NetIQ Identity Manager 4.7 Service Pack 5 Release Notes

October 2021

NetIQ Identity Manager 4.7 Service Pack 5 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 Micro Focus 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 4.7.5 provides the following key features, enhancements, and fixes in this release:

- New Features and Enhancements
- Component Updates
- Software Fixes
- What's Deprecated for Removal?

New Features and Enhancements

Identity Manager 4.7.5 provides the following key functions and enhancements in this release:

Platform Support

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

- Red Hat Enterprise Linux (RHEL) 7.7, 7.8, and 7.9
- Open Enterprise Server (OES) 2018 SP2 and 2018 SP3

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 4.7.5
- Identity Manager Remote Loader 4.7.5
- Identity Manager Fanout Agent 1.2.2
- Identity Applications 4.7.5
- Identity Reporting 6.5.0.1
- Identity Manager Designer 4.8.4.0100

NOTE: This service pack contains the same versions of Fanout Agent and Identity Reporting components that were shipped with the Identity Manager 4.7.4 version.

Updates for Dependent Components

This release adds support for the following dependent components:

- NetIQ eDirectory 9.2.5
- NetIQ iManager 3.2.5
- NetIQ Self Service Password Reset (SSPR) 4.5.0.4
- NetIQ One SSO Provider (OSP) 6.4.6
- NetIQ Sentinel Log Management for IGA 8.4

Third-Party Component Versions

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

- Azul Zulu Java 1.8.0_292
- Apache Tomcat 9.0.50
- PostgreSQL 12.7
- OpenSSL 1.0.2y
- ActiveMQ 5.15.15

Software Fixes

This release includes software fixes for the following components:

- Identity Manager Engine
- Identity Applications

Identity Manager Engine

NetIQ Identity Manager includes the following software fixes that resolves a specific issue in the Identity Manager engine:

Ability to Generate Email Using the Command Transformation Policy

The `dirxml_misc.jar` file, shipped with this version of Identity Manager, is now enhanced to generate e-mails successfully. (`Bug 261076`)

Identity Applications

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

Dashboard Tasks and Tasks of Others Page Display Values in the Assigned To and Recipient Columns

Identity Manager Dashboard correctly display values in the **Assigned To** and **Recipient** Columns on the **Tasks** and tasks of **Others** pages.(`Bug 312056`)

Dashboard Request History Page Displays the Requester Details Correctly

If a resource is assigned through a provisioning request definition, the workflow fetches the requester name and displays on the Request History page. (`Bug 230947`)

Improvement in Search Functionality on the Roles Page

The Advanced and Simple search filters on the Roles page have been improved, resulting in a more focused search result. A search term that includes a space or hyphen will also provide the desired result. For example, searching for a `Provisioning - Administrator` role yields a single result. (`Bug 312072`)

Data Item Mapping Works For Workflows Started Through REST API

The Data Items from the request form are successfully passed on to the approval form when a workflow is started using the REST API. (`Bug 383043`)

Picklist Functionality Works Consistently

The picklist dynamically retrieves the DN values from the Identity Vault without any error. (`Bug 357160`)

Error On User Application Server Startup Resolved: EboBootServlet [RBPM] Runtime exception initializing

The error `EboBootServlet [RBPM] Runtime exception initializing` that occurred when starting the User Application Server has been resolved. (`Bug 230736`)

Using DNLookup in a Workflow Without Getting a Cross-site Request Forgery Error

Using DNLookup in a workflow form after retrieving the logged-in user details through the REST API works as expected. The Cross-site Request Forgery error is no longer observed. (`Bug 230835`)

In a Clustered Environment, Requests Pending on a Non-Primary Node Are Approved

The `com.microfocus.monitor.timertask.interval` property in the `ism-configuration.properties` file ensures that the Identity Manager's cluster functionality works as expected. (`Bug 230863`)

Request History Details are Displayed Correctly on the Dashboard

When two or more requests are submitted at the same time, the details of each request is shown properly on the Request History page. (Bug 230929)

My Profile and Users Page Now Displays the Lookup Attributes for a Custom Entity

The custom entity and the corresponding attributes are now visible on the **My Profile** and **Users** pages of the Identity Manager Dashboard. (Bug 329105)

Workflow Forms Successfully Loaded While Requesting Permission

Forms are properly loading in Identity Manager 4.7.5 when requesting permission on Dashboard. (Bug 256172)

Finding Users on the New Request Page Works As Expected

Even after adding attributes to the **User Search Lookup Attribute** on the Settings page, Team Managers and Administrative users can search for users when requesting permission for others. (Bug 380009)

What's Deprecated for Removal?

Modifying resource entitlement parameters using SOAP API is deprecated from this release and will be discontinued in future. However, you can continue to modify resources through the Identity Manager Dashboard. Remember that you cannot modify a resource with one or more identities assigned to it or if that resource is already associated with a role. For more information, see Editing Resources section in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Installing or Updating to This Service Pack

The following files are available for download:

Filename	Description
`Identity_Manager_4.7.5_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.
`Identity_Manager_4.7.5_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.
`Identity_Manager_4.8.4_P1_Designer.zip`	Contains files for Designer for all platforms.
`SentinelLogManagementForIGA8.4.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 "Update Order" on page 5.

- “Updating the Identity Manager Components on Linux” on page 6
- “Updating the Identity Manager Components on Windows” on page 13
- “Upgrading Designer” on page 21

Supported Update Paths

If you are currently on Identity Manager 4.6.4 or a prior version, first upgrade your components to 4.7 and apply 4.7.5 update according to the following update paths.

Base Version	Updated Version
Identity Manager Engine and eDirectory	
Identity Manager 4.7.x, where x is 0 to 4 with eDirectory 9.1.x or eDirectory 9.2.x, where x is 0 to 4.	Identity Manager 4.7.5 with eDirectory 9.2.5
Remote Loader	
Identity Manager 4.7.x with Remote Loader 4.7.x, where x is 0, 1, 2, 3, or 4	Identity Manager 4.7.x with Remote Loader 4.7.5, where x is 0 to 4
	Identity Manager 4.7.5 with Remote Loader 4.7.x, where x is 0 to 4
Identity Manager Designer	
NOTE: 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, apply the 4.8.4 update, and then apply the 4.8.4.0100 patch.	Identity Manager Designer 4.8.4.0100
Identity Applications	
Identity Applications 4.7.x, where x is 0 to 4	Identity Applications 4.7.5
Identity Reporting	
Identity Reporting 4.7.x, where x is 0 to 4	Identity Reporting 4.7.5
NOTE: The Identity Reporting component version bundled with this service pack remains the same as the version bundled with the Identity Manager 4.7.4 version.	

Update Order

The update process requires you to update Identity Manager 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
10. One SSO Provider (OSP)
11. Self-Service Password Reset (SSPR)

NOTE:

- Standalone update of OSP is supported only on Windows.
- Standalone update of SSPR is required if it is installed on a remote machine.
- This service pack does not provide any updates to the Fanout Agent and Identity Reporting components. The Fanout Agent and the Identity Reporting versions are the same as the Identity Manager 4.7.4 versions. For more information on the component versions shipped with Identity Manager 4.7.x versions, see Identity Manager Component Versions in the System Requirements Guide for Identity Manager 4.7.x.

Considerations for Updating SSPR on Linux and Windows

The following considerations apply to Self Service Password Reset (SSPR) before you update Identity Manager to 4.7.5 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 the 4.7.5 version, SSPR is upgraded to 4.5.0.4 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_4.7.5_Linux.zip` file for updating the Identity Manager components on Linux platforms. The following sections provide details on updating the different Identity Manager components to this service pack.

- 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
- Updating Sentinel Log Management for IGA

Updating the Identity Vault

1. Download and extract the `Identity_Manager_4.7.5_Linux.zip` file from the download site.
2. Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.5_Linux/IDVault/setup` directory.
3. Run the following command:

   ```
   ./nds-install
   ```

4. Follow the prompts.

Updating the Identity Manager Components

The update of the Identity Manager components on Linux is supported through a single script. You must run the `install.sh` script to update these components. The components include Identity Manager Engine, Remote Loader, Fanout Agent, iManager Web Administration, Identity Applications, and Identity Reporting.

NOTE

- The Identity Applications update will also update the SSPR component to the latest version. If the SSPR auditing output format type is CEF, you must uninstall the NetIQ Self Service Password Reset Collector on Sentinel Syslog server before updating Identity Applications. For more information, see "Considerations for Updating SSPR on Linux and Windows" on page 6.
- Before updating the Remote Loader, ensure that the following components are stopped:
  - Remote Loader instances

    ```
    rdxml -config <filename> -u
    ```

  - Driver instances running with the Remote Loader
  - Identity Vault

    ```
    ndsmanage stopall
    ```

- Before updating the Fanout Agent, ensure that the following components are stopped:
  - Fanout Agent
  - JDBC Fanout driver

Interactive Update

1. Download and extract the `Identity_Manager_4.7.5_Linux.zip` file from the download site.
2. Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.5_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.

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

- **Remote Loader:** `rdxml -config <filename>`
- **Fanout Agent:** Perform the following steps:
  1. Navigate to `/opt/novell/dirxml/fanoutagent/bin` directory.
  2. Run the following command:

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

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

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

Silent Update

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

- To update the Identity Vault, set `IDVAULT_SKIP_UPDATE=false`
- To update the Identity Manager 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 the 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.

Perform the following actions to update the components silently:

1 Download and extract the `Identity_Manager_4.7.5_Linux.zip` file from the download site.

2 Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.5_Linux` directory.

3 Modify the `silent.properties` file as required.

4 Run the following command:

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

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

- **Remote Loader:** `rdxml -config <filename>`
- **Fanout Agent:** Perform the following steps:
  1. Navigate to `/opt/novell/dirxml/fanoutagent/bin` directory.

2. Run the following command:

   ./startAgent –config <FanoutAgent Installation Location>/config/fanoutagentconfig.properties

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

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

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

Performing a Non-Root Update

You can install Identity Manager Engine as a non-root user to enhance the security of your Linux server. You cannot install Identity Manager Engine as a non-root user if you installed the Identity Vault as root. You need to perform the following steps to install the Identity Manager Engine as a non-root user:

- Update NICI. For more information, see Updating NICI.
- Update eDirectory as a non-root user. For more information, see Updating eDirectory as a Non-root User.
- Update Identity Manager Engine as a non-root user. For more information, see Updating Identity Manager Engine as a Non-root User.

Updating NICI

Ensure that you are logged-in as a root user before updating NICI.

1 Log in as a non-root user.

2 Stop eDirectory.

```
ndsmanage stopall
```

3 Download and extract the `Identity_Manager_4.7.5_Linux.zip` file from the download site.

4 Log in as a root user.

5 Navigate to the `/<location where you have extracted the zip>/IDVault/setup` directory.

6 Run the following command:

```
rpm -Uvh nici64-3.2.0-0.00.x86_64.rpm
```

Updating eDirectory as a Non-root User

Perform the following steps to upgrade eDirectory as a non-root user:

1 Log in as a non-root user.

2 Navigate to the `/<location where you extracted the zip file>/IDVault/` directory.

3 Copy the `eDir_NonRoot.tar.gz` file to a non-root home directory.

4 Run the following command to extract the `.tar.gz` file.

```
tar -zxvf eDir_NonRoot.tar.gz
```

5 (Conditional) Ensure the below paths are set in `<non-root home directory>/.bash_profile` so that the paths are not required to be set each time the user logs in to a session.

```
export LD_LIBRARY_PATH=<non-root home directory>/eDirectory/opt/novell/
eDirectory/lib64:<non-root home directory>/eDirectory/opt/novell/eDirectory/
lib64/nds-modules:<non-root home directory>/eDirectory/opt/novell/
lib64:$LD_LIBRARY_PATH

export PATH=<non-root home directory>/eDirectory/opt/novell/eDirectory/
bin:<non-root home directory>/eDirectory/opt/novell/eDirectory/sbin:/opt/
novell/eDirectory/bin:$PATH

export MANPATH=<non-root home directory>/eDirectory/opt/novell/man:<non-root
home directory>/eDirectory/opt/novell/eDirectory/man:$MANPATH

export TEXTDOMAINDIR=<non-root home directory>/eDirectory/opt/novell/
eDirectory/share/locale:$TEXTDOMAINDIR. <non-root home directory>/eDirectory/
opt/novell/eDirectory/bin/ndspath
```

6 Add the non-root user to the eDirAdmin user group. For more information, see Adding the edirAdmin User Group in the NetIQ eDirectory Installation Guide.

7 Start eDirectory.

```
ndsmanage startall
```

Updating Identity Manager Engine as a Non-root User

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 the `<non-root home directory>/eDirectory/opt/novell/eDirectory/bin` directory.

2 Run the following command:

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

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. On the **Configure** tab, navigate to **iManager Server** > **Configure iManager**.
3. Click **Plug-in Download**.
4. Select the **Custom download site** radio button.
5. Specify the following URL in the **Download URL** field:

   ```
   https://www.novell.com/products/consoles/imanager/
   iman_mod_desc_IDM475Support.xml
   ```
6. Click **Save**.
7. On the **Configure** tab, navigate to **Plug-in Installation** > **Available NetIQ Plug-in Modules.**
8. Select the required plug-ins from the **NetIQ Plug-in Modules** list and then click **Install**.
9. Restart the Tomcat service.

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 6.
- 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_4.7.5_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 12.7.

NOTE:

- In addition to the default capabilities offered by PostgreSQL 12.7, this service pack allows you to configure the PostgreSQL database with SSL (OpenSSL 1.0.2y 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_4.7.5_Linux.zip` file from the download site.
2. Navigate to the `<extracted_patch_location>/Identity_Manager_4.7.5_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: Specify the location of the new PostgreSQL data directory. This prompt is displayed if you selected to specify a different directory other than the existing directory.

Updating Sentinel Log Management for IGA

This service pack includes a `SentinelLogManagementForIGA8.4.tar.gz` file for updating the Sentinel Log Management for Identity Governance and Administration (IGA) component.

1. Download the `SentinelLogManagementForIGA8.4.tar.gz` file to the server where you want to install this version.
2. Run the following command to extract the file:

   ```
   tar -zxvf SentinelLogManagementForIGA8.4.tar.gz
   ```
3. Navigate to the `SentinelLogManagementforIGA` directory.
4. To install SLM for IGA, run the following command:

   ```
   ./install.sh
   ```

Updating the Identity Manager Components on Windows

This service pack includes a `Identity_Manager_4.7.5_Windows.zip` file for updating the Identity Manager components on Windows platforms. The following sections provide details on updating the different Identity Manager components to this service pack.

- 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_4.7.5_Windows.zip` file.
2. Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.5_Windows\IDVault` directory and run the `eDirectory_925_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**.
7. Click **Done**.

Updating the Identity Manager Engine and Remote Loader

1. Stop the Identity Vault and Remote Loader instances.
   - **1a** Stop all Remote Loader instances.
   - **1b** Close Remote Loader console.
   - **1c** Stop all drivers.
   - **1d** Stop the Identity Vault.

2 Download and extract the `Identity_Manager_4.7.5_Windows.zip` file.

3 Navigate to the `Identity_Manager_4.7.5_Windows\IDM` directory.

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

- **For interactive mode:** Run `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, as required, 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`

6 Start the Identity Vault and Remote Loader instances.

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 Stop the Fanout Agent.

2 Stop the JDBC Fanout driver.

3 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`

4. Download and extract the `Identity_Manager_4.7.5_Windows.zip` file, navigate to `<extracted_patch_location>\Identity_Manager_4.7.5_Windows\IDM\patch\Windows\FanoutAgent\lib` location and copy the following files:
   - `FanoutAgent.jar`
   - `fanout_web.war`
   - `nxsl.jar`
   - `IDMCEFProcessor.jar`
   - `zoomdb.jar`
5. Replace the existing files in `C:\NetIQ\IdentityManager\FanoutAgent\lib` folder with the files copied in Step 4. Use the latest version of the JDBC Fanout driver.
6. Start the Fanout Agent.
7. Start the JDBC Fanout driver.

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_4.7.5_Windows.zip` file.
4. Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.5_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 18.

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 6.

---

1 Download and extract the `Identity_Manager_4.7.5_Windows.zip` file.

2 Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.5_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, modify the silent.properties file as required, and run the `install.exe -i silent -f silent.properties` command.

   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_4.7.5.0_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_4.7.5_Windows.zip` file.

2 Stop the Tomcat service.

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

3a Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.5_Windows\IdentityApplications` directory.

3b Perform one of the following actions:

GUI: `install.exe`

Silent: Modify the silent.properties file as required and then run the `install.exe -i silent -f silent.properties` command.

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 6.4.6 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_4.7.5_Windows\Reporting` directory.

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 4.7.5.

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. On the **Configure** tab, navigate to **iManager Server** > **Configure iManager**.
3. Click **Plug-in Download**.
4. Select the **Custom download site** radio button.
5. Specify the following URL in the **Download URL** field:

   ```
   https://www.novell.com/products/consoles/imanager/
   iman_mod_desc_IDM475Support.xml
   ```

6. Click **Save**.
7. On the **Configure** tab, navigate to **Plug-in Installation** > **Available NetIQ Plug-in Modules.**

8. Select the required plug-ins from the **NetIQ Plug-in Modules** list and then click **Install**.
9. Restart the Tomcat service.

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 12.7.

IMPORTANT: In addition to the default capabilities offered by PostgreSQL 12.7, this service pack allows you to configure the PostgreSQL database with SSL (OpenSSL 1.0.2y 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. Navigate to the directory where PostgreSQL is installed. For example, C:\Netiq\idm\apps.
3. Rename the `postgres` directory.

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

   ```
   sc delete <"postgres_service_name">
   ```

   For example, `sc delete "NetIQ PostgreSQL"`
5. Download and extract the `Identity_Manager_4.7.5_Windows.zip` file.
6. Navigate to the `<extracted_patch_location>\Identity_Manager_4.7.5_Windows\common\packages\postgres` directory and run the `NetIQ_PostgreSQL.exe` file. Select only PostgreSQL option during installation.

   NOTE: Ensure that you have Administrator privilege for the old and new PostgreSQL installation directories.

   ---
7. Specify the path where you want to install PostgreSQL. For example, C:\Netiq\idm\apps.
8. Click **Next**.
9. Specify the password for the postgres user.
10. Specify the PostgreSQL port. The default port is 5432.
11. Do not select the **Create database login account** and **Create empty database** check boxes.
12. Click **Next**.
13. Review the details on the Pre-Installation summary page and click **Next**.
14. Stop the newly installed PostgreSQL service.

    Go to **Services**, search for `NetIQ PostgreSQL service`, and stop the service.

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

    ---

15 Change the permissions for the newly installed PostgreSQL directory by performing the following actions:

15a (Optional) If postgres user is not created, then perform the following steps to create a `postgres` user:

15a1 Go to **Control Panel** > **User Accounts** > **User Accounts** > **Manage Accounts**.

15a2 Click **Add a user account**.

15a3 In the **Add a User** page, specify postgres as the user name and provide a password for the user.

15b Assign permissions for the postgres user to the existing and newly installed PostgreSQL directories. Right-click the corresponding directories and go to **Properties** > **Security** > **Edit**.

15c Select **Full Control for the user** to provide complete permissions.

15d Click **Apply**.

16 Access the PostgreSQL directory as `postgres` user.

16a Log in 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.

16b Delete the data directory from the new PostgreSQL installed location.

For example, `C:\Netiq\idm\apps\postgres\data`.

16c Open a command prompt and set PGPASSWORD by using the following command:

```
set PGPASSWORD=<your pg password>
```

16d Change to the newly installed PostgreSQL directory.

For example, `C:\Netiq\idm\apps\postgres\bin`.

16e Based on the encoding type that is set for the database, execute the following `initdb` commands as a `postgres` user from the `bin` directory. By default, the encoding type is set to WIN1252.

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

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

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

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

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

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

16f Navigate to the `C:\Netiq\idm\apps\postgres\data\` directory, edit the `pg_hba.conf` file, and set the **Method** type from `md5` to `trust`.

IMPORTANT: You must also set the **Method** type from `md5` to `trust` in the `pg_hba.conf` file located in the `C:\Netiq\idm\apps\postgres_old\data\` directory.

---

17 Navigate to the `C:\Netiq\idm\apps\postgres\bin` directory and run the following command:

```
pg_upgrade.exe --old-datadir "C:\Netiq\idm\apps\postgres_old\data" --new-datadir
"C:\Netiq\idm\apps\postgres\data" --old-bindir
"C:\Netiq\idm\apps\postgres_old\bin" --new-bindir
"C:\Netiq\idm\apps\postgres\bin"
```

18 Once PostgreSQL is upgraded successfully, perform the following steps:

18a Navigate to the `C:\Netiq\idm\apps\postgres_old` directory.

18b Copy the `pg_hba.conf` and `postgresql.conf` files.

18c Navigate to `C:\Netiq\idm\apps\postgres` directory.

18d Replace the files you copied in Step 18b.

19 Start the PostgreSQL service.

Go to **Services**, search for `NetIQ PostgreSQL` service, and start the service.

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

---

20 (Optional) To ensure that the old cluster's data files are deleted and the service does not start automatically, perform the following steps:

20a Log in as `postgres` user.

20b Navigate to the `C:\Netiq\idm\apps\postgres\bin` directory.

20c Run the `analyze_new_cluster.bat` and `delete_old_cluster.bat` files.

Upgrading Designer

If you are currently on Identity Manager Designer 4.7.x version, first upgrade your Designer to 4.8 version, apply the 4.8.4 update, and then apply the 4.8.4.0100 update.

To apply the 4.8.4.0100 update, you must be on Designer 4.8.4 at a minimum. For more information, see NetIQ Identity Manager Designer 4.8.4 Patch 1 Release Notes.

Known Issues

NetIQ strives to ensure our products provide quality solutions for your enterprise software needs. There are no new issues other than the issues mentioned in the NetIQ Identity Manager 4.7 Service Pack 4 Release Notes. If you need further assistance with any issue, please contact Technical Support.

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