

NetIQ Identity Manager 4.6 Release Notes

February 2017



NetIQ Identity Manager 4.6 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, "Identity Manager Component Versions," on page 11](#)
- ♦ [Section 3, "System Requirements," on page 11](#)
- ♦ [Section 4, "Installing NetIQ Identity Manager 4.6," on page 12](#)
- ♦ [Section 5, "Upgrading to NetIQ Identity Manager 4.6," on page 18](#)
- ♦ [Section 6, "Known Issues," on page 21](#)
- ♦ [Section 7, "Contact Information," on page 45](#)
- ♦ [Section 8, "Legal Notice," on page 45](#)

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 2](#)
- ♦ [Section 1.2, "What's Changed, Deprecated, or Discontinued?," on page 6](#)
- ♦ [Section 1.3, "Enhancements," on page 7](#)
- ♦ [Section 1.4, "Fixed Issues," on page 7](#)
- ♦ [Section 1.5, "Addresses Software Vulnerability," on page 10](#)
- ♦ [Section 1.6, "Setup Guide Provides Examples and Directory Paths for Advanced Edition Instead of Standard Edition," on page 10](#)
- ♦ [Section 1.7, "End User License Agreement is Not Available in All Supported Languages," on page 10](#)
- ♦ [Section 1.8, "NetIQ Corporation Does Not Provide Support for the Components in the PostgreSQL and Tomcat Installation," on page 10](#)

1.1 New Features

Identity Manager 4.6 provides the following key features, enhancements, and fixes in this release:

- ♦ [Section 1.1.1, “New Dashboard for Identity Manager,” on page 2](#)
- ♦ [Section 1.1.2, “Support for eMail Based Approval,” on page 3](#)
- ♦ [Section 1.1.3, “Identity Manager Engine Enhancements,” on page 3](#)
- ♦ [Section 1.1.4, “Reporting and Auditing with Sentinel Log Management,” on page 4](#)
- ♦ [Section 1.1.5, “Simplified Upgrade for Identity Applications and Supporting Components,” on page 5](#)
- ♦ [Section 1.1.6, “Single ISO for Identity Manager Advanced and Standard Editions,” on page 5](#)
- ♦ [Section 1.1.7, “Convenience Bundling of Identity Manager Components,” on page 5](#)
- ♦ [Section 1.1.8, “Separate Installation Programs for One SSO Provider and Self-Service Password Reset Components,” on page 5](#)
- ♦ [Section 1.1.9, “Updates for Dependent Components,” on page 5](#)
- ♦ [Section 1.1.10, “Operating System Support,” on page 5](#)

For information about the new features in NetIQ Identity Manager Designer 4.6, see [NetIQ Identity Manager Designer 4.6 Release Notes](#).

There are no new features for NetIQ Identity Manager Analyzer 4.6 except the updated Java version. For more information, see [NetIQ Identity Manager Analyzer 4.6 Release Notes](#).

1.1.1 New Dashboard for Identity Manager

This release provides a new Dashboard for accessing all of the features in the identity applications for end users.

User-specific content

The new Dashboard provides user-specific content. From the Dashboard, users can perform different actions, depending on their roles.

One stop for all identity management needs for end users

- ♦ Request permissions to roles, resources, and workflows for yourself or for others
- ♦ Approve and deny permissions requests or claim tasks and take action on them later
- ♦ Complete tasks as a proxy for someone on your team
- ♦ View all of the roles and resources assigned to you
- ♦ View the status and history of your requests
- ♦ Manage your profile settings and password
- ♦ Find other users in your organization and take relevant action

User catalog and organizational chart

- ♦ Displays all the required information about the users and their relationships
- ♦ Displays quick information about the users in the organizational chart
- ♦ Is scalable when working with a large number of users
- ♦ Easily customizable views
- ♦ Improved search functionality

Easy to customize and navigate

- ♦ Customize branding, layouts, access, and user data representation to meet your organization's branding requirements
- ♦ Add links to the Applications page in the Dashboard to useful websites or software applications
- ♦ You can configure multiple clients for different sets of users within your organization, with each client having its own branding, layout, navigation accesses and customization

Users can log in with any supported Web browser on either a desktop computer or a tablet. The Dashboard also includes context-sensitive Help to provide information when you need it. For more information, see the [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) and the Help.

1.1.2 Support for eMail Based Approval

The Dashboard includes an email-based approvals feature that enables the request reviewers to approve or deny a request using email. The notification can include action links for approval or rejection so users can easily respond to the request. Email-based approval also supports digital signatures for authenticating the message content. For more information, see “[Understanding Email-based Approvals](#)” in the [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#).

1.1.3 Identity Manager Engine Enhancements

- ♦ [Monitoring Identity Manager](#)
- ♦ [Mutual Authentication between the Remote Loader and Identity Manager Engine](#)
- ♦ [Support for New Actions for Creating Roles and Resources in Designer](#)
- ♦ [Identity Vault Supports eDirectory 9.0.2 and 8.8.8 SP9 and Later Versions](#)
- ♦ [Support for Suite B](#)
- ♦ [Activating Identity Manager with DirXML Command Line Utility](#)
- ♦ [Subscriber Service Channel](#)
- ♦ [Nashorn Script Engine](#)

1.1.3.1 Monitoring Identity Manager

This release includes support for monitoring Identity Manager engine and the health of the identity applications in your Identity Manager environment. Identity Manager supports this feature on LDAP protocol and only an LDAP client can place requests for monitoring data. For more information, see in the [NetIQ Identity Manager Driver Administration Guide](#).

1.1.3.2 Mutual Authentication between the Remote Loader and Identity Manager Engine

This release introduces support for configuring mutual authentication between the Remote Loader and the Identity Manager engine for additional security. This authentication mechanism uses certificates for mutual handshake instead of passwords. The Remote Loader and the Identity Manager engine authenticate each other by exchanging and validating their signed certificates. For more information, see “[Configuring Mutual Authentication with the Identity Manager Engine](#)” in the [NetIQ Identity Manager Setup Guide](#).

1.1.3.3 Support for New Actions for Creating Roles and Resources in Designer

This release adds support for building role and resource creation actions in Designer's Policy Builder. For more information, see “[Create Role](#)” and “[Create Resource](#)” and in the [NetIQ Identity Manager - Using Designer to Create Policies](#).

1.1.3.4 Identity Vault Supports eDirectory 9.0.2 and 8.8.8 SP9 and Later Versions

This release provides support for eDirectory 9.0.2 or later in addition to eDirectory 8.8.8 SP9 as an Identity Vault. For more information, see the [NetIQ Identity Manager Setup Guide](#).

1.1.3.5 Support for Suite B

This release includes support for Suite B algorithms for Identity Manager components. Suite B is a set of cryptographic algorithms standardized by the National Security Agency (NSA) to allow commercial products to protect traffic that is classified at secret or top secret levels. The Suite B algorithms ensure the security of classified and unclassified information passed through public networks. For more information about Suite B, see [Suite B Cryptography](#).

You can configure Suite B secured communication between the Identity Manager engine and the Remote Loader or Fan-Out agent. For more information, see “[Configuring Stronger Ciphers for SSL Communication](#)” in the [NetIQ Identity Manager Driver Administration Guide](#). Support for Suite B is included in eDirectory 9.0 and later versions.

IMPORTANT: Suite B standard is subject to change. Suite B support in Identity Manager is based on our interpretation of the NSA recommendation. Be aware that NSA may change their recommendation in future.

1.1.3.6 Activating Identity Manager with DirXML Command Line Utility

This release provides support for activating Identity Manager using the DirXML command line utility in addition to iManager. For more information, see “[Activating Identity Manager](#)” in the [NetIQ Identity Manager Setup Guide](#).

1.1.3.7 Subscriber Service Channel

Identity Manager introduces Subscriber Service Channel that enables you to separately process the out-of-band queries without interrupting the normal flow of cached events. For example, the Subscriber service channel can separately process code map refresh, data collection, and queries triggered from dxcmd. This helps to improve the performance of the driver. This functionality can be controlled by a new Engine Control Value, Enable Subscriber Service Channel. This feature is currently available for use with the JDBC Fan-Out driver only.

1.1.3.8 Nashorn Script Engine

This release includes support for Nashorn ECMAScript engine. To use the Nashorn scripting engine, change the default setting by using the Use Rhino ECMAScript engine control value.

For more information, see “[Engine Control Values](#)” in the [NetIQ Identity Manager Driver Administration Guide](#).

1.1.4 Reporting and Auditing with Sentinel Log Management

In this release, Sentinel Log Management for Identity Governance and Administration (IGA) replaces the Event Auditing Service (EAS). For your convenience, the Identity Manager 4.6 installation kit includes an installation program for Sentinel Log Management for IGA. For more information, see [Installing and Managing Sentinel Log Management for Identity Governance and Administration](#) in the [NetIQ Identity Manager Setup Guide](#).

When you upgrade to version 4.6, you can migrate your existing data from EAS to Sentinel Log Management for IGA after installing this component. For more information, see “[Migrating from Event Auditing Service to Sentinel Log Management for IGA](#)” in the [NetIQ Identity Manager Setup Guide](#).

1.1.5 Simplified Upgrade for Identity Applications and Supporting Components

For your convenience, the Identity Manager 4.6 installation kit includes an upgrade program for upgrading the identity applications and the supporting software such as OSP, SSPR, Tomcat, JDK, and ActiveMQ. For more information, see [“Upgrading Identity Applications and Supporting Components”](#) in the *NetIQ Identity Manager Setup Guide*.

1.1.6 Single ISO for Identity Manager Advanced and Standard Editions

Identity Manager 4.6 provides both Advanced and Standard Editions in a single ISO instead of separate ISO files. To understand what features are provided with each edition, see [Section 4.1, “Features Supported with Identity Manager Advanced and Standard Editions,”](#) on page 12.

This change does not affect the existing licensing model. Identity Manager continues to provide separate licenses for Advanced and Standard Editions. For more information about licensing and activation, see [“Understanding Licensing and Activation”](#) in the *NetIQ Identity Manager Setup Guide*.

For new installations, you can configure Identity Manager as Advanced Edition or Standard Edition based on the choice you specified during Identity Manager engine installation. For continued use of features, you must apply the appropriate license keys.

1.1.7 Convenience Bundling of Identity Manager Components

In addition to providing the complete Identity Manager functionality in one ISO file, NetIQ delivers various Identity Manager components in separate ISO files in convenient packages.

The convenience bundling option enables you to download only the required components for your installation. For detailed information about the ISO files provided with Identity Manager 4.6, see [Section 4, “Installing NetIQ Identity Manager 4.6,”](#) on page 12.

1.1.8 Separate Installation Programs for One SSO Provider and Self-Service Password Reset Components

For your convenience, this release provides separate installation programs to install One SSO Provider (OSP) and Self-Service Password Reset (SSPR) components. For more information, see [“Installing the Single Sign-on Component”](#) and [“Installing the Password Management Component”](#) in the *NetIQ Identity Manager Setup Guide*.

1.1.9 Updates for Dependent Components

This release adds support for the following dependent components:

- ♦ Java 8 Update 112
- ♦ OpenSSL 1.0.2j-fips
- ♦ Tomcat 8.5.9
- ♦ PostgreSQL 9.4.10 on SLES 11 SP4, PostgreSQL 9.6.1 on other supported platforms
- ♦ ActiveMQ 5.14.0

1.1.10 Operating System Support

This release adds support for the following platforms:

- ♦ SUSE Linux Enterprise Server (SLES) 12 SP1
- ♦ Red Hat Enterprise Linux (RHEL) 6.8 and RHEL 7.3

1.2 What's Changed, Deprecated, or Discontinued?

To streamline functionality, several items have changed or are no longer supported with Identity Manager 4.6. In many cases, alternative functionality replaces the items that are no longer supported.

1.2.1 Changed Functionality or Features

The following list provides an overview of the features or functions that have changed or deprecated in this release or will soon be deprecated.

Separate Access to Identity Manager Home and the Identity Manager Provisioning Dashboard

This release introduces the Dashboard, which includes the functionality previously provided by Identity Manager Home and Provisioning Dashboard. Instead of using Home and Provisioning Dashboard, you must use the new user interface. For example, if you attempt to edit Featured Items in Home, you will be directed to the new Dashboard. [\[Bug 1015183\]](#)

If you are upgrading to this release, please ensure that your users have the updated URLs to access the identity applications in the Dashboard. Also, add your Featured Items to **Dashboard > Applications**. For more information about adding featured items, see the Help for the Dashboard.

This release continues to support Home and Provisioning Dashboard. However, that functionality is redundant, so it will be deprecated in the future.

Fan-Out Agent

The Fan-Out agent is now available with the Identity Manager installation package instead of the Fan-Out driver. For information about using the Fan-Out agent with the JDBC Fan-Out driver, see [NetIQ Identity Manager Driver for JDBC Fan-Out Implementation Guide](#).

Version Numbers Not Displayed in the Splash Screens of the Identity Manager Installation Programs

The Identity Manager installer splash screens no longer display the version number of the component being installed. However, you can find the version information in the Introduction or Pre-installation Summary page of the installer.

1.2.2 Discontinued or Deprecated Functionality

The following list provides an overview of the features or functions that have been discontinued from this release or will soon be deprecated.

Event Auditing Service

Event Auditing Service is discontinued from this release. The .iso file includes an installation program for Sentinel Log Management for IGA.

If you are upgrading to this release [\[Bug 1015183\]](#), you can migrate your existing data from EAS to Sentinel Log Management for IGA after installing this component. For more information, see the [NetIQ Identity Manager Setup Guide](#).

JBoss Enterprise Application Platform (EAP), JBoss Community Edition, and WebSphere Web Application Servers

This version of Identity Manager does not include support for these web application servers. The .iso file includes an installation program for Tomcat as the supported application server. NetIQ provides support for migrating your identity applications from JBoss and WebSphere to Tomcat. You can also use your own installation of Tomcat if it is a supported version. For more information, see the [NetIQ Identity Manager Setup Guide](#).

Legacy Password Management

The Legacy Password Self-Service feature of the User Application will be deprecated in the future. You must use SSPR for logging events. For more information, see the [NetIQ Identity Manager Setup Guide](#).

OpenXDAS for Identity Applications

OpenXDAS is discontinued from this release for the identity applications component. NetIQ recommends you to use Novell Audit for logging identity applications events. This change is not applicable to other Identity Manager components that support OpenXDAS.

1.3 Enhancements

This release includes the following enhancements:

1.3.1 Ability to Send Out-of-Band Add Events on Roles and Resource Driver

In addition to Modify events, the Out of Band sync feature now allows Add events for the Roles and Resource driver. (Bug 1008938)

1.3.2 Improved Performance with Reduced LDAP Calls for Checking Administrative Permissions

Checking for permissions that resulted in multiple LDAP calls is now reduced to one call improving the performance at places where a user permission check is required. (Bug 945463)

1.4 Fixed Issues

This release includes the following software fixes:

1.4.1 Entitlements Now Available for a Resource Assignment After Restarting the Loopback Driver

The `InitEntitlementResourceObjects` policy now updates the `EntitlementConfiguration` object with all the entitlements created for the Loopback driver instead of updating only the entitlements configured in Mapping Table. (Bug 983868)

1.4.2 Drivers No Longer Fail when Role Addition and Role Assignment Type Actions are Performed Together in Policy Builder

Now, the drivers start successfully when the target identity is not specified when using the role-assignment-type action with the role addition action. (Bug 927094)

1.4.3 Startup Policy Processing Results in a Null Pointer Exception

The engine now allows both the Publisher and Subscriber threads to complete initialization when the startup policy is executed. (Bug 887766)

1.4.4 Engine Detects the Password Synchronization Command

When a password change is initiated on the Subscriber Channel of the SOAP driver, the engine detects the password synchronization command and updates the `DirXML-PasswordSyncStatus` attribute. (Bug 987595)

1.4.5 Images Are Attached with Send Email or Send Email Template on Windows

Identity Manager now includes images that are referenced from **send email** or **send email from template** actions on Windows platforms. (Bug 943464)

1.4.6 DirXML Command Line Utility in LDAP Mode Does Fetches JVM Statistics

Now, the DirXML Command Line Utility successfully returns the JVM statistics when the utility is used in LDAP mode.

1.4.7 Connection Time-Out for SOAP Driver

The SOAP driver shim now includes an HTTP connection time-out value for which the driver waits before terminating the HTTP connection. (Bug 965326)

1.4.8 Drivers Start Correctly

When you start a driver, the engine now correctly reads the driver parameters. Previously, the driver might fail to start. (Bug 998961)

1.4.9 Duplicate Password Synchronization GCVs in Password Administration Plug-In

iManager no longer displays the **Server Variables** from the driver properties. When Server Variables related to password synchronization change for a driver, the password administration plug-ins do not create duplicate entries for password synchronization GCVs to eliminate conflict with the existing GCVs. (Bug 997118)

1.4.10 Displays All Workflows from the Task Workflow Administration Plug-In

The Task Workflow Administration plug-in now correctly displays all workflows. (Bug 688126)

1.4.11 Reports are Properly Generated in the CSV File Format

Reports are now properly generated in CSV format. (Bug 999925)

1.4.12 Different Entitlement Values Are Displayed Differently in Catalog Administrator and Resource Catalog

Catalog Administrator has been updated to display **nrfResource's entitlementRef** attribute value of an entitlement to match the entitlement value that Resource Catalog displays. (Bug 948146)

1.4.13 Request on Behalf Lists Users When a Search Is Not Issued

Request On Behalf displays the search result only when you enter a search keyword. To improve the performance of the search functionality, it limits the results to 500 users. (Bug 1018268)

1.4.14 ManageTeamTilesCreate.jar Is Hard Coded to Use a Specific Category Identification Value

The **Manage Team** tile is now added to the Identity Manager Home page during the server start up. If the Administration category is available at that time, the tile is added to the uncategorized category of Home page items. (Bug 990368)

1.4.15 Search a Role or a Resource by Description When Defining a Team in Home Provisioning Dashboard

While creating a new team, Catalog Administrator now allows you to search a role or a resource by using the Description value. (Bug 973376)

1.4.16 Home Provisioning Dashboard Incorrectly Displays Tasks Sorted Using the Due Date Field

If you are sorting the tasks by the **Due Date** field, Home Provisioning Dashboard correctly list the tasks.

1.4.17 Installing Identity Reporting Does Not Overwrite the logevent.conf File

The Identity Reporting installation program no longer overwrites logevent.conf without prompting under certain circumstances. Identity Reporting now displays a warning message when auditing is enabled.

1.4.18 Downloading an RPZ File with Internet Explorer Does Not Change the File Extension

When you access Identity Reporting in an Internet Explorer browser and download a .rpz file, the file extension no longer changes. (Bug 677436)

1.4.19 Internet Explorer Does Not Display a Warning when Accessing Identity Reporting in HTTPS

If you use Internet Explorer in HTTPS to access Identity Reporting, the browser no longer displays a warning message and correctly displays the login screen for Identity Reporting. (Bug 685490)

1.4.20 Console Mode Reports a Successful Connection to the Database Message

When you install Identity Reporting using the console mode, the installation process now displays appropriate messages for a successful connection or when a test connection to the database fails. (Bug 899383)

1.4.21 Reporting Does Not Require Additional Steps to Enable Auditing on Linux

If you installed Identity Reporting and want to enable auditing, you no longer need to run additional steps on your application server. (Bug 901325)

1.4.22 Setting Up ConfigUpdate Utility When Identity Reporting Is Deployed With Identity Applications

The standalone installation of Identity Reporting now updates the configuration file for the Configupdate utility on your application server. (Bug 900846)

1.4.23 Identity Reporting Does Not Leave Any Entries in .xml Files for Tomcat After Uninstalling

When you uninstall Identity Reporting on Tomcat, the process no longer leaves any entries in the Tomcat server.xml and context.xml files. (Bug 897505)

1.4.24 Association Description Is Not Required for the Default Language when Assigning Resources to Roles

When a user access the identity applications in a language other than the default language, and you add a resource to a role, you no longer need to enter a value for the default language to get the resource added to the role. (Bug 687734)

1.4.25 IDMPProv.war File Path Is Corrected in the NetIQ-Custom-Install.log File for the liquibase Command

When you install the identity applications, the IDMPProv.war file path for the liquibase command is correctly set in the NetIQ-Custom-Install.log file. (Bug 900772)

1.5 Addresses Software Vulnerability

This release addresses [CVE-2017-7434](#) and [CVE-2016-1600](#) for Identity Manager.

1.6 Setup Guide Provides Examples and Directory Paths for Advanced Edition Instead of Standard Edition

The paths provided in the Setup Guide are for Advanced Edition. If you are installing Standard Edition, ensure that you use the correct paths. For example, when you install Standard Edition on Linux, the configupdate.sh file is located in /opt/netiq/idm/apps/IdentityReporting/bin directory. For Advanced Edition, this utility is located in the installation directory for the identity applications: /opt/netiq/idm/apps/UserApplication. For more information, see [Section 4.4, “Locating the Executables and Default Installation Paths,”](#) on page 13.

1.7 End User License Agreement is Not Available in All Supported Languages

Each installation program includes an End User License Agreement. Although the installation programs support multiple languages, the license agreement is not available in the following languages:

- ♦ Danish
- ♦ Dutch
- ♦ Russian
- ♦ Swedish

Instead, the installation program displays the license agreement in English. For more information, see [“Understanding Language Support”](#) in the *NetIQ Identity Manager Setup Guide*. (Bug 896299)

1.8 NetIQ Corporation Does Not Provide Support for the Components in the PostgreSQL and Tomcat Installation

NetIQ Corporation provides the PostgreSQL and Tomcat installation as a convenience. If your company does not already provide an application server and a database server, you can install and use these components. If you need support, go to the provider of the component. NetIQ does not provide updates, administration, configuration, or tuning information for these components, beyond what it is outlined in the *NetIQ Identity Manager Setup Guide*.

2 Identity Manager Component Versions

Identity Manager 4.6 bundles the following components:

NOTE: Identity Manager 4.6 supports two versions of eDirectory and iManager. Depending on the eDirectory version you install, you must install a compatible version of iManager to work with it.

- ♦ NetIQ eDirectory 9.0.2 with Hotfix 2

You need to apply the hotfix if you are installing eDirectory using the component installer. This action is not required when installing eDirectory with the integrated installation program.

- ♦ NetIQ eDirectory 8.8.8 Patch 9 with Hotfix 2

This version is not supported with the integrated installation program.

- ♦ NetIQ iManager 3.0.2 Patch 1 (for eDirectory 9.0.2 or later)
- ♦ NetIQ iManager 2.7.7 Patch 9 (for eDirectory 8.8.8 Patch 9 or later)
- ♦ NetIQ Identity Manager Engine 4.6
- ♦ NetIQ Identity Manager Remote Loader 4.6
- ♦ NetIQ Designer for Identity Manager 4.6
- ♦ NetIQ Identity Applications 4.6
- ♦ NetIQ Single Sign-on (One SSO) 6.1.3
- ♦ NetIQ Identity Manager Self-Service Password Reset 4.1.0
- ♦ Platform Agent 2011.1r5
- ♦ NetIQ Identity Manager Client Login Extension 3.10
- ♦ NetIQ Identity Manager Identity Reporting 5.5.0
- ♦ NetIQ Sentinel Log Management for Identity Governance and Administration 8.0.0.1 (for event auditing)
The Identity Manager installation package includes an installation program for Sentinel Log Management for Identity Governance and Administration component.
- ♦ NetIQ Analyzer for Identity Manager 4.6
- ♦ NetIQ Identity Manager drivers. For driver versions, see [Driver and Engine Version Compatibility Table](#).

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. [!\[\(Bug 995483\)\]](#)

3 System Requirements

You can install Identity Manager components on a variety of operating system platforms. For specific information about which component can be installed on which operating system, see “[Selecting an Operating System Platform for Identity Manager](#)” in the *NetIQ Identity Manager Setup Guide*.

For information about prerequisites, computer requirements, installation, upgrade or migration, see “[Considerations and Prerequisites for Installation](#)” in the *NetIQ Identity Manager Setup Guide*.

4 Installing NetIQ Identity Manager 4.6

Identity Manager 4.6 provides Advanced Edition and Standard Edition in a single ISO file. Components such as Identity Manager server, Identity Applications and Identity Reporting are also delivered in separate ISO files to ease the installation process. 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 12](#)
- ♦ [Section 4.2, “Understanding the Download Options,” on page 13](#)
- ♦ [Section 4.3, “Downloading the Installation Files,” on page 13](#)
- ♦ [Section 4.4, “Locating the Executables and Default Installation Paths,” on page 13](#)
- ♦ [Section 4.5, “Installation Prerequisites,” on page 16](#)
- ♦ [Section 4.6, “Installing NetIQ Identity Manager 4.6,” on page 17](#)

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
Catalog Administrator	Yes	No

4.2 Understanding the Download Options

After you purchase Identity Manager 4.6, log in to the [Identity Manager Product Web site](#) and follow the link that allows you to download the software. The following .iso files contain the Identity Manager components:

File Name	Description
Identity_Manager_4.6_Linux.iso	Contains Identity Manager Server (Engine, Remote Loader, Fan-Out Agent, drivers, and plug-ins), Designer, iManager, Analyzer, OSP, SSPR, Identity Applications, Identity Reporting, and Sentinel Log Management for Identity Governance and Administration (IGA)
Identity_Manager_4.6_Windows.iso	Contains Identity Manager Server (Engine, Remote Loader, Fan-Out Agent, drivers, and plug-ins), Designer, iManager, Analyzer, OSP, SSPR, Identity Applications, and Identity Reporting NOTE: Sentinel Log Management for IGA is not supported on Windows.
Identity_Manager_4.6_Linux_Framework.iso	Contains Identity Vault, Identity Manager Engine, Remote Loader, Fan-Out Agent, drivers, and plug-ins
Identity_Manager_4.6_Windows_Framework.iso	Contains Identity Vault, Identity Manager Engine, Remote Loader, Fan-Out Agent, drivers, and plug-ins
Identity_Manager_4.6_Linux_IdentityApplications.iso	Contains OSP, SSPR, Identity Applications, Identity Reporting, and PostgreSQL and Tomcat (convenience installer)
Identity_Manager_4.6_Windows_IdentityApplications.iso	Contains OSP, SSPR, Identity Applications, Identity Reporting, and PostgreSQL and Tomcat (convenience installer)

4.3 Downloading the Installation Files

- 1 Go to the [NetIQ Downloads website](#).
- 2 In the **Product or Technology** menu, select Identity Manager, then click **Search**.
- 3 On the **NetIQ Identity Manager Downloads** page, click the **Download** button next to the ISO file that you want to download.
- 4 Follow the on-screen prompts to download the file to a directory on your computer.
- 5 Either mount the downloaded .iso file as a volume, or use the .iso file to create a DVD of the software.

4.4 Locating the Executables and Default Installation Paths

The following table provides information about the location of the executables in the ISO file and the default installation paths for the Identity Manager components.

Identity Manager Component	Edition (Advanced/ Standard)	Location of the Executable within ISO	Default Installation Path
Identity Vault	Advanced and Standard	♦ Linux: nds-install located in products/eDirectory/processor_type/setup ♦ Windows: Setup.exe located in \products\eDirectory\processor_type\windows\	♦ Linux: /opt/novell/eDirectory ♦ Windows: C:\Novell\NDS
Sentinel Log Management for IGA	Advanced and Standard	♦ Linux: install-logmanager located in products/SentinelLogManagementforIGA/ ♦ Windows: Not supported on Windows	♦ Linux: /opt/novell/sentinel ♦ Windows: Not supported on Windows
iManager	Advanced and Standard	♦ Server installation ♦ Linux: iManagerInstallLinux.bin located in /extracted_directory/products/iManager/installs/Linux/ ♦ Windows: iManagerInstall.exe located in /extracted_directory/products/iManager/installs/win/ ♦ Workstation installation ♦ Linux: iManager.sh located in imanager/bin ♦ Windows: iManager.bat located in imanager\bin	♦ Linux: /opt/novell/iManager/ ♦ Windows: C:\Program Files\Novell
Identity Manager Engine, drivers, and plug-ins	Advanced and Standard	♦ Linux: install.bin located in products/IDM ♦ Windows: idm_install.exe located in \products\IDM\windows\setup	♦ Linux: /opt/novell/ ♦ Windows: C:\Novell
Remote Loader	Advanced and Standard	♦ Linux: install.bin located in products/IDM ♦ Windows: idm_install.exe located in \products\IDM\windows\setup	♦ Linux: /opt/novell ♦ Windows: C:\Novell

Identity Manager Component	Edition (Advanced/ Standard)	Location of the Executable within ISO	Default Installation Path
PostgreSQL and Tomcat (supported database and application server)	Advanced and Standard	♦ Linux: TomcatPostgreSQL.bin located in products/RBPM/postgre_tomcat_install/ ♦ Windows: TomcatPostgreSQL.exe located in products/RBPM/postgre_tomcat_install/	♦ Linux: /opt/netiq/idm/apps/tomcat ♦ Windows: C:\netiq\idm\apps\tomcat
Single Sign-on (OSP)	Advanced and Standard	♦ Linux: osp-install-linux.bin located in \products\RBPM\osp_install ♦ Windows: osp-install.exe located in \products\RBPM\osp_install	♦ Linux: /opt/netiq/idm/apps/osp ♦ Windows: C:\netiq\idm\apps\osp
Self Service Password Reset (SSPR)	Advanced and Standard	♦ Linux: sspr-install.bin located in products/RBPM/sspr_install ♦ Windows: sspr-install.exe located in \products\RBPM\sspr_install	♦ Linux: /opt/netiq/idm/apps/sspr ♦ Windows: C:\netiq\idm\apps\sspr
Identity applications	Advanced Edition only	♦ Linux: IdmUserApp.bin located in products/RBPM/user_app_install ♦ Windows: IdmUserApp.exe located in products/RBPM/user_app_install	♦ Linux: /opt/netiq/idm/apps ♦ Windows: C:\netiq\idm\apps\User Application
Designer for Identity Manager	Advanced and Standard	♦ Linux: install located in products/Designer/ ♦ Windows: install.exe located in \products\Designer\	♦ Linux: /root/designer ♦ Windows: c:\netiq\idm\apps\Designer

Identity Manager Component	Edition (Advanced/ Standard)	Location of the Executable within ISO	Default Installation Path
Identity Reporting	Complete set with Advanced Edition Limited set with Standard Edition. For more information, see Section 5.4, "Upgrading to Standard Edition," on page 20.	♦ Linux: rpt-install.bin located in products/Reporting ♦ Windows: rpt-install.exe located in \products\Reporting	♦ Linux: /opt/netiq/idm/apps/IdentityReporting ♦ Windows: C:\netiq\idm\apps\IdentityReporting
Analyzer for Identity Manager	Advanced and Standard	♦ Linux: install located in products/Analyzer/ ♦ Windows: install.exe located in \products\Analyzer\	♦ Linux: /root/Analyzer ♦ Windows: C:\netiq\idm\apps\Analyzer

4.5 Installation Prerequisites

The following considerations apply when you install this version:

- ♦ To install the Identity Manager components using the component installers, install the components in the following order:
 1. eDirectory
 2. Sentinel Log Management for IGA
 3. iManager
 4. Identity Manager Engine
 5. Apache Tomcat and PostgreSQL

Identity Manager provides a convenience installer to install these components.

 6. OSP
 7. SSPR
 8. Identity applications (not required for Standard Edition)
 9. Designer
 10. Identity Reporting
 11. Analyzer

You can install the components interactively or silently.

For information about which component can be installed on which operating system, see ["Selecting an Operating System Platform for Identity Manager"](#) in the *NetIQ Identity Manager Setup Guide*.

- ♦ Before starting the installation process on a supported RHEL platform, verify that the platform has the necessary libraries required for installing Identity Manager. On a 64-bit platform, the required libraries vary depending on your chosen method of installation. In absence of the dependent libraries, manually install the libraries before starting the Identity Manager installation. For more information, see [“Installing Identity Manager on RHEL 6.x or 7.x Servers”](#) in the *NetIQ Identity Manager Setup Guide*.
- ♦ For a guided installation of Identity Manager on SLES 12 SP1 or later platforms by using the components installers or the integrated installation program, verify that the platform has the necessary libraries already installed. The installation does not start in absence of these libraries. For more information, see [“Installing Identity Manager on SLES 12 SP1 or Later Servers”](#) in the *NetIQ Identity Manager Setup Guide*.
- ♦ The following considerations apply to using the integrated installation program:
 - ♦ Can be run on RHEL 7.3 or later and SLES 12 SP1 or later Linux platforms in addition to the supported Windows platforms.
 - ♦ Cannot not be used to install Identity Manager on RHEL 6.x and SLES 11.x platforms. Instead, use the individual component installers to install the supported components on these platforms. For information about which components are supported on which platforms, see the *NetIQ Identity Manager Setup Guide*.
 - ♦ Should not be used to install Identity Manager Standard Edition
For guidelines about installing the Identity Manager components for Standard Edition, see the *Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.6 Standard Edition*.
 - ♦ Should not be used in a clustered environment
 - ♦ Should not be used in a production environment
- ♦ Before installing Identity Manager 4.6 Standard Edition, ensure that the container where the reportAdmin role resides does not include any object with the same name.

4.6 Installing NetIQ Identity Manager 4.6

Before installing Identity Manager 4.6, NetIQ recommends that you review the information in the following sections in the *NetIQ Identity Manager Setup Guide*:

- ♦ **Interaction among Identity Manager components:** [“Introduction”](#)
This section describes the components that you might want to install for your identity management solution.
- ♦ **Planning your Identity Manager environment:** [“Planning to Install Identity Manager”](#)
This section provides a checklist and scenarios for installing Identity Manager. It also describes the prerequisites and system requirements for the computers where you want to install each Identity Manager component.
- ♦ **Deciding the type of installation for your environment:** [“Understanding the Integrated and Standalone Installation Processes”](#)
The integrated installation program bundles Identity Manager components so you can avoid the need to separately install each component. This program bundles the latest versions of all necessary components for Identity Manager for your convenience. Use this process for a test environment or for evaluating Identity Manager.

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

- ♦ Advanced Edition: [NetIQ Identity Manager Setup Guide](#)
- ♦ Standard Edition: [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.6 Standard Edition](#).

5 Upgrading to NetIQ Identity Manager 4.6

You can upgrade to Identity Manager 4.6 from Identity Manager 4.5 Advanced Edition or Standard Edition. To upgrade or migrate your data to the latest version, use the individual installation programs for each component. You cannot perform an upgrade with the integrated installation program.

- ♦ [Section 5.1, “Upgrade Order,” on page 18](#)
- ♦ [Section 5.2, “Supported Upgrade Paths,” on page 18](#)
- ♦ [Section 5.3, “Upgrading to Advanced Edition,” on page 20](#)
- ♦ [Section 5.4, “Upgrading to Standard Edition,” on page 20](#)

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

5.1 Upgrade Order

You must upgrade the Identity Manager components in the following sequence:

1. Designer
2. iManager
3. Sentinel Log Management for IGA (you need to perform a migration from EAS to Sentinel Log Management for IGA)
4. Identity Vault
5. Identity Manager Engine/Remote Loader
6. iManager Plug-Ins
7. Tomcat and PostgreSQL Components
8. Single Sign-on (One SSO Provider)
9. Self Service Password Reset
10. Identity Applications (for Advanced Edition)
11. Identity Reporting
12. Analyzer

For information about the latest supported upgrade paths, see the Release Notes for your version from the [Identity Manager Documentation web site \(https://www.netiq.com/documentation/identity-manager-46/\)](https://www.netiq.com/documentation/identity-manager-46/).

5.2 Supported Upgrade Paths

Identity Manager 4.6 includes support for NetIQ eDirectory 8.8.8 SP 9 Hotfix 2 and NetIQ eDirectory 9.0.2 Hotfix 2. This allows for different upgrade paths to Identity Manager 4.6. You can directly upgrade from Identity Manager 4.5.4 or later with eDirectory 8.8.8 SP8 or eDirectory 9.0.1 as depicted in the following table:

Base Version	Upgraded Version
Identity Manager 4.5.5 with eDirectory 9.0.2	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.5 with eDirectory 9.0.1	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.5 with eDirectory 8.8.8 SP9	Identity Manager 4.6 with eDirectory 8.8.8 SP9
	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.5 with eDirectory 8.8.8 SP8	Identity Manager 4.6 with eDirectory 8.8.8 SP9
	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.4 or later with eDirectory 9.0.1	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.4 with eDirectory 8.8.8 SP8	Identity Manager 4.6 with eDirectory 8.8.8 SP9
	Identity Manager 4.6 with eDirectory 9.0.2

To upgrade from versions lower than Identity Manager 4.5.4, see [“Upgrading from Versions Lower Than 4.5.4” on page 19](#).

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

- ♦ [NetIQ Identity Manager 4.5 Service Pack 5 Release Notes](#)
- ♦ [NetIQ Identity Manager 4.5 Service Pack 4 Release Notes](#)

5.2.1 Upgrading from Versions Lower Than 4.5.4

NetIQ does not support a direct upgrade to Identity Manager 4.6 from Identity Manager 4.5, 4.5.1, 4.5.2, or 4.5.3. To upgrade from any of these versions, you must first upgrade to version 4.5.4. For example, if you are running Identity Manager 4.5.3 with eDirectory 8.8.8.x (where x is less than 9), first upgrade to eDirectory 8.8.8.9 or 9.0.1 and Identity Manager to 4.5.4 and then upgrade to Identity Manager 4.6 as depicted in the following table:

Base Version	Intermediate Version	Upgraded Version
Identity Manager 4.5.x (where x is less than SP4) with eDirectory 8.8.8.x (where x is less than SP9)	Identity Manager 4.5.4 with eDirectory 9.0.1	Identity Manager 4.6 with eDirectory 9.0.2
	Identity Manager 4.5.4 with eDirectory 8.8.8 SP8	Identity Manager 4.6 with eDirectory 8.8.8 SP9

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

- ♦ [NetIQ Identity Manager 4.5 Service Pack 4 Release Notes](#)
- ♦ [NetIQ Identity Manager 4.5 Service Pack 3 Release Notes](#)
- ♦ [NetIQ Identity Manager 4.5 Service Pack 2 Release Notes](#)
- ♦ [NetIQ Identity Manager 4.5 Service Pack 1 Release Notes](#)
- ♦ [NetIQ Identity Manager 4.5 Release Notes](#)

5.2.2 Upgrading from Identity Manager 4.0.2

You cannot upgrade or migrate to version 4.6 from versions before 4.5. This upgrade can be performed in a two steps: first upgrade to Identity Manager 4.5 and then upgrade to 4.6 version. For more information, see the [NetIQ Identity Manager 4.5 Setup Guide](#) and one of the following Release Notes:

- ♦ [NetIQ Identity Manager 4.5 Advanced Edition Release Notes](#)
- ♦ [NetIQ Identity Manager 4.5 Standard Edition Release Notes](#)

5.3 Upgrading to Advanced Edition

NetIQ provides the following upgrade paths for upgrading to Identity Manager 4.6 Advanced Edition from a prior Advanced Edition or Standard Edition:

- ♦ Identity Manager 4.5 Advanced Edition to 4.6 Advanced Edition
- ♦ Identity Manager 4.5 Standard Edition to 4.6 Advanced Edition, in one of the following ways:
 - ♦ From Identity Manager 4.5 Standard Edition to 4.6 Standard Edition and then to 4.6 Advanced Edition
 - ♦ From Identity Manager 4.5 Standard Edition to 4.5 Advanced Edition and then to 4.6 Advanced Edition

5.4 Upgrading to Standard Edition

You can upgrade to Identity Manager 4.6 Standard Edition from Identity Manager 4.5 Standard Edition. As part of upgrading, 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 4.6 Standard Edition](#).

The Identity Manager 4.6 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 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](#).

- ♦ [Section 6.1, “Issues Common to Advanced Edition and Standard Edition,” on page 21](#)
- ♦ [Section 6.2, “Advanced Edition Issues,” on page 32](#)
- ♦ [Section 6.3, “Standard Edition Issues,” on page 44](#)

6.1 Issues Common to Advanced Edition and Standard Edition

You might encounter the following issues when you use Advanced Edition or Standard Edition:

- ♦ [Section 6.1.1, “Installation Issues,” on page 21](#)
- ♦ [Section 6.1.2, “Identity Manager Engine Issues,” on page 24](#)
- ♦ [Section 6.1.3, “Remote Loader Issues,” on page 25](#)
- ♦ [Section 6.1.4, “Driver Issues,” on page 26](#)
- ♦ [Section 6.1.5, “Identity Reporting Issues,” on page 28](#)
- ♦ [Section 6.1.6, “iManager Plug-In Issues,” on page 29](#)
- ♦ [Section 6.1.7, “Identity Manager Upgrade Issues,” on page 29](#)
- ♦ [Section 6.1.8, “Localization Issues,” on page 30](#)
- ♦ [Section 6.1.9, “Uninstallation Issues,” on page 31](#)

6.1.1 Installation Issues

- ♦ [Section 6.1.1.1, “Cannot Specify Installation Paths on Windows that Include Spaces,” on page 22](#)
- ♦ [Section 6.1.1.2, “Engine Installation is Not Started Due to Mismatch in libXrender Libraries on RHEL and SLES Platforms,” on page 22](#)
- ♦ [Section 6.1.1.3, “Pop-up Window is Displayed When Engine is Silently Installed,” on page 22](#)
- ♦ [Section 6.1.1.4, “LDAP Server Displays an Error While using VLV and SSS Controls,” on page 22](#)
- ♦ [Section 6.1.1.5, “Empty Remote Loader Installation Folder on Windows,” on page 22](#)
- ♦ [Section 6.1.1.6, “Remote Loader Trace Screen does not Close after Restart,” on page 22](#)
- ♦ [Section 6.1.1.7, “Incorrect Representation of Index Values in iMonitor,” on page 22](#)
- ♦ [Section 6.1.1.8, “Identity Applications Installer Does Not Create master-key.txt File in the File System During Installation,” on page 23](#)
- ♦ [Section 6.1.1.9, “Tables are Not Created if ConfigUpdate Utility is Launched Right After Installing Identity Applications,” on page 23](#)
- ♦ [Section 6.1.1.10, “Identity Applications Silent Properties File Contains Incorrect Entry for Microsoft SQL Server,” on page 23](#)
- ♦ [Section 6.1.1.11, “Some Installation Wizards Display an Incorrect Icon for Components,” on page 23](#)
- ♦ [Section 6.1.1.12, “Navigation Panel is Truncated in Identity Reporting Installer,” on page 23](#)

- ♦ [Section 6.1.1.13, “Installation Programs Provide Examples for Linux Instead of Windows,” on page 23](#)
- ♦ [Section 6.1.1.14, “Filter Resource Changes Are Not Automatically Applied to the Package,” on page 24](#)

6.1.1.1 Cannot Specify Installation Paths on Windows that Include Spaces

The standalone installation programs for Identity Manager might not place the installation files in the specified location if the path contains spaces. Ensure that the specified path does not contain any spaces. (Bug 620797)

6.1.1.2 Engine Installation is Not Started Due to Mismatch in libXrender Libraries on RHEL and SLES Platforms

Issue: A mismatch in libXrender libraries occurs if your operating system does not have a 32-bit libXrender library.

Workaround: Install libXrender1-32bit RPM.

6.1.1.3 Pop-up Window is Displayed When Engine is Silently Installed

Issue: The silent installation program for the Identity Manager Engine displays a pop-up window while installing the platform agent components. (Bug 900781)

Workaround: This does not cause any impact on the installation.

6.1.1.4 LDAP Server Displays an Error While using VLV and SSS Controls

Issue: When you configure an LDAP search to use VLV (Virtual List View) and SSS (Server Side Sort) controls and the LDAP server does not hold a local copy of the user objects, the search fails with an error.

Workaround: Store the user objects into your local replica to use VLV and SSS controls. For more information see the TID [7001493](#).

6.1.1.5 Empty Remote Loader Installation Folder on Windows

Issue: Sometimes the Remote Loader installation program does not place the necessary Remote Loader files in the installation folder. [!\[\(Bug 1041852 resulted in this doc update\)\]](#)

This issue has been randomly observed on both 32-bit and 64-bit Remote Loaders on Windows.

Workaround: Reinstall Remote Loader. (Select only Remote Loader option during the installation.)

6.1.1.6 Remote Loader Trace Screen does not Close after Restart

Issue: After restarting the Remote Loader server, and you stop the Remote Loader instance on Windows 2012 R2 platform for the first time, it does not close the trace screen but the driver is stopped.

Workaround: In the [Service](#) panel, set the DirXML service to **Autostart (Delayed)**.

6.1.1.7 Incorrect Representation of Index Values in iMonitor

Issue: While viewing index values such as Path attributes in iMonitor, iMonitor fails to display the correct values of the attributes.

Workaround: There is no workaround at this time. It is safe to ignore this issue as it does not cause any functionality loss. (Bug 1023742)

6.1.1.8 Identity Applications Installer Does Not Create master-key.txt File in the File System During Installation

Issue: The identity applications installer prompts you to create a new master key or import it to the file system. If you create a new master key, the installer fails to create the master-key.txt file in the <UserApp-install> directory on Tomcat. (Bug 900240)

Workaround: Use the master key value from ism-configuration.properties file. The master key value is required while setting up Tomcat clustering.

6.1.1.9 Tables are Not Created if ConfigUpdate Utility is Launched Right After Installing Identity Applications

Issue: While installing the identity applications, if you select the option for creating tables at startup and do not start the application, but rather launch configupdate and click OK, the com.netiq.idm.create-db-on-startup setting is set to false. Because you have not actually started the application, the tables are not created. This issue causes the startup to fail because the tables do not exist. (Bug 900284)

Workaround: Open ism-configuration.properties, change the value from false to true, save the file, and then restart the application.

6.1.1.10 Identity Applications Silent Properties File Contains Incorrect Entry for Microsoft SQL Server

Issue: The silent properties file for the identity applications in the *ISO-root/RBPM/user_app_install* directory has an incorrect example for Microsoft SQL Server, as shown below:

```
=====
# Leave the quotes in place. Valid values:
# MySQL
# Oracle
# MS SQL Server
# PostgreSQL
NOVL_DB_TYPE=
=====
```

The entry shown is MS SQL Server, but the correct entry is Microsoft SQL Server. (Bug 900939)

Workaround: There is no workaround at this time.

6.1.1.11 Some Installation Wizards Display an Incorrect Icon for Components

Issue: The Tomcat and PostgreSQL convenience installer displays a Java icon instead of displaying an icon for Tomcat and PostgreSQL components. This issue is also observed in One SSO Provider (OSP).

Workaround: There is no workaround at this time.

6.1.1.12 Navigation Panel is Truncated in Identity Reporting Installer

Issue: In some languages, the navigation panel that appears on the left side of the installation program for Identity Reporting appears truncated. You might not be able to see all of the Navigation panel names. (Bug 899888)

Workaround: You can safely ignore the truncated navigation panel and continue with the installation.

6.1.1.13 Installation Programs Provide Examples for Linux Instead of Windows

Issue: The installation programs provide examples for most settings that you are required to specify. Some of the examples might be for a Linux platform, even when you install on a Windows server. Ensure that you specify values that work for Windows. (Bug 896265)

Workaround: There is no workaround at this time.

6.1.1.14 Filter Resource Changes Are Not Automatically Applied to the Package

Issue: If a driver contains a package that includes a filter resource, any changes made to the filter resource are not reflected in the driver filter. For example, when a new class or an attribute is added to the filter, the changes are not merged with the driver filter. (Bug 1103241)

Workaround: Manually synchronize the changes with the package.

- 1 In the Outline view, right-click the filter resource and select **Sync to Package**.
- 2 Select the package where you want to add the filter resource and click **OK**.

6.1.2 Identity Manager Engine Issues

- ♦ [Section 6.1.2.1, “Unable to Execute Large ECMAScripts,” on page 24](#)
- ♦ [Section 6.1.2.2, “Password Synchronization Status Attribute Not Updated when a New User is Migrated,” on page 24](#)
- ♦ [Section 6.1.2.3, “Increased Length of the OSP Attribute Value Causes Login Issues,” on page 24](#)

6.1.2.1 Unable to Execute Large ECMAScripts

Issue: This issue is caused by Rhino engine's inability to parse very large scripts. (Bugs 1016963, 942241)

Workaround: Identity Manager 4.6 supports Nashorn ECMAScript engine. Use this scripting engine for executing large ECMAScripts. For more information, see [“Engine Control Values”](#) in the *NetIQ Identity Manager Driver Administration Guide*.

For information about moving to Nashorn scripting engine, see the [Rhino Migration Guide](#).

6.1.2.2 Password Synchronization Status Attribute Not Updated when a New User is Migrated

Issue: When a new user is migrated from the Identity Vault, the password synchronization status attribute of the user is not updated with the password synchronization status. (Bug 1021792)

Workaround: There is no workaround at this time. When the password is changed again, the attribute is correctly updated.

6.1.2.3 Increased Length of the OSP Attribute Value Causes Login Issues

Issue: If you do not log out after every successful login into the identity applications, the value of the OSP attribute gradually increases after multiple logins. The increased length of the value causes login issues.

Workaround: Perform any one of the following approaches to resolve this issue:

Manually clear the value of the OSP attribute in iManager.

- 1 Log in to iManager.
- 2 In **View Objects**, select the user object.
- 3 In **Other** tab, double-click **oidInstanceData** attribute and clear the value.

Or,

Decrease the Refresh token lifetime value in configupdate utility:

- 1 Launch the configupdate utility.
- 2 Select the **Authentication** tab.
- 3 In **Authentication Configuration**, decrease the **Refresh token lifetime (hours)** value.

By default, **Refresh token lifetime (hours)** is set to 48 hours.

6.1.3 Remote Loader Issues

- ♦ [Section 6.1.3.1, “Cannot Generate Audit Events for 32-Bit and 64-Bit Remote Loaders on the Same Server,” on page 25](#)
- ♦ [Section 6.1.3.2, “A Few Packages Remain Uncleaned after Upgrading a 32-Bit Remote Loader to 64-Bit Remote Loader,” on page 25](#)
- ♦ [Section 6.1.3.3, “Remote Loader Installation Program Adds Driver Files to Two Separate Directories,” on page 25](#)
- ♦ [Section 6.1.3.4, “Installing the Remote Loader by using the Standalone and the Integrated Installers on the Same Windows Computer Is Not Supported,” on page 26](#)
- ♦ [Section 6.1.3.5, “Connection Between Remote Loader 4.5.3 and Identity Manager 4.6 Engine Fails,” on page 26](#)

6.1.3.1 Cannot Generate Audit Events for 32-Bit and 64-Bit Remote Loaders on the Same Server

Issue: Although you can install both a 32-bit and a 64-bit Remote Loader on the same computer, the lcache files for these versions cannot work concurrently. The audit events are logged to the lcache file for the version that you installed first. The log file for the other version displays the message: Agent already running error. (Bug 676310)

Workaround: Do not install both versions on the same computer.

6.1.3.2 A Few Packages Remain Uncleaned after Upgrading a 32-Bit Remote Loader to 64-Bit Remote Loader

Issue: When a 32-bit Remote Loader 4.5 is upgraded to a 64-bit Remote Loader 4.6, the upgrade process does not clean the following 32-bit 4.5 packages:

- ♦ novell-DXMLbase-4.5.0-0
- ♦ novell-DXMLgw-3.5.4-20131120
- ♦ novell-DXMLrdxml-4.5.0-0
- ♦ novell-NOVLjvml-4.5.0-0

Workaround: There is no workaround at this time.

6.1.3.3 Remote Loader Installation Program Adds Driver Files to Two Separate Directories

Issue: On Windows, the standalone and integrated installation programs install the Remote Loader in separate directories. The integrated installer installs all components including the Remote Loader in the c:\netiq directory. The standalone installer installs the Remote Loader in the c:\novell directory. If you are using the integrated installer and then select a driver shim, the driver shim defaults to c:\novell, which is not the correct directory. This issue causes the driver shim to fail. (Bug 908466)

Workaround: In the Remote Loader console, manually change the default installation path of the Remote Loader from c:\novell to c:\netiq if you installed it using the integrated installer. Ensure that you do not install the Remote Loader using the standalone installer and the integrated installer on the same Windows computer.

6.1.3.4 Installing the Remote Loader by using the Standalone and the Integrated Installers on the Same Windows Computer Is Not Supported

Issue: Identity Manager does not support installing the Remote Loader by using the integrated installer and the standalone installer on the same computer. This is an unsupported configuration and creates driver errors. (Bug 908466)

Workaround: Install the Remote Loader using the integrated installer and the standalone installer on separate Windows computers.

6.1.3.5 Connection Between Remote Loader 4.5.3 and Identity Manager 4.6 Engine Fails

Issue: You cannot establish an SSL connection between Remote Loader 4.5.3 and Identity Manager 4.6 engine. (Bug 1010680)

NOTE: This issue is observed only when a native Identity Manager driver uses Remote Loader. An example of a native driver is Identity Manager driver for Active Directory.

Workaround: Depending on the eDirectory version you are using, you can re-establish the connection in one of the following ways:

- ♦ **eDirectory 8.8.8.x:** Do one of the following:
 - ♦ Modify the Remote Loader configuration in the driver properties and add `secureprotocol=TLSv1` to it. For example, `hostname=ipaddress port=8090 kmo="SSL CertificateDNS" secureprotocol=TLSv1`.
 - ♦ Upgrade Remote Loader to 4.6 version.
- ♦ **eDirectory 9.0.1 or later:** Upgrade Remote Loader to 4.6 version.

6.1.4 Driver Issues

You might encounter the following issues as you use the Identity Manager drivers:

- ♦ [Section 6.1.4.1, “Statistics Report Shows Zero for Role and License Values for an Office 365 Driver,” on page 27](#)
- ♦ [Section 6.1.4.2, “Remote Loader Instance of a Driver Might Fail to Start If the Default Width of Windows Command Prompt Window is Changed,” on page 27](#)
- ♦ [Section 6.1.4.3, “dxcmd Query with Huge Output is Executed Twice,” on page 27](#)
- ♦ [Section 6.1.4.4, “Issue with Adding DirXML Accounts Entry When a User is Migrated,” on page 27](#)
- ♦ [Section 6.1.4.5, “Driver Cache Inspector is Unable to Display the Last Entry in the Cache List,” on page 27](#)
- ♦ [Section 6.1.4.6, “JMS Driver Fails to Start Due to Conflicting Jar Files,” on page 27](#)
- ♦ [Section 6.1.4.7, “Remedy Driver Does Not Start When Run Locally with the Identity Manager Engine,” on page 27](#)

6.1.4.1 Statistics Report Shows Zero for Role and License Values for an Office 365 Driver

Issue: The Statistics report for the Office 365 driver shows zero for **Role** and **License** values in the **Assigned Entitlements Per Type** section because of a limitation in the Office 365 driver. (Bug 893248)

Workaround: There is no workaround at this time.

6.1.4.2 Remote Loader Instance of a Driver Might Fail to Start If the Default Width of Windows Command Prompt Window is Changed

Issue: If you change the width of the Windows command prompt window from the default value, the driver instance might fail to start and it does not record any trace information. (Bug 854488)

Workaround: Reset the width of the Windows command prompt window to the default value of 80.

6.1.4.3 dxcmd Query with Huge Output is Executed Twice

Issue: When you issue a dxcmd command to a driver for processing a query, by default the Identity Manager engine waits 120 seconds for a response from the driver. If there is no response, the engine retries the query after the timeout. If there is no response after another 120 seconds, the engine displays ERR_TRANSPORT_FAILURE error. This results in the driver's processing the query twice. (Bug 1014581)

Workaround: Set the **environment variable** NCPCLIENT_REQ_TIMEOUT to a value greater than the time expected to execute the query.

6.1.4.4 Issue with Adding DirXML Accounts Entry When a User is Migrated

Issue: When a user is migrated from the Identity Vault with a driver without entitlements packages, Identity Manager does not populate a value for the DirXML-Accounts attribute for the user. This issue occurs when the information for the user is same in both connected application and the Identity Vault. (Bug 1016682)

Workaround: There is no workaround at this time.

6.1.4.5 Driver Cache Inspector is Unable to Display the Last Entry in the Cache List

Issue: On web browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge, the **Driver Cache Inspector** does not display the last entry in the driver cache list.

Workaround: Perform the following actions:

- 1 Expand all the cache entries in the list by selecting **Actions > Expand All** from the main menu.
- 2 Use the keyboard arrow keys to navigate to any expanded entry from the list.

6.1.4.6 JMS Driver Fails to Start Due to Conflicting Jar Files

Issue: On Linux platform, the JMS driver fails to start due to the location of conflicting Jar files.

Workaround: Copy the jms.jar from dirxml/classes to jre/lib/ext which is loaded first. (1000741)

6.1.4.7 Remedy Driver Does Not Start When Run Locally with the Identity Manager Engine

Issue: When the driver is configured to run locally with the Identity Manager engine, the driver fails to start due to a conflicting JAXB API included in the activemq-all-5.14.jar file and reports the following error message in the trace:

```
com.sun.xml.internal.ws.spi.db.DatabindingException: Unknown JAXBContext
implementation: class com.sun.xml.bind.v2.runtime.JAXBContextImpl
```

Workaround: Perform the following actions:

- 1 Install the driver with the Remote Loader.
- 2 Remove the activemq-all-5.14.jar file from the lib folder of the Remote Loader installation directory.
- 3 Start the driver.

6.1.5 Identity Reporting Issues

You might encounter the following issues when you use Identity Reporting:

- ♦ [Section 6.1.5.1, “Extended Attributes Table Does Not Reflect Removal of Extended Attributes,” on page 28](#)
- ♦ [Section 6.1.5.2, “Cannot Modify the Frequency of a Schedule,” on page 28](#)

6.1.5.1 Extended Attributes Table Does Not Reflect Removal of Extended Attributes

Issue: If you remove an attribute that was added to the Data Collection Service driver filter policy, Identity Manager does not remove the attribute from the extended attributes table (idmrpt_ext_attr, which tracks the attributes). Also Identity Manager does not remove data from the idmrpt_ext_item_attr table. (Bug 633209)

Workaround: You must update the database based on your configuration:

- ♦ When a custom attribute or an attribute on an extended object is removed from the DCS Driver filter:

For example, you use the attribute named srvprvCapabilities1

```
UPDATE idm_rpt_data.idmrpt_ext_item_attr
SET idmrpt_syn_state = 0
WHERE attribute_id =
  (SELECT attribute_id FROM idm_rpt_data.idmrpt_ext_attr WHERE attribute_name =
    'srvprvCapabilities1');
```

- ♦ When you remove an extended object from the DCS Driver filter:

For example, you use the object named Device

```
UPDATE idm_rpt_data.idmrpt_ext_item_attr attr
SET idmrpt_syn_state = 0
WHERE EXISTS
  (SELECT 1 FROM idm_rpt_data.idmrpt_ext_idv_item item,
    idm_rpt_data.idmrpt_ext_obj obj WHERE item.object_id = obj.object_id and
    attr.cat_item_type_id = 'EXTIDVOBJ' and attr.cat_item_id = item.item_id and
    object_class = 'Device')
```

```
UPDATE idm_rpt_data.idmrpt_ext_idv_item
SET idmrpt_syn_state = 0
WHERE object_id =
  (SELECT object_id FROM idm_rpt_data.idmrpt_ext_obj WHERE object_class =
    'Device');
```

6.1.5.2 Cannot Modify the Frequency of a Schedule

Issue: You cannot change the frequency of a schedule. For example, from week to month. (Bug 677430)

Workaround: To change the frequency, delete the schedule and create a new one.

6.1.6 iManager Plug-In Issues

You might encounter the following issues as you use iManager:

- ♦ [Section 6.1.6.1, “Exception on Windows 2016 When Using KMO,” on page 29](#)
- ♦ [Section 6.1.6.2, “Dependency on NDS-to-NDS Driver Certificates Wizard,” on page 29](#)
- ♦ [Section 6.1.6.3, “Some Actions Are Not Available in Policy Builder Plug-In,” on page 29](#)
- ♦ [Section 6.1.6.4, “Images Created by the Driver Set Dashboard Plug-In Are Not Removed After Leaving the Plug-In,” on page 29](#)

6.1.6.1 Exception on Windows 2016 When Using KMO

Issue: When you export a CA certificate in a .b64 format from iManager, a blank line is added at the end of the certificate. This makes the certificate invalid. (Bug 1018732)

Workaround: Manually remove the blank line from the certificate.

6.1.6.2 Dependency on NDS-to-NDS Driver Certificates Wizard

Issue: iManager needs the NDS-to-NDS Driver Certificates Wizard for proper functioning.

Workaround: To use the NDS-to-NDS Driver Certificates Wizard, download and install the iManager plug-in for NetIQ Certificate Server.

6.1.6.3 Some Actions Are Not Available in Policy Builder Plug-In

Issue: This release does not support building the following actions by using Policy Builder in iManager. (Bug 1018354)

- ♦ Create role
- ♦ Create resource
- ♦ Add resource
- ♦ Remove resource
- ♦ Generate XDAS event

Workaround: To build these actions, use Policy Builder in Designer.

6.1.6.4 Images Created by the Driver Set Dashboard Plug-In Are Not Removed After Leaving the Plug-In

Issue: Identity Manager temporarily creates the graphic files used by the Identity Manager Overview and Driver Set Dashboard plug-ins in the *<iManager Install Folder>/nps/images/temp* directory. (Bug 1002940)

The files created by the Driver Set Dashboard plug-in are not cleaned when you leave the plug-in or when Tomcat is stopped.

Workaround: Manually remove the file from the directory.

6.1.7 Identity Manager Upgrade Issues

- ♦ [Section 6.1.7.1, “Upgrading from Identity Manager 4.5 to 4.6 Deletes CA Certificates,” on page 30](#)
- ♦ [Section 6.1.7.2, “Progress Indicator Shows Truncated Directory Names for Some Components During Upgrade,” on page 30](#)
- ♦ [Section 6.1.7.3, “Upgrade Process Fails due to Missing Port Values in the URL,” on page 30](#)

6.1.7.1 Upgrading from Identity Manager 4.5 to 4.6 Deletes CA Certificates

Issue: The upgrade program replaces the old JRE folder but deletes all custom certificates from the folder. For example, the certificates are placed in the /opt/novell/eDirectory/lib64/nds-modules/jre/lib/security/cacerts directory on 64-bit Linux platforms. (Bug 794590)

Workaround: Complete the following steps:

- 1 Save the CA certificates in a custom location.
- 2 Upgrade Identity Manager 4.5 to 4.6.
- 3 Copy the certificates back to the JRE directory depending on your platform.

After the upgrade, verify the JRE version is 1.8.0_112.

6.1.7.2 Progress Indicator Shows Truncated Directory Names for Some Components During Upgrade

Issue: While upgrading OSP, SSPR, and the identity applications components, the installation directory names for these components appear truncated in the progress indicator.

Workaround: There is no workaround at this time.

6.1.7.3 Upgrade Process Fails due to Missing Port Values in the URL

Issue: If the port numbers are not specified in the **OSP OAuth redirect URL** parameter for each identity application, the upgrade process fails.

Workaround: Before launching the upgrade program, you must manually enter the port numbers in Configuration Update utility. Perform the following steps to specify the port values:

- 1 Launch the **Configuration Update** utility.
- 2 In **SSO Clients** tab, specify the appropriate port values in all the required URLs.
Use the following format: protocol://server:port/path
For example, http://192.0.2.0:80/dash

6.1.8 Localization Issues

- ♦ [Section 6.1.8.1, "Identity Manager Fails to Install Specific Drivers in Non-English Locales," on page 30](#)
- ♦ [Section 6.1.8.2, "Identity Manager Installers Contain Corrupt Characters in the Console Mode On Windows," on page 31](#)
- ♦ [Section 6.1.8.3, "Some Component Installers Are Not Localized," on page 31](#)

6.1.8.1 Identity Manager Fails to Install Specific Drivers in Non-English Locales

Issue: When you install selected drivers by using the **Customize the Selected Components** option in non-English locales, installation fails. (Bug 926490)

Workaround: Perform any one of the following actions:

- ♦ Select English as the language for installing Identity Manager instead of non-English languages.
- ♦ On Windows, copy the necessary JAR files from the installation media to the Identity Manager installation folder. On Linux, browse to products/IDM/linux/setup/packages in the installation media and run the following command:
 - ♦ **New installation:** rpm -ivf <file name>
 - ♦ **Upgrade:** rpm -Uvf <file name>

6.1.8.2 Identity Manager Installers Contain Corrupt Characters in the Console Mode On Windows

Issue: If you select Brazilian Portuguese, Danish, Dutch, English, French, German, Italian, Swedish, Spanish, or Russian as your choice of language for installing Identity Manager, the installer displays corrupt characters during installation.

If you select English, the installer contains a corrupt character on the *Select Language* page of the installation program. However, the characters display correctly for the Asian languages when the installer is run on Asian Windows. (Bug 672070)

Workaround: For the characters to display correctly, ensure that you change the default font of your Windows computer to Lucida Console by using the following steps before installing Identity Manager:

- 1 Go to **Start > Run > Regedit >**
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage and change the value of **OEMCP** from 850 to 1252.
For Russian, change the value of **OEMCP** from 866 to 1251 in the
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage directory.
- 2 Go to **Start > Run** and type **cmd** in the **Open** text box, then click **Enter** to launch the command prompt.
- 3 Right-click the title bar of the Command Prompt window to open the pop-up menu.
- 4 Scroll down in the pop-up menu and select the **Defaults** option to open the Console Windows Properties dialog box.
- 5 Click the **Font** tab and change the default font from **Raster** to **Lucida Console (TrueType)**.
- 6 Click **OK**.
- 7 Restart the computer.

6.1.8.3 Some Component Installers Are Not Localized

Issue: Localized versions of Apache Tomcat and PostgreSQL convenience installer, OSP, and Identity Reporting installation programs are not available in this release. You should run these component installers only in the English language.

Workaround: There is no workaround at this time. Select **English** as the language for installing Identity Manager instead of non-English languages. (Bug: 1008039)

6.1.9 Uninstallation Issues

- ♦ [Section 6.1.9.1, “Identity Manager Framework Uninstallation Does Not Remove all of the Folders from the Installation Directory,” on page 31](#)
- ♦ [Section 6.1.9.2, “On Windows, Identity Manager Framework Uninstallation Log Files Are Not Created in the Uninstallation Folder,” on page 32](#)
- ♦ [Section 6.1.9.3, “Uninstall the Identity Manager Entry from the Control Panel after Identity Manager Engine Upgrade on Windows,” on page 32](#)
- ♦ [Section 6.1.9.4, “Incorrect Message Is Displayed During Uninstallation,” on page 32](#)

6.1.9.1 Identity Manager Framework Uninstallation Does Not Remove all of the Folders from the Installation Directory

Issue: On Windows, the JAR files from the `lib` directory are not removed. (Bug 643077)

Workaround: Manually remove the JAR files from the `lib` directory.

6.1.9.2 On Windows, Identity Manager Framework Uninstallation Log Files Are Not Created in the Uninstallation Folder

Issue: The uninstallation log files are created in the temp directory. (Bug 613225)

Workaround: There is no functionality loss. You can ignore the issue.

6.1.9.3 Uninstall the Identity Manager Entry from the Control Panel after Identity Manager Engine Upgrade on Windows

Issue: After upgrading the Identity Manager engine to version 4.5, if you run the uninstallation program from the Control Panel, it successfully removes the necessary Identity Manager files except a specific registry key that leads to the Identity Manager entry being displayed in the Control Panel even after running the uninstallation. (Bug 901219)

Workaround: Delete the registry key from the following registry path when you run the uninstallation:

- ♦ **For 32-bit computers:**

\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Identity Manager

- ♦ **For 64-bit computers:**

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Identity Manager

6.1.9.4 Incorrect Message Is Displayed During Uninstallation

Issue: During uninstallation, the program displays the message, "InstallAnywhere is preparing to install...", while the program is actually uninstalling.

Workaround: There is no workaround at this time.

6.2 Advanced Edition Issues

- ♦ [Section 6.2.1, "Identity Manager Integrated Installation Issues," on page 32](#)
- ♦ [Section 6.2.2, "Identity Applications Issues," on page 36](#)

6.2.1 Identity Manager Integrated Installation Issues

- ♦ [Section 6.2.1.1, "Restart the Operating System After Installing Identity Manager on Linux," on page 33](#)
- ♦ [Section 6.2.1.2, "Installing Identity Manager with All Components in Silent Mode on Linux Fails to Create the Identity Applications," on page 33](#)
- ♦ [Section 6.2.1.3, "Installation Fails on Windows When You Use UNC Paths," on page 33](#)
- ♦ [Section 6.2.1.4, "authsamlProviderID Attribute Is Not Created for the SAML Authorization Object on Windows," on page 33](#)
- ♦ [Section 6.2.1.5, "Installation fails If the TMP or TEMP Directory Is Not Available On the C Drive," on page 34](#)
- ♦ [Section 6.2.1.6, "Cannot Restart Tomcat with Task Manager on Windows," on page 34](#)
- ♦ [Section 6.2.1.7, "Configuration Completion Page Does Not Close," on page 34](#)
- ♦ [Section 6.2.1.8, "Conflict with iManager Default Port When the Computer Is Restarted Before Configuring Identity Manager," on page 34](#)
- ♦ [Section 6.2.1.9, "Configuring a Password Policy for Identity Applications on a Secondary Server Displays Error Messages," on page 34](#)

- [Section 6.2.1.10, “Adding Rights to the User Container for Identity Applications on a Secondary Server Displays Error Messages,” on page 35](#)
- [Section 6.2.1.11, “Deselecting the Analyzer option on RHEL Platforms,” on page 35](#)
- [Section 6.2.1.12, “Label Names are Truncated in the Configuration Window on Linux,” on page 35](#)
- [Section 6.2.1.13, “Configures E-Mail Only for Identity Reporting,” on page 35](#)
- [Section 6.2.1.14, “Might Set Up a Wrong Identity Manager Edition on Windows,” on page 35](#)
- [Section 6.2.1.15, “Identity Vault Uninstallation Hangs in Silent Mode on Windows,” on page 36](#)
- [Section 6.2.1.16, “Uninstaller Does Not Completely Clean the Installation Folder on Windows,” on page 36](#)

6.2.1.1 Restart the Operating System After Installing Identity Manager on Linux

Issue: When you install all the Identity Manager components on Linux, auditing might not work properly. (Bug 900256)

Workaround: Restart the operating system after the installation has successfully completed. This is necessary so that auditing works properly.

6.2.1.2 Installing Identity Manager with All Components in Silent Mode on Linux Fails to Create the Identity Applications

Issue: When you install Identity Manager in silent mode by using the integrated installer without X Windows option, the Identity Manager driver deployment fails which causes the Identity Applications and Identity Reporting configurations to fail. This issue occurs on Linux where X Windows support is not available. This is because of the Eclipse 4.x version that invokes an unavailable user interface which is not required and subsequently the driver deployment fails. (Bug 914056)

Workaround: There is no workaround at this time.

6.2.1.3 Installation Fails on Windows When You Use UNC Paths

Issue: You cannot use UNC paths for installation and configuration when you use the Identity Manager integrated installation program. For example, \\myserver\share\Identity_Manager_4.6_Windows.iso. (Bug 627597)

Workaround: Create an actual mapped drive.

6.2.1.4 authsamlProviderID Attribute Is Not Created for the SAML Authorization Object on Windows

Issue: iManager does not list the authsamlProviderID attribute under **Valued Attributes**. This issue occurs only on the Windows server platform when Access Manager creates the SAML authorization object. (Bug 763167, Bug 762319)

Workaround: Complete the following steps:

- 1 Select authsamlProviderID in the **Unvalued Attributes** list and move it to the **Valued Attributes** list by clicking the left arrow.
- 2 In the input field, enter a value in the following format:

cn=<Name of the SAML Object>

For example:

cn=SCCp16ouo,cn=nids,ou=accessManagerContainer,o=novell

6.2.1.5 Installation fails If the TMP or TEMP Directory Is Not Available On the C Drive

Issue: If the TMP or TEMP folder is not available on the C drive, the installer fails to install Identity Manager. (Bug 891868)

Workaround: Create a TMP or TEMP directory on the C drive before starting the installer.

6.2.1.6 Cannot Restart Tomcat with Task Manager on Windows

Issue: You cannot use the Task Manager to restart Tomcat on a Windows server. (Bug 898945)

Workaround: To restart Tomcat, use one of the following methods:

- ♦ In the Services control panel, right-click **IDM Apps Tomcat Service** then click **Restart**.
- ♦ Use the command prompt to stop then start Tomcat:

```
net stop "IDM Apps Tomcat Service"
net start "IDM Apps Tomcat Service"
```

or

```
sc stop "IDM Apps Tomcat Service"
sc start "IDM Apps Tomcat Service"
```

6.2.1.7 Configuration Completion Page Does Not Close

Issue: Sometimes the configuration completion page does not close even if you press the **Done** button when Identity Manager is installed by using the integrated installation program.

Workaround: Terminate the installation program. (Bug 900241)

6.2.1.8 Conflict with iManager Default Port When the Computer Is Restarted Before Configuring Identity Manager

Issue: If you restart the computer after installing Identity Manager by using the integrated installer before configuring it, and attempt to configure it by running `./configure.bin`, it displays an error message. This error is because of the conflict between the installer and the iManager default port 8080. (Bug 900428)

Workaround: Stop iManager and the User Application Tomcat instance by running the following commands:

```
/etc/init.d/novell-tomcat8 stop
```

```
/etc/init.d/idmapps_tomcat_init stop
```

Proceed with the configuration using the integrated installer.

6.2.1.9 Configuring a Password Policy for Identity Applications on a Secondary Server Displays Error Messages

Issue: The following error messages are displayed: "D:\\install\\utilities\\ldapmodify.exe" - ZZ -h xx.x.x.xx -p 389 -D "cn=Admin,ou=services,o=xxxx" -w ***** -a -c -f "D:\\install\\utilities\\rbpm_sspr_uadmin_pwdpolicy.ldif" exitValue = 32

Workaround: To configure a password policy for identity applications on a secondary server, perform the following steps:

1. Edit the DN values for `rbpm_sspr_uadmin_pwdpolicy.ldif` from the <path to the file>`rbpm_sspr_uadmin_pwdpolicy.ldif` location.
2. Run the following command:

```
"D:\\install\\utilities\\ldapmodify.exe" -ZZ -h xx.x.x.xx -p 389 -
D"cn=Admin,ou=services,o=xxxx" -w ***** -a -c -
f"D:\\install\\utilities\\rbpm_sspr_uadmin_pwdpolicy.ldif"
```

3. (Optional) Verify whether you are able to configure the password policy for identity applications.

6.2.1.10 Adding Rights to the User Container for Identity Applications on a Secondary Server Displays Error Messages

Issue: The following error messages are displayed:

```
LD_LIBRARY_PATH="/mnt/install/utilities" "/mnt/install/utilities/ldapmodify" -ZZ -
h xxx.xx.xxx.16 -p 389 -D "cn=admin,ou=servers,o=system" -w ***** -a -c -f "/mnt/
install/utilities/sspr-edir-rights.ldif" exitValue = 32
```

Workaround: To add rights to the user container for identity applications on a secondary server, perform the following steps:

1. Modify the DN of the sspr-edir-rights.ldif file.
2. Run the following command:

```
LD_LIBRARY_PATH="/mnt/install/utilities" "/mnt/install/utilities/ldapmodify" -
ZZ -h xxx.xx.xxx.16 -p 389 -D "cn=admin,ou=servers,o=system" -w ***** -a -c -f
"/mnt/4.5/build/II/GMC1/147/install/utilities/sspr-edir-rights.ldif"

LD_LIBRARY_PATH="/mnt/utilities" "/mnt/install/utilities/ldapmodify" -ZZ -h
xxx.xx.xxx.16 -p 389 -D "cn=admin,ou=servers,o=system" -w ***** -a -c -f "/
mnt/utilities/sspr-edir-rights.ldif"
```

3. (Optional) Verify whether you are able to add rights to the user container.

6.2.1.11 Deselecting the Analyzer option on RHEL Platforms

Issue: Analyzer installation fails on RHEL platforms, because these platforms are not supported for Analyzer.

Workaround: Deselect the Analyzer option during installation.

6.2.1.12 Label Names are Truncated in the Configuration Window on Linux

Issue: Some label names appear truncated in the Configuration Window if the screen resolution is not properly set.

Workaround: Set the desktop resolution to 1920 x1080.

6.2.1.13 Configures E-Mail Only for Identity Reporting

Issue: The integrated installer uses the values specified for e-Mail (SMTP) server parameter to configure Identity Reporting and not the identity applications.

Workaround: After completing the installation, use **iManager** or **Configuration Update Utility** to configure the outgoing e-Mail server information used to configure the identity applications.

6.2.1.14 Might Set Up a Wrong Identity Manager Edition on Windows

Issue: Sometimes the installation program might not set up the correct version of Identity Manager. (Bug 900943)

Workaround: Run the following steps on your application server:

- 1 Copy products\IDM\windows\setup\.idme to the DIBFiles folder (for example, c:\NetIQ\IdentityManager\NDS\DIBFiles) and restart eDirectory.
- 2 Run the C:\NetIQ\IdentityManager\apps\UserApplication\configupdate.bat - use_console=false command.
- 3 In the RBPM configuration user interface, click **Show Advanced Options**.
- 4 Select **RBPM Security**.
- 5 Restart the application server.

6.2.1.15 Identity Vault Uninstallation Hangs in Silent Mode on Windows

Issue: The Identity Vault uninstallation hangs when you run the nds-uninstall command. (Bug 643781)

Workaround: To successfully uninstall the Identity Vault, complete the following steps:

- 1 Stop the DHost from the Task Manager.
- 2 Start the NDS service.
- 3 Start the uninstallation program.

6.2.1.16 Uninstaller Does Not Completely Clean the Installation Folder on Windows

Issue: The following command might fail with an exit value of 1:

```
cmd /c copy
"C:\Users\Administrator\AppData\Local\Temp\2\I1285831815\Windows\resource\jre\..\i
awin64_x64.dll"
"C:\Program Files (x86)\Novell\Identity
Manager\Uninstall_Roles-Based_Provisioning_Module_for_Novell_Identity_Manager\reso
urce\iawin64_x64.dll
```

The uninstaller does not remove the <Install> and the <system drive>\Novell\conf folders. (Bug 643077)

Workaround: Manually remove these folders.

6.2.2 Identity Applications Issues

You might encounter the following issues when you use the identity applications, which includes the Dashboard, Catalog Administrator, and the User Application:

- ♦ [Section 6.2.2.1, "SSPR Does Not Prompt to Set Security Questions in the First Login," on page 37](#)
- ♦ [Section 6.2.2.2, "Dashboard Displays Erroneous Count of Total Users," on page 38](#)
- ♦ [Section 6.2.2.3, "Pop-up Windows Might Display Contents in a Mix of Browser and Client Default Languages," on page 38](#)
- ♦ [Section 6.2.2.4, "Request and Approval Workflow Forms Have Right-Aligned Field Labels," on page 38](#)
- ♦ [Section 6.2.2.5, "CLE Restricted Browser Blocks Access to the Forgotten Password Page," on page 38](#)
- ♦ [Section 6.2.2.6, "Catalog Administrator Changes Focus after Creating a New Role or Resource," on page 38](#)

- ♦ Section 6.2.2.7, “Access Role and Resource Administration Requires Full Permissions,” on page 39
- ♦ Section 6.2.2.8, “Cannot Change Revoke Process from Quorum to Serial,” on page 39
- ♦ Section 6.2.2.9, “Cannot Display Dynamic Fields when a Resource is Mapped to a Role,” on page 39
- ♦ Section 6.2.2.10, “Copying Text in the Detail Portlet Displays an Error Message,” on page 39
- ♦ Section 6.2.2.11, “Content for the User Application Driver is Missing Trustees for Attestation Reports,” on page 39
- ♦ Section 6.2.2.12, “PostgreSQL Does Not Support Number Format of Simplified Chinese,” on page 40
- ♦ Section 6.2.2.13, “Can Approve or Deny a Role Request after the Role has been Deleted,” on page 40
- ♦ Section 6.2.2.14, “Creating and Copying the Base Package for the User Application Drivers causes Roles Based Provisioning Module to Fail,” on page 40
- ♦ Section 6.2.2.15, “Database Generation with the SQL File Produces an Erroneous Failure Message,” on page 40
- ♦ Section 6.2.2.16, “Cannot Start a Password for a User Application Account with the < Character,” on page 40
- ♦ Section 6.2.2.17, “Log File Reports Irrelevant Errors after a Successful Installation,” on page 40
- ♦ Section 6.2.2.18, “Home Postal Address Is Not Correctly Displayed in the User Application,” on page 41
- ♦ Section 6.2.2.19, “Issues in iPad iOS 6 Safari Browser,” on page 41
- ♦ Section 6.2.2.20, “Home and Provisioning Dashboard Issues,” on page 41
- ♦ Section 6.2.2.21, “Oracle 12c Database Creation Might take a Long Time,” on page 42
- ♦ Section 6.2.2.22, “User Application Navigation Items are Not Displayed When Using Safari on an iPad,” on page 43
- ♦ Section 6.2.2.23, “Customized CSS does not Synchronize with the Cluster Nodes,” on page 43
- ♦ Section 6.2.2.24, “ClientAbortException While Logging Out of the User Applications on Windows,” on page 43
- ♦ Section 6.2.2.25, “Role and Resource Service Driver Does Not Support Recalculation of Roles, Resources, and DirXML-EntitlementRef Attribute for a User,” on page 43
- ♦ Section 6.2.2.26, “catalina.out File Does Not Rotate the Log,” on page 43

6.2.2.1 SSPR Does Not Prompt to Set Security Questions in the First Login

Issue: This issue occurs when you log in to the identity applications with a user name containing a white space. (Bug 1025713)

Workaround: Replace the white space with an underscore ' _ ' in the user name before logging in to the application for the first time.

6.2.2.2 Dashboard Displays Erroneous Count of Total Users

Issue: The following issues are reported:

- ♦ When you add users and immediately refresh the view, the Dashboard lists the new users but does not update the count of total users. However, the updated total count of users is correctly displayed if you refresh the view after a few seconds.
- ♦ If a user has multiple values for either the given name or sn, the Dashboard shows different values for Search Count and Total Count. (Bug 1006448)

Workaround: There is no workaround at this time.

6.2.2.3 Pop-up Windows Might Display Contents in a Mix of Browser and Client Default Languages

Issue: When you perform an action that opens a pop-up window, the Dashboard might display a section of the window contents in the client's language instead of the browser's language. For example, viewing the details for a task opens a pop-up window. This issue occurs in Microsoft Internet Explorer or Edge browsers after the user changes the browser's language to one that is not the client's default language. (Bug 1019020)

Workaround: After changing the browser's language, close the current tab. Then open a new tab to log in to the Dashboard.

6.2.2.4 Request and Approval Workflow Forms Have Right-Aligned Field Labels

Issue: When accessing Request and Approval forms in the Dashboard, form field labels are right-aligned. (Bug 921403)

Workaround: To make the form field labels on Request and Approval workflows align from the left, add the following statement to each form's onload event:

```
$("#div.nv-formFieldLabel").parent().css("text-align", "left");
```

6.2.2.5 CLE Restricted Browser Blocks Access to the Forgotten Password Page

Issue: When you restrict access to websites but whitelist the Landing page for the identity applications, CLE Restricted Browser might block access to the Forgotten Password page for Self Service Password Reset. Users might see the following error:

"Access is restricted to your Target Server"

(Bug 1021647)

Workaround: In the whitelist, add the URL to the Forgotten Password page.

Also, if you upgrade from Identity Manager 4.5, update the link to Landing to direct users to the new Dashboard (/idmdash/#/landing) instead of Identity Manager Home (/landing) in the SSPR redirect URL section.

6.2.2.6 Catalog Administrator Changes Focus after Creating a New Role or Resource

Issue: After you create a role or a resource, Catalog Administrator does not maintain the user interface focus on that role or resource. Maintaining focus on the new role or resource allows you to more easily manage that role or resource. Instead, Catalog Administrator changes the focus to the first role or resource in the list.

Workaround: To manage a role or resource, scroll down or search the catalog.

6.2.2.7 Access Role and Resource Administration Requires Full Permissions

Issue: Accounts that do not have full permission for role and resource administration cannot access Catalog Administrator. The user cannot be a delegated administrator or have permission for only one domain.

Workaround: There is no workaround at this time.

6.2.2.8 Cannot Change Revoke Process from Quorum to Serial

Issue: If you change the revoke approval process from quorum to serial approval, the approval process does not change as expected.

Workaround: Change the approval process from quorum to none, and then change it to serial. Be aware that when you change the process from quorum to none, all associated approvers are lost, so ensure that you take note of the approvers and associate them to the process after you change it from none to serial.

6.2.2.9 Cannot Display Dynamic Fields when a Resource is Mapped to a Role

Issue: For resources that require fields to be supplied with values when the resource is requested, Catalog Administrator does not display the fields when you map the resource to a role.

Workaround: There is no workaround at this time.

6.2.2.10 Copying Text in the Detail Portlet Displays an Error Message

Issue: In Firefox or Dojo, if you attempt to copy text in the Detail portlet, an error message is displayed. (Bug 604174)

The following sequence of events cause this message to appear:

1. Log in to the User Application as administrator and go to the **Administration** tab.
2. Click **Portlet Admin > Detail Portlet** in Portlet Applications.
3. Click **Preferences > View/Edit custom Preferences > continue**.
4. Click the **HTML Layout edit** icon and enter some sample text, such as TEST.
5. Select the text and click **Copy**.

If you follow these steps, you see the following error message:

```
"Exception... "Access to XPCConnect service
denied" code: "1011" nsresult: "0x805303f3
(NS_ERROR_DOM_XPCONNECT_ACCESS_DENIED)" location:
"http://111.11.1.11:8180/IDMProv/resource//portal-general/javascript/
html_editor.js
Line: 531" " when clicked on Copy button.
```

You might also see this message when performing cut and paste operations.

Workaround: There is no workaround at this time.

6.2.2.11 Content for the User Application Driver is Missing Trustees for Attestation Reports

Issue: If you redeploy the User Application driver from Designer after running the integrated installation program, the trustees for the Attestation Report provisioning request definitions are deleted and no one can execute the report. This issue occurs because the trustees are added to the Attestation Report provisioning request definitions when the User Application starts. Because Designer does not know about the trustees, an attempt to redeploy the User Application driver from Designer removes the trustees. (Bug 641781)

Workaround: After starting the User Application, import these objects from eDirectory to synchronize the trustees.

6.2.2.12 PostgreSQL Does Not Support Number Format of Simplified Chinese

Issue: PostgreSQL does not install successfully if you install PostgreSQL on a server that is set up with Simplified Chinese as the number format (by using **Control Panel > Clock, Language, and Region > Region and Language > Formats tab > Format > Chinese, Simplified,PRC**). (Bug 683839)

Workaround: Ensure that the Simplified Chinese Number format is changed on the server where you are installing PostgreSQL.

6.2.2.13 Can Approve or Deny a Role Request after the Role has been Deleted

Issue: If an administrator deletes a role that requires a workflow after a user has made a role request, the workflow addressee for the role request still sees the workflow in the Task List and is able to approve or deny the request. (Bug 752860)

Workaround: There is no workaround at this time.

6.2.2.14 Creating and Copying the Base Package for the User Application Drivers causes Roles Based Provisioning Module to Fail

Issue: When you perform certain operations on the User Application base package that you created, such as removing the role configuration object, it causes RBPM to fail. (Bug 879595)

Workaround: NetIQ recommends that you do not create or copy the User Application driver base package.

6.2.2.15 Database Generation with the SQL File Produces an Erroneous Failure Message

Issue: When you use a SQL file to generate the schema in the Identity Applications database, the process attempts to create two database changelog tables. The second attempt fails because the table already exists.

Workaround: Ignore the error message. (Bug 896919)

6.2.2.16 Cannot Start a Password for a User Application Account with the < Character

Issue: You cannot use the special character "<" as the first character in a password for the User Application. For example, <testing12. The browser interprets the password as badly formatted HTML text, and the user cannot log in. (Bug 759297)

Workaround: There is no workaround at this time.

6.2.2.17 Log File Reports Irrelevant Errors after a Successful Installation

Issue: Although identity applications are successfully installed, the NetIQ-Custom-Install.log file displays the following errors:

```
ERROR: log4j:WARN No appenders could be found for logger  
org.apache.commons.configuration.PropertiesConfiguration).
```

```
ERROR: log4j:WARN Please initialize the log4j system properly.
```

Workaround: Do not take any action for these errors because the installation was successful. (Bug 898228)

6.2.2.18 Home Postal Address Is Not Correctly Displayed in the User Application

Issue: If you populate a user's home postal address in iManager using the **Other** tab, the User Application view of this address contains extra characters (delimiters). The Identity Manager User Application does not support the Postal Address Syntax (0.9.2342.19200300.100.1.39). (Bug 900613)

Workaround: There is no workaround at this time.

6.2.2.19 Issues in iPad iOS 6 Safari Browser

The following issues have been observed on Safari browser on iOS 6. No such issues are reported on other browsers, such as Chrome and Safari on iOS 7.

Fails to Display Navigation Items in Portrait Mode

Issue: If you are running the identity applications using Safari on an iPad that is in portrait orientation, the header navigation items do not always display properly.

Workaround: To display the header navigation item, select a navigation item on the left.

New Resource Button Does Not Work when Private Mode Setting is Disabled

Issue: The New Resource button does not work if the private mode setting is disabled. (Bug 867530)

Workaround: Enable the private mode setting on the browser before attempting to create a new resource.

Separation of Duties Editor Fails to Load the SoD Form in the Right Panel

The SoD editor does not load the SoD form. (Bug 867528)

Map Resources Button does not Work

The Map Resources button does not work as expected. (Bug 867526)

6.2.2.20 Home and Provisioning Dashboard Issues

The following issues occur in the Home and Provisioning Dashboard. Note that this feature will be deprecated in future. Please use the Dashboard introduced with this release.

Identity Manager Home and Provisioning Dashboard do not Support Digital Signatures in Workflows

Issue: The Identity Manager Home and Provisioning Dashboard do not currently support Request or Approval provisioning request definitions and workflows that require digital signatures.

Workaround: To request or approve a resource, and if your form requires a digital signature, use the User Application user interface to perform the action. (Bug 855367)

Provisioning Dashboard Displays all Possible Values for Valued Entitlements

If you use the Provisioning Dashboard to request a resource associated with a valued entitlement, the value field does not filter entitlements based on what you enter. Instead, the value field displays all the possible values for the entitlement, regardless of what you enter in the field. (Bug 857911, Bug 857829)

Workflows Report an Error when Using dateToString for Timestamp Control

Issue: Workflows that you created in the User Application and that use the form script method `dateToString` for a timestamp do not function appropriately in Identity Manager Home. The `dateToString` form script in the API includes seconds, while the new Date/Time control in Identity Manager Home does not. The new script uses a different format. To ensure that your

forms function with Identity Manager Home, you must replace `dateToString` with the new script:

```
new Date().toString('Date.CultureInfo.formatPatterns.shortDate'+
"+Date.CultureInfo.formatPatterns.shortTime');
```

Workaround: To replace the control for a single date in your form, you might use the following code:

```
document.getElementById('%Field-Name').value = new
Date().toString('Date.CultureInfo.formatPatterns.shortDate'+
"+Date.CultureInfo.formatPatterns.shortTime');
```

However, you might need to replace controls that represent two dates. For example, you might have a form requiring that the user specify a start and end time for an entitlement request.

To specify `startDate`, use the following type of code:

```
document.getElementById('_startDate').value = new
Date().toString('Date.CultureInfo.formatPatterns.shortDate'+
"+Date.CultureInfo.formatPatterns.shortTime');
```

To specify an `endDate` that occurs three days after the starting date, use the following type of code:

```
var s = new Date().getTime();
s = s + 3 * 1000 * 24 * 60 * 60;
document.getElementById('_furDate').value = new
Date(s).toString('Date.CultureInfo.formatPatterns.shortDate'+
"+Date.CultureInfo.formatPatterns.shortTime');
```

In this example, the workflow responds with the following information:

```
startDate: 3/14/2014 12:03 PM
endDate: 3/17/2014 12:03 PM
```

NOTE: In the above codes, if you want to use only `DatePicker` in your form you can exclude `'Date.CultureInfo.formatPatterns.shortTime'` from the code.

For example, if you want to specify only date for `startDate`, you can use following type of code:

```
document.getElementById('_startDate').value = new
Date().toString('Date.CultureInfo.formatPatterns.shortDate');
```

Email Approval Failure Notification is Displayed in Identity Manager System Language For Already Processed Tasks

The Provisioning Dashboard sends an email approval failure notification in the system language instead of the specified language for the already processed tasks. (Bug 1024491)

Duplicate Email Responses When Email Service Protocol is Changed

Issue: The Provisioning Dashboard sends duplicate email responses for already processed emails if you switch the email service protocol from IMAP to POP3 or vice-versa. (Bug 1024688)

Workaround: Clear the processed emails from the incoming email server before switching the email service protocol.

6.2.2.21 Oracle 12c Database Creation Might take a Long Time

Issue: In this release, creating an Oracle 12c database takes significantly longer than creating databases in previous releases. The creation does not time out if there is no problem with the database creation, so plan for the extra time.

Workaround: There is no workaround at this time.

6.2.2.22 User Application Navigation Items are Not Displayed When Using Safari on an iPad

Issue: If you are running the User Application using Safari on an iPad that is in portrait orientation, the header navigation items do not always display properly.

Workaround: To display the header navigation item, select a navigation item on the left.

6.2.2.23 Customized CSS does not Synchronize with the Cluster Nodes

Issue: In Identity Manager Dashboard, when you upload the customized CSS in the cluster, CSS changes are not applied on all the cluster nodes. (1025836)

Workaround: Ensure that each node in the cluster has the same copy of CSS in the following location:

<user home directory>/netiq_custom_css

6.2.2.24 ClientAbortException While Logging Out of the User Applications on Windows

Issue: If you try to list users either by selecting **Identity Manager Dashboard > People > Users** or by selecting **Manage Users** and then log out of the identity applications before Dashboard displays the total count of users in the browser, this process generates a `ClientAbortException` exception in the `catalina.out` file. This exception can also occur in the following cases while working with the identity applications:

- ♦ The browser window is closed.
- ♦ Network is disconnected.
- ♦ Session has timed-out.

Workaround: There is no workaround at this time. It is safe to ignore this exception as it does not cause any functionality loss.

6.2.2.25 Role and Resource Service Driver Does Not Support Recalculation of Roles, Resources, and DirXML-EntitlementRef Attribute for a User

Issue: If you resynchronize a user in the Role and Resource Service driver, the driver checks the user attributes in the filter and synchronizes them, but it does not recalculate the roles and resources assigned to the user. (Bug 1093450)

Workaround: There is no workaround at this time.

6.2.2.26 catalina.out File Does Not Rotate the Log

Issue: If you installed Identity Applications on Linux or Windows, the `catalina.out` file does not rotate the log.

Workaround on Linux: Perform the following actions:

- 1 Open a text editor and create a `netiq-tomcat` file at `/etc/logrotate.d/` with the following entries:

```

/opt/netiq/idm/apps/tomcat/logs/catalina.out {
    copytruncate
    daily
    dateext
    dateformat -%Y-%m-%d
    rotate 25
    notifempty
    missingok
    compress
    su novlua novlua
}

```

- 2 Verify that logrotate is scheduled to run at midnight.
- 3 Verify that novlua user and novlua group permissions are set for the catalina.out file.
- 4 Verify that the log is correctly rotated.

Run the following command:

```
/usr/sbin/logrotate -d /etc/logrotate.d/netiq-tomcat
```

You should see messages similar to the below in the screen.

```

reading config file /etc/logrotate.d/netiq-tomcat
Handling 1 logs
rotating pattern: /opt/netiq/idm/apps/tomcat/logs/catalina.out after 1 days (25
rotations)
empty log files are not rotated, old logs are removed
switching euid to 485 and egid to 0
considering log /opt/netiq/idm/apps/tomcat/logs/catalina.out
log does not need rotating
switching euid to 0 and egid to 0

```

Workaround on Windows: There is no workaround at this time.

6.3 Standard Edition Issues

- [Section 6.3.1, “Delimited Text Driver Loops Endlessly on a Publisher Channel Event when Permission Collection and Reconciliation Service is Enabled,” on page 44](#)
- [Section 6.3.2, “Reporting Admin Role Must Exist Before Beginning Identity Manager Standard Edition Reporting Installation,” on page 44](#)

6.3.1 Delimited Text Driver Loops Endlessly on a Publisher Channel Event when Permission Collection and Reconciliation Service is Enabled

Issue: The Permission Collection and Reconciliation Service (PCRS) functionality is not supported in the Standard Edition. This issue might occur in Standard Edition when PCRS is enabled. When there is a change in an event in the Publisher channel, it causes a change in one or more permission attributes defined in the custom entitlements (.csv file). The driver keeps checking for the creation of the resources and loops endlessly. (Bug 907031)

Workaround: Disable PCRS.

6.3.2 Reporting Admin Role Must Exist Before Beginning Identity Manager Standard Edition Reporting Installation

If you install Identity Reporting using the Identity Manager Standard Edition installation, the Report Admin role must exist before you start the installation process.

Workaround: If you completed the installation without creating the Report Admin role, run the Configuration Update utility (configupdate.sh) to create the role.

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](http://www.netiq.com/support/process.asp#phone) (<http://www.netiq.com/support/process.asp#phone>).

For general corporate and product information, see the [NetIQ Corporate website](http://www.netiq.com/) (<http://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 © 2017 NetIQ Corporation. All Rights Reserved.

