NetIQ Identity Manager 4.7 Service Pack 4 Release Notes

March 2020

NetIQ Identity Manager 4.7 Service Pack 4 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 Web site.

What's New and Changed?

Identity Manager 4.7.4 provides the following key features, enhancements, and fixes in this release:

- New Features
- Component Updates
- Software Fixes

New Features

Identity Manager 4.7.4 provides the following key functions and enhancements in this release:

Platform Support

In addition to the existing operating systems, this service pack supports SUSE Linux Enterprise Server (SLES) 12 SP5.

New Features and Enhancements in Identity Applications

Identity Applications component includes the following new features and enhancements:

Ability to Customize the Search Results on Roles and Resources Page

Dashboard introduces a new feature under the **General Settings** that allows you to customize the search results on loading the Roles and Resources pages.

The **Enable Eager Search Results in Roles and Resources Page** option, when enabled, displays all roles on Roles page. Similarly, all resources are displayed on the Resources page. The roles and resources are listed in an alphabetical order. By default, this option is enabled.

If you select to disable the **Enable Eager Search Results in Roles and Resources Page** option, then the roles and resources will be displayed on its respective page(s) based on the search criteria. This helps in reducing the page load time, hence improving the performance of the user interface.

Ability to Modify Entitlements After Resource Creation

This service pack adds support for editing resource entitlements. You can now add entitlement to a resource after its creation through the Identity Applications Dashboard. Note that an entitlement cannot be modified if that resource is already assigned to a user.

You can edit a dynamic resource to enable or disable the resource/entitlement assignment multiple times with different values. The **Allow this resource and entitlement to be assigned multiple times with different values** option is available while modifying the entitlement on **Resource** details page. Previously, this option was available on resource creation page only.

Support for Integration with Identity Governance Version 3.6

This service pack introduces support for a new version of Identity Governance. In addition to Identity Governance version 3.5.x, the Identity Manager 4.7.4 can be integrated now with Identity Governance version 3.6 also. The required configuration files namely `uaconfig-ig-defs` and `uaconfig-ig36-defs` for Identity Governance 3.5 and Identity Governance 3.6 respectively are available at the following extracted patch location:

- **Linux:** `<extracted_patch_location>/Identity_Manager_4.7.4_Linux/osp/ig`
- **Windows:** `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\osp\ig`

For more information, see Configuring Identity Manager for Integration in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Ability to Return Values for More than One Attribute Using the IDVault.get And IDVault.globalQuery Functions

With a new enhancement in Identity Manager 4.7.4, it is now possible to obtain values of multiple attributes using the **IDVault.get** and **IDVault.globalQuery** functions.

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 4.7.4
- Identity Manager Remote Loader 4.7.4
- Identity Applications 4.7.4
- Identity Reporting 6.5.0.1
- Identity Manager Designer 4.8.0.1

Updates for Dependent Components

This release adds support for the following dependent components:

- NetIQ eDirectory 9.2.1

  For considerations about upgrading eDirectory, see "Supported Update Paths" on page 7.
- NetIQ iManager 3.2.1.2

  You must install iManager 3.2.1.2 to support eDirectory 9.2.1. 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) 6.3.8

Third-Party Component Versions

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

- Azul Zulu 1.8.0_242 (except Analyzer)
- Apache Tomcat 9.0.31
- PostgreSQL 12.1
- ActiveMQ 5.15.11

Software Fixes

NetIQ Identity Manager includes software fixes for the following components:

- Installation and Upgrade
- Identity Manager Engine
- Identity Reporting
- Identity Applications

For information about the software fixes in NetIQ Identity Manager Designer 4.8.0.1, see NetIQ Identity Manager Designer 4.8 Hot Fix 1 Release Notes.

Installation and Upgrade

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

Re-evaluation of Role Based Entitlement Policies

The iManager installer on Linux platform allows Role-Based Entitlement Plug-ins to re-evaluate role-based entitlement policies successfully. (Bug 1145494)

Identity Manager Engine

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

Audit Log Events Getting Generated upon Restarting eDirectory

The eDirectory crash issue observed in the Novell Audit log events is resolved. An eDirectory restart will recreate the `dxicert.pem` and `dxipkey.pem` files in the `/dib` directory of eDirectory. These files contains the path and filename for the certificate and private key file that allows you to generate audit log events. (Bug 1151070)

Ability to Parse Custom Event ID 1241 Successfully

Identity Manager engine is parsing the custom Event ID 1241 in hexadecimal format. (Bug 1154388)

eDirectory ndsrepair -U Utility Hangs When Executed on Identity Manager Server in a MultiServer Environment

You can execute the `ndsrepair -U` command on an Identity Manager server 72 hours after executing it the first time. (Bug 1156163)

Events from Identity Manager Engine dxevent Module Contains Encrypted Data

dxevent does not contain encrypted data anymore. A dxevent log will show only relevant data. (Bug 1157637)

All the Required Fields Present in Custom CEF Events in Sentinel

A new version of Universal CEF Collector 2011.1r4 is now available wherein the custom CEF events have been enhanced to display the required fields in Sentinel. In addition to these fields, if you wish to add extra fields, you can provide event string field in Generate Event policy action. Event name can be customized by providing "event_name" string in the Generate Event action. (Bug 1151894)

Identity Reporting

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

User Details Getting Synchronizing Between Identity Vault and Reporting Database

User assigned to two different resources, one with approval and other without approval is getting synchronized between the Identity Vault and the Reporting Database without any error. (Bug 1143378)

Identity Applications

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

Tomcat Successfully Deploys IDMProv.war over Restart

Restarting tomcat on identity application server deploys the `IDMProv.war` file successfully. No intermittent error *java.lang.NoClassDefFoundError: Could not initialize class org.infinispan.commands.write.RemoveCommand* is observed.(Bug 1155669)

Content in the localization.csv File is Retained After Identity Applications Upgrade

The Identity Applications upgrade process retains all the previous values in the `localization.csv` file present in the `IDMdb.jar` located at `/opt/netiq/idm/apps/tomcat/webapps/IDMProv/WEB-INF/lib/` directory. (Bug 1148843)

Ability to Successfully Submit Multiple Request Forms that are Opened on the Browser

When you have two or more request forms open on a browser, you can now successfully submit all the forms. (Bug 1151015)

Viewing Request History for Others Allows You to Search Users

If you want to view the request history for others, you will now be able to search for users even when the client is configured with complex filters. (Bug 1150040)

Ability to Search for Users When you are Requesting for a Workflow

The search operation works correctly when you are requesting for a workflow for self or for others. You can now search for any users for whom you want to request the workflow. (Bug 1155022)

IDMProv and idmdash Display All Tasks Correctly When A User Belongs to 1000 or More Groups

When a user is part of more than 1000 groups, the number of tasks displayed for the user on `IDMProv` and `idmdash` are consistent. (Bug 1160118)

Ability to Select More Than One Entitlement While Creating a Resource

You can now select multiple entitlements while creating a resource. (1161887)

PRD Containing an Integration Activity Displays the SOAP Request in the Debug Logging

A PRD containing an integration activity now displays the input payload and SOAP request when debug is enabled. (1157661)

Permission Index Getting Initialized Successfully

The permission index query mechanism has been enhanced and you can now access the Identity Applications user interface when the permission index is being updated. To enable fetching of permissions from eDirectory while creation of permission index, you must add the property com.microfocus.idm.perm.usePageQuery=false in `ism-configuraiton.properties` file and restart the Tomcat. (Bug 1161880)

NOTE: When requesting information from eDirectory, the `com.microfocus.idm.perm.usePageQuery` parameter may prevent the use of the LDAP Paged Search Control that can result in increased memory usage on startup.

Collecting Identity Applications Audit Events through CEF Auditing with SSL Enabled

On enabling SSL connection between the Identity Manager and the Security Event Log Management (such as Sentinel), the Identity Applications CEF events are getting logged successfully. (Bug 1151250)

Ability to Reassign a Group Task When the Helpdesk User Has Provisioning Administrator Rights

When you are logged-in as a Provisioning Administrator, you can reassign a group task even if you are a Helpdesk User. (Bug 1153492)

Dashboard Correctly Displays the Permissions For Non-English Locales When the Permission Name Contains Special Characters

When you search for permissions that contains special characters, the Dashboard displays the correct results for non-English locales too. (Bug 1164286)

Ability to Access Entities When They Are Associated To A Non-default Client

You can now perform the CRUD (Create, Read, Update, Delete) operations when you are logged-in as a non-default client and that client is associated with a valid unique entity. (Bug 1119972)

Dashboard Displays the Images, Icons, and GIFs in the Workflow Forms

Images, icons, and GIFs missing from the Workflow form are now displayed in the Identity Manager Dashboard 4.7.4 version.(Bug 1122142)

Permissions Getting Listed on Teams Page

Dashboard correctly displays the team permissions on the **Edit Team** page.(Bug 1161748)

Improved Performance When Searching Permissions For Others

The response time for fetching permissions for others in the Identity Manager Dashboard has been improved. (Bug 1143892)

Ability to Hide the Helpdesk Controls On Requests History Page And Dashboard Menu

Identity Manager Dashboard now provides you an option to hide the helpdesk controls from the Requests History Page and the Dashboard Menu. (Bug 1138485)

Installing or Updating to This Service Pack

NOTE: After upgrading Identity Manager to 4.7.4, 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_4.7.4_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_4.7.4_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_4.8.0.1_Designer.zip`	Contains files for Designer for all platforms.

For more information about the order of upgrading the components, see "Update Order" on page 8.

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 4.7.4 update according to the following update paths.

Base Version	Updated Version
Identity Manager engine and eDirectory	
Identity Manager 4.7, 4.7.1, 4.7.2, or 4.7.3 with eDirectory 9.1, 9.1.1, 9.1.2, or 9.1.4.1	Identity Manager 4.7.4 with eDirectory 9.2.1
Remote Loader	
Identity Manager 4.7.x with Remote Loader 4.7.x, where x is 0, 1, 2, or 3	Identity Manager 4.7 with Remote Loader 4.7.4
	Identity Manager 4.7.4 with Remote Loader 4.7
	Identity Manager 4.7.4 with Remote Loader 4.7.4
	Identity Manager 4.7.4 with Remote Loader 4.8
	Identity Manager 4.8 with Remote Loader 4.7.4

Base Version	Updated Version
Identity Manager Designer	
If you are currently on Identity Manager Designer 4.7.x version (where x is 0, 1, 2, or 3), first upgrade your Designer to 4.8 version and then apply 4.8.0.1 update.	Identity Manager Designer 4.8.0.1
Identity Applications	
Identity Applications 4.7, 4.7.1.x, 4.7.2, or 4.7.3.x	Identity Applications 4.7.4
Identity Reporting	
Identity Reporting 4.7, 4.7.1, 4.7.2, or 4.7.3	Identity Reporting 4.7.4

Update Order

You must update the components in the following order:

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

   NOTE: Update of Sentinel Log Management for IGA is required only if the version is not 8.2.2.

10. One SSO Provider (OSP)

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

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 4.7.4 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 4.7.4 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_4.7.4_Linux.zip` file for updating the Identity Manager components on Linux platforms.

Updating the Identity Vault

1. Download and extract the `Identity_Manager_4.7.4_Linux.zip` file from the download site.
2. Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.4_Linux/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**
- **Identity Manager Fanout Agent**
- **iManager Web Administration**

- Identity Reporting
- Identity Applications

NOTE: •The Identity Applications update program will update SSPR along with other dependent components. If SSPR auditing output format type is CEF, then make sure to uninstall the NetIQ Self Service Password Reset Collector on Sentinel Syslog server before you update the Identity Applications. For more information, see "Considerations for Updating SSPR on Linux and Windows" on page 9.

- Before updating the Remote Loader, ensure that the following components are stopped:
  - Remote Loader instances
  - Driver instances running with the Remote Loader
  - Identity Vault

Interactive Update

1. Download and extract the `Identity_Manager_4.7.4_Linux.zip` file from the download site.
2. Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.4_Linux` 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.

   If you want to update the Identity Vault, select **N** and follow the steps from "Updating the Identity Vault" on page 9.

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_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 extract the `Identity_Manager_4.7.4_Linux.zip` file from the download site.
2. Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.4_Linux` directory and modify the `silent.properties` file to update the required components.
3. Run the following command:

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

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
   ```

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

This section applies if you have performed a non-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
   ```

Post-Update Tasks for Identity Manager Drivers

(Conditional) This section applies if you want to update to the following versions for these drivers:

- REST 1.1.2.1
- SOAP 4.1.0.1
- Oracle EBS 4.1.2.1
- MSGW 4.2.2.1

In your deployment, if two or more of these drivers are running, and you update one of the drivers to the latest version and then update the Jetty JAR to the latest version (9.4.34.v20201102), NetIQ recommends that you also update the other drivers and the Jetty JAR for those drivers to the latest versions.

For more information on using the `jetty-all-9.4.34.v20201102-uber.jar`, see the NetIQ Identity Manager REST 1.1.2.1 Readme, NetIQ Identity Manager SOAP 4.1.0.1 Readme, NetIQ Identity Manager Oracle EBS 4.1.2.1 Readme, and the NetIQ Identity Manager 4.2.2.1 Managed System Gateway Driver Readme.

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" on page 9.

- 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_4.7.4_Linux.zip` file.
2. Navigate to the `<extracted_patch_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 12.1.

NOTE:

- In addition to the default capabilities offered by PostgreSQL 12.1, this service pack allows you to configure the PostgreSQL database with SSL (OpenSSL 1.0.2t built with FIPS). This service pack also bundles the PostgreSQL Contrib packages.
- When Identity Vault and PostgreSQL are installed on a single server, update Identity Vault before you upgrade PostgreSQL.

---

1. Download and extract the `Identity_Manager_4.7.4_Linux.zip` file from the download site.
2. Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.4_Linux/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/postgres12.1/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_4.7.4_Windows.zip` file for updating the Identity Manager components on Windows platforms.

- 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 extract the `Identity_Manager_4.7.4_Windows.zip` file.
2. Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\IDVault` directory and run the `eDirectory_921_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 extract the `Identity_Manager_4.7.4_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 Remote Loader instances.

2b Close Remote Loader console.

2c Stop all drivers.

2d Stop the Identity Vault.

3 Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\IDM` directory.

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:** Locate the `patchUpgradeSilent.Properties` file from the extracted directory 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`

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`

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:
   - `FanoutAgent.jar`
   - `fanout_web.war`
   - `nxsl.jar`
   - `IDMCEFProcessor.jar`
   - `zoomdb.jar`
2. Download and extract the `Identity_Manager_4.7.4_Windows.zip` file, navigate to `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\IDM\patch\Windows\FanoutAgent\lib` location and copy the following files:
   - `FanoutAgent.jar`
   - `fanout_web.war`
   - `nxsl.jar`
   - `IDMCEFProcessor.jar`
   - `zoomdb.jar`
3. Replace the existing files in `C:\NetIQ\IdentityManager\FanoutAgent\lib` folder with the files copied in Step 2. Use the latest `JDBC 4.2.1.0` Fanout driver.
4. 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 extract the `Identity_Manager_4.7.4_Windows.zip` file.
4. Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\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. For more information, see Configuring iManager for IPv6 Addresses after Installation in the *NetIQ Identity Manager Setup Guide for Windows*.

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 19.

Updating the Identity Applications

NOTE: If SSPR auditing output format type is CEF, then make sure to uninstall the NetIQ Self Service Password Reset Collector on Sentinel Syslog server before you update the Identity Applications. For more information, see "Considerations for Updating SSPR on Linux and Windows" on page 9.

---

1 Download and extract the `Identity_Manager_4.7.4_Windows.zip` file.

2 Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\IdentityApplications` directory.

3 Perform one of the following actions:

GUI: `install.exe`

Silent: In the command prompt, go to the `<extracted_patch_path>` location and run `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_4.7.4.0_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.

Updating Identity Reporting

1 Download and extract the `Identity_Manager_4.7.4_Windows.zip` file.

2 Stop Tomcat.

3 (Conditional) If Identity Reporting is installed on a Standalone server, execute the following steps:

3a Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\IdentityApplications` directory.

3b Perform one of the following actions:

GUI: `install.exe`

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

The Identity Applications update program will update Tomcat and JRE. If Identity Reporting and OSP are installed on the same server, then OSP will also get updated.

NOTE: If OSP is installed on a separate server, ensure that OSP is upgraded to 6.3.8 version before you upgrade Identity Reporting.

---

4 Create a backup directory outside of the Tomcat installation path.

5 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 4.

- `IDMRPT-CORE.war`
- `IDMRPT.war`
- `idmdcs.war`
- `IDMDCS-CORE.war`
- `dcsdoc.war`

6 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.

7 Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\Reporting` directory (Step 1).

8 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`

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

10 (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.

11 Start the Tomcat service.

12 Clear your browser cache before accessing Identity Reporting.

Post-Update Tasks

Perform the following actions after applying this service pack. This section is applicable when updating from 4.7.x to 4.7.4.

Post-Update Tasks for Identity Manager Drivers

(Conditional) This section applies if you want to update to the following versions for these drivers:

- REST 1.1.2.1
- SOAP 4.1.0.1
- Oracle EBS 4.1.2.1
- MSGW 4.2.2.1

In your deployment, if two or more of these drivers are running, and you update one of the drivers to the latest version and then update the Jetty JAR to the latest version (9.4.34.v20201102), NetIQ recommends that you also update the other drivers and the Jetty JAR for those drivers to the latest versions.

For more information on using the `jetty-all-9.4.34.v20201102-uber.jar`, see the NetIQ Identity Manager REST 1.1.2.1 Readme, NetIQ Identity Manager SOAP 4.1.0.1 Readme, NetIQ Identity Manager Oracle EBS 4.1.2.1 Readme, and the NetIQ Identity Manager 4.2.2.1 Managed System Gateway Driver Readme.

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 4.7.4.0.
4. Restart the Tomcat.

Post-Update Steps for Identity Applications

Clear the browser cache.

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 12.1.

IMPORTANT: In addition to the default capabilities offered by PostgreSQL 12.1, this service pack allows you to configure the PostgreSQL database with SSL (OpenSSL 1.0.2t 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 extract the `Identity_Manager_4.7.4_Windows.zip` file.
5. Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.4_Windows\common\packages\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. 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\postgres\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\postgres9.6.12\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: ◆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`*

Upgrading Designer

If you are currently on Identity Manager Designer 4.7.x version, first upgrade your Designer to 4.8 and then apply 4.8.0.1 update.

You must be on Designer 4.8 at a minimum to apply this update. For more information, see NetIQ Identity Manager Designer 4.8 Hot Fix 1 Release Notes.

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.

Unable to Re-evaluate Role Based Entitlements

Issue: In iManager 3.2.1, 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 Windows platform. `(Bug 1145494)`

Workaround: To update iManager plug-ins to re-evaluate role based entitlements, perform the following actions:

1. Stop the Tomcat.
2. Navigate to the iManager installed location, for example, `C:\Program Files\Novell\Tomcat\webapps\nps\WEB-INF\` and modify the Tomcat `web.xml` file to add the following tags 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>
```

3. Restart the Tomcat.
4. Log in to iManager and install the Role-Based Entitlements plug-in. For more information, see "Post-Update Steps for iManager" on page 19.

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 1164389)

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_4.7.4_Linux.zip` from the NetIQ Download website.
5. Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.4_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> &"`

Forms Fail to Load Properly Within Specific Workflows After 4.7.4 Upgrade

Issue: After upgrading Identity Manager to 4.7.4 version, forms for some workflows are not loading properly while requesting permissions in the Identity Applications Dashboard. (0CTCR28Q256172)

Workaround: Perform the steps from TID 7025276.

Workflows Fail with Cross-site Request Forgery and StackOverflowError After 4.7.4 Upgrade

Issue: After upgrading Identity Manager to the 4.7.4 version, custom workflows for resource approval are failing, causing the session to log out. (0CTCR28Q257183)

Workaround: Upgrade Tomcat to version 9.0.36 or later. For more information on how to update Tomcat, see the **Resolution** section of TID 7025276.

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.

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/.