



NetIQ® Identity Manager 4.8 Service Pack 5 Release Notes

February 2022

Legal Notice

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

Copyright (C) 2022 NetIQ Corporation. All rights reserved.

Contents

About this Book	5
1 What's New and Changed?	7
New Features and Enhancements	7
Platform Support	7
Enhancements in Identity Applications	7
Enhancements in Identity Manager Containers	8
Component Updates	8
Identity Manager Component Versions	8
Updates for Dependent Components	9
Third-Party Component Versions	9
What's Deprecated and Marked for Removal?	10
Designer Deprecates Support for PAM Driver 4.8 Packages	10
Identity Applications Deprecates Support for Custom Context	10
Software Fixes	11
Installation and Upgrade	11
Identity Applications	11
Identity Reporting	13
Designer	13
2 Installing or Updating to This Service Pack	15
3 Known Issues	17
java.lang.UnsatisfiedLinkError Reported When Installing Identity Manager 4.8.5 on Windows Server 2016	17
Unable to Create a Data Synchronization Policy on Microsoft Azure	17
An Error is Displayed While Trying to Access SSPR as an Administrator	19
Resource Approval Form Displays Duplicate Entitlement Values	20
Clients are Unable to Access Identity Applications After the Domain Controller is Restored to Service	21

About this Book

NetIQ Identity Manager 4.8 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 NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product and the latest release notes are available on the NetIQ Web site on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the [Identity Manager Documentation Website](#).

1 What's New and Changed?

Identity Manager 4.8.5 provides the following key features, enhancements, and fixes in this release:

- ♦ [“New Features and Enhancements” on page 7](#)
- ♦ [“Component Updates” on page 8](#)
- ♦ [“What’s Deprecated and Marked for Removal?” on page 10](#)
- ♦ [“Software Fixes” on page 11](#)

New Features and Enhancements

Identity Manager 4.8.5 provides the following key functions and enhancements in this release:

- ♦ [“Platform Support” on page 7](#)
- ♦ [“Enhancements in Identity Applications” on page 7](#)
- ♦ [“Enhancements in Identity Manager Containers” on page 8](#)

Platform Support

In addition to the existing operating systems (OS), this service pack provides support for the following OS:

- ♦ Red Hat Enterprise Linux (RHEL) 8.5
- ♦ SUSE Linux Enterprise Server (SLES) 15 SP3
- ♦ Windows Server 2022
- ♦ macOS Monterey (version 12) for Designer on the Intel Macs

Enhancements in Identity Applications

Identity Applications includes the following enhancement:

Introduction of a New Configuration Property Key to Disable Nested Group Search

When retrieving the access permissions of a user, Identity Applications looks for the group membership attribute and displays all permissions granted to that user by direct group assignment and through nested group membership. This functionality is enabled by default. However, if you wish to disable the default nested group search and have it only check for direct group assignments, add the following property to the `ism-configuration.properties` file and restart Tomcat:
`DirectoryService/realms/jndi/params/USE_NESTED_GROUPS=false`

New Property Introduced In the Roles and Resource Service Driver

A new parameter is added to the Role and Resource Service Driver that lets you to configure how the driver handles MOT transactions. By default, when a role is assigned to a dynamic group, the driver uses Multi Object Transaction (MOT) to update multiple attributes of the user and group entities using a single thread. However, if you want to enable parallel processing of multiple threads at the same time, set the value of the **Disable Dynamic Group evaluation in a single MOT transaction** property to `true` in the driver configuration wizard.

Extended Functionality of the User Application Driver's Enable `oidpInstanceData` attribute clean-up Property

The **Enable `oidpInstanceData` attribute clean-up** property now provides enhanced functionality. In addition to the `oidpInstanceData` attribute cleanup, this property now handles the `DirXML-EntitlementResult` cleanup.

By default, the entitlement result that caused an event is purged from the `DirXML-EntitlementResult` attribute after notifying the User Application driver. Starting with this release, if the entitlement results are not purged and continue to increase in number, the driver will delete them from the `DirXML-EntitlementResult` attribute when its value reaches 5000 or greater.

Enhancements in Identity Manager Containers

This release allows you to deploy Identity Manager containers on Azure cloud service provider. The deployment of Identity Manager containers is automated with the help of Terraform and Helm charts. For more information, see [Deploying Identity Manager Containers on Microsoft Azure](#) in the *NetIQ Identity Manager 4.8.5: Installation and Upgrade Guide*.

Component Updates

This section provides details on the component updates.

Identity Manager Component Versions

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

- ◆ Identity Manager Engine 4.8.5
- ◆ Identity Manager Remote Loader 4.8.5
- ◆ Identity Applications 4.8.5
- ◆ Identity Reporting 6.6.8

- ♦ Identity Manager Designer 4.8.5
- ♦ Identity Manager Fan Out Agent 1.2.6
- ♦ Identity Analyzer 4.8.5

Updates for Dependent Components

This release adds support for the following dependent components:

- ♦ NetIQ eDirectory 9.2.6
- ♦ NetIQ iManager 3.2.6
- ♦ NetIQ One SSO Provider (OSP) 6.5.3
- ♦ Sentinel Log Management for IGA 8.5.0.1

Third-Party Component Versions

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

- ♦ Azul Zulu 1.8.0_312
- ♦ Apache Tomcat 9.0.55-1
- ♦ PostgreSQL 12.7
- ♦ OpenSSL 1.0.2za
- ♦ Nginx 1.21.3
- ♦ ActiveMQ 5.15.15

NOTE: ♦The current log4j 2.17.1 version is now supported by the following Identity Manager components:

- ♦ Identity Manager Engine
- ♦ Identity Manager Remote Loader
- ♦ Identity Applications
- ♦ Identity Reporting
- ♦ Identity Manager Designer
- ♦ Identity Analyzer
- ♦ Identity Manager Fan Out Agent
- ♦ The current version of ActiveMQ 5.15.5, which uses log4j 1.2.17, is not impacted by log4j vulnerabilities. For more information, refer to the [Apache ActiveMQ update](#) page.
- ♦ Legacy form is now updated to jQuery 3.5.1. This version supersedes the previously supported 2.0.3 version. Between version 2.0.3 and 3.5.1, jQuery stopped supporting a few APIs and announced deprecation of a few others. As a result, existing workflows with legacy forms using outdated jQuery functions will throw an error after upgrading to Identity Manager 4.8.5. You must replace these functions manually and re-deploy the forms from Designer. For a detailed

information on this issue and the suggested workaround, see [Workflow Legacy Forms Displaying Errors After Upgrading to Identity Manager 4.8.5 Version](#) in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

- ◆ The supported version of the Universal CEF collector is the same as Identity Manager 4.8.4. For more information on the supported versions for these components, see [Third-Party Component Versions](#) in the *NetIQ Identity Manager 4.8 Service Pack 4 Release Notes*.
-

What's Deprecated and Marked for Removal?

Identity Manager deprecates the following features or functionalities:

- ◆ [Designer Deprecates Support for PAM Driver 4.8 Packages](#)
- ◆ [Identity Applications Deprecates Support for Custom Context](#)

Designer Deprecates Support for PAM Driver 4.8 Packages

This release deprecates the following PAM driver packages:

- ◆ NOVLPUMBASE - 4.8.0.20190801142309
- ◆ NOVLPUMCFG - 4.8.0.20190801160509
- ◆ NOVLPUMENT - 4.8.0.20190801160528
- ◆ NOVLPUMMSINF - 4.8.0.20190801160545
- ◆ NOVLPUMPWD - 4.8.0.20190801160557

NOTE: Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

Identity Applications Deprecates Support for Custom Context

Custom context will be deprecated in the next Identity Manager Service Pack release. NetIQ recommends using the default `IDMProv` deployment context. If you are using custom context in your deployment and keeping the same after upgrade, you may observe the following issues:

- ◆ The **Roles** and **Self tasks** widgets on the Dashboard will not display any data. Because the REST API URL for these widgets use the default `IDMProv` context.
- ◆ Workflows with Role Request Activity and Resource Request Activity will fail if custom context is used. For more information, see [NetIQ Identity Manager 4.8 Service Pack 2 Release Notes \(https://wwwtest.netiq.com/documentation/identity-manager-48/releasenotes_idm482/data/t4klbif9iix3.html\)](https://wwwtest.netiq.com/documentation/identity-manager-48/releasenotes_idm482/data/t4klbif9iix3.html).

Software Fixes

NetIQ Identity Manager includes software fixes for the following components:

- ♦ [“Installation and Upgrade” on page 11](#)
- ♦ [“Identity Applications” on page 11](#)
- ♦ [“Identity Reporting” on page 13](#)
- ♦ [“Designer” on page 13](#)

In addition, this service pack resolves security vulnerability CVE-2022-26329 which addresses a potential information disclosure vulnerability in Identity Manger versions prior to 4.8.5. Special thanks go to Kajetan Rostojek for responsibly disclosing this information to us.

Installation and Upgrade

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

Ability to Save Email Template with Image Successfully

This release allows you to edit and save an email template with an image file referenced in the HTML without displaying any errors. (Bug 380030)

Identity Applications

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

Ability to Map a Static Resource to a Role Successfully

Mapping a static resource with administrator-assigned values to a role works as expected. Identity Applications no longer return a null pointer exception. (Bug 317258)

Activity.getUser() Expression Used to Map Data Items in an Approval Activity Works as Expected

Identity Applications successfully evaluates the `Activity.getUser()` expression in an approval activity and moves the form data into the target flowdata field, without logging error or failure messages in the `catalina.out` event logs. (Bug 381158)

Request to the getWorkEntriesRequest SOAP API Return Work Details for All Addressees in the Query

The `getWorkEntriesRequest` SOAP Endpoint has been updated to handle the request and returns the appropriate responses for all addressees, even if work entries for one or more addressees are missing or an addressee’s Fully Qualified Distinguished Name (FQDN) does not exist. (Bug 438023 and 438024)

Workflows with Legacy Forms Loading Properly

With the latest version of Tomcat 9.0.55-1 bundled with Identity Manager 4.8.5, there is no longer any delay while loading workflows with legacy forms on the Identity Applications Dashboard. (Bug 450031)

Roles and Resource Names with a Colon Sign is Now Correctly Listed in the Search Results

Dashboard now takes the colon sign into account when searching for entities such as roles, resources, and permissions, and displays the search results correctly. (Bug 328633)

Identity Applications No Longer Takes Time to Retrieve the Client Configurations of a Logged-in User

Identity Applications promptly retrieves the client configurations of a logged-in user via the `users/userDefaults` REST API, even if a custom `groupMembership` attribute is added to the user entity. (Bug 329642)

Identity Applications Validates and Loads the Extended Session Based on the User Credentials

When a Dashboard session is extended with a different credential, the previous session is closed, and a new session based on the new user credentials is launched. (Bug 367148)

Request to the `getWorkEntriesRequest` SOAP Endpoint Return Work Details Without Errors

The `getWorkEntriesRequest` SOAP endpoint has been updated to successfully return the work details in response to a query with an array of addressees. (Bug 379272)

Slow Loading of the Dashboard and Applications Pages Is Now Fixed

After upgrading to Identity Manager 4.8.5, the **Dashboard** and **Applications** pages load seamlessly (without a delay), regardless of the number of applications assigned to a user. (Bug 383012)

Resource Assignments Search Functionality Return Accurate Search Results

The search functionality is updated to search all resource assignments in the application and provide accurate search results based on the search criteria. (Bug 328314)

Ability to Send an Image in the Email Notification Works as Expected

When an email server is configured to use SMTP TLS for secure transmission, the attached or embedded image in the email is displayed successfully. (Bug 348018)

Identity Applications Checks the Entity Type in IDVault.get() Function to Retrieve an Entity's Attribute Values Correctly

When using the `IDVault.get()` function in a new JSON form, Identity Applications will validate the entity type in the same way that they did in legacy forms. (Bug 360020)

Role Assignments Search Functionality Return Accurate Search Results

The search functionality is updated to search all role assignments in the application and provide accurate search results based on the search criteria. (Bug 405005)

Dashboard Creates Resources for Administrator-Defined Entitlements Correctly

When creating a resource for an administrator-defined entitlement type, Dashboard displays the **Resource Description** text box correctly. Identity Applications then creates an eDirectory resource object with appropriate values for all resource attributes. (Bug 328129)

Users Can be Seamlessly Migrated From One Organization Unit to Another With No Errors

The migration of users from one organization unit to another is working as expected. Users can perform their tasks successfully after the migration. Identity Applications no longer display errors in the `catalina.out` event logs. (Bug 340041)

Identity Reporting

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

Successfully Starts the DCS Driver Using DCS Public Key Certificate

The updated driver option enables Data Collection Service Driver to start and synchronize with the service. (Bug 325011)

Issue to Store the Managerid Instead of DN Value in the Identity Information Database

Identity Reporting is updated to successfully handle manager id in the Reporting Identity table. (Bug 441087)

Designer

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

Configuring Authentication Method to OAuth2 Mandates REST Auth URL

REST Auth URL is a mandatory field only when you configure the authentication method as OAuth2. When configured as Basic, the Designer does not display REST Auth URL field. (Bug 389026)

Issue Importing Driverset Servers while Importing Designer from Identity Vault

Designer import from Identity Vault no longer ignores importing servers associated with driverset. (Bug 327242)

Allows to Successfully Initiate do-invoke-rest-endpoint Action

This release updates the Designer to use appropriate request type attribute for do-invoke-rest-endpoint action. (Bug 379452)

Introduces Text Box for Local Variable Field to Provide Tab Support

The 4.8.5 release updates local variable field in the argument builder to text box. (Bug 414434)

Ability to Export Schema Attributes With a Colon in Class Name Successfully

The 4.8.5 release enables Designer to reconcile successfully when you add schema class name that contains a colon. (Bug 441037)

2 Installing or Updating to This Service Pack

For information on installing or updating to this service pack, see the [NetIQ Identity Manager 4.8.5: Installation and Upgrade Guide](#).

3 Known Issues

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

- ♦ [“java.lang.UnsatisfiedLinkError Reported When Installing Identity Manager 4.8.5 on Windows Server 2016” on page 17](#)
- ♦ [“Unable to Create a Data Synchronization Policy on Microsoft Azure” on page 17](#)
- ♦ [“An Error is Displayed While Trying to Access SSPR as an Administrator” on page 19](#)
- ♦ [“Resource Approval Form Displays Duplicate Entitlement Values” on page 20](#)
- ♦ [“Clients are Unable to Access Identity Applications After the Domain Controller is Restored to Service” on page 21](#)

java.lang.UnsatisfiedLinkError Reported When Installing Identity Manager 4.8.5 on Windows Server 2016

Issue: While updating identity applications to 4.8.5 on Windows Server 2016, an unexpected fatal error: `java.lang.UnsatisfiedLinkError` is reported, resulting in installation failure. It occurs when the installer is unable to locate the `msvcr100.dll` file locally. The `msvcr100.dll` is a part of the Microsoft Visual C++ 2010 Redistributable Package and is required for the application to function properly on a Windows server. In a distributed server configuration, where the identity applications run on one server and the database on another, the Microsoft Visual C++ 2010 Redistributable Package is not installed on the application server, resulting in this error. (Bug 516149)

Workaround: To fix the error, install the Microsoft Visual C++ 2010 Redistributable Package, which contains the `msvcr100.dll` file. The package is available for download on the [Microsoft download website \(https://www.microsoft.com/en-in/download/details.aspx?id=26999\)](https://www.microsoft.com/en-in/download/details.aspx?id=26999).

Unable to Create a Data Synchronization Policy on Microsoft Azure

Issue: In Microsoft Azure, when the reporting database is SSL enabled, you might see the following exception in `catalina.out` while creating data synchronization policy in Identity Manager Data Collection Services web user interface:

```
org.postgresql.util.PSQLException: FATAL: no pg_hba.conf entry for host
"52.151.202.8", user "postgres", database "idmrptdb", SSL off
```

```
at
```

```
org.postgresql.core.v3.ConnectionFactoryImpl.doAuthentication(ConnectionFa
ctoryImpl.java:443)
```

```
at
```

```
org.postgresql.core.v3.ConnectionFactoryImpl.openConnectionImpl(Connection
FactoryImpl.java:217)

    at
org.postgresql.core.ConnectionFactory.openConnection(ConnectionFactory.jav
a:52)

    at org.postgresql.jdbc.PgConnection.<init>(PgConnection.java:216)

    at org.postgresql.Driver.makeConnection(Driver.java:404)

    at org.postgresql.Driver.connect(Driver.java:272)


(Defect 474021)
```

Workaround: Perform the following steps to resolve this issue:

To enable the SSL on the database in Sentinel:

- 1 Launch command line interface of Sentinel VM.
- 2 Navigate to the `/var/opt/novell/sentinel/3rdparty/postgresql/data/postgresql.conf` file and update the following values:
 - ◆ `listen_addresses = '*'`
 - ◆ `ssl = on`
- 3 Navigate to the `/var/opt/novell/sentinel/3rdparty/postgresql/data/pg_hba.conf` file and update the following value in **# IPv4 local connections: host all all 127.0.0.1/32 md5**.
`IPv4 local connections: hostssl all all 0.0.0.0/0 md5`
- 4 To restart the Sentinel, run the following command:
`rcsentinel restart`

To add a new data policy in the Identity Manager Data Collection Services user interface:

- 1 Log in to your connected system.
- 2 Click **Settings > Data Sync Policies**.
- 3 Click  .
- 4 Go to **Database Server Details**, and add the following value:
 - 4a Specify the following value for **Name**:
`idmrptdb?compatible=true&ssl=true`
 - 4b Specify the value for reporting database admin password obtained from key vault. Ensure you get the secret value from Azure portal.
To obtain the password, perform the following steps:
 - 4b1 Log in to Azure portal.
 - 4b2 Click your Resource group.
 - 4b3 Go to Resources, click the Key vault associated with your account.
 - 4b4 Go to **Settings > Secrets**, click `rptdbusersharepwd`.

4b5 Under Current Version, click printed value.

4b6 Click **Show Secret Value**.

5 Click **Create**.

After successfully updating all the required fields, a new data synchronization policy will be created in your database. For more information, refer to [Data Sync Policies](#).

An Error is Displayed While Trying to Access SSPR as an Administrator

Issue: When you are trying to access SSPR as an Administrator user, you might see the following error:

```
2022-01-20T08:01:15Z, FATAL, servlet.AbstractPwmServlet, {19,uaadmin}
unexpected error: 5027 ERROR_UNAUTHORIZED (admin privileges required)
```

This issue is specific to Identity Manager Docker container deployment on Azure. (Defect 479135)

Workaround: Perform the following steps to resolve this issue:

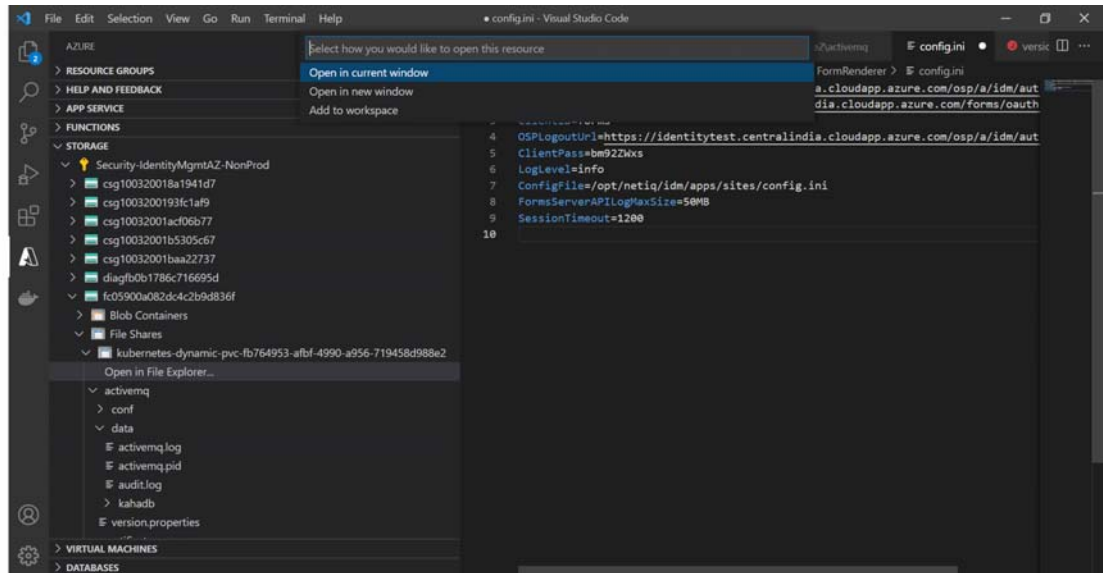
1 Log in to the Visual Studio Code application.

2 Click .

3 Go to **STORAGE > Security-IdentityMgmtAZ-NonProd > fc05900a082dc4c2b9d836f > File shares > Kubernetes dynamic pvc > Open in File Explorer > Open in current window**. Refer to [Figure 3-1 on page 20](#).

NOTE: In the above navigation path, the **Security-IdentityMgmtAZ-NonProd** and **fc05900a082dc4c2b9d836f** key is mentioned for your reference and would change as per your login credentials.

Figure 3-1 Visual studio code configuration view



4 Click `sspr > SSPRConfiguration.xml`.

5 Update the following values under Administrator Permission.

```
<value>{"ldapProfileID":"default","ldapQuery":"(objectClass=*)","ldapBase":"cn=admin,ou=sa,o=system"}</value>
```

```
<value>{"ldapProfileID":"default","ldapQuery":"(objectClass=*)","ldapBase":"cn=uaadmin,ou=sa,o=data"}</value>
```

6 Go to **File** menu, click **Save**.

After saving the changes, the system automatically triggers the deployment of SSPR containers with the updated values.

Resource Approval Form Displays Duplicate Entitlement Values

Issue: When a user requests a resource for multiple entitlements in a single request, the approver will see multiple copies of the same entitlement on the resource approval form. For example, a resource lists three options for Company Locations: Cambridge, MA 02440, Waltham, MA 02451, and Provo, UT 97288. If a user requests permission for all three locations in one request, the approval form displays the first location, Cambridge, MA 02440, three times. However, once the request is approved, the resource is successfully provisioned, and the user is assigned all selected entitlements. (Bug 469028)

Workaround: There is no workaround at this time. However, there is no loss of functionality due to this issue.

Clients are Unable to Access Identity Applications After the Domain Controller is Restored to Service

Issue: If Identity Applications is configured to use Kerberos authentication and the Domain Controller is unavailable for some reason, login to the Identity Applications will fail. This issue happens only when a client attempting to access Identity Applications requests a ticket from the Kerberos Key Distribution Center (KDC) while the Domain Controller is still unreachable. However, if the Domain Controller is restored to service before a client makes a request to the KDC, the issue is not seen. (Bug 492123)

Workaround: After the Domain Controller is restored, restart Tomcat on the Identity Applications server to allow clients to access Identity Applications. Execute the following command in the command prompt to restart Tomcat:

```
systemctl restart netiq-tomcat.service
```

