables you to select the option whether or not to display the prompt for every driver import. (Bug 231324)

Logs the Driver Traces Successfully into the Trace File When the Trace File Limit is Set to 2148 MB or Higher While Simulating a Policy

Simulation now successfully displays trace of policy processing with trace file size limit set to 2148 MB or higher. (Bug 232088)

Allows You to Reconcile an Attribute that Contains a Colon in the Attribute Name

Designer is updated to support schema attribute with special characters and reconcile the attribute successfully. (Bug 231452)

Allows You to Select the OU Container While Setting Membership Scope for Role Based Entitlement Policy

You can now use the Begin Search at field to browse and select an OU successfully. (Bug 232032)

Fetches the Query Values Successfully When Adding an Entitlement for a Role Based Entitlement Policy

Role Based Entitlement Editor is streamlined to retrieve query values for entitlement policy with admin-defined values. (Bug 232033)

All the Appropriate Live Menu Options are Displayed and Function Correctly Irrespective of the View in Designer

Designer is enhanced to operate Live menu options in both outline and modeller view for a selected object. (Bug 230651)

Copy Functionality for a Policy Allows Renaming the New File

Copy a policy action now enables you to rename the old filename with new, instead of appending them. (Bug 231527)

Introduces the Retrieve Application Schema Option to Determine Whether the Driver has to Query for the Application Schema or Not.

With introduction of Retrieve Application Schema option, the Identity Manager Engine now no longer displays error when there exists an application schema uncertainty. (Bug 259116)

Enhances the do-create-resource Action to Use Rest API.

Policy Editor now allows you to set a new field and select to use Rest services. (Bug 231393)

Deployment and Compare of Driver Correctly Updates the Trace Values in eDirectory

Driver trace configured values are successfully updated in eDirectory. (Bug 232050)

2 Installing or Updating to This Service Pack

Log in to the NetIQ Downloads page and follow the link that allows you to download the software.

The following files are available:

Filename	Description
`Identity_Manager_4.8.2_Linux.iso`	Contains files for Identity Manager Server (Identity Manager Engine, Remote Loader, Fanout Agent, and iManager), Identity Applications, and Identity Reporting for Linux platforms.
`Identity_Manager_4.8.2_Windows.iso`	Contains files for Identity Manager Server (Identity Manager Engine, Remote Loader, Fanout Agent, and iManager), Identity Applications, and Identity Reporting for Windows platforms.
`Identity_Manager_4.8.2_Containers.tar.gz`	Contains individual container images for Identity Manager Engine, Remote Loader, Fanout Agent, ActiveMQ, Form Renderer, OSP, Identity Applications, Identity Reporting, iManager, PostgreSQL, and SSPR.
`Identity_Manager_4.8.2_Designer.zip`	Contains files for Designer for all platforms.
`SentinelLogManagementForIGA8.3.0.0tar.gz`	Contains Sentinel Log Management for Identity Governance and Administration (IGA) files. **NOTE:** This installation is supported only on Linux.

For more information about the order of upgrading the components, see "Update Order" on page 20.

Supported Update Paths

The update process requires you to update Identity Manager components in a specific order.

NOTE: If you are currently on Identity Manager 4.7.4 or a prior version, first upgrade your components to 4.8 and apply 4.8.2 update according to the following update paths.

Base Version	Updated Version
Identity Manager Engine 4.8, 4.8.0.1 or 4.8.1 and eDirectory 9.2, 9.2.1, or 9.2.2	Identity Manager Engine 4.8.2 with eDirectory 9.2.3
Identity Manager 4.8.x with Remote Loader 4.8.x, where x is 0 or 1	Identity Manager 4.8.x with Remote Loader 4.8.2, where x is 0,1 or 2
	Identity Manager 4.8.2 with Remote Loader 4.8.x, where x is 0,1 or 2
Identity Manager Designer 4.8, 4.8.0.1, 4.8.1, or 4.8.1.1	Identity Manager Designer 4.8.2
Identity Applications 4.8, 4.8.0.1, 4.8.1, or 4.8.1.1	Identity Applications 4.8.2
Identity Reporting 4.8 or 4.8.1	Identity Reporting 4.8.2
Identity Analyzer 4.8	Identity Analyzer 4.8
Fanout Agent 1.2.2 or 1.2.3	Fanout Agent 1.2.4
Sentinel Log Management for IGA 8.2.2	Sentinel Log Management for IGA 8.3.0

Update Order

You must update the components in the following order:

1. Identity Vault
2. Identity Manager Engine
3. Remote Loader
4. Fanout Agent
5. iManager Web Administration
6. Identity Applications (for Advanced Edition)
7. Identity Reporting
8. Designer
9. Sentinel Log Management for IGA

   NOTE: Update of Sentinel Log Management for IGA is required only if the version is not 8.3.0

10. Self-Service Password Reset (SSPR)

    NOTE: Standalone update of SSPR is required if it is installed on a remote machine.

Considerations for Updating SSPR on Linux and Windows

The following considerations apply to Self Service Password Reset (SSPR) before you update Identity Manager to 4.8.2 version on Linux and Windows platforms:

- If auditing is enabled on SSPR server with Syslog output format type as CEF, then you must uninstall the NetIQ Self Service Password Reset Collector from Sentinel Syslog server, else the Syslog server will not be able to parse the SSPR audit events.
- SSPR supports both CEF and JSON output format type for auditing events. SSPR 4.5.0.2 will continue to support NetIQ Self Service Password Reset Collector for JSON output format type. If there are more than one SSPR servers connected to a single Sentinel Syslog server, then you must select only one format type for auditing events across all servers.

After you update Identity Manager to 4.8.2 version, SSPR is upgraded to 4.5.0.2 version which requires Universal CEF Collector for collecting auditing events in CEF format type.

NOTE: If you are enabling the SSPR auditing in CEF output format type for the first time, ensure that the NetIQ Self Service Password Reset Collector is not configured on the Sentinel Syslog server.

Updating the Identity Manager Components on Linux

This service pack includes a `Identity_Manager_4.8.2_Linux.iso` file for updating the Identity Manager components on Linux platforms.

IMPORTANT: ◆Before you update Identity Manager to 4.8.2 version, ensure that you install the `zip` and `unzip` RPM packages.

NOTE: NetIQ recommends you to obtain the dependent packages from your operating system subscription service to ensure continued support from your operating system vendor. If you do not have a subscription service, you can find the recent packages from a website such as http://rpmfind.net/linux.

- (Conditional) If you are updating the Identity Manager from 4.8 to 4.8.2 directly, then you must apply the Identity Applications 4.8.0.1 patch before 4.8.2 version in the following scenarios:
  - eDirectory 9.2 and Identity Applications 4.8 are installed on the same server.
  - iManager 3.2 and Identity Applications 4.8 are installed on the same server.
  - Identity Applications 4.8 and PostgreSQL are installed on the same server.

  The Identity Applications 4.8.0.1 patch resolves the dependencies between the NGINX module and the OpenSSL libraries. For instructions on applying the patch, see the NetIQ Identity Applications 4.8.0 Hotfix 1 Release Notes.

If you do not apply the Identity Applications 4.8.0.1 patch, the Identity Vault update fails and the installer reports the following error message:

```
Problem: patterns-edirectory-9.2.2-6.x86_64 requires netiq-openssl =
1.0.2u, but this requirement cannot be provided not installable
providers: netiq-openssl-1.0.2u-32.x86_64[edirectory-9.2.2]
Solution 1: deinstallation of netiq-nginx-1.14.2-1.x86_64
Solution 2: do not install patterns-edirectory-9.2.2-6.x86_64
Solution 3: break patterns-edirectory-9.2.2-6.x86_64 by ignoring some
of its dependencies
```

Updating the Identity Vault

1. Download and mount the `Identity_Manager_4.8.2_Linux.iso` file from the download site.
2. Navigate to the `<ISO mounted location>/IDVault/setup` directory.
3. Run the following command:

   ```
   ./nds-install
   ```

4. Specify inputs in the prompt.

Updating the Identity Manager Components

You can update the following components interactively or silently:

- Identity Manager Engine
- Identity Manager Remote Loader Service

  NOTE: Before updating the Remote Loader, ensure that the following components are stopped:

  - Remote Loader instances
  - Driver instances running with the Remote Loader
  - Identity Vault

- Identity Manager Fanout Agent
- iManager Web Administration
- Identity Applications
- Identity Reporting

Interactive Update

1. Download and mount the `Identity_Manager_4.8.2_Linux.iso` file from the download site.
2. Navigate to the <ISO mounted location> and run the following command:

   ```
   ./install.sh
   ```

3. Choose the components to update from the list of components available for upgrade.

   NOTE: You can update only one component at a time.

4. To start the Identity Manager components, run the following commands:
   - **Remote Loader:** `rdxml -config <filename>`
   - **Fanout Agent:** `startAgent –config <FanoutAgent Installation Location>/config/fanoutagentconfig.properties`
   - **Identity Applications:** `systemctl start netiq-tomcat.service`
   - **Identity Reporting:** `systemctl start netiq-tomcat.service`
5. (Conditional) If you have applied any customizations on Identity Applications and Identity Reporting components, restore the customizations and restart the Tomcat service.
6. (Conditional) Clear your browser cache before accessing the updated Identity Applications Dashboard.

Silent Update

Locate the `silent.properties` file from the extracted directory and modify the file to update the required components.

- To update the Identity Vault, set `IDVAULT_SKIP_UPDATE=false` always
- To update the Engine, set `INSTALL_ENGINE=true`
- To update the Remote Loader, set `INSTALL_RL=true`
- To update the Fanout Agent, set `INSTALL_FOA=true`
- To update iManager, set `INSTALL_IMAN=true`
- To update Identity Reporting, set `INSTALL_REPORTING=true`
- To update the Identity Applications, set `INSTALL_UA=true`

NOTE: ◆You must set the value to `true` for only one component at a time.

- While updating any component other than Identity Vault, you must always set the value of `IDVAULT_SKIP_UPDATE` to `true` to skip the Identity Vault update.
- When you update iManager, it automatically updates the iManager plug-ins (if any).

Perform the following actions to update the components silently:

1. Download and mount the `Identity_Manager_4.8.2_Linux.iso` file from the download site.
2. Navigate to the <ISO mounted location> directory.
3. Run the following command:

```
./install.sh -s -f silent.properties
```

4 To start the Identity Manager components, run the following commands:

- **Remote Loader:** `rdxml -config <filename>`
- **Fanout Agent:** `startAgent –config <FanoutAgent Installation Location>/config/fanoutagentconfig.properties`
- **Identity Applications:** `systemctl start netiq-tomcat.service`
- **Identity Reporting:** `systemctl start netiq-tomcat.service`

5 (Conditional) If you have applied any customizations on Identity Applications and Identity Reporting components, restore the customizations and restart the Tomcat service.

6 (Conditional) Clear your browser cache before accessing the updated Identity Applications Dashboard.

Installing or Updating the Identity Manager Containers

This release allows you to perform a fresh installation of containers along with the option of updating the containers from the previous versions. NetIQ recommends you to directly use the 4.8.2 version of containers if you are using containers for the first time. For more information abut deploying containers, see the *NetIQ Identity Manager: Deploying Identity Manager 4.8.2 Containers*.

Performing a Non-Root Update

Updating NICI Package

NICI package should be updated before you update the eDirectory and Identity Engine. You can update the NICI only as a root user.

Root User Updating NICI

1. To update 64-bit NICI, run the following command from the location where you have mounted the Identity Vault setup:

   ```
   rpm -Uvh nici64-3.1.0-2.x86_64.rpm
   ```

Updating eDirectory

This section guides you through the process of updating eDirectory as a non-root user. For upgrading instructions, see Upgrading eDirectory in NetIQ eDirectory Installation Guide.

Updating Identity Engine

Perform this action only if you have installed Identity Manager engine as a non-root user.

1 Download and mount the `Identity_Manager_4.8.2_Linux.iso` for non-root user to access.

2 Log in as non-root user.

3 Run the following command from the location where you have mounted the `Identity_Manager_4.8.2_Linux.iso`:

```
./install.sh
```

4 Select **Identity Manager Engine** and press **Enter**.

5 Specify the non-root install location for Identity Vault.

For example, `/home/user/eDirectory/`.

6 Specify **Y** to complete the update.

Post-Update Tasks

Perform the following actions after applying service pack.

Extending the Identity Vault Schema

(Conditional) This section does not apply if you have already upgraded to 4.8.1 and extended the Identity Vault Schema.

However, this section applies:

- if you have installed Identity Manager as a root or a non-root user, and
- if you want to extend the Identity Vault schema for the Resource Weightage feature

To extend the Identity Vault schema, perform the following steps:

1 Log in to the server where you want to extend the Identity Vault schema.

2 Navigate to `/opt/novell/eDirectory/bin` directory.

3 Run the following command to extend the schema:

```
./idm-install-schema
```

4 Update the Role and Resource Service Driver to 4.8.2. For more information, refer to the section "Update Driver Packages" on page 25.

5 Restart the Identity Vault.

Update Driver Packages

NOTE: Before updating the User Application driver and Role and Resource Service driver packages to 4.8.2, ensure that you have the Identity Applications latest version.

Once the Identity Application is updated to latest version, you can now update User Application driver and Role and Resource Service Driver (RRSD) to 4.8.2. For more information on updating RRSD, see *NetIQ Identity Manager Role and Resource Service Driver 4.8.2 Readme*.

Performing a Standalone Update of SSPR

NOTE:

- If SSPR auditing output format type is CEF, make sure to uninstall the NetIQ Self Service Password Reset Collector on Sentinel Syslog server before updating SSPR. For more information, see Considerations for Updating SSPR on Linux and Windows.

- Use this method if SSPR is:
  - Installed on a different server than the Identity Applications server.
  - Installed in a Standard Edition.

Perform the following steps to update SSPR:

1. Download and mount the `Identity_Manager_4.8.2_Linux.iso` file.
2. Navigate to the `<ISO mounted location>/sspr` directory.
3. Run the following command:

   ```
   ./install.sh
   ```

4. Specify inputs in the prompt.

Updating PostgreSQL

(Conditional) This service pack has the same version of PostgreSQL as in Identity Manager 4.8.1. You can skip updating PostgreSQL if version 12.2 is already installed.

NOTE:

- In addition to the default capabilities offered by PostgreSQL 12.2, this service pack allows you to configure the PostgreSQL database with SSL (OpenSSL 1.0.2u built with FIPS). This service pack also bundles the PostgreSQL Contrib packages.

---

1. Download and mount the `Identity_Manager_4.8.2_Linux.iso` file from the download site.
2. Navigate to the `<ISO mounted location>/common/scripts` directory and run the `pg-upgrade.sh` script.

   NOTE: To specify a different directory than the existing directory, run the `SPECIFY_NEW_PG_DATA_DIR=true ./pg-upgrade.sh` command.

   The upgrade script performs the following actions:

   - Takes a backup of the existing postgres to a different folder. For example, from `/opt/netiq/idm/postgres` to `/opt/netiq/idm/postgres-<timestamp>-backup.`
   - Updates the existing Postgres directory. For example, `/opt/netiq/idm/postgres`.
3. Specify the following details to complete the installation:

   Existing Postgres install location: Specify the location where PostgreSQL is installed. For example, `/opt/netiq/idm/postgres`.

   Existing Postgres Data Directory: Specify the location of the existing PostgreSQL data directory. For example, `/opt/netiq/idm/postgres/data`.

   Existing Postgres Database Password: Specify the PostgreSQL password.

   Enter New Postgres Data Directory [/opt/netiq/idm/postgres12.2/data]: Specify the location of the new PostgresSQL data directory. This prompt is displayed if you selected to specify a different directory other than the existing directory.

Updating the Identity Manager Components on Windows

This service pack includes a `Identity_Manager_4.8.2_Windows.iso` file for updating the Identity Manager components on Windows platforms.

NOTE: If Identity Manager Engine is installed on the same server as Identity Applications or Identity Reporting, then the Identity Applications or the Identity Reporting update process will restart the Identity Vault (eDirectory) service.

Updating the Identity Vault

1. Download and mount the `Identity_Manager_4.8.2_Windows.iso` file.
2. Navigate to the `<ISO mounted location>\IdentityManagerServer\eDirectory` directory and run the `eDirectory_923_Windows_x86_64.exe` file.

   NOTE: The Identity Vault update process restarts the Identity Vault (eDirectory) server.

   Tree Name

   Verify the tree name for Identity Vault.

   Server FDN

   Verify the server FDN.

   Tree Admin

   Specify an administrator name for Identity Vault in NCP or dot format.

   Admin Password

   Specify the administrator password.
3. In the **Install Location** field, verify the location where Identity Vault is installed.
4. In the **DIB Location** field, verify the location where the DIB files are located.
5. Select the **NICI** check box.
6. Click **Upgrade**.

Updating the Identity Manager Server Components

This section describes how to update Identity Manager Server Components:

1. Download and mount the `Identity_Manager_4.8.2_Windows.iso` file from the download site.
2. Stop the Identity Vault and Remote Loader instances.

(Conditonal) This step is applicable only if you are upgrading Remote Loader.

2a Stop all Remote Loader instances.

2b Close Remote Loader console.

2c Stop all drivers.

2d Stop the Identity Vault.

3 Update the components using the interactive or silent mode:.

- **Interactive:** Perform the following steps to upgrade Identity Manager Server components using interactive mode:
  1. Navigate to the `<ISO mounted location>\IdentityManagerServer` directory.
  2. Run `install.exe` file.
  3. Select the component that you want to update from the list and click **Next**.

     To update the Identity Manager Engine, select **Identity Manager Engine**.

     To update the 32-bit Remote Loader, select **32-Bit Remote Loader Service**.

     To update the 64-bit Remote Loader, select **64-Bit Remote Loader Service**.

     To update the .NET Remote Loader, select **.NET Remote Loader Service**.

     To update the Fanout Agent, select **Fanout Agent**.

     To update the iManager, select **iManager**.
  4. In the **Pre-Installation Summary** page click **Install**.
- **Silent:** Perform the following steps to upgrade the Identity Manager Server components using silent mode:
  1. Navigate to the `<ISO mounted location>\IdentityManagerServer\response-file` directory.
  2. Copy the `install.properties` file to a different location.
  3. Edit the `install.properties` file and set the value of the components as appropriate.

     To update Identity Manager Engine, set the value of **NETIQ_UPGRADE_ENGINE** to **True**.

     To update the Remote Loader (root and non-root), set the value of **NETIQ_UPGRADE_REMOTE_LOADER** to **True**.

     To update the 32-bit Remote Loader, set the value of **NETIQ_UPGRADE_REMOTE_LOADER_32** to **True**.

     To update the 64-bit Remote Loader, set the value of **NETIQ_UPGRADE_REMOTE_LOADER_64** to **True**.

     To update the Fanout Agent, set the value of **NETIQ_UPGRADE_FANOUT_AGENT** to **True**.

     To update the iManager, set the value of **NETIQ_UPGRADE_iManager** to **True**.
  4. In the command prompt, run the following command:

     ```
     install.exe -i silent -f <absolute path of install.properties>
     ```

Updating the Identity Applications

(Conditional) Delete or take a back-up of the existing logs from the `<install_directory>\IDM\apps\tomcat\logs` directory.

1. Download and mount the `Identity_Manager_4.8.2_Windows.iso` file from the download site.
2. Navigate to the `<ISO mounted location>\IdentityApplications` directory.
3. Perform one of the following actions:

   GUI: `install.exe`

   Silent: In the command prompt, go to the `<ISO mounted location>\IdentityApplications` location and run `install.exe -i silent`

   The Identity Applications update program will update User Application, OSP, SSPR, Tomcat, and JRE.
4. For GUI, on the **Introduction** page, click **Next**.
5. Review the **Deployed Applications** page, then click **Next**.

   This page lists the currently installed components with their versions.
6. On the **Available Patches** page, click **Next**.

   This page lists the available updates for the installed components.
7. Review the required disk space and available disk space for installation in the **Pre-Install Summary** page, then click **Install**.

   The installation process might take some time to complete.

   Before applying the service pack, the installation process automatically stops the Tomcat service.

   The process also creates a back-up of the current configuration for the installed components.

   In case, the installation reports any warnings or errors, see the logs from the Service Pack Installation/Logs directory.

   For example, `C:\NetIQ\IDM\apps\Identity_Apps_4.8.2.0_Install\Logs`. You must fix the issues and manually restart the Tomcat service.
8. Start the Tomcat service.
9. (Optional) To verify that the service pack has been successfully applied, launch the upgraded components and check the component versions.
10. Clear your browser cache before accessing Identity Applications.

NOTE: To modify any settings in the configuration update utility, launch `configupdate.bat` from the `<install_directory>\IDM\apps\configupdate` directory.

Updating Identity Reporting

(Conditional) Delete or take a back-up of the existing logs from the `<install_directory>\IDM\apps\tomcat\logs` directory.

1. Download and mount the `Identity_Manager_4.8.2_Windows.iso` file.
2. Navigate to the `<ISO mounted location>\IdentityReporting` directory.
3. Perform following steps:

   Silent: In the command prompt, go to the `<ISO mounted location>\IdentityReporting` location and run `install.exe -i silent`

   GUI: In the `IdentityReporting` directory, double-click on `install.exe`
4. For GUI, on the **Introduction** page, click Next.
5. Review the **Deployed Applications** page, then click **Next**.

   This page lists the currently installed components with their versions.
6. On the **Available Updates** page, click **Next**.

   This page lists the available updates for the installed components.
7. On the **Pre-Installation Summary** page, click **Install**.
8. Start the Tomcat service.
9. Clear your browser cache before accessing Identity Reporting.

NOTE: To modify any settings in the configuration update utility, launch `configupdate.bat` from the `<install_directory>\IDM\apps\configupdate` directory.

Post-Update Tasks

Perform the following actions after applying this service pack.

Extending the Identity Vault Schema

(Conditional) This section does not apply if you have already upgraded to 4.8.1 and extended the Identity Vault Schema.

This section applies if you want to extend the Identity Vault schema for the Resource Weightage feature.

To extend the Identity Vault schema, perform the following steps:

1. Log in to the server where you want to extend the Identity Vault schema.
2. Create a new file in your preferred directory.

   For example, create `nrf-extensions.sch` file in the `C:\Temp` directory.
3. Open the `nrf-extensions.sch` file and add the following content:

```
--
-- The nrfResourceWeightage attribute contained by nrfResource object
class specifies the weightage of
-- resource object which is used for assignment/revocation based on
priority
--
NDSSchemaExtensions DEFINITIONS ::=
BEGIN
"nrfResourceWeightage" ATTRIBUTE ::=
{
                Operation                           ADD,
                Flags
{DS_SYNC_IMMEDIATE, DS_SINGLE_VALUED_ATTR},
             SyntaxID                          SYN_INTEGER,
                ASN1ObjID                          {2 16 840 1 113719 1
33 4 174}
}


"nrfResource" OBJECT-CLASS ::=
{
    Operation   MODIFY,
    MayContain  {"nrfResourceWeightage"}
}
END
```

4 Navigate to the `C:\NetIQ\eDirectory\` directory.

5 Run the following command to extend the schema:

```
ice -l <schema_update_log> -C -a -S SCH -f <file that you created in
step 2> -D LDAP -s <eDirectory DNS name/IP> -p <LDAP port> -d
<eDirectory_admin_dn> -w <eDirectory_admin_password>
```

where,

`-C -a` updates the destination schema.

`-f` indicates the schema file (sch).

`-p` indicates the port number of the LDAP server. The default port is 389. For secure communication, use port 636. Secure communication needs an SSL Certificate.

`-L` indicates a file in DER format containing a server key used for SSL authentication.

`-s` indicates the DNS name or IP address of the LDAP server.

For example,

```
ice -l schemaupdate.log -C -a -S SCH -f C:\Temp\nrf-extensions.sch -D
LDAP -s idmorg.com -p 636 -d cn=admin,ou=idm,o=microfocus -w password -
L cert.der
```

6 Update the Role and Resource Service Driver to 4.8.2. For more information, refer to the section "Update Driver Packages" on page 32.

7 Restart the Identity Vault.

Update Driver Packages

NOTE: Before updating driver packages to 4.8.2, ensure that you have the Identity Applications latest version.

Once the Identity Application is updated to latest version, you can now update Role and Resource Service Driver (RRSD) to 4.8.2. For more information on updating RRSD, see *NetIQ Identity Manager Role and Resource Service Driver 4.8.2 Readme*.

Updating the PostgreSQL Database

(Conditional) This service pack has the same version of PostgreSQL as in Identity Manager 4.8.1. You can skip updating PostgreSQL if version 12.2 is already installed.

IMPORTANT: In addition to the default capabilities offered by PostgreSQL 12.2, this service pack allows you to configure the PostgreSQL database with SSL (OpenSSL 1.0.2u built with FIPS) and without zlib. This service pack also bundles the PostgreSQL Contrib packages.

1. Stop and disable the PostgreSQL service running on your server.
2. Rename the postgres directory from `C:\Netiq\IDM\apps`.

   For example, rename `postgres` to `postgressql_old`.
3. Remove the old PostgreSQL service by running the following command:

   `sc delete <"postgres_service_name">`

   For example, `sc delete "NetIQ PostgreSQL"`
4. Download and mount the `Identity_Manager_4.8.2_Windows.iso` file.
5. Navigate to the `<ISO mounted location>\common\postgres` directory and run the `NetIQ_PostgreSQL.exe` file. Select only PostgreSQL option during installation.

   NOTE: ◆Do not provide any database details in PostgreSQL details page. Ensure that **Create database login account** and **Create empty database** options are unchecked.

   - Ensure that you have Administrator privilege for the old and new PostgreSQL installation directories.
6. Stop the newly installed PostgreSQL service (NetIQ PostgreSQL).

   Go to **Services**, search for `<PostgreSQL version number>` service, and stop the service.

   NOTE: Appropriate users can perform stop operations after providing valid authentication.
7. Change the permissions for the newly installed PostgreSQL directory by performing the following actions:

   (Optional) If postgres user is not created, then perform the following steps to create a `postgres` user:

   1. Go to **Control Panel** > **User Accounts** > **User Accounts** > **Manage Accounts**.

2. Click **Add a user account**.
3. In the **Add a User** page, specify postgres as the user name and provide a password for the user.

Provide permissions to postgres user to the existing and newly installed PostgreSQL directories:

1. Right click the PostgreSQL directory and go to **Properties** > **Security** > **Edit**.
2. Select **Full Control for the user** to provide complete permissions.
3. Click **Apply**.

8 Access the PostgreSQL directory as `postgres` user.

1. Login to the server as postgres user.

   Before logging in, make sure that postgres can connect to the Windows server by verifying if a remote connection is allowed for this user.
2. Delete the data directory from the new postgres install location.

   For example, `C:\NetIQ\IDM\apps\postgres\data`.
3. Open a command prompt and set PGPASSWORD by using the following command:

   ```
   set PGPASSWORD=<your pg password>
   ```
4. Change to the newly installed PostgreSQL directory.

   For example, `C:\netiq\IDM\apps\postgresql\bin`.
5. Based on the encoding type that is set for the database, execute the following `initdb` commands as a `postgres` user from the `bin` directory.

   If the encoding type is set to UTF8, run the following command:

   ```
   initdb.exe -D <new_data_directory> -E <Encoding> UTF8 -U postgres
   ```

   For example, `initdb.exe -D C:\NetIQ\IDM\apps\postgres\data -E UTF8 -U postgres`

   If the encoding type is set to WIN1252, run the following command:

   ```
   initdb.exe -D <new_data_directory> -E <Encoding> WIN1252 -U postgres
   ```

   For example, `initdb.exe -D C:\NetIQ\IDM\apps\postgres\data -E WIN1252 -U postgres`

9 Upgrade PostgreSQL from new PostgreSQL bin directory. Run the following command and click **Enter**:

```
pg_upgrade.exe --old-datadir "C:\NetIQ\IDM\apps\postgres9.6.12\data" --new-datadir
"C:\NetIQ\IDM\apps\postgres\data" --old-bindir
"C:\NetIQ\IDM\apps\postgres9.6.12\bin" --new-bindir
"C:\NetIQ\IDM\apps\postgres\bin"
```

NOTE: ◆`C:\NetIQ\IDM\apps\postgres9.6.12` refers to the postgressql_old directory created in step 2.

- Ensure that you set the Method type from md5 to trust in the `pg_hba.conf` file for both old and new postgres directories (path: `C:\NetIQ\idm\apps\postgres\data\` directory).
- Change the `old PostgreSQL` directory according to the folder name.

---

10 After successful upgrade, replace the `pg_hba.conf` and `postgresql.conf` files from the old postgres data directory to the new postgres data directory (`C:\NetIQ\IDM\apps\postgres\data`).

11 Start the upgraded PostgreSQL database service.

Go to **Services**, search for <`PostgreSQL version number`> service, that is NetIQ PostgreSQL and start the service.

NOTE: Appropriate users can perform start operations after providing valid authentication.

---

12 (Optional) Delete the old data files from the `bin` directory of the newly installed PostgreSQL service to ensure that the service does not start automatically.

1. Log in as `postgres` user.
2. Navigate to the bin directory and run `analyze_new_cluster.bat` and `delete_old_cluster.bat` files.

   For example,*`C:\NetIQ\IDM\apps\postgres\bin`*

Updating Designer

You must be on Designer 4.8 at a minimum to apply this update. The update process includes the following tasks:

Performing the Update

You can apply the update in one of the following ways:

Online Update (using the Auto Update feature)

You can apply this update using the built-in auto-update feature of Designer. The auto-update feature notifies you of new features available at the Designer Download Site. This feature allows you to download Designer package and software updates when the computer that has Designer installed is connected to the Internet.

1 Launch Designer.

2 From Designer's main menu, click **Help > Check for Designer Updates**.

3 Click **Yes** to accept the Designer updates.

4 Restart Designer for the changes to take effect.

Offline Update (Using the download page to apply the update)

This service pack includes a `Identity_Manager_4.8.2_Designer.zip` file for updating Designer. You also can perform an offline update of Designer when the computer that has Designer installed is not connected to the Internet. To perform an offline update, first download this service pack on a local or remote computer and then point Designer to the directory containing the downloaded files.

To update Designer in an offline mode, create an offline copy of the Designer update files and then configure Designer to read the patch updates from the files copied to the local directory.

To create an offline copy of the Designer update files:

1. Go to NetIQ Downloads Page.
2. Under **Patches**, click **Search Patches**.
3. Specify `Identity_Manager_4.8.2_Designer.zip` in the search box and download the file.
4. Log in to the computer that has Designer installed and create a local directory.
5. Unzip the downloaded files into the local directory.

To configure Designer to read the patch updates from the local directory:

1. Launch Designer.
2. From Designer's main menu, click **Windows > Preferences**.
3. Click **NetIQ > Identity Manager** and select **Updates**.
4. For URL, specify `file:///media/<path_to_update_file>/updatesite1_0_0/`

   For a Linux mounted ISO, use the following URL format:

   `file:///media/designer482offline/updatesite1_0_0/`
5. Click **Apply**, then click **OK**.
6. From Designer's main menu, click **Help > Check for Designer Updates**.
7. Select the required updates and click **Yes** to accept and update the Designer.
8. Restart Designer for the changes to take effect.

Updating Azul Zulu OpenJRE 1.8.0_265

This service pack updates Designer to support Azul Zulu OpenJRE 1.8.0_265 (64-bit).

1. On the server where you installed Designer, download and install the Azul Zulu OpenJRE 1.8.0_265 files in a local directory.
2. Open the `Designer.ini` file located in the Designer installation directory.
3. Update the JRE path in the `Designer.ini` file.

Updating Azul Zulu OpenJRE 1.8.0_265 for Analyzer

This service pack updates Analyzer to support Azul Zulu OpenJRE 1.8.0_265 (64-bit).

1. On the server where you installed Analyzer, download and install the Azul Zulu OpenJRE 1.8.0_265 files in a local directory.
2. Open the `Analyzer.ini` file located in the Analyzer installation directory.
3. Update the Java path in the `Analyzer.ini` file.

Updating Sentinel Log Management for IGA

(Conditional) NetIQ Universal CEF Collector 2011.1r5 should be installed for CEF auditing. This service pack has the same version of Sentinel Log Management for IGA as in Identity Manager 4.8.1. You can skip updating Sentinel Log Management for IGA if version 8.3.0 is already installed.

This service pack includes a `SentinelLogManagementForIGA8.3.0.0tar.gz` file for updating the Sentinel Log Management for Identity Governance and Administration (IGA) component. Ensure that the required port is available before you update Sentinel.

1. Download the `SentinelLogManagementForIGA8.3.0.0.tar.gz` file from NetIQ Download Website `https://dl.netiq.com/index.jsp` to the server where you want to install this version.
2. Run the following command to extract the file:

   ```
   tar -zxvf SentinelLogManagementForIGA8.3.0.0.tar.gz
   ```

   NOTE: Ensure that you extract the `SentinelLogManagementForIGA8.3.0.0.tar.gz` file to a directory that has `novell` user permissions. NetIQ recommends that you extract the file under the `tmp` or `opt` directories.
3. Navigate to the `SentinelLogManagementforIGA` directory.
4. To install Sentinel Log Management for IGA, run the following command:

   ```
   ./install.sh
   ```

   NOTE: Identity Manager 4.8.2 supports Universal CEF Collector 2011.1r5 for CEF auditing.

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, contact Technical Support.

Unable to Assign the Role with SoD Constraint to a User

Issue: In a normal scenario, when you request a role for users that conflicts with the user's current role, the SoD policy applied to the conflicting role invokes an SoD approval flow. The SoD approvers, which may be selected approvers or default approvers set in the separation of duties settings, receive a corresponding task in their Tasks list. Once the task is approved, the requested role is assigned to the user. However, when you add a new user to the default approvers' list in the separation of duties settings, the SoD policy fails to add a task in the newly-added user's task list. This results in an error message and the subsequent failure of the role assignment. (`Defect 267078`)

Workaround: To resolve this issue, restart the tomcat service in the identity applications server whenever you add a new user to the default approvers list in the separation of duties settings.

Permission Related Errors Reported When Running Report Definitions SQL Scripts on Oracle

Issue: Database configuration process reports permission related errors and while running report definition SQL scripts on Oracle. (`Bug 230857`)

Workaround: To workaround this issue, perform the following steps before you configure Identity Reporting:

1. Log in to the Identity Reporting server as database admin (sysdba) user.
2. Open a database administrator tool such as Oracle SQL developer.
3. Run the following scripts:

```
alter session set "_ORACLE_SCRIPT"=true;

CREATE OR REPLACE PROCEDURE create_dcs_roles_and_schemas(
    idm_rpt_data_password character varying,
    idmrptuser_password character varying)
AUTHID CURRENT_USER
AS
    cnt number;
BEGIN

    /* Create user IDM_RPT_DATA if it does not exist already */
    select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDM_RPT_DATA';
    IF cnt = 0 THEN
        execute immediate 'CREATE USER idm_rpt_data IDENTIFIED BY ' ||
idm_rpt_data_password;
        DBMS_OUTPUT.put_line('Created user idm_rpt_data');
    END IF;

    /* Grant rights to the idm_rpt_data user */
    execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE
to idm_rpt_data';
    DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_data');

    /* Create user IDMRPTUSER if it does not exist */
    select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDMRPTUSER';
    IF cnt = 0 THEN
        execute immediate 'CREATE USER idmrptuser IDENTIFIED BY ' ||
idmrptuser_password;
        DBMS_OUTPUT.put_line('Created user idmrptuser');
    END IF;

    /* Grant rights to the idmrptuser user */
    execute immediate 'GRANT CREATE SESSION to idmrptuser';
    DBMS_OUTPUT.put_line('Granted rights to user idmrptuser');
END;
/


CREATE OR REPLACE PROCEDURE create_rpt_roles_and_schemas(
    idm_rpt_cfg_password character varying)
AUTHID CURRENT_USER
AS
    cnt number;
BEGIN

    /* Create user IDM_RPT_CFG if it does not exist */
    select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDM_RPT_CFG';
    IF cnt = 0 THEN
        execute immediate 'CREATE USER idm_rpt_cfg IDENTIFIED BY ' ||
idm_rpt_cfg_password;
        DBMS_OUTPUT.put_line('Created user idm_rpt_cfg');
```

```
    END IF;

    /* Grant rights to the idm_rpt_cfg user */
    execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE
to idm_rpt_cfg';
    DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_cfg');
END;
/
exec CREATE_DCS_ROLES_AND_SCHEMAS('<DB password>','<DB password>');
/
exec CREATE_RPT_ROLES_AND_SCHEMAS('<DB password>');
/
alter session set "_ORACLE_SCRIPT"=false;
```

4. Configure Identity Reporting.

Unable to Initialize a Zoomdb-based Driver Using the Java Remote Loader

Issue: When you start an Identity Manager driver that uses ZoomDB (such as LDAP driver) using Java Remote Loader, initialization of class com.microfocus.database.builder.ZoomDBBuilder fails and you receive the following error in publisher channel:

```
An unexpected error occurred in the publisher channel: Could not initialize
class com.microfocus.database.builder.ZoomDBBuilder
```

```
(Bug 1162310)
```

Workaround: Perform the following actions:

1. On the server that hosts the Identity Manager engine, navigate to the `/opt/novell/eDirectory/lib64/nds-modules/` location and copy the `libzoomdb.so` file to a location that you can access from the computer running Java Remote Loader.
2. Sign out from the Identity Manager engine server.
3. Log in to the computer where the Java Remote Loader is installed.
4. On Linux platforms, perform the following steps:
   a. *(Conditional) This step applies only if you are upgrading Identity Manager directly from the 4.8 version to the 4.8.2 version. In other words, you can skip this step if you are upgrading from the Identity Manager 4.8.1 version.*
      i. Download and mount the `Identity_Manager_4.8.2_Linux.iso` from the NetIQ Download website.
      ii. Navigate to the `<iso mounted location>/IDM/packages/java_remoteloader/` directory and copy the `dirxml_jremote.tar.gz` file to the desired location. For example, `/home`.
      iii. Unzip and extract the `dirxml_jremote.tar.gz` file.

      For example, `tar -zxvf dirxml_jremote.tar.gz`

   For more information about upgrading Java Remote Loader, see Upgrading Java Remote Loader in *NetIQ Identity Manager Setup Guide for Linux.*

b. Place the `libzoomdb.so` file that you copied in Step 1 to the `<location where you have extracted the dirxml_jremote.tar.gz file>/lib64/` directory.

   For example, `/home/lib64/`

c. Initialize an instance of the LDAP driver using an RL configuration file.

   For example, `"./dirxml_jremote -config <RemoteLoader_Configuration_file> -sp <password> <password>"`

d. Start the Remote Loader instance using the command:

   `"./dirxml_jremote -config <RemoteLoader_Configuration_file> &"`

5. On Windows platforms, perform the following steps:

   a. *(Conditional) This step applies only if you are upgrading Identity Manager directly from the 4.8 version to the 4.8.2 version. In other words, you can skip this step if you are upgrading from the Identity Manager 4.8.1 version.*

      i. Download and extract the `Identity_Manager_4.8.2_Windows.iso` from the NetIQ Downloads website.

      ii. Navigate to the `<iso mounted location>\IdentityManagerServer\IDM\java_remoteloader` directory.

      iii. Unzip and extract the `dirxml_jremote.tar.gz` file to the desired location.

      For example, use 7-Zip or supported software to unzip the file.

      For more information about upgrading Java Remote Loader, see Upgrading Java Remote Loader in *NetIQ Identity Manager Setup Guide for Windows.*

   b. Set the CLASSPATH environment variable to all jars that are present in the `lib` folder. If you have dependent jars specific to any driver, copy those jar files to the `lib` folder, then set the CLASSPATH environment variable to these jars also.

      For example, set:

      ```
      CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\commondriversshim.jar;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\delimitedtextutil.jar;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_misc.jar;E:\RL\JAVARL\lib\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3environment.jar;E:\RL\JAVARL\lib\mail.jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shimwrapper.jar;E:\RL\JAVARL\lib\xds.jar;E:\RL\JAVARL\lib\xp.jar
      ```

   c. Set the PATH environment variable to bin folder of JDK or JRE for Java.exe.

   d. Based on the operations you want to perform on the Remote Loader, run the following commands:

      i. To specify a Remote Loader password:

      ```
      java.exe -Djava.library.path="<absoluteLocation>\lib64" -classpath %CLASSPATH% com.novell.nds.dirxml.remote.loader.RemoteLoader -config <RemoteLoader_Configuration_file> -sp <password> <password>
      ```

      For example,

      ```
      java.exe -classpath %CLASSPATH% com.novell.nds.dirxml.remote.loader.RemoteLoader -config config8000.txt -sp novell novell
      ```

ii. To start the Remote Loader:

```
java.exe -Djava.library.path="<absoluteLocation>\lib64" -
classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
<RemoteLoader_Configuration_file>
```

For example,

```
java.exe -Djava.library.path="<absoluteLocation>\lib64"-
classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
config8000.txt
```

iii. To stop the Remote Loader:

```
java.exe -Djava.library.path="<absoluteLocation>\lib64" -
classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
<RemoteLoader_Configuration_file> -unload
```

For example,

```
java.exe -Djava.library.path="<absoluteLocation>\lib64" -
classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
config8000.txt -unload
```

Unable to Download and Save the Reports From the Identity Reporting User Interface

Issue: On Linux platforms, the download and save operations fail while trying to download the reports from the Identity Reporting user interface. (Bug 1171715)

Workaround: To work around this issue, follow one of the below procedures:

Modifying the web.xml file

1. Log in to the server where Identity Reporting is installed.
2. Navigate to the `/opt/netiq/idm/apps/tomcat/conf/` directory.
3. Modify the `web.xml` file and add the following under the `httpHeaderSecurity` filter.

```
<init-param>
       <param-name>blockContentTypeSniffingEnabled</param-name>
       <param-value>false</param-value>
</init-param>
```

4. Save the `web.xml` file.
5. Restart Tomcat.

```
systemctl restart netiq-tomcat.service
```

Downloading the reports from CDN website

1. Log in to the server where Identity Reporting is installed.
2. Download the reports from Download website.

NOTE: For convenience, the `IDM_Reports.zip` is included in the Identity Manager 4.8.1 ISO.

- **Linux:** `<ISO mounted location>/reporting/packages/IDM_Reports.zip`
- **Windows:** `<ISO mounted location>\IdentityReporting\Patch\IDM_Reports.zip`

DCS Driver Fails to Start After Upgrading Identity Reporting

Issue: On some Linux platforms such as SLES 15.x and RHEL 8.x, DCS driver does not start after you upgrade Identity Reporting to the 4.8.2 version. (`Defect OCTCR28Q261124`)

Workaround: To work around this issue, perform the following steps:

1. Log in to the server where Identity Reporting is installed.
2. Navigate to the `/var/opt/novell/eDirectory/data/dib` directory.
3. Delete the following MapDB state cache files, where * represents the version of the files.
   - `DCSDriver_<driver instance guid>-*`
   - `<driver instance guid>-*`
4. Restart eDirectory.

Issue When token-map Verb is Used in a Designer Project

Issue: When a `token-map` verb is used in a project that contains the `src` attribute, the project does not work as expected when you try to edit the mapping from Designer. This issue is observed because the `src` attribute is no longer supported.

Workaround: To work around this issue, perform the following steps:

1. Log in to Designer.
2. Navigate to the policy containing the `token-map` verb.
3. Navigate to the **XML Source** tab.
4. Modify all the occurrences of `src` attribute to `source` manually.
5. Save the policy.
6. Deploy the changes.

Workflows with Role Request Activity and Resource Request Activity Fail When Custom Context is Used

Issue: Workflows with role request activity fail in Identity Manager 4.8.2. The following error is reported: `Error while processing the external application request.` It happens when you change the default `IDMProv` deployment context to a custom context. This error is also seen in workflows that contain resource request activity. (`Bug 286037`)

Workaround: NetIQ recommends using the default `IDMProv` deployment context.

If you do encounter the error, you can resolve it by changing the deployment context back to `IDMProv` using either of the two methods listed below:

- Set the `portal.context` property to `IDMProv` in the `ism-configuration.properties` file, or
- Launch `configupdate.sh` from the `/opt/netiq/idm/apps/configupdate/` directory of the Identity Applications, select the **Change RBPM Context Name** check box in **User Application** > **Miscellaneous**, and make sure that the **RBPM Context Name** is set to `IDMProv`.