**SAILPOINT UPGRADE IdentityIQ-8.3 version**

**Version1. January 30, 2024**

**Shahzada Rabbani.**

1. Contents

[1. Introduction 3](#_Toc158056411)

[2. Upgrade Procedure 3](#_Toc158056412)

[3. Requirements for IIQ 8.3 upgrade 3](#_Toc158056413)

[Application Servers 3](#_Toc158056414)

[Databases 3](#_Toc158056415)

[Software Requirements 3](#_Toc158056416)

[4. IdentityIQ **8.3 Feature Updates** 4](#_Toc158056417)

[5. Backup Existing Version of IdentityIQ 5](#_Toc158056418)

[6. Shutdown of IdentityIQ services. 5](#_Toc158056419)

[7. Upgrade from IIQ 8.2 to IIQ 8.3 GA 5](#_Toc158056420)

[7.1 Download and Expand the Installation Files 5](#_Toc158056421)

[8. Database connection configuration 6](#_Toc158056422)

[8a. Update database connection configuration 6](#_Toc158056423)

[9. Download the Accelerator Pack 8.3 zip file from Compass 6](#_Toc158056424)

[10. Launch of IdentityIQ Console 7](#_Toc158056425)

[11. Build Issues and Remediation 8](#_Toc158056426)

[1. Unable to check IdentityIQ database version 8](#_Toc158056427)

[2. Quicklink erros - 8](#_Toc158056428)

[3. Unexpected behaviour in AD provisioning && aggregation and other similar issue – 8](#_Toc158056429)

[4. Variables not substituted with values in email templates 9](#_Toc158056430)

[Extra attention during upgrade – 10](#_Toc158056431)

[12. Validation after upgrade IIQ8.3 10](#_Toc158056432)

[13. High level test steps after upgrade 10](#_Toc158056433)

# Introduction

This document describes SailPoint Upgrade procedure from *IIQ8.2\_*to\_*IIQ8.3* which we implement with issues/errors and Remediation. *IIQ8.3* release includes updates to the translations files, SAML Electronic Signatures, the Oracle Fusion HCM Accounts Connector. This version also includes updates to various connectors (Azure Active Directory, Duo, Okta, Web Services, Active Directory, RSA etc.).

# Upgrade Procedure

This document details out steps for upgrading version in dev/Prod environment. SailPoint IdentityIQ is a complete identity and access management solution that integrates governance and provisioning into a single solution leveraging a common identity repository and governance platform. Because of this approach, IdentityIQ consistently applies business and security policy and role and risk models across all identity and access-related activities - from access requests to access certifications and policy enforcement, to account provisioning and user lifecycle management. Through the use of patent-pending technologies and analytics, IdentityIQ improves security, lowers the cost of operations, and improves an organization's ability to meet compliance and provisioning demands. IdentityIQ 8.3 provides new features and capabilities across the product, including Compliance Manager, Lifecycle Manager, the Governance Platform, and Connectivity

# Requirements for IIQ 8.3 upgrade

# Application Servers

* Apache Tomcat 9.0
* Oracle WebLogic 14c and 12cR2
* IBM WebSphere 9.0
* JBoss Enterprise 7.4 and 7.3
* IBM WebSphere Liberty 21.0 and 20.0

# Databases

* IBM DB2 11.5
* MySQL 5.7 and 8.0
* MS SQL Server 2019 and 2017
* Oracle 19c

# Software Requirements

**Java Platform**

* Sun, Oracle or IBM JDK 1.8 (8),
* JDK 11 and JDK 17 for all application servers that support those versions
* OpenJDK11 is now supported on all environments
* JDK 8 is supported as needed by the specific application servers

# IdentityIQ **8.3 Feature Updates**

IdentityIQ 8.3 introduces the following new features or enhancements.

|  |  |
| --- | --- |
| **Feature/Enhancement** | **Description** |
| Role Management & Analysis | IdentityIQ now can more efficiently track the relationship of an organization’s roles (as defined in IdentityIQ) to the entitlements and permissions in the Entitlement Catalog, by providing a new database table to store the associations between roles and entitlements.  This allows roles to be filtered based on details of the entitlements included directly in their profiles, or in the profiles of other roles with a required/permitted/inherited relationship.  New filters have been added in the following locations   * **Role Management > Role Search**: filter roles based on the state of the profile (are applications/entitlements valid), entitlement/permission details, relationship of entitlement to role (direct/indirect), entitlement/permission application, attribute, and attribute value * **Advanced Analytics > Role Search**: similar to Role Search above * **LCM Manage User Access**: filter requestable roles based on entitlement details.   Certification owners can pre-filter roles to include in **Targeted Certifications**, based on the details of their entitlements or permissions.  A new **Associated Roles** tab for entitlements or permissions in the Entitlement Catalog shows the roles associated with the access.  A new **Roles By Entitlement** report provides details about roles based on entitlement parameters, with results including the nature of relationship of the role to the queried entitlement.  The **Role Members Report** has been updated to include these entitlement parameters. |
| Active Directory Native Move/Rename Support | In many places in IdentityIQ, the default identifier for Active Directory accounts and groups is DistinguishedName (DN). Some native changes, such as when an account or group is moved within the Active Directory OU or when a person’s name changes, result in a change to the DN. In previous versions of IdentityIQ, this could result in additional objects being created on aggregation.  IdentityIQ8.3 version will detect when an account or group object’s DN has been changed on Active Directory. The existing account or group object will be updated, and the change will be propagated to areas where the DN is referenced in the IdentityIQ object model. |
| AI Recommendations for Roles | IdentityIQ users can now leverage AI Services to gain deeper insights and recommendations for access request approvals and access reviews for roles. These new AI features build on the integration with AI Services introduced in IdentityIQ version 8.0, which provided AI recommendations for Access Request Approvals and Access Reviews for entitlements. |
| SAML Authentication for e-Signatures | With SAML-based SSO enabled for e-Signatures, the user performing the electronic signature is routed to your SAML provider for authentication, then seamlessly returned to the IdentityIQ UI to complete the signature. This provides increased security when users e-sign critical requests or certifications, and can be used to expand the authentication methods, such as smart cards or biometrics, that can be used in electronic signatures. |
| OAuth2.0 Authentication for Email | To keep your IdentityIQ environment current, IdentityIQ now supports the OAuth2 authentication protocol for sending email notification via HTTP/HTTPS. This option is recommended for use with Microsoft Office 365, as an alternative to the SMTP/Basic method which is being deprecated by Microsoft. |
|  |  |

# Backup Existing Version of IdentityIQ

Backup activities of identityiq deployment folder and the identityiq schema from DB need to be done. We should perform the database backup and customization backup before performing the upgrade procedure**.**

# Shutdown of IdentityIQ services.

We should perform stopping/shutdown of services before upgrade.

* Stopping schedulers,
* Stopping LifeCycle- events.
* Stopping IIQ Services
* Stopping CustomWindowServiceComponent.
* Turn off email notifications during Upgrade.

# Upgrade from IIQ 8.2 to IIQ 8.3 GA

# 7.1 Download and Expand the Installation Files

* + Clear or take a backup of any existing IdentityIQ installation files before downloading the new version.
  + Download the IdentityIQ installation files, and we should place in SSB
* Downloaded **identityiq-8.3.zip** from SailPoint compass will be moved to

“**identityiq \base\ga**” folder.

* Update the following entries in “build.properties”
  + “**IIQVersion= 8.3” –** GA version
  + **“IIQPatchLevel= ” -** Patch Level (if any)
* The IdentityIQ installation package contents are as follows:

*identityiq.war*

*database*

*doc*

*integration*

* 1. Copy the configuration files saved in SSB for the installation:
     1. iiq.properties -> WEB-INF/classes
     2. \*Extended.hbm.xml -> WEB-INF/classes/sailpoint/object
     3. *[AlertExtended.hbm.xml; ApplicationExtended.hbm; BundleExtended.hbm; CertificationItemExtended.hbm; IdentityExtended.hbm; LinkExtended.hbm; ManagedAttributeExtended.hbm; ServerExtended.hbm; TargetExtended.hbm]*
     4. JDBC drivers -> WEB-INF/lib

* 1. Update the following entries in “build.properties”

“IIQVersion= 8.3” – GA version

“IIQPatchLevel= ” - Patch Level

* 1. Use the iiq script to run the schema command to create/modify the database creation/modification scripts based on your changes to the .hbm.xml files.
     1. cd identityiq\_home\WEB-INF\bin
     2. iiq schema
  + Run upgrade scripts
  1. Run this file in Database - upgrade\_identityiq\_tables.sqlserver
  2. Open command prompt
     1. cd identityiq\_home\WEB-INF\bin
     2. iiq upgrade

# Database connection configuration

# 8a. Update database connection configuration

* + Replace/edit the iiq.properties file in Tomcat\_home\webapps\identityiq\WEB-INF\classes folder with the database details.
  + Replace the log4j2.properties file with the custom settings

**7b. Post Upgrade Database Script**

• Execute identityiq-8.3\database\post\_upgrade\_identityiq\_tables.sql to clean up the tables that are no longer necessary.

# Download the Accelerator Pack 8.3 zip file from Compass

8a. Extract the Accelerator Pack zip file to a temporary location.

8b. Update the Hibernate configuration files in IdentityIQ installation directory.

To merge the Accelerator Pack Hibernate files with our existing IdentityIQ Hibernate files:

* + 1. In the unzipped Accelerator Pack location’s /web/WEBINF/classes/sailpoint/object/ folder, open each of the \*.hbm.xml files that has a corresponding file in the[IdentityIQ\_Install\_Dir]/WEBINF/classes/sailpoint/object/folder.
    2. In each of the Accelerator Pack’s \*.hbm.xml files, find the <!--OOTB END--> marker in the file.
    3. Select and copy the contents of the file below the <!--OOTB END--> marker, and paste it at the end of the IdentityIQ \*.hbm.xml file of the same name.
    4. Save your changes to the IdentityIQ \*.hbm.xml files.

8c. Copy these Accelerator Pack artifacts from the unzipped Accelerator Pack location to the corresponding location in your IdentityIQ installation directory.

* 1. Copy [AP\_Unzip\_Dir]/web/WEB-INF/lib/AcceleratorPack.jar to [IdentityIQ\_Install\_Dir]/WEB-INF/lib
  2. Copy all files and subfolders under [AP\_Unzip\_Dir]/web/WEBINF/config/to [IdentityIQ\_Install\_Dir]/WEB-INF/config/
  3. Copy all files under [AP\_Unzip\_Dir]/web/images/icons/ to [IdentityIQ\_Install\_Dir]/images/icons/
  4. Copy [AP\_Unzip\_Dir]/web/define/applications/IdentityIQLoopback.xhtml to [IdentityIQ\_Install\_Dir]/define/applications/

8d. Merge the iiqCustom.properties file from the Accelerator Pack with the corresponding file in IdentityIQ installation directory:

* Open the Accelerator Pack custom properties file: [AP\_Unzip\_Dir]/web/WEBINF/classes/sailpoint/web/messages/iiqCustom.properties
* Select and copy the full contents of the file (although you may not need the first 13 entries if they are already in your existing iiqCustom.properties file)
* Open the IdentityIQ custom properties file: [IdentityIQ\_Install\_Dir]/WEBINF/classes/sailpoint/web/messages/iiqCustom.properties
* Paste the copied contents from the Accelerator Pack iiqCustom.properties file to the end of IdentityIQ iiqCustom.properties file. Note that if you have made any customizations to this file, you should paste the contents from the Accelerator Pack below all your customizations.
* Save your changes.

8e. Import the Accelerator Pack updates (from iiq console):

* import upgrade-acceleratorpack.xml
* Restart your IdentityIQ application.
* Verify that your Accelerator Pack installation was successful by opening IdentityIQ and clicking on Administrative Tasks > Installed Accelerator Pack in the Quicklinks menu, and verifying that your installed features are displayed. You can also validate the version by navigating to the Debug pages in Configuration Objects -> System Configuration and verifying that this line is there:
* <entry key="acceleratorPackVersion" value="8.3"/>

8f. Deploy the final target upgrade version in the lower environment

8g. Restart application server

# Launch of IdentityIQ Console

We have to run the iiq console command from the identityiq\_home\WEBINF\bin directory. We will be using import utility to import the configuration objects as mentioned:

iiq console

> import init.xml

> quit

. And Start your application server.

# Build Issues and Remediation

### Unable to check IdentityIQ database version

*org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'versionChecker' defined in class path resource [configBeans.xml]: Invocation of init method failed; nested exception is java.lang.RuntimeException: Unable to check IdentityIQ database version: Invalid object name 'spt\_database\_version'.*

If we find above error while connecting to iiq console, there is an issue of default schema. Run below command to fix –

**ALTER USER <user thru which you are connecting> WITH DEFAULT\_SCHEMA = <DB schema>;**

**Eg - ALTER USER identityiq WITH DEFAULT\_SCHEMA = IIQ\_PQA01;**

### Quicklink erros -

*rest.ui.jaxrs.AllExceptionMapper:26 - Uncaught JAX-RS exception. java.lang.NullPointerException:*



*And error on saving / updating dynamic scope –*



**Reason** – quicklink option got corrupt during deployment.

**Fix –** Run this rule to delete those QuickLink Option object which have null quicklink value



Or it can be fixed updating table - spt\_quick\_link\_options (delete those rows which have NULL in quicklink column)

SELECT TOP (1000) [id] ,[quick\_link] FROM IIQ\_PQA01].[IIQ\_PQA01].[spt\_quick\_link\_options] where [quick\_link] is null;

delete FROM [IIQ\_PQA01].[IIQ\_PQA01].[spt\_quick\_link\_options] where [quick\_link] is null;

### Unexpected behaviour in AD provisioning && aggregation and other similar issue –

Reason- Accelerator pack default files were not imported.

**Fix** – We have to make sure to import files in right order

1. import init.xml
2. import init-lcm.xml
3. init-acceleratorpack.xml
4. Import sp.init-custom.xml (must be the last to import otherwise customizations may be overwritten by default files)

### Variables not substituted with values in email templates

**Reason** – Email Template had few variables given as **$variableName** (which is a VLT syntax) and few as **$( variableName)**

***VTL vs. $(variableName) Notation***

*The VTL reference syntax must not be confused with the $(variableName) notation used for variable referencing in other IdentityIQ XML objects, such as Workflows. Velocity does not recognize this syntax and is unable to parse text that uses it. When IdentityIQ detects this syntax in any element of an email template, that portion of the message is not passed to Velocity for rendering at all. Instead, its contents are rendered by a simpler mechanism that is capable of doing the variable substitution based on the template's arguments. However, none of the Velocity directives are interpreted. Any Velocity commands included in the same element with a variable that uses the $(variableName) notation is treated as normal text and printed as-is in the final message.*

#### CSRF error –

**Reason** - comes when e-fixes do not match with IIQ version.

**Solution** - Deploy latest e-fixes.

#### SQL Error: 207, SQLState: S0001, Invalid column name 'extended5'

*2021-09-01T11:05:59,264 WARN QuartzScheduler\_Worker-5 engine.jdbc.spi.SqlExceptionHelper:137 - SQL Error: 207, SQLState: S0001  
2021-09-01T11:05:59,264 ERROR QuartzScheduler\_Worker-5 engine.jdbc.spi.SqlExceptionHelper:142 - Invalid column name 'extended5'.*

**Reason** – seems some index got removed/missed during upgrade.

**Solution** –

* Run command – iiq extendedSchema (to generate extended DB scripts)
* Run the scripts in database.

#### Unable to instantiate EmailNotifier: sailpoint.services.standard.emailnotifier.enhanced.EnhancedNotifier

**Fix-** Check services folder under –

*C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\identityiq\WEB-INF\classes\sailpoint\services\standard\emailnotifier\enhanced*

Make sure services folder is in place along with all its classes.

#### Invalid path : lcmFileUploadRenderer.xhtml

**Cause** – occurred due to change in Access Request business process.

**Fix** – LCM business processes should be selected as configured.

### Extra attention during upgrade –

1. Must merge our changes done in Accelerator pack files with the new version.
2. Verify the events after upgrade

# Validation after upgrade IIQ8.3

* + On the Login page of IdentityIQ we could see the version updated to 8.3 in about of debug page.
  + Verify if we are able to login to IdentityIQ
  + Navigate through different tabs on the UI and verify if the pages load correctly.
  + Go to Debug page, Debug 🡪 About and verify if the version is updated to 8.3.
  + Validate new Features “*Role Discovery and Access Modeling Using AI Services*”.
  + Validate new Features “ *Reporting Enhancement* “.
  + Validate new Features “ *Enhancements to Advanced Analytics* “.
  + Validate new Features “*Require Comment on Access Requests and Approvals*“.
  + Validate new Features “*Privileged Access Management (PAM) Enhancements*“.
  + Validate new Features “ *Scalability Enhancements* “.

# High level test steps after upgrade

|  |  |
| --- | --- |
| **#** | **UseCase** |
| 1 | Rules |
| 2 | Workflows |
| 3 | Identity Mappings |
| 4 | Entitlement extended attributes |
| 5 | Account Mappings |
| 6 | Version |
| 7 | Admin Account Creation |
| 8 | Service Account Creation |
| 9 | Access Request |
| 10 | Group Management |
| 11 | Joiner |
| 12 | Rehire |
| 13 | LOA |
| 14 | HOLD |
| 15 | Furlough |
| 16 | LOA/HOLD/Furlough to rehire |
| 17 | Leaver |
| 18 | Lifecycle Events (only currently active ones should be enabled) |
| 19 | Application & test connection & Aggregation |
| 20 | Entitlement & group aggregation of AD |
| 21 | Reports |
| 22 | Certification |
| 23 | Scheduled task |
| 24 | Full Text Index Refresh |
| 25 | Contractor creation |
| 26 | Contractor termination |
| 27 | Role |
| 28 | password reset |
| 29 | account unlock |