NetIQ Identity Manager 4.8 Service Pack 1 Release Notes

May 2020

NetIQ Identity Manager 4.8 Service Pack 1 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.

What's New and Changed?

Identity Manager 4.8.1 provides the following key features, enhancements, and fixes in this release:

- New Features and Enhancements
- Component Updates
- Software Fixes

New Features and Enhancements

Identity Manager 4.8.1 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) 12 SP5
- Red Hat Enterprise Linux (RHEL) 7.7 and 8.1
- MacOS Catalina (version 10.15) for Designer

New Features and Enhancements in Identity Applications

Identity Applications component includes the following new features and enhancements:

New Features in Organization Chart

The Organization Chart feature in Identity Manager Dashboard has been enhanced with new options and settings that allows you to search and view the organization chart of any entity in your organization. The organization chart is a hierarchical representation of relationship between entities such as user, group, or custom entity. With Identity Manager 4.8.1, you can now select from a set of default relationships, namely Manager-Employee, User Groups, and Group's membership that you want to view in the Organization Chart page. You can also create custom relationship in the Directory Abstraction Layer using Designer. For more information, see NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications.

The organization chart is a way to discover people in your organization by navigating through the relationship hierarchy to find a person in a certain role or at a reporting level. You can also view the next level above and the peers of an individual, their contact details and send e-mails. For more information, see Managing the Organization Chart in the *NetIQ Identity Manager - User's Guide to the Identity Applications*.

Support for New Localized Languages for Identity Applications

The end-user screens of Identity Applications support Hebrew and Polish as translation languages.

For more information about the supported translation languages, see Translated Components and Installation Programs in the *NetIQ Identity Manager Overview and Planning Guide*.

Support for Resource Weightage Feature for Entitlements

The entitlement resource in Identity Manager Applications is added with resource weightage attribute, for drivers to assign entitlement to connected system. Resource weightage controls the order of entitlement allocation.

In case of a complex connected systems (SAP, EBS, Azure AD and so on), where multiple entitlements exists and have dependencies on one another, the resource weightage helps to allocate entitlements to a user through driver. For more information on resource weightage feature, see Assigning Weightage to the Resource in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Ability to Handle SoD Conflicts for Groups and Containers

Identity Manager 4.8.1 enables you to identify members of groups and containers with conflicting roles.

When you are assigning or requesting for a role based on the defined Separation of Duties (SoD), the role conflict is identified and the affected members/users gets displayed in a new modal for the target recipients (groups or containers). For more information, see Requesting Permissions in the *NetIQ Identity Manager - User's Guide to the Identity Applications*.

New Features and Enhancements in Identity Reporting

Identity Reporting includes the following new features and enhancements:

Support for New Reporting Client

Identity Reporting 6.6 introduces a new `rptw` client, a single sign-on client for the Identity Reporting to the authentication server. The existing `rpt` client can still be used.

Reverse Proxy Server Support for Identity Reporting

Identity Manager 4.8.1 enables you to use Reverse Proxy Server through Identity Reporting.

The server that runs Identity Reporting must have Internet access to be able to access and download the most current reports for Identity Manager from the Micro Focus Reporting Content Delivery Network (CDN).

If an Identity Reporting server does not have Internet access, you must have a reverse proxy server that can access and send the information to the Identity Reporting server. NetIQ recommends that you use reverse proxy to communicate with the Identity Reporting server. This allows to isolate the Identity Reporting server from the Internet. For more information, see Configuring the Identity Reporting Server to Use Reverse Proxy Server in the *Administrator Guide to NetIQ Identity Reporting*.

Segregation of Identity Manager Reports on the Download Page

Prior to Identity Reporting 6.6, all Identity Manager and Identity Governance reports were available for download from the same download page. With Identity Reporting 6.6, the Identity Manager and Identity Governance reports are available in the `idm/` and `ig/` directories respectively on the Download site.

New Features and Enhancements in Designer

Designer includes the following enhancements:

Ability to Revert the Customized Changes on a Driver Filter

This release introduces a new option to revert the customizations made on the driver filter. For example, if you want to import a custom package to a driver, Designer allows you to revert any prior customizations made on the driver filter. After the changes are reverted, you can seamlessly add the custom packages to the driver.

Perform the following steps to revert the changes applied to the driver filter:

1. Launch Designer.
2. In the Outline view, navigate to the required driver.
3. Right-click **Driver Filter** and then click **Revert Customization**.
4. Click **OK**.

Ability to Copy the ECVs To All the Servers in a Multi-server Environment

This release introduces a new option that allows you to copy the ECV values to all the servers in a multi-server environment.

Perform the following steps to copy the ECV values to all the servers:

1. Launch Designer.
2. Navigate to **Windows** > **Preferences**.

3 Expand **NetIQ** > **Identity Manager** > **Configuration**.

4 In the **General** tab, select the **Set ECVs on all the Associated Servers during package installation** check box.

Ability to View All the Attributes Inherited From the Parent Class

Designer allows to view all the attributes inherited from the parent class.

Perform the following steps to view all the inherited attributes:

1 Open Schema Editor.

2 Select a class and add it to the editor.

3 In the editor, select the class and click **Insert Identity Vault Attributes**.

Ability to Create Multiple Notification Templates within Designer

Designer allows you to create multiple notification templates and send emails with custom email address. You can create a new custom notification collection besides Default Notification Collection. Include host property details of email server under the new collection and the host can serve all the templates.

New Options in Email Notification Server

This release introduces two more options to configure in email notification template and enables

- SSL
- Timeout Value

Perform the following steps to view these new configured options:

1. Import Identity Vault, driverset, and default notification collection.
2. Double-click on **Default Notification Collection**.

Ability to Reconnect to Designer Successfully if the Connection Times Out after Import, Compare, or Deploy Operations are Performed

Designer reconnects and enables you to run deploy, compare and import operations.

Support for Send Email and Entitlement Operation Options to Operational Events

Allows you to select the Send Email and Entitlement Operations for logging specific events. Audit events get generated to report the state of the entitlement when a driver implementing entitlement completes processing the DirXML event.

Support for the `<arg-dn>` and `<arg-association>` Arguments for `if-dest-attr` and `if-src-attr` Actions

This release adds the class attributes `<arg-dn>` and `<arg-association>` to the `if-dest-attr` and `if-src-attr` actions.

Support to Reuse Inputs for All the Policies while Performing Driver Level Simulation

The 4.8.1 release includes a new option in the Preferences Page for continuing the use of initial inputs for the rest of the policies in sequence. To configure the initial document as input for all the policies setting, go to Designer > Windows > Preferences > NetIQ > Identity Manager > Simulation > Options.

For Driver Level simulation, you can select the Use initial input document for policy simulation option in Input page to reuse the input for other policies.

Configuring this setting in Designer Preferences automatically enables the option in Input page.

New Features and Enhancements in Form Builder

Form Builder includes the following enhancements:

Ability to Render the Content for All Tabs

This release introduces a new setting for rendering the content for all tabs when they are loaded for the first time.

Perform the following steps to enable this setting:

1. Launch Form Builder.
2. Navigate to **Layout Components**.
3. Drag-and-drop the **Tab** component to the form creation area.
4. In the **Display** tab, select the **Render all tabs content** check box.
5. Save the form.

This setting renders the content for each tabs when they are loaded for the first time. By default, the content will be rendered only for the first tab.

Ability to Set the Options for Select Field Using API calls

This release introduces a new setting to allow you to set the options for the **Select** component in Form Builder through API calls.

Perform the following steps to enable this setting:

1. Launch Form Builder.
2. Navigate to **Basic Components**.
3. Drag-and-drop the **Select** component to the form creation area.
4. In the **Data** tab, select *Asynchronous API* in the **Data Source Type** field. Use this option when API call is used to set options for the select component asynchronously.
5. Save the form.

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 4.8.1
- Identity Manager Remote Loader 4.8.1
- Identity Applications 4.8.1
- Identity Reporting 6.6

- Identity Manager Designer 4.8.1
- Identity Manager Fanout Agent 1.2.3

Updates for Dependent Components

This release adds support for the following dependent components:

- NetIQ eDirectory 9.2.2

  For considerations about upgrading eDirectory, see "Supported Update Paths" on page 14.
- NetIQ iManager 3.2.2

  You must install iManager 3.2.2 to support eDirectory 9.2.2. 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) 4.5.0.0
- NetIQ One SSO Provider (OSP) 6.3.9
- 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_252
- Apache Tomcat 9.0.33-1
- PostgreSQL 12. 2
- Oracle 19c
- ActiveMQ 5.15.12
- Microsoft SQL Server 2019

  NOTE: You must use mssql-jdbc-8.2.2.jre8.jar with Microsoft SQL Server 2019.

Software Fixes

NetIQ Identity Manager includes software fixes for the following components:

- Identity Manager Engine
- Identity Reporting
- Identity Applications
- Designer

Identity Manager Engine

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

Ability to Display Dashboard Successfully when the Driver Set Name Contains a Space

Dashboard correctly displays when you select a Driver set with and without space in name. (Bug 1138704 and Bug 1165489)

Identity Manger Handles Memory Leak when Auditing is Enabled

The Identity Manager successfully handles memory leak when auditing is enabled. (Bug 1169405)

Labels for all the dxcmd Events are Displayed Correctly

The labels for all the dxcmd events are displayed correctly and the modified events are available for selection from Identity Manager Engine, Designer, and iManager. (Bug 1158878 and Bug 1164972)

Ability to Parse Custom Event ID 1241 Successfully

Identity Manager Engine is parsing the custom Event ID 1241 in hexadecimal format. (Bug 1158734, Bug 1158738, and Bug 1154388)

Ability to Generate Events for Starting and Stopping of Identity Manager Drivers

The Identity Manager drivers start successfully after an eDirectory restart. The start and stop events for the drivers are successfully logged in CEF format. (Bug 1167839)

eDirectory No Longer Crashes When Syncing Encrypted Attributes that Contains More than 1024 Characters

The eDirectory crash issue is resolved for the REST driver and the Dxevent successfully synchronizes the encrypted attributes that contains more than 1024 characters. (Bug 1167693)

Ability of Drivers not to Query for Application Schema

Identity Manager introduces a new ECV variable “Retrieve Application Schema”. If this variable is set to False, it can prevent a driver from attempting to retrieve a schema from a connected system that cannot provide this information. Default value is True.(Bug 1065074 and Bug 1167181)

Ability to Manually Upgrade the 32-Bit Remote Loader to 4.8.1 Version

The 32-bit RPM for Remote Loader is modified to allow users to manually upgrade the Remote Loader version to 4.8.1. (Bug 1162664)

Ability to Synchronize Events on the Publisher Channel Successfully

The policies on the Publisher channel is enhanced to successfully synchronize the events when the dirxml.engine.optimize-modify-merge is set to True. (Bug 1164320)

Ability to Successfully Synchronize the eDirectory Password When a Password is Changed in Active Directory

When a user changes the password in Active Directory, the password change is successfully synchronized to eDirectory. (Bug 1147067)

Identity Reporting

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

Identity Reporting Database Supports Multi-Valued Attribute

The Identity Reporting database schema is enhanced to support multi-valued attributes. In addition, the size of the attribute is increased to specify large multi-valued data. (Bug 1159453)

Ability to Successfully Synchronize the Identity Vault Objects to the Identity Reporting Database

When you try to synchronize the Identity Vault objects to the Identity Reporting database using the Data Collection Services driver, the null pointer exception is not reported. Instead, a warning message indicating the non-existence of an association is reported in the catalina.out file. (Bug 1138113)

Ability to Calculate the Size of Tables in the Database Statistics Report Correctly

The Identity Reporting database statistics report is updated to display the correct values. (Bug 1149085)

Identity Reporting Displays Correct Exception Message When the Data Cleanup Request Fails

Identity Reporting now logs an appropriate error message in the catalina.out file, when the data cleanup request fails. (Bug 1132858)

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 Linux platforms, the entities will display the German umlauts ö, ä, and ü (extended characters) correctly on the Identity Manager Dashboard. However, the German umlauts ö, ä, and ü (extended characters) are not displayed correctly on Windows platform. To troubleshoot this issue on Windows, see the troubleshooting procedure in the NetIQ Identity Manager - Administrator's Guide to the Identity Applications. (Bug 231334)

Data Grid Component Accepts Inputs From the Data Item Mapping Defined in a Workflow

While designing a form, the data grid component can now fetch inputs from the data item mapping that is defined in a workflow. (Bug 1160440)

Ability to Fetch Attributes From DAL While Performing an Advanced Search on Entities

The advanced search capability on the Entities page is enhanced to search for attributes configured in DAL. (Bug 1134434)

Automatic Refresh for Identity Applications Caching Mechanism

The Identity Applications now refresh it's cache automatically, respecting the value configured in the DirectoryService.GroupCacheHolder field. (Bug 1161144)

Ability to Create Resources Under the Right Container After Modifying the LDAP Settings

The resources are created under the selected sub-container when the LDAP settings are modified in the ism-configuration-properties file. The LDAP settings are no longer case-sensitive. (Bug 139202)

Ability to Select and Deselect Values Successfully for the Select Component in Form Builder

The enhanced Form Builder allows you to successfully change your selection when using the Select component. (Bug 1157551)

Ability to Populate the Content For All Tabs When the Form is Loaded Using Form Builder

The Form Builder is enhanced to populate all the content automatically on loading the form. When you switch between multiple tabs, the values stored previously on the other tabs are retained. (Bug 1160680)

Request History Page Displays Correct Results

The paging functionality is enhanced on the Request History page in Identity Manager dashboard. It now displays correct results on all the pages. (Bug 1136813)

Ability to Clear the Search Results on Internet Explorer

Identity Manager Dashboard now allows you to clear the search results on Internet Explorer successfully. (Bug 1124682)

Support for Java LDAP Read Timeout Control

Identity Applications now supports LDAP read timeout control to refresh the driver successfully within the defined timeline. You can still use the Socket timeout over LDAP control. (Bug 616347)

Ability to Identify SoDs and Display Role Conflicts at Group or Container Level

Identity Applications now enables to identify SoDs, detect the conflicting roles at group or container level, and lists details of the conflict. (Bug 1136231)

Ability to Search Users Using CN in Create Delegation Assignments

Identity Applications is enhanced to allow a team manger use CN as search criteria to list users in Delegation Assignments. (Bug 1134624)

PRD Approval Forms Display Information as per the Locale

All the information in the approval form is rendered as per the selected locale in My Profile. (Bug 1164829)

Ability to Display Login Expiration Time Attribute Correctly

The Day and Date Fields set in Request Form are correctly retrieved for Login Expiration Time Attribute. (Bug 1159475)

Allows Team Manager to View Other Users in Request History Page

Team manager can now view list of all members of the team and their requests history in the Request History page. (Bug 1098011)

Restricted View of the Export to CSV Button on the Entity Search Pages

The Entity search pages display the Export to CSV button only for the following users: (Bug 1132616)

- Security Administrator
- Provisioning Administrator

Ability to Set Dates Successfully for Role Request Activity

The Effective Date and Expiry Dates are set successfully in workflow for role request activity. (Bug 1159959 and Bug 1165248)

Ability to Assign Permissions to Application Items with Nested Groups

Identity Applications now enables you to assign and access the defined permissions as a nested group member on the Application page. (Bug 1139091)

Identity Manager Dashboard Displays the Buttons Correctly Over Initial Login

Clearing the browser cache displays the Dashboard buttons correctly after the initial login and for the subsequent logins as well. (Bug 1143947)

Ability to Create Resource with CN that Exceeds 128 Characters in Length Successfully

Identity Applications is enhanced to remove a size limit restriction of 128 characters in a resource name. The new CN field introduced in this release accepts up to 64 characters.(Bug 1123604)

Workflow Plugin Runs Successfully

The Workflow Plugin runs all the processes without encountering exceptions and allows terminating a selected process successfully. (Bug 1166475)

Ability to Select and View Values Successfully for the Select Boxes in Form Builder

The Form Builder allows you to check the Calculated Value field to select values in Select Boxes successfully. (Bug 1165283)

Ability to Organize the Display Order of the Attributes in Profile Page

The Identity Manager Dashboard allows you to arrange the order of attributes and display the same order in Profile page. (Bug 1115738)

Ability to Delete the Desired Role Category of a Role Correctly

Identity Applications is updated and enables to delete only the selected role category from multiple role categories assigned to a role. (Bug 1118357)

Inclusion of Script to Workflow Loads a Form Correctly

The Form Builder enables you to load a form successfully after including script in the workflow. (Bug 1162096)

Utils.get Call Displays Response to All the Parameters

The enhanced Form Builder provides response to all the query parameters in utils.get call. (Bug 1163075)

Content Component Supports Space Characters in the Text

The enhanced Form Builder enables you to enter space characters in content field. (Bug 1157887)

Ability to Perform Custom Validation for Day Component Successfully

The Form Builder is updated to allow custom validation for Day component. Validation displays the invalid comment as an outcome. (Bug 1158612)

Ability to Sort the Entries Displayed in Dynamic Entity Component

The updated Form Builder enables you to sort entries based on attributes and order in Dynamic Entity.(Bug 1161744)

Stash All Inapplicable Options for Form Integration in Form Builder

The enhanced Form Builder does not contain any components that are not required for the Form integration. (Bug 1165217)

Text Field Set for the Value of Triggered Button Action in Form Builder is Editable.

The NetIQ Form Builder is enhanced and now allows you to edit the text field after task completion. (Bug 1159361)

Ability to Load the Form with Multiple Select Component Values in Form Render Successfully

When you use multiple Select Component values in Request Form, the list of available and selected values display correctly. In addition, the form submission containing selected multiple values is successful. (Bug 1157560)

Ability to Edit the Data Grid Field Post Deletion of Default Value line from Data Grid

The enhanced Form Builder enables you to edit the Data Grid field even with the grid rows removed. (Bug 1157673)

Select Component Displays Values for Selection Correctly.

Select Component with a custom default value retrieves correct value for the selection in the drop-down. (Bug 1162749)

Data Grid Component Successfully Fetches Inputs from Data Item Mapping From a WorkFlow

The enhanced version of Form Builder successfully fetches values for the Data Grid component from the Data Item Mapping field defined in a PRD and renders those values on the Form Renderer page. (Bug 1160440)

Role Vault Macro Does Not Display Errors When Used in a Workflow

Role Vault macro works as expected for all the activities within a workflow. (Bug 1170808)

Designer

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

Designer Allows to Scroll and Access Locales in the Localization Window

Designer now enables you to scroll and view the list of locales when the locales configured exceeds 28. (Bug 1146694)

Deploy, Compare, and Import Operations In Designer Display Correct Results

Designer is enhanced to display correct results when performing an import, deploy, or compare operations on drivers. (Bug 1139935)

Ability To Import Schema From LDIF When objectClasses are Listed Before attributeTypes

Designer now allows you to correctly import schema from a LDIF file, if an object class is imported before an attribute. (Bug 1133716)

Ability to Create New Versions of Designer Packages

New UA Designer Package with queries gets installed on the UA Driver successfully and allows you to create other versions of Designer packages. (Bug 1134440)

Ability to Establish Connection and Reconnect Designer Successfully

Designer reconnects and refreshes the server specific connection which enables you to run deploy and compare operations successfully. (Bug 1104056, Bug 1100414 and Bug 1101051)

Designer Successfully Launches Package Update with Basic Authentication

Designer now allows you to use credentials and launch package update. (Bug 1158129)

Ability to Browse and Select Role Object in Policy Builder

The Policy builder lists provisioning object in Model Browser and you can now browse the role object. (Bug 1158024)

Counter Start Option Accepts only an Integer Value

The counter start option is represented using an integer to start the counter. (Bug 1133462)

Designer Successfully Synchronizes Filter Resource

An updated Filter Resource in the editor successfully synchronizes all the changes to an open package designer. (Bug 1159358)

Direct Import of Project to Designer Utilizes Maximum Disk Space

Project import functionality in Designer is enhanced to utilize the disk space efficiently. (Bug 1127263)

Ability to Upgrade User Application Driver Package Successfully

The User Application driver package upgrades successfully without any timeout connection and exceptions. (Bug 1148852)

Editor Correctly Displays a Policy or Mapping Table in the Outline View

When you open a policy or any other object in the outline view, the editor displays the policy successfully. (Bug 1161006)

Ability to Successfully Launch Form Builder on Linux platforms

Designer loads the Form Builder successfully with execute rights correctly set on necessary files. (Bug 1161006)

Designer Handles Memory Leak in the Policy and Modeler Editor Successfully

Designer successfully handles memory leak in the Editors and enhances the Designer performance. (Bug 1166193)

Launches Designer Successfully despite of Package Name with Underscores or the Package Folder in macOS with .DS_Store files.

Designer is enhanced to handle the .DS_Store files in the package folder and allow package name with special characters.(Bug 1161892)

Displays the Default Configured Values after a Package is Upgraded or Downgraded, if the init Prompt Settings are Configured for any Driver

Designer now displays default configured values on init prompt settings on upgrade or downgrade of a package. (Bug 1141877)

Allows You to Use a Hyphen in a Local Variable that Contains the "var-text" Syntax

Syntax is updated to include a hyphen in text field while setting a local variable. (Bug 1155211)

Updated Blackboard Driver in the Enterprise Palette

The existing Blackboard driver has been replaced with new BlackboardREST driver. In addition, a new Shim ID is included with update of the driver. (Bug 1169592)

Ability to Successfully Import Roles with a Contained Role Field

The updated Designer allows you to import Roles with contained role field defined in CSV file successfully. (Bug 1132899)

Designer Deploys User Application Driver Successfully with Base Package Version 4.5.1 or above

Designer Deploys User Application Driver successfully and displays correct attribute values in Role Configuration. (Bug 1143689)

Selection of an Available Event in Field Events do not Overwrite an Existing Event.

Designer on MAC enables you to select an event in the Field Events without overwriting other events. (Bug 1143938)

Ability to Apply Dependency Policy Linkages in Base Package Successfully

Designer is updated to apply correct linkages in base package, which are defined in the dependency package. (Bug 1150993)

Displays Correct Results when the Import or Compare Operation is not Chosen for Role Catalog

Selection of an option on Importing/Comparing Role Catalog window displays the desired results. (Bug 1151872)

Package Upgrade or Downgrade Successfully Updates the Driver Filter

Driver Filter is enhanced to successfully update on upgrade or downgrade of the package. (Bug 1150991)

Installing or Updating to This Service Pack

NOTE: After upgrading Identity Manager to 4.8.1, the i5/OS and OS/400 (Midrange) driver stops working due to the latest Java update available in this version of Identity Manager. To work around this issue, perform one of the following operations:

- Using an SSH tunnel (Recommended)
- Continue with the older version of Identity Manager
- Remove the SSL configuration from the driver (Not recommended)

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_4.8.1_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_4.8.1_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_4.8.1_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 15.

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 4.8.1 update according to the following update paths.

Base Version	Updated Version
Identity Manager Engine 4.8 or 4.8.0.1 and eDirectory 9.2 or 9.2.1	Identity Manager Engine 4.8.1 with eDirectory 9.2.2
Identity Manager 4.8 with Remote Loader 4.8	Identity Manager 4.8 with Remote Loader 4.8.1
	Identity Manager 4.8.1 with Remote Loader 4.8
	Identity Manager 4.8.1 with Remote Loader 4.8.1
Identity Manager Designer 4.8 or 4.8.0.1	Identity Manager Designer 4.8.1
Identity Applications 4.8 or 4.8.0.1	Identity Applications 4.8.1
Identity Reporting 4.8	Identity Reporting 4.8.1
Identity Analyzer 4.8	Identity Analyzer 4.8
Fanout Agent 1.2.2	Fanout Agent 1.2.3
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

   NOTE: Ensure to upgrade eDirectory 9.2.2 before upgrading 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. One SSO Provider (OSP)
11. 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 4.8.1 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 4.5.0.0 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 4.8.1 version, SSPR is upgraded to 4.5.0.0 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_4.8.1_Linux.iso` file for updating the Identity Manager components on Linux platforms.

IMPORTANT

- Before you update Identity Manager to 4.8.1 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) Before you update Identity Manager to 4.8.1 version in the following scenarios, you must apply the Identity Applications 4.8.0.1 patch:
  - 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_4.8.1_Linux.iso` file from the download site.
2. Navigate to the `<ISO mounted location>/IDVault/setup` directory.
3. Run the following command:

   ```
   ./nds-install
   ```

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_4.8.1_Linux.iso` file from the download site.
2. Navigate to the `<ISO mounted location>` and run the following command:

   ```
   ./install.sh
   ```

3 Select **Y**, then choose the components to update from the list of available components.

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

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

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

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

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_4.8.1_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 (Conditional) If you have applied any customizations on Identity Applications and Identity Reporting components, restore the customizations and restart the Tomcat service.

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

- **Remote Loader:** `rdxml -config filename -sp`
- **Fanout Agent:** `startAgent –config <FanoutAgent Installation Location>/config/fanoutagentconfig.properties`

- **Identity Applications:** `systemctl start netiq-tomcat.service`
- **Identity Reporting:** `systemctl start netiq-tomcat.service`

Performing a Non-Root Update

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

1. Run the following command from the location where you have mounted the `Identity_Manager_4.8.1_Linux.iso`:

   ```
   ./install.sh
   ```

2. Select **Identity Manager Engine** and press **Enter**.
3. Specify the non-root install location for Identity Vault.

   For example, `/home/user/eDirectory/`.
4. Specify **Y** to complete the update.

Post-Update Tasks

Perform the following actions after applying service pack.

Extending the Identity Vault Schema

(Optional) 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 User Application driver package to 4.8.1.*xxxxx* version, where *xxxxx* indicates the time stamp when the driver package was created.
5. Update the Role and Resource Service driver to 4.8.1 version. For more information, see *NetIQ Identity Manager Role and Resource Service Driver 4.8.1 Readme*.
6. Restart the Identity Vault.

Post-Update Check for Identity Applications

Ensure that you clear the browser cache after you update the Identity Applications.

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_4.8.1_Linux.iso` file.
2. Navigate to the `<ISO mounted location>/sspr` directory.
3. Run the following command:

   ```
   ./install.sh
   ```

Updating PostgreSQL

(Conditional) If you are using PostgreSQL as your database, this service pack requires you to update your existing PostgreSQL database version to 12.2.

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_4.8.1_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_4.8.1_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
- Updating the Identity Manager Engine and Remote Loader
- Updating the Fanout Agent
- Updating iManager
- Updating the Identity Applications
- Updating Identity Reporting
- Post-Update Tasks
- Updating the PostgreSQL Database

Updating the Identity Vault

1. Download and mount the `Identity_Manager_4.8.1_Windows.iso` file.
2. Navigate to the `<ISO mounted location>\IdentityManagerServer\eDirectory` directory and run the `eDirectory_922_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 Engine and Remote Loader

1. Download and mount the `Identity_Manager_4.8.1_Windows.iso` file from the download site.
2. Stop the Identity Vault and Remote Loader instances.
   - **2a** Stop all Remote Loader instances.
   - **2b** Close Remote Loader console.
   - **2c** Stop all drivers.
   - **2d** Stop the Identity Vault.
3. Navigate to the `<ISO mounted location>\IdentityManagerServer\IDM` directory.
4. Install the updates by interactive or silent mode of installation.
   - **For interactive mode:** Run `install.bat` file and select the component that you want to update from the list.

     To update Identity Manager Engine, select **Metadirectory 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**.
   - **For silent mode:** Locate the `patchUpgradeSilent.Properties` file and modify the file to update the required components.

     To update Engine (root and non-root), set **install_Engine=true**.

     To update the 32-bit Remote Loader, set **install_RL32=true**.

     To update the 64-bit Remote Loader, set **install_RL64=true**.

     To update the .Net Remote Loader, set **install_DotNetRL=true**

     In the command prompt, run `install.bat -i silent -f patchUpgradeSilent.Properties`
5. (Conditional) If you added a custom trusted root certificate to the existing Java keystore (`C:\NetIQ\idm\jre\lib\security\cacerts`), import the certificate to the new keystore.

   ```
   keytool -importkeystore -srckeystore <Old-cacerts> -destkeystore
   C:\NetIQ\idm\jre\lib\security\cacerts -srcstoretype JKS -deststoretype JKS -
   srcstorepass <storePassword> -deststorepass changeit -srcalias <mycertAlias>
   ```

   Run this command for each custom certificate created. Alternatively, copy the keystore to the new location.

   For example, the old cacerts files are backed-up in the following locations on Windows:

   - `\backup location\cacerts.32 from 32-bit JRE`
   - `\backup location\cacerts.64 from 64-bit JRE`

Updating the Fanout Agent

IMPORTANT: The update program does not detect the already installed Fanout Agent on your computer. Therefore, it does not provide an option for updating this component.

1. Navigate to the `C:\NetIQ\IdentityManager\FanoutAgent\lib` folder and take a back-up of following files:
   - `IDMCEFProcessor.jar`
   - `activemq-all-*.jar`
   - `dirxml.jar`
   - `dirxml_misc.jar`
   - `dirxml_remote.jar`
   - `fanout_web.war`
   - `nxsl.jar`
   - `zoomdb.jar`
2. Navigate to the `C:\NetIQ\IDM\FanoutAgent\bin` and take a back up of the `zoomdb.dll` and the `startAgent.bat` files.
3. Download and mount the `Identity_Manager_4.8.1_Windows.iso` file.
4. Navigate to `<ISO mounted location>\IdentityManagerServer\IDM\patch\Windows\FanoutAgent\lib` location and copy the following files:
   - `IDMCEFProcessor.jar`
   - `activemq-all-*.jar`
   - `dirxml.jar`
   - `dirxml_misc.jar`
   - `dirxml_remote.jar`
   - `fanout_web.war`
   - `nxsl.jar`
   - `zoomdb.jar`
5. Replace the existing files in `C:\NetIQ\IdentityManager\FanoutAgent\lib` folder with the files copied in Step 4. Use the latest JDBC driver.
6. Navigate to the `<ISO mounted location>\IdentityManagerServer\IDM\patch\Windows\FanoutAgent\bin` location and copy the `zoomdb.dll` and `startAgent.bat` files.
7. Replace the `zoomdb.dll` and the `startAgent.bat` files in `C:\NetIQ\IdentityManager\FanoutAgent\bin` folder with the files you copied in Step 6.
8. Restart the Fanout Agent.

Updating iManager

1. Log in as a user with administrator privileges on the computer where you want to upgrade iManager.
2. Take a backup of the `server.xml` and `context.xml` configuration files at a different location before performing the upgrade.

   The upgrade process replaces the configuration files.
3. Download and mount the `Identity_Manager_4.8.1_Windows.iso` file.
4. Navigate to the `<ISO mounted location>\IdentityManagerServer\iManager\installs\win` directory and run the `iManagerInstall.exe`.
5. Select the language that you want to use for the installation and click **OK**.
6. In the **Introduction** page, click **Next**.
7. Read and accept the license agreement and then click **Next**.
8. (Conditional) If the setup program detects a previously installed version of iManager, it may prompt you to upgrade the installed version. Click **Yes** to upgrade. The program replaces the existing JRE and Tomcat versions with the latest versions. This will also upgrade the iManager to the latest version.
9. Review the **Detection Summary** window and click **Next**.

   The **Detection Summary** window lists the latest version of Servlet container and JVM software that iManager will use once it is upgraded.
10. Select the public key algorithm for the TLS certificate to use from following options:
    - RSA
    - ECDSA 256
11. Select the cipher suite for TLS communication from the following options:
    - NONE
    - LOW
    - MEDIUM
    - HIGH
12. (Optional) To use IPv6 addresses with iManager, click **Yes** in the **Enable IPv6** window.

    You can enable IPv6 addresses after you upgrade iManager.
13. Read the **Pre-Installation Summary** page and click **Install**.

    The upgrade process can take several minutes. The process might add new files for iManager components or change the iManager configuration.
14. Click **Done**.

NOTE: After iManager update, you need to update the existing plug-ins. For more information, see "Post-Update Steps for iManager" on page 27.

Updating the Identity Applications

(Conditional) Delete or take a back-up of the existing logs from the `C:\NetIQ\IDM\apps\tomcat\logs` directory.

1. Download and mount the `Identity_Manager_4.8.1_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_4.8.1.0_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>\apps\configupdate` directory.

Updating Identity Reporting

(Conditional) Delete or take a back-up of the existing logs from the `C:\NetIQ\IDM\apps\tomcat\logs` directory.

1 Download and mount the `Identity_Manager_4.8.1_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>\apps\configupdate` directory.

Post-Update Tasks

Perform the following actions after applying this service pack.

Extending the Identity Vault Schema

(Optional) 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 User Application driver package to 4.8.1.*xxxxx* version, where *xxxxx* indicates the time stamp when the driver package was created.
7. Update the Role and Resource Service driver to 4.8.1 version. For more information, see *NetIQ Identity Manager Role and Resource Service Driver 4.8.1 Readme*.
8. Restart the Identity Vault.

Post-Update Steps for iManager

After you upgrade your iManager, the installation process does not update the existing plug-ins. Ensure that the plug-ins match the correct iManager version.

To update the Identity Manager plug-ins from iManager, perform the following actions:

1. Log in to iManager.
2. Navigate to **Configure** > **Plug-in Installation** > **Available NetIQ Plug-in Modules**
3. Update the plug-ins for 4.8.1.0.
4. Restart the Tomcat.

Updating the PostgreSQL Database

(Conditional) If you are using PostgreSQL as your database, this service pack requires you to update your existing PostgreSQL database version to 12.2.

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_4.8.1_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_4.8.1_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_4.8.1_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/designer481offline/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_252

This service pack updates Designer to support Azul Zulu OpenJRE 1.8.0_252 (64-bit).

1. On the server where you installed Designer, download and install the Azul Zulu OpenJRE 1.8.0_252 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_252 for Analyzer

This service pack updates Analyzer to support Azul Zulu OpenJRE 1.8.0_252 (64-bit).

1. On the server where you installed Analyzer, download and install the Azul Zulu OpenJRE 1.8.0_252 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

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 4.8.1 supports Universal CEF Collector 2011.1r4 for CEF auditing.

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 Re-evaluate Role Based Entitlements” on page 32
- “Unable to Initialize a Zoomdb-based Driver Using the Java Remote Loader” on page 32
- “Existing Relationships Defined in Designer are Not Available During the Compare and Deploy Operations” on page 33

- "Exception Logged in catalina.out After Upgrading Identity Reporting" on page 33
- "Unable to Download and Save the Reports From the Identity Reporting User Interface" on page 33

Unable to Re-evaluate Role Based Entitlements

Issue: In iManager, the Role-Based Entitlements plug-in encounters an error while trying to re-evaluate the existing role based entitlement policies and generates the following exception: `org.jdom.input.JDOMParseException` on Linux and Windows platform. `(Bug 1145494 and Bug 1166586)`

Workaround: To re-evaluate the role based entitlements, perform the following actions:

1. Stop Tomcat.
2. Navigate to the location where iManager is installed, for example, `C:\Program Files\Novell\Tomcat\webapps\nps\WEB-INF\`.
3. Modify the `Tomcat web.xml` file and add the following parameters within the `<web-app>` XML tag:

```
<context-param>
                <param-name>param1</param-name>
                <param-value>XMLEditor</param-value>
</context-param>
<context-param>
                <param-name>param2</param-name>
                <param-value>XMLEditor_Packed</param-value>
</context-param>
<context-param>
                <param-name>param</param-name>
                <param-value>XMLData</param-value>
</context-param>
```

4. Start Tomcat.
5. Log in to iManager and install the Role-Based Entitlements plug-in. For more information, see "Post-Update Steps for iManager" on page 27.

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. Download and extract the `Identity_Manager_4.8.1_Linux.iso` from the NetIQ Download website.

   NOTE: If you want to update to the latest version of the Java Remote Loader, use the `dirxml_jremote.tar.gz` file from the `Identity_Manager_4.8.1_Linux.iso`. For more information about upgrading Java Remote Loader, see Upgrading Java Remote Loader in *NetIQ Identity Manager Setup Guide for Linux.*

5. Navigate to the `<extracted_patch_location>/Identity_Manager_4.8.1_Linux/IDM/packages/java_remoteloader/` directory and copy the `dirxml_jremote.tar.gz` file to the desired location. For example, `/home`.
6. Unzip and extract the `dirxml_jremote.tar.gz` file.

   For example, `tar -zxvf dirxml_jremote.tar.gz`
7. Place the `libzoomdb.so` file that you copied in Step 1 to `<extracted_folder>/lib64/` location.

   For example, `/home/lib64/`
8. Initialize an instance of the LDAP driver using an RL configuration file.

   For example, `"./dirxml_jremote -config <RemoteLoader_Configuration_file> -sp <password> <password>"`
9. Start the Remote Loader instance using the command:

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

Existing Relationships Defined in Designer are Not Available During the Compare and Deploy Operations

Issue: After upgrading Designer, some existing relationships and the corresponding objects are not displayed when you want to perform a compare or deploy operation. This issue is observed if you have selected **This entity's key** in the **Source Attribute** field while defining a relationship. (`Bug 1171264`)

Workaround: After upgrading Designer, you must manually modify the objects again so that the objects are available for selection.

Exception Logged in catalina.out After Upgrading Identity Reporting

Issue: If you are using Oracle 18c database for Identity Reporting, the following exception is logged into the `catalina.out` file after upgrading Identity Manager to 4.8.1 version. (`Bug 1171571`)

```
WARNING [main] org.apache.tomcat.util.scan.StandardJarScanner.processURLs Failed
to scan [file:/opt/netiq/idm/apps/tomcat/lib/oraclepki.jar] from classloader
hierarchy
java.io.FileNotFoundException: /opt/netiq/idm/apps/tomcat/lib/oraclepki.jar (No
such file or directory)
```

Workaround: Ignore the exception as it does not cause any functionality loss.

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`

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our commun6ity. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice

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