

NetIQ Identity Manager 4.8 Release Notes

October 2019



NetIQ Identity Manager 4.8 includes 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](#), our community Web site that also includes product notifications, blogs, and product user groups.

For information about what's new in previous releases, see the "Previous Releases" section in the [Identity Manager Documentation Web site](#).

For more information about this release and for the latest release notes, see the [Documentation page](#). To download this product, see the [Identity Manager Product Web site](#).

- ◆ [Section 1, "What's New and Changed?," on page 1](#)
- ◆ [Section 2, "Supported Component Versions," on page 8](#)
- ◆ [Section 3, "System Requirements," on page 9](#)
- ◆ [Section 4, "Installing NetIQ Identity Manager 4.8," on page 9](#)
- ◆ [Section 5, "Upgrading to NetIQ Identity Manager 4.8," on page 14](#)
- ◆ [Section 6, "Known Issues," on page 18](#)
- ◆ [Section 7, "Contact Information," on page 25](#)
- ◆ [Section 8, "Legal Notice," on page 26](#)

1 What's New and Changed?

The following sections outline the key features and functions provided by this version, as well as features that have been removed from the product, and issues resolved in this release:

- ◆ [Section 1.1, "New Features," on page 1](#)
- ◆ [Section 1.2, "Operating System Support," on page 6](#)
- ◆ [Section 1.3, "Fixed Issues," on page 6](#)
- ◆ [Section 1.4, "What's Changed, Deprecated, or Discontinued?," on page 8](#)

1.1 New Features

Identity Manager 4.8 provides the following key features, enhancements, and fixes in this release:

- ◆ [Section 1.1.1, "New Features in Identity Applications," on page 2](#)
- ◆ [Section 1.1.2, "Simplified Installation on Windows Platforms," on page 4](#)
- ◆ [Section 1.1.3, "Support for Containerizing Identity Manager Components," on page 4](#)
- ◆ [Section 1.1.4, "Simplified Packaging of Remote Loader Installation Files," on page 4](#)

- ♦ [Section 1.1.5, “Relocating the Client Settings Configuration,” on page 4](#)
- ♦ [Section 1.1.6, “Microsoft SQL Database Support for Identity Reporting,” on page 5](#)
- ♦ [Section 1.1.7, “Support for New Actions in Designer,” on page 5](#)
- ♦ [Section 1.1.8, “New Features in Designer,” on page 5](#)

For information about the new features in NetIQ Identity Manager Designer 4.8, see [NetIQ Identity Manager Designer 4.8 Release Notes](#).

There are no new features for NetIQ Identity Manager Analyzer 4.8 except the updated Java version. For more information, see [NetIQ Identity Manager Analyzer 4.8 Release Notes](#).

1.1.1 New Features in Identity Applications

Identity Applications provides the following new features:

1.1.1.1 New Workflow Form Builder

Identity Manager offers a new simplified tool for creating and managing forms for Provisioning Request Definitions. The tool has a simple and intuitive interface. It supports simple drag and drop features that enable you to quickly create and modify forms. The forms are stored in the JSON format under the `Workflow Forms` container in the User Application driver.

The Workflow Form Builder is integrated with Designer. You can launch it from the Workflow Forms container under User Application Driver in Designer. You are recommended to use the Workflow Form Builder for creating new forms.

Currently, there is no tool to migrate the legacy forms to the new forms. The only way to accomplish it is by manually creating a new form in the Workflow Form Builder and then mapping the data items to the new form. However, you can still continue to use the legacy forms. For more information, see the [NetIQ Identity Manager - User's Guide to Form Builder](#).

1.1.1.2 Add Workflow to Roles and Resources

Identity Manager introduces a new simplified method for adding a workflow to role and resource. The Identity Applications user interface includes a new option, namely **Add Workflow**, in the Roles and Resources pages, that allows you to add a workflow to the role and resource.

You can now quickly create a workflow in Identity Applications without switching to Designer. A set of pre-defined System Templates and Template Forms are available that you can use to add a workflow. It also provides option to add workflow based on custom templates created in Designer.

The Add Workflow user interface is illustrative, easy-to-understand with a step-by-step wizard based workflow creation process. This new method is targeted to ease the user experience of creating workflows. For greater flexibility and ease of use, NetIQ recommends that you use this method whenever possible. For more information, see [Adding Workflow to Roles and Resources](#) in the [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#).

1.1.1.3 Access to Identity Governance

Identity Manager introduces a new entry named Identity Governance Settings under the **Configuration** tab of Identity Manager Dashboard. This is a step towards ease of integration between Identity Applications and Identity Governance. This will enable you to request and approve both Identity Manager and Identity Governance permissions at a single place.

The Identity Governance Settings page also enables you to configure the Workflow Engine as a common request and approval service for Identity Applications and Identity Governance. For more information, see [Configuring the Identity Governance Settings](#) in the [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#).

1.1.1.4 Workflow Engine as a Separate Service

Identity Manager provides Workflow Engine as a separate service. This Workflow Engine will replace the Workflow Engine that was embedded with the Identity Applications in the previous versions of the product. This change is targeted to enable the Workflow Engine to execute business process definitions at runtime from Identity Applications and Identity Governance and act as a common request and approval service for both products.

By default, the Workflow Engine is installed as part of Identity Applications installation. The Workflow Engine persists the workflow state information in a new database named `igaworkflowdb`. If an existing workflow process is in a running state, its data is moved to `igaworkflowdb` before the new Workflow Engine starts managing it. The Identity Applications installer copies the data from the Identity Applications database `idmuserappdb` to `igaworkflowdb`.

The Workflow Engine uses REST service to obtain the tasks and workflow history from the Workflow Engine service. The Identity Applications installation program automatically registers the Workflow Engine service as a client with One SSO Provider (OSP) to ensure communication with other Identity Applications components. The installer stores these connection and authentication properties in the `ism-configuration.properties` file. For more information, see [Workflow Service](#) in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

1.1.1.5 Managing the State of In-Progress Workflows

Identity Manager enables you to pause and resume in-progress workflows through REST APIs. This is typically useful when you want to upgrade your workflow database without losing the workflow states. The workflow migration APIs perform the following tasks:

- 1 Stops the Workflow Engine and pauses the running workflows. It cannot process any new requests in this state.
- 2 Calls the **Export** REST API that reads the workflow state information and writes it to a JSON file for each table. It then zips all these JSON files and returns them as a response.
- 3 Calls **Import** REST API that imports the data from the zipped JSON files that were created by the **Export** REST API.
- 4 Resumes the Workflow Engine service to process the running workflows and handle new requests.

Alternatively, use the console-based migration tool from `<LINUX_ISO>/user_application/IDM_Tools/WorkflowMigrationAPI.zip` and `<WINDOWS_ISO/IdentityApplications/IDM_Tools/WorkflowMigrationAPI.zip`. The tool includes a silent properties file where you can specify the details about the source and destination workflow database servers. It internally uses the same REST APIs as mentioned in the above procedure to migrate the workflow states from the source server to the destination server.

1.1.1.6 Support for New Localized Languages for Identity Applications

The end-user screens of Identity Applications support Czech and Norwegian as translation languages.

For more information about the supported translation languages, see [Translated Components and Installation Programs](#) in the *NetIQ Identity Manager Overview and Planning Guide*.

1.1.1.7 IDVault.get and IDVault.globalQuery Functions

Identity Manager introduces new functions `IDVault.get` and `IDVault.globalQuery` of the workflow script engine to obtain the values of multiple attributes.

For more information about these new functions, see [User Application API](#) in the *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*.

1.1.2 Simplified Installation on Windows Platforms

Identity Manager offers a new simplified installation program for Windows platforms. The new installation program provides a concise method for installing Identity Manager components in graphical user interface (GUI) mode.

Identity Manager provides a wizard-based installation method for installing and configuring the following Identity Manager components:

- ◆ Identity Manager Server
- ◆ Identity Applications
- ◆ Identity Reporting

The new installer introduces typical and custom configuration modes. A typical configuration uses common defaults for most values and is suitable for quickly installing the product. Custom configuration is suited for production environments. For more information, see the [NetIQ Identity Manager Setup Guide for Windows](#)

1.1.3 Support for Containerizing Identity Manager Components

We are shipping a preview version of Docker Container-based deployment with Identity Manager 4.8 for customers to use and provide feedback. Customers willing to deploy containers in a production environment will be supported only with a Professional Services engagement.

1.1.4 Simplified Packaging of Remote Loader Installation Files

This version provides simplified packaging of Remote Loader in a separate ISO for Linux and Windows operating systems. You can now install this component separately instead of installing it from the Identity Manager ISO file. This change is aimed at easing the installation experience of this component. The configuration process continues to remain the same as prior versions. The file names are:

- ◆ **Linux:** Identity_Manager_4.8_RL_Linux.iso
- ◆ **Windows:** Identity_Manager_4.8_RL_Windows.iso

For more information, see the [Installing Remote Loader in the NetIQ Identity Manager Setup Guide for Linux](#) and [Installing Java Remote Loader in the NetIQ Identity Manager Setup Guide for Windows](#).

1.1.5 Relocating the Client Settings Configuration

Identity Applications allow you to customize UI settings, behavior, branding, and access to the application through the client settings. The client settings configuration includes branding settings, custom CSS, access settings, and custom behaviors. A single Identity Applications instance can have multiple client settings and different sets of users can map to different clients. The client settings configuration is saved either in the Identity Applications database or on the file system as part of application configuration. This release allows you to relocate the client settings configuration between the database and the file system through a migration tool named `MigrationSettings`. You can use this tool to perform the following tasks:

- ◆ Transfer settings from one Identity Manager instance to another. For example, transfer setting from your staging server to the production server.
- ◆ To migrate client settings when storage option is changed from file to database or vice versa.
- ◆ Take a backup of all client settings and restore the settings later.

The migration tool is located in the ISO files at <LINUX_ISO>/user_application/IDM_Tools and <WINDOWS_ISO>/IdentityApplications/IDM_Tools. For more information, see [Copying the Client Settings](#) in the [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#).

1.1.6 Microsoft SQL Database Support for Identity Reporting

With this release, the Microsoft SQL Database support is extended for the Identity Reporting component.

1.1.7 Support for New Actions in Designer

This release adds support for the following actions in Designer's Policy Builder. For more information, see the respective documentation links.

- ◆ [Delete Resource](#)
- ◆ [Delete Role](#)
- ◆ [If Operation Entitlement](#)
- ◆ [Invoke REST Endpoint](#)
- ◆ [Modify Resource](#)
- ◆ [Modify Role](#)
- ◆ [Remove Named Password](#)
- ◆ [Set Named Password](#)

1.1.8 New Features in Designer

Designer provides the following new features:

1.1.8.1 Using Git for Package Version Control

Identity Manager introduces Git, an open source version control system, for managing versions of packages in Designer. Git allows you to manage, track, maintain the history of changes, or retrieve an earlier state or compare different states of packages with speed and efficiency. For more information, see [Managing Package Versions Using Git](#) in the [NetIQ Designer for Identity Manager Administration Guide](#).

1.1.8.2 Support for Creating Forms using the new Workflow Form Builder

Identity Manager introduces a new tab named **JSON Forms** in the Provisioning Request Definition editor of Designer for creating and managing forms in the new Workflow Form Builder. The forms that are created using this tab are saved in the JSON format. After creating the form, you can associate the form with a Provisioning Request Definition. For more information, see the [NetIQ Identity Manager - User's Guide to Form Builder](#).

For more information about working with the **JSON Forms** tab, see the [Guide to New Features in Designer](#).

1.1.8.3 Performance Improvement

To improve the performance of Designer, the following changes have been made to the Designer software:

- ♦ To improve the speed of launching Designer, the legacy driver configuration files are no longer a part of the Designer startup script. Instead, these files are included in a separate plug-in located in the Designer installation package. You must manually load the configuration files from the plug-in for the drivers needed in your environment.
- ♦ Designer enables you to manage the installed packages in your Identity Manager environment to help you keep only the required packages in your environment.

The Manage Package window is displayed when Designer is launched for the first time. Alternatively, navigate to **Help > Manage Packages**. For more information, see [Managing Installed Packages](#) in the *NetIQ Designer for Identity Manager Administration Guide*.

- ♦ Due to high memory consumption, expanding User Application Driver in the **Outline** view is no longer supported in 4.8 release and onwards. Use the **Provisioning** view to make any changes to User Applications objects.

1.2 Operating System Support

This release adds support for the following platforms:

- ♦ SUSE Linux Enterprise Server (SLES) SLES 12 SP4, SLES 15, and SLES 15 SP1
- ♦ Red Hat Enterprise Linux (RHEL) 7.5, RHEL 7.6, and RHEL 8
- ♦ Open Enterprise Server (OES) 2018 SP2
- ♦ Microsoft Windows Server 2016, 2019

For a complete list of supported operating systems, see the [Identity Manager System Requirements](#) page. For information about the components packaged, databases, and browsers supported with this release, see [Section 2, "Supported Component Versions,"](#) on page 8.

1.3 Fixed Issues

This release includes the following software fixes:

- ♦ [Section 1.3.1, "Ability to Return Values for More than One Attribute Using the IDVault.get And IDVault.globalQuery Functions,"](#) on page 7
- ♦ [Section 1.3.2, "Dashboard Correctly Displays the Permissions When the Permission name Contains Special Characters,"](#) on page 7
- ♦ [Section 1.3.3, "Creation of Role Succeeds When a Workflow is Created,"](#) on page 7
- ♦ [Section 1.3.4, "OSP Search Filter Includes objectClass=User when SAML Authentication is Used,"](#) on page 7
- ♦ [Section 1.3.5, "Improved Performance While Comparing Two User Application Drivers in Designer,"](#) on page 7
- ♦ [Section 1.3.6, "Designer Successfully Authenticates When the LDAP Server Uses Certificates Signed by An External Certificate Authority,"](#) on page 7
- ♦ [Section 1.3.7, "Successfully Re-installs Identity Applications After an Uninstallation,"](#) on page 7
- ♦ [Section 1.3.8, "Ability to Update Designer Successfully When Palette Extensions are Installed,"](#) on page 7
- ♦ [Section 1.3.9, "Events Originating from the DXEvent Module Does Not Contain Encrypted Information,"](#) on page 7

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

It is now possible to obtain values of multiple attributes using the IDVault.get and IDVault.globalQuery functions (Bug 1146109)

1.3.2 Dashboard Correctly Displays the Permissions When the Permission name Contains Special Characters

When you search for permissions that contains special characters, the Dashboard successfully displays the correct results. (Bug 1101866)

1.3.3 Creation of Role Succeeds When a Workflow is Created

When you create a workflow having an integration activity, then the role is created successfully. (Bug 1122158)

1.3.4 OSP Search Filter Includes objectClass=User when SAML Authentication is Used

The search filter in OSP has been enhanced to include the objectClass=User when SAML authentication method is used. (Bug 1133744)

1.3.5 Improved Performance While Comparing Two User Application Drivers in Designer

The response time for comparing two User Application driver has been improved. (Bug 1099198)

1.3.6 Designer Successfully Authenticates When the LDAP Server Uses Certificates Signed by An External Certificate Authority

You can now use certificates signed by an external certificate authority for LDAP server authentication. (Bug 1127233)

1.3.7 Successfully Re-installs Identity Applications After an Uninstallation

Identity Applications can now be successfully re-installed after an uninstallation. (Bug 1119806)

1.3.8 Ability to Update Designer Successfully When Palette Extensions are Installed

When you are performing an update of Designer, a new pop-up message is introduced for backing up the customized plug-ins. (Bug 1139932)

1.3.9 Events Originating from the DXEvent Module Does Not Contain Encrypted Information

The DXEvent module has been enhanced to display all the DXEvent events that contain a command XML. (Bug 1112724)

1.4 What's Changed, Deprecated, or Discontinued?

To streamline functionality, several items have changed or are no longer supported with Identity Manager 4.8. In many cases, alternative functionality replaces the items that are no longer supported.

1.4.1 Deprecated Features or Functionality

This release does not support the Identity Manager Driver for Office 365. NetIQ recommends you to use the Identity Manager Driver for Azure Active Directory and provides a method to transition to the Azure Active Directory driver. For more information on transitioning from Office 365 driver to Azure driver, see the [NetIQ Identity Manager Driver Implementation Guide for Azure Active Directory](#).

1.4.2 Discontinued Features or Functionality

Auditing with NAudit and XDAS for the Identity Manager components is discontinued from this release. NetIQ recommends that you move to CEF auditing before upgrading to 4.8. For more information, see [NetIQ Identity Manager - Configuring Auditing in Identity Manager](#).

2 Supported Component Versions

- ◆ [Identity Manager Component Versions](#)
- ◆ [Third-Party Component Versions](#)
- ◆ [Database](#)
- ◆ [Web Browser](#)

2.1 Identity Manager Component Versions

Identity Manager 4.8 bundles the following components:

- ◆ NetIQ eDirectory 9.2
- ◆ NetIQ iManager 3.2
- ◆ NetIQ Identity Manager Engine 4.8
- ◆ NetIQ Identity Manager Remote Loader 4.8
- ◆ NetIQ Identity Manager Fanout Agent 1.2.2
- ◆ NetIQ Designer for Identity Manager 4.8
- ◆ NetIQ Identity Applications 4.8
- ◆ NetIQ Single Sign-on (One SSO) 6.3.6
- ◆ NetIQ Identity Manager Self-Service Password Reset 4.4.0.3
- ◆ NetIQ Identity Manager Client Login Extension 4.2
- ◆ NetIQ Identity Manager Identity Reporting 6.5
- ◆ NetIQ Sentinel Log Management for IGA 8.2.2 (for event auditing)
- ◆ NetIQ Analyzer for Identity Manager 4.8
- ◆ NetIQ Identity Manager drivers. For driver versions, see the [NetIQ Identity Manager Drivers](#) page.

NOTE: The Identity Manager driver versions are independent of the engine version and do not indicate the minimum engine version required for a driver to run.

2.2 Third-Party Component Versions

This release adds support for the following dependent components:

- ♦ Azul Zulu 1.80_222
- ♦ OpenSSL 1.0.2r-33
- ♦ Apache Tomcat 9.0.22-1
- ♦ PostgreSQL 9.6.12
- ♦ Apache ActiveMQ 5.15.9

2.3 Database

In addition to PostgreSQL 9.6.12, this release adds support for the following databases:

- ♦ Oracle 18c (only for Identity Applications)
- ♦ MS SQL 2017

2.4 Web Browser

Any of the following browsers, at a minimum:

- ♦ Google Chrome 77
- ♦ Mozilla Firefox 68
- ♦ Apple Safari 12
- ♦ Microsoft Edge 44

3 System Requirements

For information about hardware requirements and supported operating systems, see the [Identity Manager System Requirements](#) page.

4 Installing NetIQ Identity Manager 4.8

Identity Manager 4.8 provides Advanced Edition and Standard Edition in a single ISO file. Before downloading the installation files, you must understand what features are contained in each edition and the options for downloading the Identity Manager components.

- ♦ [Section 4.1, “Features Supported with Identity Manager Advanced and Standard Editions,” on page 10](#)
- ♦ [Section 4.2, “Downloading Identity Manager,” on page 10](#)
- ♦ [Section 4.3, “Locating the Executables and Default Installation Paths,” on page 11](#)
- ♦ [Section 4.4, “Installing NetIQ Identity Manager 4.8,” on page 13](#)

4.1 Features Supported with Identity Manager Advanced and Standard Editions

To meet different customer needs, the Identity Manager functionality is delivered in two product groups:

- ◆ Identity Manager Advanced Edition
- ◆ Identity Manager Standard Edition

Identity Manager features provided with Identity Manager Standard Edition are also included in Identity Manager Advanced Edition, along with additional features. The following table provides a comparison of features available in Identity Manager Advanced and Standard Editions:

Feature	Advanced Edition	Standard Edition
Rule-based automated user provisioning	Yes	Yes
Real-time identity synchronization	Yes	Yes
Password management and password self-service	Yes	Yes
Uniform identity information tool (Analyzer)	Yes	Yes
REST APIs and single sign-on support	Yes	Yes (limited support)
Current state reporting	Yes	Yes
Role-based enterprise-level provisioning	Yes	No
Automated approval workflows for business policy enforcement	Yes	No
Advanced self-service in the identity applications	Yes	No
Resource model and catalog for easy resource provisioning	Yes	No
Historical state reporting	Yes	No
Connected systems reporting	Yes	No
Role and resource administration	Yes	No

4.2 Downloading Identity Manager

After you purchase Identity Manager 4.8, log in to the [Identity Manager Product Web site](#) and follow the link that allows you to download the software. The following files contain the Identity Manager components:

File Name	Description
Identity_Manager_4.8_Linux.iso	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration), Identity Applications, and Identity Reporting.
Identity_Manager_4.8_RL_Linux.iso	Contains the Identity Manager Remote Loader for Linux
Identity_Manager_4.8_Containers.tar.gz	Contains individual container images for Identity Manager Engine, Remote Loader, Fanout Agent, ActiveMQ, PostgreSQL, Form Renderer, OSP, Identity Applications, Identity Reporting, SSPR, and iManager (for SLES and Ubuntu platforms)
Identity_Manager_4.8_Windows.iso	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration), Identity Applications, and Identity Reporting.
Identity_Manager_4.8_RL_Windows.iso	Contains the 64-bit and .NET Remote Loader for Windows
Identity_Manager_4.8_Designer_Linux.tar.gz	Contains Designer for Linux platforms
Identity_Manager_4.8_Designer_Windows.zip	Contains Designer for Windows platforms
Identity_Manager_4.8_Designer_MacOSX.dmg	Contains Designer files for MacOS 10.14 (Mojave)
Identity_Manager_4.8_Analyzer_Linux.tar.gz	Contains Analyzer for Linux platforms
Identity_Manager_4.8_Analyzer_Windows.zip	Contains Analyzer for Windows platforms
SentinelLogManagementForIGA8.2.2.0.tar.gz	Contains Sentinel Log Management for Identity Governance and Administration (IGA)
	This installation is supported only on Linux.

- 1 Go to the [NetIQ Downloads website](#).
- 2 In the **Product or Technology** menu, select **Identity Manager** followed by **Version** from the drop-down list. Click **Search**.
- 3 On the **NetIQ Identity Manager Downloads** page, click the **Download** button next to the file that you want to download.
- 4 Follow the on-screen prompts to download the file to a directory on your computer.

4.3 Locating the Executables and Default Installation Paths

- ◆ [Executables and Default Installation Paths on Linux](#)
- ◆ [Executables and Default Installation Paths on Windows](#)

4.3.1 Executables and Default Installation Paths on Linux

Identity Manager Component	Location of the Executable within ISO	Default Installation Path
Identity Manager Server (Contains Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration)	install.sh in the mounted location	<ul style="list-style-type: none"> ◆ Engine: /opt/novell/eDirectory/lib/dirxml ◆ Remote Loader: /opt/novell/dirxml/bin/x86_64 ◆ Fanout Agent: /opt/novell/dirxml/fanoutagent ◆ iManager: /var/opt/novell/iManager
Identity Applications (Identity Manager Dashboard, Identity Manager Administration Interface, User Application, Role and Resource Service driver, User Application driver, Configuration Update Utility, One SSO Provider, Self Service Password Reset)	install.sh in the mounted location	<ul style="list-style-type: none"> ◆ Identity Applications: /opt/netiq/idm/apps ◆ User Application: /opt/netiq/idm/apps/UserApplication ◆ Configuration Update Utility: /opt/netiq/idm/apps/configupdate ◆ Form Renderer: /opt/netiq/idm/apps/sites ◆ NGINX: /opt/netiq/common/nginx
Designer for Identity Manager	/designer/packages	/root/designer
Identity Reporting	install.sh in the mounted location	/opt/netiq/idm/apps/IDMReporting
Password Management Component (Standard Edition)	./install.sh in the /sspr directory from the mounted location	/opt/netiq/idm/apps/sspr
Analyzer for Identity Manager	/analyzer/packages	/root/analyzer
Sentinel Log Management for IGA	./install.sh in the /SentinelLogManagementforIGA directory of the SentinelLogManagementForIGA8.2.2.0.tar.gz file	/opt/novell/sentinel

4.3.2 Executables and Default Installation Paths on Windows

Identity Manager Component	Location of the Executable within ISO	Default Installation Path
Identity Manager Server (Contains Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration)	install.exe located in \<iso mounted location>\IdentityManagerServer\	<ul style="list-style-type: none"> ◆ Engine: C:\netiq\idm ◆ Remote Loader: C:\netiq\idm\RemoteLoader ◆ Fanout Agent: C:\netiq\idm\FanoutAgent ◆ iManager: C:\netiq\idm\iManager
Identity Applications (Identity Manager Dashboard, Identity Manager Administration Interface, User Application, Role and Resource Service driver, User Application driver, Configuration Update Utility, One SSO Provider, Self Service Password Reset)	install.exe located in \<iso mounted location>\IdentityApplications\	<ul style="list-style-type: none"> ◆ Identity Applications: C:\netiq\idm\apps\ ◆ User Application: C:\netiq\idm\apps\UserApplication ◆ Configuration Update Utility: C:\netiq\idm\apps\UserApplication\configupdate ◆ Form Renderer: C:\netiq\idm\apps\sites ◆ NGINX: C:\netiq\common\nginx
Designer for Identity Manager	install.exe located in \designer_install\ folder of the Identity_Manager_4.8_Designer_Windows.zip file	C:\netiq\
Identity Reporting	install.exe located in \<iso mounted location>\IdentityReporting\	C:\netiq\idm\apps\IdentityReporting
Analyzer for Identity Manager	install.exe located in \analyzer_install\ folder of the Identity_Manager_4.8_Analyzer_Windows.zip file	C:\netiq\

4.4 Installing NetIQ Identity Manager 4.8

Depending on the edition you are installing, review the information from one of the following resources:

- ◆ Advanced Edition: [NetIQ Identity Manager Setup Guide for Linux](#) or [NetIQ Identity Manager Setup Guide for Windows](#)
- ◆ Standard Edition: [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager Standard Edition](#)

5 Upgrading to NetIQ Identity Manager 4.8

You can directly upgrade to Identity Manager 4.8 from Identity Manager 4.7.x and 4.6.4 versions.

(Conditional) If you are directly upgrading to Identity Manager 4.8 from 4.6.4, 4.7.3, or later versions, you must apply the `Identity_Manager_4.8.0_Upgrade_Enablement_Patch.zip` file before initiating the upgrade process. For more information, see [NetIQ Identity Manager 4.8 Upgrade Enablement Patch Release Notes](#).

Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your current version.

- ◆ [Upgrading from Identity Manager 4.7.x Versions](#)
- ◆ [Upgrading from Identity Manager 4.6.x Versions](#)
- ◆ [Upgrading to Advanced Edition](#)
- ◆ [Upgrading to Standard Edition](#)

For more information about upgrading Identity Manager, see “[Upgrading Identity Manager](#)” in the [NetIQ Identity Manager Setup Guide for Linux](#) or [Upgrading Identity Manager in NetIQ Identity Manager Setup Guide for Windows](#).

5.1 Upgrading from Identity Manager 4.7.x Versions

The following table lists the component-wise upgrade paths for Identity Manager 4.7.x versions:

Component	Base Version	Upgraded Version
Identity Manager Engine	4.7.x	<ol style="list-style-type: none">1. Upgrade the operating system to a supported version.2. Upgrade Identity Vault to 9.2.3. Upgrade Identity Manager Engine to 4.8.
Remote Loader/Fanout Agent	4.7.x	Install 4.8 Remote Loader/Fanout Agent
Designer	4.7.x	Install Designer 4.8.

Component	Base Version	Upgraded Version
Identity Applications	4.7.x	<p>Before you upgrade Identity Applications, ensure that the Identity Vault and Identity Manager engine are upgraded to 9.2 and 4.8 respectively.</p> <ol style="list-style-type: none"> 1. Upgrade the operating system to a supported version. 2. Stop Tomcat. 3. Upgrade the database to a supported version. For the supported database versions, see the NetIQ Identity Manager Technical Information website. 4. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.8 version. 5. Update the User Application driver and Roles and Resources driver packages. 6. Upgrade Identity Applications to 4.8. 7. Start Tomcat.
Identity Reporting	4.7.x	<ol style="list-style-type: none"> 1. Upgrade the operating system to a supported version. 2. Upgrade the database to a supported version. For more information about the supported database versions, see the NetIQ Identity Manager Technical Information website. 3. Upgrade SLM for IGA to a supported version. You can upgrade to SLM 8.2.2 from SLM 8.2 or later version. 4. Update the Data Collection Services and Managed Services Gateway driver packages. 5. Upgrade Identity Reporting to 4.8. 6. (Conditional) Create a data synchronization policy from the Identity Manager Data Collection Services page. 7. Start Tomcat.

Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your version from the [NetIQ documentation](#) page.

5.2 Upgrading from Identity Manager 4.6.x Versions

The following table lists component-wise upgrade paths for Identity Manager 4.6.x versions:

Component	Base Version	Intermediate Step	Upgraded Version
Identity Manager Engine	4.6.x, where x is 0 to 3	Apply the 4.6.4	<ol style="list-style-type: none"> 1. Upgrade the operating system to a supported version. 2. Upgrade Identity Vault to 9.2. 3. Upgrade Identity Manager Engine to 4.8.
Remote Loader/ Fanout Agent	4.6.x, where x is 0 to 3	Apply the 4.6.4	Install 4.8 Remote Loader/Fanout Agent.
Designer	4.6.x, where x is 0 to 3		Install Designer 4.8.
Identity Applications	4.6.x, where x is 0 to 3	4.6.4	<p>Before you upgrade Identity Applications, ensure that Identity Vault and Identity Manager engine are upgraded to 9.2 and 4.8 versions respectively.</p> <ol style="list-style-type: none"> 1. Upgrade the operating system to a supported version. 2. Stop Tomcat. 3. Update the User Application driver and Roles and Resources driver packages. 4. Upgrade the database to a supported version. For the supported database versions, see the NetIQ Identity Manager Technical Information website. 5. (Conditional) If SSPR is installed on a separate server, upgrade the component to 4.8 version. 6. Upgrade Identity Applications to 4.8. 7. Start Tomcat.

Component	Base Version	Intermediate Step	Upgraded Version
Identity Reporting	4.6.x, where x is 0 to 3	4.6.4	<ol style="list-style-type: none"> 1. Upgrade the operating system to a supported version. 2. Upgrade the database to a supported version. For more information about the supported database versions, see the NetIQ Identity Manager Technical Information website. 3. Upgrade SLM for IGA to a supported version. 4. Update the Data Collection Services and Managed Services Gateway driver packages. 5. Migrate Identity Reporting to 4.8. 6. <i>(Conditional) Applies if you are upgrading from 4.6.4.</i> Delete the existing policies in Sentinel and create a data synchronization policy from the Identity Manager Data Collection Services page. 7. Start Tomcat.

Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your version from the [NetIQ documentation](#) page.

5.3 Upgrading to Advanced Edition

NetIQ provides the following upgrade paths for upgrading to Identity Manager 4.8 Advanced Edition from a prior Advanced Edition or Standard Edition:

- ◆ Identity Manager 4.7 Advanced Edition to 4.8 Advanced Edition
- ◆ Identity Manager 4.7 Standard Edition to 4.8 Advanced Edition, in one of the following ways:
 - ◆ From Identity Manager 4.7 Standard Edition to 4.8 Standard Edition and then to 4.8 Advanced Edition
 - ◆ From Identity Manager 4.7 Standard Edition to 4.7 Advanced Edition and then to 4.8 Advanced Edition

5.4 Upgrading to Standard Edition

You can upgrade to Identity Manager 4.8 Standard Edition from Identity Manager 4.7 Standard Edition. If you are upgrading from a version prior to Identity Manager 4.6, you need to migrate Identity Reporting from your existing application server to Tomcat on both Linux and Windows platforms. For upgrade instructions, see [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.8 Standard Edition](#).

The Identity Manager 4.8 Standard Edition continues to provide support for the following reports:

- ◆ Authentication by user
- ◆ Authentication by server

- ◆ Database statistics
- ◆ Self-password changes
- ◆ Password resets
- ◆ Identity Vault Driver Associations Report Current State
- ◆ Identity Vault User Report Current State
- ◆ User Password Change Events Summary

For more information, see [Administrator Guide to NetIQ Identity Reporting](#).

IMPORTANT: To use the reports, import the latest report definitions into Identity Reporting. Log in to the Reporting application and use the **Download** page within the application to download the reports.

6 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](#). For the list of known issues in Designer, see the [NetIQ Identity Manager Designer 4.8 Release Notes](#).

- ◆ [Section 6.1, “Identity Manager Engine Issues,” on page 18](#)
- ◆ [Section 6.2, “Driver Issues,” on page 18](#)
- ◆ [Section 6.3, “Identity Applications Issues,” on page 19](#)
- ◆ [Section 6.4, “Identity Reporting Issues,” on page 20](#)
- ◆ [Section 6.5, “Containerization Issues,” on page 25](#)

6.1 Identity Manager Engine Issues

You might encounter the following issue when you use the Identity Manager engine.

6.1.1 Object Creation in Source/Destination Datastore fails

Issue: When you create an object with attribute values by using a combination of `<do-add-src-object>` and `<do-add-src-attr-value>` or `<do-add-dest-object>` and `<do-add-dest-attr-value>` policy actions, Identity Manager Engine performs these actions separately in the source/destination datastore. Therefore, object creation fails when a mandatory attribute is needed for its creation. (Bug 1157343)

Workaround: There is no workaround at this time.

6.2 Driver Issues

You might encounter the following issues when you use the Identity Manager drivers.

6.2.1 Google Apps Driver May Not Work After Upgrading Identity Manager Engine

Issue: After upgrading the Identity Manager Engine version to 4.8, the Google Apps driver may not work due to conflicting classes.

Workaround: Manually remove the `guava-19.0.jar` file:

1. Stop eDirectory.
2. Remove the `guava-19.0.jar` that is located at the following directories:
 - ♦ **Linux:** `/opt/novell/eDirectory/lib/dirxml/classes`
 - ♦ **Windows:** `C:\NetIQ\IDM\NDS\lib`
3. Start eDirectory.

6.2.2 Delimited Text Driver Does Not Process the Input Files

Issue: The Delimited Text driver shipped with Identity Manager 4.8 does not process the input XML files.

Workaround: Apply the Delimited Text 4.0.2.1 driver patch. For upgrade instructions, see the [Delimited Text 4.0.2.1 Driver Readme](#).

6.3 Identity Applications Issues

You might encounter the following issues when you use the identity applications, which includes Dashboard, Identity Applications Administration interface, and the User Application:

- ♦ [Section 6.3.1, “Searching an Entity With Substring Value for Boolean Attributes Is Not Supported,” on page 19](#)
- ♦ [Section 6.3.2, “5093 Node Service Error Reported in Identity Applications and SSPR Catalina,” on page 19](#)
- ♦ [Section 6.3.3, “Global Query Not Fetching the String Attribute of Custom Entity,” on page 20](#)
- ♦ [Section 6.3.4, “Extending the Session After Time Out Message is Showing an Error,” on page 20](#)

6.3.1 Searching an Entity With Substring Value for Boolean Attributes Is Not Supported

Issue: The Identity Applications allow substring search on the attributes defined in **Customization > Configure Entity > Search Attribute**. However, if the defined attribute is a boolean type (and not string), searching with substring value is not supported.

For example, if you created an entity named `Mobile` with attributes such as `CN`, `OSVersion`, `RAMSize`, `Processor`, and `isDualSIM` (where `isDualSIM` is a boolean attribute), and issued a search based on `isDualSIM` by specifying the substring value `*Fal*` in the search text field, the correct entities are not returned (Bug 1144267).

Workaround: To search an entity with a Boolean attribute, provide the absolute value `*True*` or `*False*` in the search text field. Using the same example to elaborate, search the entity `Mobile` with `isDualSIM` attribute as `false` by entering the value `*False*` in the search text field. Correct list of entities is returned.

6.3.2 5093 Node Service Error Reported in Identity Applications and SSPR Catalina

Issue: If you see the following error in the `catalina.out` file on the Identity Applications and SSPR servers, ignore the error:

```
ERROR, node.NodeService, error starting up node service: 5093
ERROR_NODE_SERVICE_ERROR (ldap node service requires that setting LDAP -> LDAP
Directories -> default -> Connection -> LDAP Test User is configured)
```

(Bug 1138941)

This error occurs due to an SSPR functionality that is not leveraged by Identity Manager. It does not cause any loss of functionality.

Workaround: There is no workaround at this time.

6.3.3 Global Query Not Fetching the String Attribute of Custom Entity

Issue: In Identity Applications, when you perform a search in new JSON form, the global query will not fetch the string attribute for a custom entity. The form field gets populated with DN value of the entity instead of the required attribute.

Workaround: When using global queries in new forms, the logged in user must have compare, read, and browse ACLs permission for the searched entity.

6.3.4 Extending the Session After Time Out Message is Showing an Error

Issue: On receiving session timeout warning message, you click **Extend** and provide the login credentials. The login fails showing the following error:

```
java.lang.IllegalArgumentException: Request header is too large
```

In an active session of Identity Applications, when the user access both idmdash and idmadmin components, two different cookies gets generated to store the access tokens for the same domain leading to an increase in request header size.

Workaround: To resolve this issue, perform the following steps:

- 1 Stop the Tomcat service.
- 2 Navigate to the server.xml file located at:
 - ♦ **Linux:** /opt/netiq/idm/apps/tomcat/conf
 - ♦ **Windows:** C:\NetIQ\IDM\apps\tomcat\conf
- 3 Edit the file to add below configuration in the Tomcat SSL connector:

```
>maxHttpHeaderSize="65536"
```
- 4 Save the file and restart the Tomcat service.

6.4 Identity Reporting Issues

You might encounter the following issue when you use Identity Reporting.

6.4.1 Liquibase Errors Reported When Using Oracle as the Identity Reporting Database

Issue: If you are using Oracle 18c or 19c as the database for Identity Reporting, the database configuration process reports liquibase errors and the schema creation fails. (Bug 1167076)

Workaround: To workaround this issue, perform the following steps before you configure Identity Reporting:

- 1 Log in to the server where Identity Reporting is installed.
- 2 Open a database administrator tool such as Oracle SQL developer.
- 3 Run the following scripts:

```

alter session set "_ORACLE_SCRIPT"=true;

CREATE OR REPLACE PROCEDURE create_dcs_roles_and_schemas(
    idm_rpt_data_password character varying,
    idmrptuser_password character varying)
AUTHID CURRENT_USER
AS
    cnt number;
BEGIN

    /* Create user IDM_RPT_DATA if it does not exist already */
    select count(*) into cnt from ALL_USERS WHERE USERNAME = 'IDM_RPT_DATA';
    IF cnt = 0 THEN
        execute immediate 'CREATE USER idm_rpt_data IDENTIFIED BY ' ||
idm_rpt_data_password;
        DBMS_OUTPUT.put_line('Created user idm_rpt_data');
    END IF;

    /* Grant rights to the idm_rpt_data user */
    execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE
PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE to
idm_rpt_data';
    DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_data');

    /* Create user IDMRPTUSER if it does not exist */
    select count(*) into cnt from ALL_USERS WHERE USERNAME = 'IDMRPTUSER';
    IF cnt = 0 THEN
        execute immediate 'CREATE USER idmrptuser IDENTIFIED BY ' ||
idmrptuser_password;
        DBMS_OUTPUT.put_line('Created user idmrptuser');
    END IF;

    /* Grant rights to the idmrptuser user */
    execute immediate 'GRANT CREATE SESSION to idmrptuser';
    DBMS_OUTPUT.put_line('Granted rights to user idmrptuser');
END;
/

```

```

CREATE OR REPLACE PROCEDURE create_rpt_roles_and_schemas(
    idm_rpt_cfg_password character varying)
AUTHID CURRENT_USER
AS
    cnt number;
BEGIN

    /* Create user IDM_RPT_CFG if it does not exist */
    select count(*) into cnt from ALL_USERS WHERE USERNAME = 'IDM_RPT_CFG';
    IF cnt = 0 THEN
        execute immediate 'CREATE USER idm_rpt_cfg IDENTIFIED BY ' ||
idm_rpt_cfg_password;
        DBMS_OUTPUT.put_line('Created user idm_rpt_cfg');
    END IF;

    /* Grant rights to the idm_rpt_cfg user */
    execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE
PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE to
idm_rpt_cfg';
    DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_cfg');
END;
/
exec CREATE_DCS_ROLES_AND_SCHEMAS('<DB password>', '<DB password>');
/
exec CREATE_RPT_ROLES_AND_SCHEMAS('<DB password>');
/
alter session set "_ORACLE_SCRIPT"=false;

```

4 Configure Identity Reporting.

6.4.2 Some Reports Do Not Fetch Any Data While Using MS SQL Database

Issue: If you are using MS SQL as the Identity Reporting database, the [Access Requests by Recipient](#), [Access Requests by Requester](#), and [Access Requests by Resource](#) reports do not return any data. (Bug 1171336)

Workaround: To fetch the data for the above reports, perform the following steps:

- 1 Log in to the server where Identity Reporting is installed.
- 2 Open a database administrator tool such as SQL Server Management Studio.
- 3 Run the following query:

NOTE: Specify the appropriate Identity Reporting database name in the <identity reporting database name> field.

```

USE [<identity reporting database name>]
GO

/***** Object: UserDefinedFunction [IDM_RPT_DATA].[get_formatted_user_dn]
Script Date: 5/9/2020 7:03:55 PM *****/
DROP FUNCTION [IDM_RPT_DATA].[get_formatted_user_dn]
GO

/***** Object: UserDefinedFunction [IDM_RPT_DATA].[get_formatted_user_dn]
Script Date: 5/9/2020 7:03:55 PM *****/
SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO

CREATE FUNCTION [IDM_RPT_DATA].[get_formatted_user_dn]
(
    -- Add the parameters for the function here
    @user_path nvarchar(max)
    , @user_name nvarchar(200)
)
RETURNS nvarchar(max)
AS
BEGIN
    DECLARE
        @new_path          nvarchar(200),
        @new_path_2       nvarchar(max),
        @l_user_path      nvarchar(max),
        @l_old_delimiter  nvarchar(1) = '\\',
        @l_new_delimiter  nvarchar(1) = '.',
        @MyCursor         CURSOR,
        @MyField          nvarchar(max);

    if @user_path is not null
    BEGIN
        SET @l_user_path = SUBSTRING(@user_path , 2 , (LEN(@user_path)-1));
        SET @MyCursor = CURSOR FOR
            SELECT value FROM STRING_SPLIT( @l_user_path ,
@l_old_delimiter )
        OPEN @MyCursor
        FETCH NEXT FROM @MyCursor
        INTO @MyField
        WHILE @@FETCH_STATUS = 0
        BEGIN
            if @MyField is not null
            BEGIN
                SET @new_path = @l_new_delimiter + @MyField;
            END
            if @new_path_2 is not null
            BEGIN
                SET @new_path = @new_path + @new_path_2;
            END
            SET @new_path_2 = @new_path;
            FETCH NEXT FROM @MyCursor
            INTO @MyField
        END
        CLOSE @MyCursor
        DEALLOCATE @MyCursor
    END

```

```

        if @new_path is not null
            BEGIN
                SET @new_path = @user_name + @new_path;
            END
        else
            BEGIN
                SET @new_path = @user_name;
            END
        END
    return LTRIM(RTRIM(@new_path));
END;

GO

CREATE FUNCTION [IDM_RPT_DATA].[patternReplace]
(
    @InputString VARCHAR(4000),
    @Pattern VARCHAR(100),
    @ReplaceText VARCHAR(4000)
)
RETURNS VARCHAR(4000)
AS
BEGIN
    DECLARE @Result VARCHAR(4000) SET @Result = ''
    -- First character in a match
    DECLARE @First INT
    -- Next character to start search on
    DECLARE @Next INT SET @Next = 1
    -- Length of the total string -- 8001 if @InputString is NULL
    DECLARE @Len INT SET @Len = COALESCE(LEN(@InputString), 8001)
    -- End of a pattern
    DECLARE @EndPattern INT

    WHILE (@Next <= @Len)
    BEGIN
        SET @First = PATINDEX('%' + @Pattern + '%', SUBSTRING(@InputString, @Next,
@Len))
        IF COALESCE(@First, 0) = 0 --no match - return
        BEGIN
            SET @Result = @Result +
                CASE --return NULL, just like REPLACE, if inputs are NULL
                    WHEN @InputString IS NULL
                    OR @Pattern IS NULL
                    OR @ReplaceText IS NULL THEN NULL
                ELSE SUBSTRING(@InputString, @Next, @Len)
            END
        END
        BREAK
    END
    ELSE
    BEGIN
        -- Concatenate characters before the match to the result
        SET @Result = @Result + SUBSTRING(@InputString, @Next, @First - 1)
        SET @Next = @Next + @First - 1
    END

    SET @EndPattern = 1
    -- Find start of end pattern range

```



```

WHILE PATINDEX(@Pattern, SUBSTRING(@InputString, @Next, @EndPattern)) = 0
    SET @EndPattern = @EndPattern + 1
-- Find end of pattern range
WHILE PATINDEX(@Pattern, SUBSTRING(@InputString, @Next, @EndPattern)) > 0
    AND @Len >= (@Next + @EndPattern - 1)
    SET @EndPattern = @EndPattern + 1

--Either at the end of the pattern or @Next + @EndPattern = @Len
SET @Result = @Result + @ReplaceText
SET @Next = @Next + @EndPattern - 1
END
END
RETURN(@Result)
END;

GO

```

- 4 Navigate to the [CDN](#) website.
- 5 Click the **Access Requests by Recipient** report.
- 6 Download the .rpz and .zip files for the **Access-Requests-by-Recipient** report.
- 7 Perform steps 5 and 6 for the **Access Requests by Requester**, and **Access Requests by Resource** reports.

6.5 Containerization Issues

You might encounter the following issues when you use the Identity Manager containers.

6.5.1 Duplicate Prompts are Displayed When Configuring Identity Reporting Container

Issue: During Identity Reporting container configuration, duplicate prompts for Tomcat keystore passwords are displayed. (Bug 1149803)

Workaround: There is no workaround at this time. However, there is no functionality loss.

7 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 \(https://www.netiq.com/support/process.asp\)](https://www.netiq.com/support/process.asp).

For general corporate and product information, see the [NetIQ Corporate website \(https://www.netiq.com/\)](https://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our [community \(https://www.netiq.com/communities/\)](https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

8 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/>.

Copyright © 2019 NetIQ Corporation. All Rights Reserved.