NetIQ Identity Manager 4.7 Service Pack 3 Release Notes

June 2019

NetIQ Identity Manager Service Pack 3 provides new features, 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 Web site.

1 What's New?

Identity Manager 4.7.3 provides the following key features, enhancements, and fixes in this release:

- New Features
- Component Updates
- What's Deprecated for Removal or Discontinued?
- Software Fixes

1.1 New Features

This release provides the following key functions:

1.1.1 Platform Support

In addition to the existing operating systems, this service pack supports the following platforms:

- SUSE Linux Enterprise Server 12 SP4
- Red Hat Enterprise Linux 7.6
- MacOS 10.14 (only for Designer)

1.2 Component Updates

This section provides details on the component updates.

1.2.1 Identity Manager Component Versions

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

- Identity Manager Engine 4.7.3
- Identity Manager Remote Loader 4.7.3

- Identity Manager Fanout Agent 1.2.2
- Identity Applications 4.7.3
- Identity Reporting 6.5
- Identity Manager Designer 4.7.3

1.2.2 Updates for Dependent Components

This release adds support for the following dependent components:

- NetIQ eDirectory 9.1.4.1

  For considerations about upgrading eDirectory, see Section 2.1, “Supported Update Paths,” on page 9.
- NetIQ iManager 3.1.4

  You must install iManager 3.1.4 to support eDirectory 9.1.4. 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) 4.4.0.2
- NetIQ One SSO Provider (OSP) 6.3.3
- Sentinel Log Management for Identity Governance and Administration 8.2.2

1.2.3 Third-Party Component Versions

- Azul Zulu 1.80_212 (except Analyzer)
- Apache Tomcat 8.5.40
- PostgreSQL 9.6.12
- ActiveMQ 5.15.9

1.3 What’s Deprecated for Removal or Discontinued?

This version does not deprecate or discontinue any feature or functionality of Identity Manager. Refer to the following links to see the details about features or functionalities deprecated in the previous releases:

- Identity Manager 4.7.2 (https://www.netiq.com/documentation/identity-manager-47/releasenotes_idm472/data/releasenotes_idm472.html#deprecated-in-identity-manager-472)
- Identity Manager 4.7.1 (https://www.netiq.com/documentation/identity-manager-47/releasenotes_idm471/data/releasenotes_idm471.html#what-is-deprecated-identity-manager-471)
- Identity Manager 4.7 (https://www.netiq.com/documentation/identity-manager-47/releasenotes_idm47/data/releasenotes_idm47.html#deprecated-features-functions-identity-manager-47)

Refer to the following links to see the details about features or functionalities discontinued in the previous releases:

- Identity Manager 4.7.2 (https://www.netiq.com/documentation/identity-manager-47/releasenotes_idm472/data/releasenotes_idm472.html#discontinued-in-identity-manager-472)

- Identity Manager 4.7.1 (https://www.netiq.com/documentation/identity-manager-47/releasenotes_idm471/data/releasenotes_idm471.html#what-is-discontinued-identity-manager-471)
- Identity Manager 4.7 (https://www.netiq.com/documentation/identity-manager-47/releasenotes_idm47/data/releasenotes_idm47.html#discontinued-features-functions-identity-manager-47)

1.4 Software Fixes

NetIQ Identity Manager includes software fixes for the following components:

- Identity Manager Engine
- Remote Loader
- Identity Reporting
- Identity Applications
- Designer for Identity Manager
- Identity Manager 4.7.x Patch Installer

1.4.1 Identity Manager Engine

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

1.4.1.1 Ignoring Optimization of Modify Events When the Publisher Channel is Performing a Merge Event

This release introduces a new Engine Control Value named **Optimize Modify on Publisher Merge**. This control enables the Identity Manager Engine to decide whether to optimize the changes that are sent to the Identity Vault at the time when the Publisher channel is processing a merge operation. By default, this is set to `true`. This setting allows the Identity Manager Engine to optimize the changes sent to the Identity Vault.`(Bug 1117428)`

1.4.1.2 Starting Workflows with Empty Data Items from a Driver

The do-start-workflow action now allow you to start a workflow from a driver when an empty data item is added to the data item array of the workflow. `(Bugs 1123280, 1127453)`

1.4.2 Remote Loader

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

1.4.2.1 Correct Location of State Files for Drivers Running Remote Loader As a Service

When you run Remote Loader as a service with Identity Manager drivers, the state files are now correctly created in the Remote Loader folder. `(Bug 1123742)`

1.4.2.2 Ability to Record Appropriate Log Messages in the .NET Remote Loader Trace File in Absence of Password Files

The Remote Loader trace has been enhanced to display appropriate messages when password files are missing so that issue can be easily comprehended and appropriate action taken. `(Bug 1113268)`

1.4.2.3 Correct Error Message Is Reported by the dirxml_remote_msg.dll File

The `dirxml_remote_msg.dll` file of the Remote Loader has been enhanced to display correct error messages in the Event Viewer. `(Bug 1131121)`

1.4.3 Identity Reporting

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

1.4.3.1 Duplicate Rows in the Resource Assignments by Users Report

The Resource Assignments by Users report no longer creates duplicate rows for a single resource assignment. `(Bug 1070743)`

1.4.3.2 Deleting a Value for a Custom Multi-Valued Attribute Deletes All Values From the Reporting Database

If you delete a value of a multi-valued attribute, the remaining values are now preserved in the reporting database. The database shows a value of `TRUE` only for the deleted value. It shows `FALSE` for the remaining values. `(Bug 1100979)`

1.4.3.3 Ability to Add Custom Attributes to the Oracle Database

This version of Identity Reporting sets the `enableLike` parameter to `true` that enables `LIKE` comparisons instead of = comparisons in the SQL `where` clause that is allowed by Oracle. `(Bug 1123055)`

1.4.3.4 Correctly Populating the FirstName Column of the Database

If you create a user without first name, the firstName column in the Identity Reporting database is blank as it is not a mandatory attribute. If you add a first name to the user, the firstName column is correctly updated with the first name of the user. `(Bug 1123021)`

1.4.3.5 Identity Vault User Report Shows Correct Value in the Employee Type Column

After creating a user in the Identity Vault and adding a value to the employeeType attribute, when you run the Identity Vault User report from Identity Reporting, the Employee Type column of the report now shows the correct value for the user. `(Bug 1134742)`

1.4.3.6 No Exception from Data Sync Policy When the Sentinel Server or Database Is Listening on a Port Higher Than 20000

This release extends the limit of ports to use to 65535, which is the largest allowed TCP/IP network port number. This change will allow Sentinel server and database to listen on any ports within 65535. `(Bug 1109764)`

1.4.3.7 Handling a Null Value for IP Address by Authentication by Server and Authentication by User Reports

The Authentication by Server and Authentication by User reports are now equipped with an improved JavaScript that properly handles null values when the source or target IP address is not populated in the database for an event. `(Bug 1130034)`

1.4.4 Identity Applications

NetIQ Identity Manager includes software fixes that resolve several previous issues in the identity applications.

1.4.4.1 Support for Specifying Availability

You can now specify which resource requests with a delegate assignment you are unavailable to work on during a particular time period. During the time period when you are unavailable for a particular request, the user delegated to act on that request can work on it. (Bug 1110556)

The following documentation resources are updated:

- *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*
  - Configuring Delegation and Proxy Settings
  - **Set Availability while creating a Delegation Assignment** under General Settings (https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin_473/data/netiq-change-identity-applications-cliet-settings.html#t45h47zitwab)
- Managing Your Availability in the *NetIQ Identity Manager - User's Guide to the Identity Applications*
- Dashboard help

1.4.4.2 Support for Disabling Virtual List View Search

If the VLV ((Virtual List View) search is not performing as expected, you can disable it through a new property named `com.microfocus.idm.enable.vlv` and perform a plain LDAP search instead. The upgrade process adds this property to the `ism-configuration.properties` file. By default, `com.microfocus.idm.enable.vlv` is set to `true`. To disable the VLV search, manually change the value of the property to `false`.

When using a plain LDAP search, you must define the following new properties that will be added to the `ism-configuration.properties` file by the upgrade process.

- **com.microfocus.idm.max.users.limit:** Specifies the search limit. The default is 1000. You must change this value depending on your search scope.
- **com.microfocus.idm.min.search.characters:** Specifies the minimum number of characters to issue a search. The default is 3 characters.

Sorting and pagination of the results is automatically taken care when the VLV search is disabled. (Bug 1126537)

1.4.4.3 Ability to Redirect a User to the SSPR Page When the Hostname Contains the SSPR String

Identity Applications successfully redirects users to the SSPR page when the hostname contains the SSPR string. (Bug 1123508)

1.4.4.4 No Delay Caused When a PRD Containing Multiple Conditions Is Repeatedly Called

Identity Applications have been enhanced to prevent processing delays when PRDs containing multiple conditions are called multiple times in a workflow. To further enhance the performance of Identity Applications, set the value for the `maxTotal` property for your database in the `server.xml` file located at `/opt/netiq/idm/apps/tomcat/conf` or `C:\NetIQ\idm\apps\tomcat\conf` to 200. (Bug 1132313)

For example,

```
<Resource auth="Container" driverClassName="org.postgresql.Driver"
factory="com.netiq.tomcat.jdbc.pool.CustomBasicDataSourceFactory" initialSize="10"
maxTotal="200" maxIdle="10" minIdle="10" name="shared/IDMUADataSource"
password="<passsword>" testOnBorrow="true" type="javax.sql.DataSource"
url="jdbc:postgresql://<ip-address>:port/idmuserappdb" username="idmadmin"
validationInterval="120000" validationQuery="SELECT 1"/>
```

1.4.4.5 Display Expression is Correctly Shown When a Mapped Resource Uses a Custom Entitlement of Type idm4 and ID2 Field Is Not Populated

The Mapped Resources list section in the Role Details page now correctly shows the display name of the entitlement value. `(Bug 1130193)`

1.4.4.6 Dashboard Allows Creation of Resources with Valued Entitlements with Free-Form Text Values

The Dashboard allows you to create resources with entitlements configured to use the free-form text values. `(Bug 1121572)`

1.4.4.7 Handling the Login Functionality When the Identity Vault Password Has Expired

If you are an Active Directory user and your Active Directory password is active and your Identity Vault password has expired, you can still log in to the Identity Manager Dashboard with your Active Directory password if SSPR is not used for managing password. Identity Manager introduces a new property named `com.netiq.rbpm.pwd-expiry.sspr.redirect.enable` in the `ism-configuration.properties` file that enables you to log in to the dashboard when it is set to `False`. `(Bug 1120777)`

1.4.4.8 Reassigning Tasks That Are Assigned to a Group by a Team Manager

If a workflow or a PRD is assigned to a group, you can now successfully reassign the workflow or the PRD to the individual members belonging to the group. `(Bug 1136097)`

1.4.4.9 Successful Task Reassignment by Provisioning Administrators

A task can be reassigned either by a Helpdesk or a Provisioning Administrator user. The former can reassign a task to the approver's manager while the latter can reassign the task to any user, group, or a role. This behavior has been corrected for Provisioning Administrator in this release. `(Bug 1134913)`

1.4.4.10 Request History Shows Task Details and Comments for HelpDesk Users

Users with the HelpDesk role can now correctly view task details and comments in the Request History page. `(Bug 1134911)`

1.4.4.11 getGroupRequest Soap Call Returns Correct Results

This release fixes the Directory Access Layer communication issue with the getGroupRequest Soap call that resulted in an error. `(Bug 1128206)`

1.4.4.12 Support for Migration Settings Tool

The migration settings tool (MigrationSettings.jar) helps you migrate the client settings from one Identity Manager instance to another. If you are using the tool to change the storage option from file to database, the tool now correctly imports the generated JSON file into the database. `(Bug 1121430)`

1.4.4.13 Software Fixes When Using MS SQL 2016 as Identity Applications Database

This release includes the following software fixes to improve the interaction of Identity Applications with the MS SQL 2016 database.

1.4.4.14 Code Map Is Correctly Refreshed When the Name of a Group Containing Case-Sensitive Characters Is Renamed

The issue occurred because Identity Applications added new entitlement parameters and then deleted the old or unused entitlements from the provisioning view value table. Now the order of updating the table has been changed where the old or unused entitlements are deleted before adding the new entitlement parameters to the table. `(Bug 1129305)`

Additionally, this fix has been verified on Oracle and PostgreSQL databases.

1.4.4.15 Support for Displaying Tasks Whose Names Exceed 20 Characters

The maximum size for the parseJson function has been increased to 2000 characters. This allows Identity Applications to correctly evaluate the task name from the ECMA expression that contains a large number of characters. `(Bug 1127915)`

1.4.4.16 Ability to Correctly Filter Roles When Requesting a Role on Behalf of Someone

The roles are now filtered at the same time when they are queried for based on the search input. The search returns all the matching records based on the maximum limit set for the search. `(Bug 1123485)`

1.4.4.17 Workflow Preactivity Correctly Runs Only Once When Invoked from Dashboard and Administration Interface

The workflow preactivity expression is evaluated only once from the Dashboard or the administration interface. Identity Applications reuses the reference to the data item list in the subsequent calls.

Identity Applications now calls the function only once and reuses the reference to the data item list in the subsequent calls. `(Bug 1042214)`

1.4.4.18 Logout Tile Correctly Logs You Out

When you click the tile with `/idmdash/#/logout` URL, you are successfully logged out of the application. `(Bug 1112847)`

1.4.4.19 Team Manager With Role Administrator Permission Can See Other Users Approval Tasks in the Tasks Page

When the team manager is a Role Administrator and a Provisioning Administrator, the Provisioning Administrator role takes precedence. This allows the team manager to see other users' approval tasks in the Tasks page. `(Bug 1130926)`

1.4.4.20 Expiry Date of Role Assignment Is Correctly Updated

When you assign a role to a user and select an expiry date and then clear the date, the change is correctly reflected before the role assignment is saved in the application. `(Bug 1129311)`

1.4.4.21 Indirectly Assigned Team Manager Can Reassign Approval Tasks

The Java API that obtains the details of the teams when a directly assigned user is a team manager or a group is as a team manager has been enhanced to return the teams. This allows the indirectly assigned team manager to reassign the approval tasks `(Bug 1131802)`

1.4.5 Designer for Identity Manager

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

1.4.5.1 Policy Builder Shows Subsequent Rules When Actions and Rules are Edited

If the policy rules are expanded, and the first rule is collapsed or an action is edited from the first rule and then saved, the subsequent rules become visible again. `(Bug 1131379)`

1.4.5.2 Ability to Add an Organization (o=data) as a Trustee for a Role While Creating the Role in the Role Overview Page

Designer allows you to add objects such as driverset, driver, OU, O, and CN as trustees while creating a role in the Role Overview page. `(Bug 1133970)`

1.4.5.3 Filtering Entry Records at the Same Time When They Are Queried Leads to Performance Improvement of the Search

The entity records are filtered at the same time when they are queried for based on the search input. The search returns all the matching records based on the maximum limit set for the search. In addition, you can change the maximum limit for search results in the Entities editor. `(Bugs 1121015)`

1.4.5.4 Progress Information Bar Is Displayed During Compare Operations on macOS

The display of a progress bar during Compare operations shows a responsive user interface until the result of the operation is displayed. `(Bug 1089435)`

1.4.5.5 No Exception While Importing a Driver With a Link to an External ECMAScript Library

When you import a driver that has a link to an external ECMAScript library from a driver configuration file into Designer, the driver is successfully imported. Designer no longer reports an exception. `(Bug 1121781)`

1.4.5.6 No Mismatch in PRD Version

The xmldata attribute of a newly created Provisioning Request Definition (PRD) now matches with the runtime version of Identity Applications for which the newly created PRD is being deployed. Designer retrieves the PRD version directly from the User Application package and no longer updates it when a PRD is opened in the editor. (Bug 1125293)

1.4.5.7 Properties of Form Fields Are Properly Displayed in Workflows on macOS

If a **Form Field** is selected with a mouse or keyboard up/down arrows, the Properties section displays correct values for the field. `(Bug 1092106)`

1.4.5.8 Deploying User Application Driver If the Schema Contains an Attribute Named Visible

By design, one of the User Application driver objects contains a node attribute named Visible. If the driver schema contains a custom attribute of the same name, Designer considers them separate items and successfully deploys the User Application driver. `(Bug 1125958)`

1.4.5.9 Successfully Updates Driver Packages from the Package Catalog

Designer properly handles updating of driver packages from the Package Catalog. It no longer reports any exceptions. `(Bug 1129726)`

1.4.5.10 Valid LDAP Search Base for Selecting Entitlements Queried from an Application

This issue occurred because Designer replaced the base DN for containers such as `ou,o`, and `country` with `CN`. Designer now properly points the base DN to a valid container in the Identity Vault. `(Bug 1132847)`

1.4.6 Identity Manager 4.7.x Patch Installer

This patch installer includes the following software fix:

1.4.6.1 Identity Manager 4.7.x Installer Now Preserves the java.security File

The Identity Manager 4.7.x installer now includes a new JRE RPM structure that does not overwrite the java.security file. (`Bug 1126521`)

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_4.7.3_Linux.zip`	Contains files for Identity Manager Server (Identity Manager Engine, Remote Loader, Fanout Agent, and iManager), Identity Applications, and Identity Reporting for Linux platforms. **NOTE:** This file also contains JDBC Fanout and Managed System Gateway driver files.
`Identity_Manager_4.7.3_Windows.zip`	Contains files for Identity Manager Server (Identity Manager Engine, Remote Loader, Fanout Agent, and iManager), Identity Applications, and Identity Reporting for Windows platforms. **NOTE:** This file also contains JDBC Fanout and Managed System Gateway driver files.
`Identity_Manager_4.7.3_Designer.zip`	Contains files for Designer for all platforms.
`SentinelLogManagementForIGA8.2.2.tar.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 Section 2.2, “Update Order,” on page 10.

- Section 2.1, “Supported Update Paths,” on page 9
- Section 2.2, “Update Order,” on page 10
- Section 2.3, “Updating the Identity Manager Components on Linux,” on page 11
- Section 2.4, “Updating the Identity Manager Components on Windows,” on page 15
- Section 2.5, “Updating Designer,” on page 22
- Section 2.6, “Updating Sentinel Log Management for IGA,” on page 23
- Section 2.7, “Enabling CEF Auditing for SSPR,” on page 23

2.1 Supported Update Paths

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

If you are currently on Identity Manager 4.6.4 or a prior version, first upgrade your components to 4.7 and apply 4.7.3 update according to the following update paths.

Base Version	Updated Version
Identity Manager engine and eDirectory	
Identity Manager 4.7, 4.7.1, or 4.7.2 with eDirectory 9.1, 9.1.1, or 9.1.2	Identity Manager 4.7.3 with eDirectory 9.1.4
Remote Loader	
Identity Manager 4.7, 4.7.1 or 4.7.2 with Remote Loader 4.7	Identity Manager 4.7 with Remote Loader 4.7.3 Identity Manager 4.7.3 with Remote Loader 4.7 Identity Manager 4.7.3 with Remote Loader 4.7.3
Identity Manager Designer	
Identity Manager Designer 4.7.2	Identity Manager Designer 4.7.3
Identity Applications	
Identity Applications 4.7, 4.7.1, or 4.7.2	Identity Applications 4.7.3
Identity Reporting	
Identity Reporting 4.7, 4.7.1 or 4.7.2	Identity Reporting 6.5

2.2 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 Reporting
7. Identity Applications (for Advanced Edition)
8. Designer
9. Sentinel Log Management for IGA
10. One SSO Provider (OSP)

    NOTE: Standalone update of OSP is supported only on Windows.

11. Self-Service Password Reset

2.3 Updating the Identity Manager Components on Linux

This service pack includes a `Identity_Manager_4.7.3_Linux.zip` file for updating the Identity Manager components on Linux platforms.

- Updating the Identity Vault
- Updating the Identity Manager Components
- Performing a Non-Root Update
- Post-Update Tasks
- Performing a Standalone Update of SSPR
- Updating PostgreSQL

2.3.1 Updating the Identity Vault

1. Download and extract the `Identity_Manager_4.7.3_Linux.zip` file from the download site.
2. Locate the **IDVault/setup** directory in the extracted file (Step 1).
3. Run the following command:

```
./nds-install
```

NOTE: Compound indexes created prior to Identity Vault version 9.1.4.1 must be recreated. The upgrade program schedules automatic recreation of indexes immediately after the upgrade is completed. The recreation activity recreates the indexes and flags them as recreated. To verify which indexes have been recreated, look for the following message in the `ndsd.log` file:

```
"Deleting compound index <index name> for recreation"
```

The process of recreating indexes completely can take several minutes in large DIBs. Therefore, some searches issued from Identity Applications might fail until the indexes are ready for use.

2.3.2 Updating the Identity Manager Components

You can update the following components interactively or silently:

- **Identity Manager Engine**
- **Identity Manager Remote Loader Service**
- **Identity Manager Fanout Agent**
- **iManager Web Administration**
- **Identity Reporting**
- **Identity Applications**

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

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

Interactive Update

1. Download and extract the `Identity_Manager_4.7.3_Linux.zip` file from the download site.
2. Run the following command from the extracted directory:

   ```
   ./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.

   If you want to update the Identity Vault, select **N** and follow the steps from "Updating the Identity Vault" on page 11.

Silent Update

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

- To update to the Identity Vault, set `IDVAULT_SKIP_UPDATE=False`
- To update the Engine, set `INSTALL_ENGINE = true`
- To update the Remote Loader, set `INSTALL_RL = true`
- To update the Fanout Agent, set `INSTALL_FA = 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.
- 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 extract the `Identity_Manager_4.7.3_Linux.zip` file from the download site.
2. Modify the file to update the required components.
3. Run the following command:

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

2.3.3 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 extracted directory:

   ```
   ./install.sh
   ```

   NOTE: Do not use the `idm-nonroot-install` script located under `/<Linux zip file extracted location>/IDM/` directory to perform a non-root installation. If you use that script, the `netiq-zoomdb-1.1.0-0.noarch.rpm` and `novell-IDMCEFProcessorx-1.0.0-0.x86_64.rpm` will not be installed.

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.

2.3.4 Post-Update Tasks

Perform the following actions after applying service pack. This section is applicable only when updating from 4.7 to 4.7.3.

2.3.4.1 Extending the Identity Vault Schema

This section applies if you have performed a root installation of Identity Manager Engine.

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

1. Navigate to /opt/novell/eDirectory/bin directory.
2. Run the following command:

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

2.3.4.2 Updating Driver Packages

Designer 4.7.2 is shipped with incorrect versions for some packages for these drivers: Delimited Text, Lotus Notes, and Office 365.

To ensure that these drivers work properly in your environment, update the specified package for each driver. For more information about which package version to update, see Section 3.5, “Updating Driver Packages,” on page 25.

2.3.4.3 Post-Update Steps for Identity Applications

- Ensure that you clear the browser cache after you update the Identity Applications.
- Perform this action only if the following conditions are true:
  - Identity Applications are installed silently.
  - NETIQ_DATABASE_CONFIG_ADMIN is different than NETIQ_DATABASE_ADMIN. For example, idmadmin and postgres.

  If the schema does not update properly, run the liquibase command with NETIQ_DATABASE_CONFIG_ADMIN credentials.

This command is located in the /var/opt/netiq/idm/log/idmconfigure.log file. Ensure that you modify the parameters as per your need. For example,

```
/opt/netiq/common/jre/bin/java -Dwar.context.name=IDMProv -Ddriver.dn="cn=User
Application Driver,cn=driverset1,o=system" -Duser.container="o=data" -jar /opt/
netiq/idm/apps/UserApplication/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/opt/netiq/idm/postgres/postgresql-
9.4.1212.jar:/opt/netiq/idm/apps/tomcat/webapps/IDMProv.war --
changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://:5432/
idmuserappdb?compatible=true" --contexts="prov,newdb,updatedb" --logLevel=debug --
username=***** --password=**** update >> /var/opt/netiq/idm/log/db.out
```

2.3.5 Performing a Standalone Update of SSPR

NOTE: 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 extract the `Identity_Manager_4.7.3_Linux.zip` file.
2. Locate the `sspr` directory in the extracted file (Step 1).
3. Run the following command:

   ```
   ./install.sh
   ```

2.3.6 Updating PostgreSQL

(Conditional) If you are using PostgreSQL as your database, this service pack requires you to update your existing PostgreSQL database version to 9.6.12.

The following considerations apply when you update PostgreSQL:

Update PostgreSQL used with Identity Manager 4.7: The PostgreSQL update program backs up the existing PostgreSQL home directory and appends the existing PostgreSQL version number. For example, the existing PostgreSQL directory is renamed from `/opt/netiq/idm/postgres` to `/opt/netiq/idm/postgres9.6.6`. The new PostgreSQL is installed in the `/opt/netiq/idm/postgres` directory.

1. Download and extract the `Identity_Manager_4.7.3_Linux.zip` file from the download site.
2. Navigate to the `Identity_Manager_4.7.3_Linux/common/scripts` directory in the extracted file 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-201810221903-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.

2.4 Updating the Identity Manager Components on Windows

This service pack includes a `Identity_Manager_4.7.3_Windows.zip` file for updating the Identity Manager components on Windows platforms.

- Updating the Identity Vault
- Updating the Identity Manager Engine and Remote Loader
- Manually Updating the Fanout Agent
- Updating Identity Reporting
- Updating the Identity Applications
- Post-Update Tasks
- Updating Driver Packages
- Updating the PostgreSQL Database

2.4.1 Updating the Identity Vault

1. Download and extract the `Identity_Manager_4.7.3_Windows.zip` file.
2. Locate the `IDVault` directory in the extracted file (Step 1).
3. Run the `eDirectory_914_Windows_x86_64.exe` file:

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

   Tree Name

   Specify a tree name for Identity Vault.

   Server FDN

   Specify a server FDN.

   NOTE: Though Identity Vault allows you to set the NCP server object's FDN up to 256 characters, NetIQ recommends that you restrict the variable to a much lesser value because Identity Vault creates other objects of greater length based on the length of this object.

   Tree Admin

   Specify an administrator name for Identity Vault.

   Admin Password

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

NOTE: Compound indexes created prior to Identity Vault version 9.1.4.1 must be recreated. The upgrade program schedules automatic recreation of indexes immediately after the upgrade is completed. The recreation activity recreates the indexes and flags them as recreated. To verify which indexes have been recreated, look for the following message in the `ndsd.log` file:

```
"Deleting compound index <index name> for recreation"
```

The process of recreating indexes completely can take several minutes in large DIBs. Therefore, some searches issued from Identity Applications might fail until the indexes are ready for use.

2.4.2 Updating the Identity Manager Engine and Remote Loader

1 Download and extract the `Identity_Manager_4.7.3_Windows.zip` file.

NOTE: This file also contains JDBC Fanout and Managed System Gateway driver files.

2 Stop the Identity Vault and Remote Loader instances.

2a Stop all drivers.

2b Stop all Remote Loader instances.

NOTE: You must close the Remote Loader console before upgrading the Remote Loader.

2c Stop the Identity Vault.

3 Locate the `IDM` directory in the extracted file (Step 1).

4 Install the updates by interactive or silent mode of installation.

- **For interactive mode:** Run `<patch_path>\install.bat` 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:** Run `<patch_path>\install.bat -i silent -f patchUpgradeSilent.Properties`.

When you update the Identity Manager engine, the JDBC Fanout and Managed Service Gateway drivers are also updated.

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`

2.4.3 Manually 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. Replace the existing `FanoutAgent.jar` and `fanout_web.war`, files in `C:\NetIQ\IdentityManager\FanoutAgent\lib` folder from the `\Identity_Manager_4.7.3_Windows\IDM\patch\Windows\FanoutAgent\lib` folder in the `Identity_Manager_4.7.3_Windows.zip` file.
2. (Conditional) Add the `IDMCEFProcessor.jar` and `zoomdb.jar` files from`\Identity_Manager_4.7.3_Windows\IDM\patch\Windows\FanoutAgent\lib` to `C:\NetIQ\IdentityManager\FanoutAgent\lib and use the latest JDBC 4.2.1.0. Fanout driver.`
3. Restart the Fanout Agent.
4. Restart the Identity Vault.

2.4.4 Updating Identity Reporting

Before starting the Identity Reporting upgrade, ensure that OSP is upgraded to 6.3.3 version.

1. Download and extract the `Identity_Manager_4.7.3_Windows.zip` file.
2. Stop Tomcat.
3. Create a backup directory outside of the Tomcat installation path.
4. Locate the `C:\NetIQ\idm\apps\tomcat\webapps` directory in the extracted file and copy the following files to the backup directory you created in Step 3.
   - `IDMRPT-CORE.war`
   - `IDMRPT.war`
   - `idmdcs.war`
   - `IDMDCS-CORE.war`
   - `dcsdoc.war`
5. Delete the following files from these directories:
   - `IDMRPT-CORE`, `IDMRPT`, `idmdcs`, `IDMDCS-CORE`, and `dcsdoc` folders from the `C:\NetIQ\idm\apps\tomcat\webapps` directory.
   - `localhost` folder from the `C:\NetIQ\idm\apps\tomcat\work\Catalina` directory.
   - All files and folders from the `C:\NetIQ\idm\apps\tomcat\temp` directory.
   - `cache` and `plugins` folders from the `C:\NetIQ\idm\apps\IdentityReporting\reportContent` directory.
6. Locate the `Reporting` directory in the extracted file (Step 1).
7. Copy the following files to the `C:\NetIQ\idm\apps\tomcat\webapps` directory.
   - `IDMRPT-CORE.war`
   - `IDMRPT.war`
   - `idmdcs.war`
   - `IDMDCS-CORE.war`
   - `dcsdoc.war`

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

9 (Conditional) If the Syslog appender uses TCP or UDP protocol, add the path to the `idm.jks` keystore file in `C:\netiq\idm\apps\tomcat\conf\idmrptcore_logging.xml` by adding the below entries in the file.

```
<keystore-file>C:\netiq\idm\apps\tomcat\conf\idm.jks
</keystore-file>
```

You cannot access the reporting application in absence of this entry in the file.

10 Start the Tomcat service.

11 Clear your browser cache before accessing Identity Reporting.

2.4.5 Updating the Identity Applications

1 Download and extract the `Identity_Manager_4.7.3_Windows.zip` file.

2 Locate the `IdentityApplications` directory in the extracted file (Step 1).

3 Perform one of the following actions:

GUI: `install.exe`

Silent: `install.exe -i silent -f silent.properties`

The Identity Applications update program will update User Application, OSP, SSPR, Tomcat, and JRE.

4 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 To restore the certificates for communication between the identity applications and the LDAP server, specify the JRE truststore password and then click **Next**.

For example, if your certificate is located in *`C:\netiq\idm\jre\lib\security\cacerts`*, specify the password to access the certificate.

The identity applications need certificates (`cacerts` or custom keystore) for communicating with the Identity Manager server.

8 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_4.7.3.0_Install\Logs`*. You must fix the issues and manually restart the Tomcat service.

9 Start the Tomcat service.

10 (Optional) To verify that the service pack has been successfully applied, launch the upgraded components and check the component versions.

2.4.6 Post-Update Tasks

Perform the following actions after applying this service pack. This section is applicable when updating from 4.7 to 4.7.3.

2.4.6.1 Extending the Identity Vault Schema

To extend the Identity Vault schema, navigate to the `C:\NetIQ\eDirectory\` directory and run the following command:

```
ice -l <schema_update_log> -C -a -S SCH -f <Identity_Manager_4.7.3_Windows.zip
Extracted
location>\Identity_Manager_4.7.3_Windows\IDM\patch\Windows\engine\schema\edirector
y-schema.sch -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:\Identity_Manager_4.7.3_Windows\IDM\patch\Windows\engine\schema\edirectoryschema
.sch -D LDAP -s idmorg.com -p 636 -d cn=admin,ou=idm,o=microfocus -w password -L
cert.der
```

2.4.6.2 Post-Update Steps for Identity Applications

- Clear the browser cache.
- If the LDAP server name in the LDAP server certificate subject is different from what is used in the Identity Applications, change the name of the LDAP server in the Identity Applications configuration to the name of the LDAP server available in the LDAP server certificate subject.

  Identity Manager 4.7.3 upgrades Java to 1.8.0_212. Java has enabled endpoint identification on LDAPS connections from JRE 1.8.0_181. This requires you to use the same server name for connecting to the Identity Manager server that was provided with the LDAP server certificate subject. Otherwise, the connection fails.

  To change the name of the server in the Identity Applications configuration:

  1. Open the ConfigUpdate utility (`configupdate.sh` or `configupdate.bat`).
  2. Navigate to the **User Application** tab, click **Identity Vault server**, and change the name of the server to what is provided with the LDAP server certificate subject.

     This action updates the `DirectoryService/realms/jndi/params/AUTHORITY` property in the `ism-configuration.properties` file.
- (Conditional) Perform this action only if the following conditions are true:
  - Identity Applications are installed silently.
  - `NETIQ_DATABASE_CONFIG_ADMIN` is different than `NETIQ_DATABASE_ADMIN`. For example, `idmadmin` and `postgres`.

If the schema does not update properly, run the `liquibase` command with `NETIQ_DATABASE_CONFIG_ADMIN` credentials to update it.

The command can be found in the `C:\netiq\idm\apps\UserApplication\NetIQ-Custom-Install` file. Ensure that you modify the parameters as per your need.

For example:

```
"C:\netiq\idm\apps\jre\bin\java" -Xms256m -Xmx256m -
Dlog4j.configuration=file:C:\netiq\idm\apps\tomcat\conf\userapp-log4j.xml -
Dwar.context.name=IDMProv -Ddriver.dn="cn=UserApplication,cn=Driver
Set,o=system" -Duser.container="o=data" -jar
"C:\netiq\idm\apps\UserApplication\liquibase.jar" --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --
classpath="C:\NetIQ\idm\apps\postgres\postgresql-
9.4.1212.jdbc42.jar;C:\netiq\idm\apps\tomcat\webapps\IDMProv.war" --
changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://:5432/
idmuserappdb?compatible=true" --contexts="prov,newdb,updatedb" --logLevel=info
--username=******** --password=******** update >>
C:\netiq\idm\apps\UserApplication\db.out
```

2.4.7 Updating Driver Packages

Designer 4.7.2 is shipped with incorrect versions for some packages for Delimited Text, Lotus Notes, and Office 365 drivers.

To ensure that these drivers work properly in your environment, update the specified package for each driver. For more information about which package version to update, see Section 3.5, “Updating Driver Packages,” on page 25.

2.4.8 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 9.6.12.

1. Stop and disable the PostgreSQL service.
2. Rename the postgres directory from `C:\Netiq\idm\apps`.

   For example, rename postgres to postgres9.6.12.
3. Remove the old PostgreSQL service by running the following command:

   `sc delete "postgres_service_name"`

   For example, `sc delete "postgresql-x64-9.6"`
4. Download and extract the `Identity_Manager_4.7.3_Windows.zip` file.
5. Navigate to the `Identity_Manager_4.7.3_Windows\common\packages\postgres` directory and run the `NetIQ_PostgreSQL.exe` file.
6. Stop the newly installed PostgreSQL service. Go to **Services**, search for PostgreSQL `version` 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:

   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\postgres9.6.12\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\postgresql9612\bin`.
5. Execute initdb as postgres database user from the new PostgreSQL `bin` directory.

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

   For example, `initdb.exe -D C:\NetIQ\idm\apps\postgres9.6.12\data -E UTF8 -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\postgres9.6.9\data" --new-datadir

"C:\NetIQ\idm\apps\postgres9.6.12\data" --old-bindir

"C:\NetIQ\idm\apps\postgres9.6.9\bin" --new-bindir

"C:\NetIQ\idm\apps\postgres9.6.12\bin"
```

10 After successful upgrade, replace the `pg_hba.conf and postgresql.conf` files located in the new postgres data directory (`C:\NetIQ\idm\apps\postgres\data`) with the files from old postgres directory (`C:\NetIQ\idm\apps\postgres9.6.9\data`).

11 Start the upgraded PostgreSQL database service.

Go to **Services**, search for the upgraded PostgreSQL service, 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.

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\postgresql9612\bin`*

2.5 Updating Designer

You must be on Designer 4.7.2 at a minimum to apply this update. The update process includes the following tasks:

2.5.1 Performing the Update

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

2.5.1.1 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.

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

This service pack includes a `Identity_Manager_4.7.3_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_4.7.3_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/designer473offline/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.

2.5.2 Updating Azul Zulu OpenJRE 1.8.0_212

This service pack updates Designer to support Azul Zulu OpenJRE 1.8.0_212 (64-bit).

1. On the server where you installed Designer, download and install the Azul Zulu OpenJRE 1.8.0_212 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.

IMPORTANT: Designer 4.7.2 is shipped with wrong versions for some packages for Delimited Text, Lotus Notes, and Office 365 drivers. To ensure that these drivers work properly in your environment, update the specified package for these drivers. For more information about which package version to update, see Section 3.5, “Updating Driver Packages,” on page 25.

2.6 Updating Sentinel Log Management for IGA

This service pack includes a `SentinelLogManagementForIGA8.2.2.0.tar.gz` file for updating the Sentinel Log Management for Identity Governance and Administration (IGA) component. You must be on NetIQ Sentinel Log Management for IGA 8.2.0 at a minimum to apply this update.

1. Download the `SentinelLogManagementForIGA8.2.2.0.tar.gz` file to the server where you want to install this version.
2. Run the following command to extract the file:

   ```
   tar zxvf SentinelLogManagementForIGA8.2.2.0.tar.gz
   ```
3. Navigate to the `SentinelLogManagementforIGA` directory.
4. To install Sentinel Log Management for IGA, run the following command:

   ```
   ./install.sh
   ```

2.7 Enabling CEF Auditing for SSPR

For more information about enabling CEF auditing for SSPR, see Auditing for Self Service Password Reset in the *Self Service Password Reset Administration Guide*.

3 Known Issues

NetIQ strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

3.1 Roles Not Searched Correctly in the Conflicting Role 2 Field While Creating a New SoD Policy

Issue: While creating a new SoD policy, the dashboard correctly searches for roles in the **Conflicting Role 1** field but fails to correctly search the roles in the **Conflicting Role 2** field. `(Bug 1137928)`

Workaround: Search the role with '`*`' or add a search string followed by `*` in the **Conflicting Role 2** field. For example, if you are searching for `xyz`, enter either '`*`' or '`xyz*`'.

3.2 Identity Reporting Is Not Redirected to OSP After Upgrade If IP Address Is Used for Configuration

Issue: After upgrading Identity Reporting, it does not allow you to access the reporting application if the IP address is used for configuring the reporting settings in the original version of Identity Reporting. `(Bug 1137504)`

Workaround: Add the OSP hostname entry in `/etc/hosts` file of the computer that hosts Identity Reporting.

3.3 Policy Builder Plug-In of iManager Removes Some Mapping Table Strings From a Policy Containing a Map Verb

Issue: When a policy containing mapping table strings is modified in the Policy Builder plug-in of iManager, the CrossScripting filter removes the `src` tag from the request parameter values. `(Bug 1105387)`

Workaround: To preserve the value of the `src` parameter, add the context parameters in the `web.xml` file. This prevents the CrossScripting filter from removing the values from these parameters. In this case, include the `XMLEditor` parameter as a context parameter in the file.

1. Place the following entries in `/var/opt/novell/iManager/nps/WEB-INF/web.xml`:

```
<context-param>
      <param-name>param1</param-name>
      <param-value>XMLEditor</param-value>
  </context-param>
```

2. Restart the Tomcat service.
3. Log in to iManager 3.1.3.
4. Navigate to the Policy Builder and open the policy.
5. Add `src= ""` to the policy.

This action will preserve the value of the `src` parameter.

NOTE: This issue has also been observed when the `src` parameter is used in the `img` tag in the Email notification template. Use a similar workaround to resolve it by changing the XML parameter to `messageBody`.

3.4 Performance Issues with People Search using Server Side Sorting in Identity Applications

Issue: When you configure an LDAP search to use the Server Side Sort control, the search takes a long time to return the results from the Identity Vault. `(Bug 1126537)`

Workaround: Perform the following actions to improve the performance of the search:

- Ensure that the size of eDirectory cache is adequate for the DIB size and the hit ratio of the cache is sufficiently high. For more information about managing eDirectory cache memory, see the *eDirectory Tuning Guide* (https://www.netiq.com/documentation/edirectory-91/edir_tuning/data/bqmivb8.html).

- Server Side Sort uses Given Name and Surname as sorting key attributes to perform searches. To maximize the performance of a search, create an index with the sorting key attributes in addition to the attributes that are configured to be used as search attributes. The order of attributes is important. Place the Given Name and Surname attributes as the first two attributes for the index to be used when sorting the data.

  If the users are searched within a container in the tree, you can further improve the performance by adding AncestorsID information to the index. Currently, you can only create an index with AncestorsID by using the `ndsindex` command. For example:

  ```
  ndsindex add -a -D <admin LDAP DN> -W -s <Server LDAP DN> "GnSnFnCNAncID;Given
  Name\$Surname\$Full Name\$CN;value"
  ```

  This command creates an index that searches on Given Name, Surname, FullName, and CN attributes. The `-a` switch adds the AncestorsID details to the command.

  After creating an index with AncestorsID, set the original index that uses only Given Name and Surname attributes offline and eventually delete it. This ensures that the new index is selected for future searches. For more information about working with eDirectory indexes, see "Index Manager (https://www.netiq.com/documentation/edirectory-91/edir_admin/data/a5tuuu5.html)" in the *eDirectory Administration Guide* (https://www.netiq.com/documentation/edirectory-91/edir_admin/).

For more information about improving the Server Side Sorting or VLV performance, see "Support for Disabling Virtual List View Search" on page 5.

3.5 Updating Driver Packages

Issue: Designer 4.7.2 is shipped incorrect versions for the following driver packages:

- **Delimited Text:** Delimited Text Base
- **Lotus Notes:** Entitlements
- **Office 365:** Office 365 Base, Office 365 Driver Entitlements, and Office 365 Password Synchronization

Workaround: Update the packages to the following versions:

Identity Manager Driver	Package to Update
Delimited Text	NOVLDTXTBASE_2.3.4.20190614114535
Lotus Notes	NOVLNOTEENT_2.4.0.20190614125203
Office 365	◆ NOVLOFFENT_2.7.0.20190614112658 ◆ NOVLOFFIPSWD_2.4.2.20190614112614 ◆ NOVLOFFIBASE_2.12.0.20190614112259

4 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 community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

5 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/.