NetIQ Identity Manager 4.7 Release Notes

March 2018

NetIQ Identity Manager 4.7 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.

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:

- “What’s Changed, Deprecated, or Discontinued?” on page 14
- “Separate Setup Guides for Linux and Windows Platforms” on page 16
- “End User License Agreement is Not Available in All Supported Languages” on page 16
- “NetIQ Corporation Does Not Provide Support for the Components in the PostgreSQL and Tomcat Installation” on page 16

New Features

Identity Manager 4.7 provides the following key features, enhancements, and fixes in this release:

- “Simplified Installation on Linux Platforms” on page 2
- “Uniform Auditing” on page 3
- “Extended Support of Subscriber Service Channel for New Drivers” on page 3
- “Simplified Permission Reconciliation Services” on page 3
- “Changed Access to Identity Manager Data Collection Services” on page 3
- “Ability to Filter Entitlement Events of Other Drivers” on page 4
- “New Features and Enhancements in Identity Applications” on page 4
- “Simplified Packaging of Installation Files” on page 5

For information about the new features in NetIQ Identity Manager Designer 4.7, see NetIQ Identity Manager Designer 4.7 Release Notes.

There are no new features for NetIQ Identity Manager Analyzer 4.7 except the updated Java version. For more information, see NetIQ Identity Manager Analyzer 4.7 Release Notes.

Simplified Installation on Linux Platforms

Identity Manager offers a new simplified and scripted installation program for Linux platforms. The new installation program supports interactive and silent methods for installing Identity Manager components. The installation process comprises of an install phase and a configuration phase. The install phase lays down the required binaries. The configuration phase configures the Identity Manager components. The new installer introduces typical and advanced configuration modes.

A typical configuration uses common defaults for most values and is suitable for quickly installing the product. Custom configuration is suited for production environments. The new installer also contains a utility to generate the silent property file in an interactive mode. The new installer does not support graphical user interface (GUI) installation method.

For information about downloading the installation files, see “Installing NetIQ Identity Manager 4.7” on page 23. For installation instructions, see the *NetIQ Identity Manager Setup Guide for Linux*.

Uniform Auditing

Identity Manager introduces Common Event Format (CEF), an open log management standard, for auditing events across all Identity Manager components. CEF is an extensible, text-based format designed to support multiple device types by offering the most relevant information. Using CEF reduces the message syntaxes to work with Embedded Syslog Manager normalization. CEF defines a syntax for log records comprised of a standard header and a variable extension, formatted as key-value pairs.

CEF logging is disabled by default. To enable it, see Configuring Identity Manager Components to Log Audit Events in CEF Format in the *NetIQ Identity Manager - Configuring Auditing in Identity Manager*.

NOTE: If you upgrade to Identity Manager 4.7, XDAS is still available for Identity Manager components except identity applications. NetIQ recommends to use CEF for auditing for all components. XDAS will be deprecated in the future.

Extended Support of Subscriber Service Channel for New Drivers

The Subscriber Service Channel support that was introduced for the JDBC Fan-Out driver in Identity Manager 4.6 has been extended to the following Identity Manager drivers in this release: Active Directory, Multi-Domain Active Directory, and JDBC.

The Subscriber Service Channel enables you to separately process the out-of-band queries without interrupting the normal flow of cached events. Examples of out-of-band queries are code map refresh queries, data collection queries and queries triggered from dxcmd. This helps to improve the performance of the driver while processing cached events.

For more information, see Improving Driver Performance Using Subscriber Service Channel in the *NetIQ Identity Manager Driver Administration Guide*.

Simplified Permission Reconciliation Services

Permission Collection Reconciliation Services (PCRS) is simplified for Active Directory, Multi-Domain Active Directory (MDAD) and LDAP drivers. This implementation is known as Controlled Permission Reconciliation Services (CPRS).

In the new implementation, CPRS is integrated with Identity Manager Dashboard to assist you reconcile the connected system’s permissions with identity applications. For more information, see Using Controlled Permission Reconciliation Services in the *NetIQ Identity Manager - Administrator’s Guide to the Identity Applications*.

Identity Manager supports migrating permissions from PCRS to CPRS for Active Directory, MDAD, and LDAP drivers. For other Identity Manager drivers, you can continue using PCRS. For more information, see Migrating to CPRS in the *NetIQ Identity Manager - Administrator’s Guide to the Identity Applications*.

Changed Access to Identity Manager Data Collection Services

Identity Manager introduces a new web page to access Data Collection Services (DCS). You can directly launch the DCS page from the identity applications user interface or access it from a browser. This is a step towards making the user interface consistent across Identity Manager components.

The DCS page allows you to configure the settings for the connected systems that you want to report, and provide information for Identity Reporting. For more information, see Exploring Identity Manager Data Collections Services in the *Administrator Guide to NetIQ Identity Reporting*.

Ability to Filter Entitlement Events of Other Drivers

With this release, events on DirXMLEntitlement-Ref attribute contain only the entitlement changes of that particular driver. This functionality can be controlled by a new Engine Control Value, Ignore Entitlement Changes of other drivers. For more information, see Engine Control Values in the *NetIQ Identity Manager Driver Administration Guide*.

New Features and Enhancements in Identity Applications

The Identity Applications component includes the following new features and enhancements:

Support for Helpdesk

Identity Manager introduces a new Helpdesk feature to help users to troubleshoot any issues while performing their tasks in Identity Manager. Some of the tasks that Helpdesk can perform are:

- Reassign an approval request that is unattended for a long time
- Browse all tasks or filter tasks for a selected user
- Request permissions on behalf of other users

Users can contact Helpdesk by using the Helpdesk email ID, contact number, or raise a Helpdesk ticket. After setting up a Helpdesk, the administrator can customize the Helpdesk information for your clients from the Dashboard client settings.

For more information, see the following links:

- Understanding a Client Helpdesk in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*
- Using Helpdesk in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*
- Raising a Helpdesk Ticket in the *NetIQ Identity Manager - User's Guide to the Identity Applications*

Support for Resource Expiration

This release allows you to set the expiration time period for the identity applications resources. This time period decides when access to a particular resource should expire from the date of assigning the resource. Additionally, users can request a resource for a specific time period. For more information, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Support for Delegation

This feature allows you to delegate your tasks to other users based on delegation configuration. You can configure delegation through the Dashboard in the identity applications.

For more information, see Creating and Managing Delegations in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* and Managing Delegations in the *NetIQ Identity Manager - User's Guide to the Identity Applications*.

Revoke on Behalf

This release extends support for administrators and team managers to revoke a permission on behalf of someone else. It is also possible to revoke multiple permissions at one time.

For more information, see Revoking Permissions in the *NetIQ Identity Manager - User's Guide to the Identity Applications*.

Support for Customizing the Dashboard

This release allows you to customize the widgets on your dashboard. Administrators can set preferences for the client users to add or remove widgets on their dashboards. For more information, see Customizing the Identity Applications for Your Enterprise in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Modernized Roles and Resource Management

This release integrates role and resource administration capabilities with the dashboard. This functionality was previously provided by Catalog Administrator. The new interface provides richer user interface experience for role and resource management. It also provides capability to assign or revoke roles and resources. For more information, see Creating and Managing Roles and Creating and Managing Resources in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Roles and Resource Service Driver Performance Improvements

The Roles and Resource Service driver has been enhanced to include multiple threads to handle different tasks such as role and resource assignments, targeted to significantly improve the driver performance. For more information, see Multi-Threaded Role and Resource Service Driver in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Purging Resource History in Role and Resource Service Driver

By default, the driver is configured to purge the resource history on a daily basis. The driver only purges data from the resource history that is older than the retention value (in days) specified for the Store resource history for days setting. Any historical data that is more recent than the specified retention value is retained.

Support for Return and Reassign Tasks

Now different users can reassign and return the reassigned tasks through the Identity Manager Dashboard. Identity Manager personas such as Team Manager, Administrators, Helpdesk, and End Users have different capabilities to reassign and return tasks. For more information, see Managing Requests for Approval or Denial in the *NetIQ Identity Manager - User's Guide to the Identity Applications*.

Proxied Authorization Control for User Application

Proxied Authorization Control for User Application provides a mechanism for specifying an authorization identity on a per-operation basis, benefiting administrators who need to perform operations efficiently on behalf of other users. This eliminates User Application's need for SAML certificates while performing any operations on the Identity Vault.

Simplified Packaging of Installation Files

This version provides simplified packaging of Identity Manager components in a single ISO, each for Linux and Windows operating systems. Designer and Analyzer are also provided in separate files. Sentinel for IGA is provided in a separate file for ease of configuration with Identity Reporting.

Operating System Support

This release adds support for the following platforms:

- SUSE Linux Enterprise Server (SLES) 12 SP2, SLES 12 SP3
- Red Hat Enterprise Linux (RHEL) 7.3, RHEL 7.4, and RHEL 7.5

- Open Enterprise Server (OES) 2018 Update 3, OES 2018 SP1
- Microsoft Windows Server 2012 R2, 2016

IMPORTANT: Sentinel Log Management for Identity Governance and Administration (IGA) is not supported on OES 2018.

For a complete list of supported operating systems, see the Technical Information for Identity Manager page. For information about the components packaged, databases, and browsers supported with this release, see "Supported Component Versions" on page 17.

Fixed Issues

This release includes the following software fixes:

- "SSPR No Longer Prompts to Set Security Questions in the First Login" on page 8
- "Identity Applications Installer Successfully Creates master-key.txt File in the File System During Installation" on page 8
- "Applications Page Now Opens an External Application in a Different Tab" on page 8
- "Identity Manger Engine Installation Includes novell-DXMLsch package on Linux" on page 8
- "Identity Manager Engine Applies Restriction on Addition of Auxiliary Classes in a Driver Filter" on page 8
- "Tomcat's server.xml Connection String Correctly Includes a Non-default Port Specified for Oracle Database When Identity Reporting Is Configured on Linux" on page 8
- "Create_rpt_roles_and_schemas.sql Required Before Identity Reporting Installation with Oracle Database on Linux" on page 8
- "Ability to Control File Rights with Writelog to AJC-JavaScript" on page 9
- "Remote Loader Password Ignores Parentheses" on page 9
- "Token Map Returns Empty Result in Case of a No Match" on page 9
- "Duplicate View of idmrpt_identity_v1 Is Removed" on page 9
- "do-remove-role Token Supports Correlation ID" on page 9
- "Identity Reporting Correctly Creates Placeholder Entries in the Oracle Database" on page 9
- "Output Transform Policy Correctly Issues a Fatal Status Message Indicating to Stop the Driver" on page 9
- "Identity Manager Engine Honors optimize-modify="false" Filter Setting on Publisher Merge" on page 9
- "Password Policy Plug-in Shows Correct Information About the Permitted Password Length" on page 9
- "Home Email Field in User ProfileProperty Pages Plug-in Allows Value Exceeding Thirty Two Characters" on page 9
- "dxcmd Batch Mode Includes Get Priority Sync Cache Statistics" on page 10
- "Office365 Driver Subscriber Matching Policy Uses token-src-name Instead of token-src-attr" on page 10
- "Reporting Database Is Correctly Updated After a Resource Removal Action Requiring an Approval Is Executed" on page 10
- "Identity Manager Linux Installer Prompts an Error Message If the Mounted Directory Has a Space in It" on page 10
- "Calling a Java Function with Thirty Six Parameters from A Driver Policy Fails after Upgrading from Identity Manager 4.0.2" on page 10

- “Ability to Sort Request History in the Dashboard” on page 13
- “Role and Resource Service Driver” on page 14
- “Upgrading NetIQ iManager to 3.1 Does Not Display any Error Message on Identity Manager Overview Page” on page 14

SSPR No Longer Prompts to Set Security Questions in the First Login

When you log in to the identity applications with a user name containing a white space, SSPR no longer prompts you to set security questions in the first login. (Bug 1025713)

Identity Applications Installer Successfully Creates master-key.txt File in the File System During Installation

The Identity Applications installer now creates the `master-key.txt` file in the `<UserApp-install>` directory on Tomcat. You must read the master key value from this file instead of `ism-configuration.properties` file while setting up Identity Applications components on a Tomcat cluster. (Bug 900240)

Applications Page Now Opens an External Application in a Different Tab

In Identity Manager Dashboard, when you click an external application from the **Applications** page, it opens the application in a different tab instead of opening it in the same tab. (Bug 1079325)

Identity Manger Engine Installation Includes novell-DXMLsch package on Linux

This release introduces a customized installation and configuration process on Linux platforms. The installation process for Identity Manager engine installs novell-DXMLsch package for all installation scenarios. (Bug 1054169)

Identity Manager Engine Applies Restriction on Addition of Auxiliary Classes in a Driver Filter

The auxiliary classes are not processed by the Identity Manager engine. It ignores this operation and reports a warning in the driver trace file. (Bug 1041056)

Tomcat’s server.xml Connection String Correctly Includes a Non-default Port Specified for Oracle Database When Identity Reporting Is Configured on Linux

The new Identity Manager installation program for Linux uses the value specified for a non-default database port during the configuration phase to update the connection URL in the Tomcat server.xml file. (Bug 1063010)

Create_rpt_roles_and_schemas.sql Required Before Identity Reporting Installation with Oracle Database on Linux

When you run the installation program for Identity Reporting on Linux, the process lays down the `.sql` files required for configuring the database schema. (Bug 1063009)

Ability to Control File Rights with Writelog to AJC-JavaScript

ECMAScript has been enhanced to include a new function, setFilePermissions, to allow you to change the posix file rights on Linux. (Bug 1023201)

Remote Loader Password Ignores Parentheses

Identity Manager successfully processes a Remote Loader password with or without close-parenthesis specified for establishing a connection with the Identity Manager engine. (Bug 919823)

Token Map Returns Empty Result in Case of a No Match

The token map policy does not execute if it does not find a matching token. (Bug 1063065)

Duplicate View of idmrpt_identity_v1 Is Removed

The idmrpt_identity_v1 view was similar to the idmrpt_identity_cs_v view. The idmrpt_identity_v1 has been removed from the database schema to remove duplication. (Bug 824615)

do-remove-role Token Supports Correlation ID

The do-remote-role token has been enhanced to accept a correlation id value. By default, it uses the correlation id value from the operation event id unless it is specified. (Bug 933953)

Identity Reporting Correctly Creates Placeholder Entries in the Oracle Database

Identity Reporting no longer processes a user belonging to a group that does not exist in the Oracle database. (Bug 1075816)

Output Transform Policy Correctly Issues a Fatal Status Message Indicating to Stop the Driver

The output transform policy has been enhanced to issue a fatal status message in the Publisher trace indicating that the driver should be shut down. (Bug 1050608)

Identity Manager Engine Honors optimize-modify="false" Filter Setting on Publisher Merge

After a successful match on the publisher channel, when all attribute values are correctly set in the Identity Vault, the engine correctly process an operation containing all attributes with publisher="sync" and optimize-modify="false" settings. (Bug 794273)

Password Policy Plug-in Shows Correct Information About the Permitted Password Length

The Password policy plug-in user interface has been updated to state that the password policy does not honor passwords with less than three characters. (Bug 936162)

Home Email Field in User ProfileProperty Pages Plug-in Allows Value Exceeding Thirty Two Characters

The Home Email field in the User ProfileProperty Pages plug-in now allows you to specify a value more than thirty two characters. (Bug 997453)

dxcmd Batch Mode Includes Get Priority Sync Cache Statistics

dxcmd now provides Priority Sync Cache Statistics in both batch and interactive mode. (Bug 1014476)

Office365 Driver Subscriber Matching Policy Uses token-src-name Instead of token-src-attr

The use of token-src-name prevents the driver from forcing an unnecessary query back to the Identity Vault before each and every match. This improves the performance of the driver during heavy load such as initial migration of users. (Bug 881132)

Reporting Database Is Correctly Updated After a Resource Removal Action Requiring an Approval Is Executed

Once the approver approves the resource revocation, the identity_trust table is correctly updated and the Trust status changes from 1 to 0. (Bug 1067991)

Identity Manager Linux Installer Prompts an Error Message If the Mounted Directory Has a Space in It

The Identity Manager Linux installer has been enhanced to report an error when it finds a space in the directory where you are mounting the ISO file. (Bug 910386)

Calling a Java Function with Thirty Six Parameters from A Driver Policy Fails after Upgrading from Identity Manager 4.0.2

The Identity Manager engine has been enhanced to successfully process thirty six arguments. (Bug 1055873)

Using dxcmd in Non-interactive Mode for Clearing Cache Contents

You can now delete a driver's cache using dxcmd in a non-interactive mode, and any time. (Bug 1006754)

Driver Set Dashboard Plug-in Cleans up the Temporary Directory of Images

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. The temp directory is now cleaned when the Tomcat server hosting iManager is restarted. (Bug 1001237)

Members in Group Distribution or Mail-Enabled Security Are Not Synchronized in Azure Active Directory

A group member from Identity Vault is successfully synchronized with Azure Active Directory groups. (Bug 1077198)

OSP Performs Post-Authentication Check When Configured with Kerberos

If you have configured OSP with Kerberos, OSP now preforms the post-authentication check for the user to determine if the user has an expired password or needs to answer Challenge Response questions. (Bug 924221)

Identity Manager Engine Allows Additional Driver Health Jobs

The Identity Manager engine is enhanced to store and process multiple health job configurations on a driver attribute. (Bug 870219)

Identity Manager Installer That Has Its Location Configured as The Netherlands Defaults to German on Windows

This issue has been fixed now. Now the installer defaults to English. (Bug 768958)

Importing SQL File for Oracle Database Does Not Returns Errors

The SQL file is generated when **Write SQL** option is selected during identity applications installation. The identity applications now successfully imports the SQL file into the Oracle database. (Bug 1057368)

Identity Applications Upgrade Utility Provides Information About the Versions of the Components It Is Upgrading to on Windows

The upgrade utility now displays the new versions of the components that it will upgrade the currently installed components to. (Bug 1031435)

Identity Applications Upgrade Utility Handles Custom Context

You can now use a different context instead of the default context (IDMProv) during the upgrade. (Bug 1028475)

Ability to Use a Non-Standard E-Mail Port in Identity Manager Configuration

You can now have your E-Mail server listen on a non-standard SMTP port. (Bug 1041493)

Remote Loader Trace Screen Closes After System Reboot on Windows 2012

This issue no longer exists. The Remote Loader trace screen properly closes. (Bug 892034)

Ability to Search a User with a Full Name in the Dashboard

All the user attributes that are marked as search in DAL can now be marked as search attribute in the User Catalog from the settings page in the Dashboard. (Bug 1073463)

Request History for a Specific Period Is Displayed

The Dashboard has been updated to display your requests for the period specified by your administrator. (Bug 1061696)

Improved View of Permission List

The Dashboard displays only direct assignments. It also include an icon to allow you to view the list of all permissions. (Bug 1061516)

Resource Notification Pop-up displays CN Instead of FQDN in the Dashboard

The Dashboard now displays only the resource cn in the notification panel. (Bug 1055622)

Adding Workflows, Resources, or PRD on the Applications Page

In the new user interface, you can create deep-links in the Applications page for workflows, resources, and PRDs. When you click on a tile in this page, it opens the form in a new tab. After submitting the request, it brings you back to the Application page. (Bug 988818)

Provision for Retracting Role and Resource Assignment Request By Using SOAP/REST Endpoint

You can now issue a role grant or a role revoke request through a Role SOAP or REST endpoint in addition to being able to do perform this action through the user interface. (Bug 846736)

Dynamic Resource Assignment Search Correctly Returns the Desired Entitlements

If you use the Dashboard to request a resource associated with a valued entitlement, the Dashboard correctly filters the entitlements based on your search criteria. (Bug 995889)

Deleted Approvers Are Not Displayed in the Approvers List

The deleted approvers are no longer listed in the roles catalog of the new Administration page. (Bug 632362)

Update Role And Role Relationship String is Correctly Translated in Spanish

This issue has been fixed in this release. (Bug 1076780)

Opening PRDs from Applications Page in the Dashboard

Based on the settings in the Request and Applications page, you can open PRDs either in a new tab or the same window. (Bug 1076155)

Integration Activity Supports Communication with Servers Enabled with Mutual Authentication

When provided with client and private certificate, you can successfully communicate with a server enabled with mutual authentication through Integration Activity. (Bug 1075309)

Dashboard’s OrgChart Displays Objects and Attributes Permitted for a User

OrgChart correctly displays information that the user is authorized to see. (Bug 1076155)

idmapps_tomcat_init Script No Longer Requires etc/rc.d/init.d/functions to Have Execute Permissions to Run the Service as a Daemon on Linux

The installation software has been updated to remove this dependency. (Bug 1064603)

Default Notification Collection Templates Display Correct Languages

The default notification templates are correctly translated in the specified language. (Bug 1063967)

Dashboard Correctly Displays Tasks if the Datatype for the METAXML Column is ntext

If you modify the column types of METAXML in AFDOCUMENT to `ntext` argument data type, the Dashboard successfully processes the modified argument data type. (Bug 1062342)

Request History Comments Display Full Name of a User Instead of CN

The comments section of Request History now displays the full name of a user instead of CN. When you click the full name of the user, the Dashboard shows a popup with quick information about that user and a deep link to navigate to the users page for more details about that user. (Bug 1060709)

List Field Width Does Not Change When Date Is Changed

When you set or change a date on a User Application form, the list fields width is no longer changed to the width of the first list. (Bug 1049919)

PRD Correctly Opens in a New Tab

When running a custom PRD from the Applications tab, the Request Form settings are now loaded at the right time so that the PRD opens in a new tab instead of a new window. (Bug 1044350)

Requester fdn <req> on a User Object for Roles and Resources Is Changed When the User is Renamed

The `<req>` containing the requester `fdn <req>` on a user object for nrfassignedroles and nrfassignedresources attributes is successfully updated when a user is renamed. (Bug 1028476)

getRoleLevels Returns Correct Information

The getRoleLevels SOAP endpoint has been updated to return the role levels in the correct order. (Bug 935105)

NETIQ_TOMCAT_USER Variable Is Removed from the Tomcat PostgreSQL Installer on Windows

The NETIQ_TOMCAT_USER variable is removed from the silent installation file of the Tomcat PostgreSQL installer for Windows. The new Linux installer allows creation of silent properties file based on user input instead of bundling a hard-coded properties file. This change is no longer applicable to Linux. (Bug 925699)

Ability to Sort Request History in the Dashboard

The request history page now lists the request history in reverse order (by date). (Bug 1061515)

Role and Resource Service Driver

Ability to Prioritize Customer Initiated Requests Over Scheduled Requests

The Role and Resource Service driver has been enhanced to prioritize user generated requests over the requests generated by the driver itself. (Bug 1008920)

Deleting Roles Does Not Remove the Overlapping Entitlement Values

The Role and Resource Service driver builds a temporary cache of create resource association events before resynchronizing the deleted resource association and recalculating the resources based on a missing role. This ensures that only those associations are removed from the user that are not mapped with any other assigned roles. (Bug 1040935)

Ability to Handle Object Moves

The driver's recovery mechanism now properly handles a user movement action when the driver is assigning roles and resources to that user. (Bug 1061399)

Role and Resource Service Driver Properly Handles a Failed Dynamic Group Membership Change

The driver has been enhanced to handle a failed Dynamic Group membership change. (Bug 736047)

Upgrading NetIQ iManager to 3.1 Does Not Display any Error Message on Identity Manager Overview Page

On Identity Manager 4.6.x environment, if you upgrade NetIQ iManager 3.0 to 3.1, the **Identity Manager Overview** page displays an error message. This is fixed in Identity Manager 4.7 plugins. Update your Identity Manager plugins to 4.7 to resolve this issue. (Bug 1088853)

Addresses Software Vulnerability

This release addresses the following Common Vulnerabilities and Exposures (CVE) for Identity Manager:

- CVE-2018-7676
- CVE-2018-7674
- CVE-2018-7673
- CVE-2018-1350
- CVE-2018-1349
- CVE-2018-1348

What's Changed, Deprecated, or Discontinued?

To streamline functionality, several items have changed or are no longer supported with Identity Manager 4.7. In many cases, alternative functionality replaces the items that are no longer supported.

What's Deprecated for Removal?

This release deprecates the following features of the User Application:

WARNING: Identity Manager 4.7.1 will provide a new user interface for administering these features in place of the existing User Application interface. You must use the new user interface because User Application interface will be discontinued from this release. This is a step towards making the user interface consistent for all Identity Applications functionality.

Identity Self-Service, Work Dashboard, Compliance, Roles and Resources Administration

This version of Identity Manager introduces Identity Applications Administration interface. Instead of using these features in the User Application, you must use the new interface. These features of the User Application are not supported from this release. For more information, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Portal Pages and Portlets

This release does not support the portal functionality in the User Application. For more information about configuring the identity applications, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Guest and Single Sign-On Access

This release no longer supports the guest access and guest shared pages for the identity applications.

Starting Identity Manager 4.5, the method used for providing single sign-on access to the identity applications has changed. If you previously used SAP Logon Ticket, Kerberos, or Custom SSO Provider, NetIQ recommends that you familiarize yourself with the new OSP OAuth process.

For more information, see *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.

Attestation

The attestation feature of the User Application is not supported from this release.

Legacy Password Management

The Legacy Password Self-Service feature of the User Application is not supported from this release. Instead, use Self Service Password Reset (SSPR). The installation process enables SSPR by default when you install or upgrade to the latest version of Identity Manager. For more information, see *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.

What's Discontinued?

The following list includes the features that have been discontinued from this release:

Integrated Installation Program

Identity Manager 4.7 does not include support for integrated installation program. This installer is discontinued from this release.

XDAS Auditing for Identity Applications

Auditing with XDAS for the identity applications components is discontinued from this release. You must use CEF for logging identity applications events.

This change is not applicable to other Identity Manager components that support XDAS. NetIQ recommends to use CEF auditing for all Identity Manager components.

Separate Access to Identity Manager Home and Provisioning Dashboard, and Catalog Administrator

This release provides an enhanced version of Identity Manager Dashboard that replaces Home and Provisioning Dashboard. Identity Manager Home and Provisioning Dashboard is discontinued from this release.

The functionality provided by Catalog Administrator is included in the Identity Applications Administration interface. Catalog Administrator is discontinued from this release.

REST Interface Service (RIS)

This version of Identity Manager provides access to a majority of identity applications functionality through Application Programming Interface (API). The API is HTTP based, with a RESTful programming interface. You can invoke the API by using a REST client or by using curl command in scripts to help automate the administrative tasks. RIS is discontinued from this release.

RHEL 6.x and SLES 11.x Platforms

Support for RHEL 6.x and SLES 11.x platforms is discontinued from this release.

Separate Setup Guides for Linux and Windows Platforms

This release provides separate guides for installing and configuring, upgrading, and uninstalling Identity Manager components on Linux and Windows platforms. For more information, see one of the following links:

- *NetIQ Identity Manager Setup Guide for Linux*
- *NetIQ Identity Manager Setup Guide for Windows*

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 Identity Manager Localization" in the *NetIQ Identity Manager Overview and Planning Guide*. (Bug 896299)

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

PostgreSQL and Tomcat components are automatically installed on a Linux server. On Windows, these components are installed using a separate installation program. Be informed that 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 for Linux or the *NetIQ Identity Manager Setup Guide for Windows*.

Supported Component Versions

- Identity Manager Component Versions
- Third-Party Component Versions
- Database
- Web Browser

Identity Manager Component Versions

Identity Manager 4.7 bundles the following components:

- NetIQ eDirectory 9.1
- NetIQ iManager 3.1
- NetIQ Identity Manager Engine 4.7
- NetIQ Identity Manager Remote Loader 4.7
- NetIQ Identity Manager Fanout Agent 1.2
- NetIQ Designer for Identity Manager 4.7
- NetIQ Identity Applications 4.7
- NetIQ Single Sign-on (One SSO) 6.2.1
- NetIQ Identity Manager Self-Service Password Reset 4.2.0.4
- Platform Agent 2011.1r6
- NetIQ Identity Manager Client Login Extension 4.2
- NetIQ Identity Manager Identity Reporting 6.0
- NetIQ Sentinel Log Management for IGA 8.1.1 (for event auditing)
- NetIQ Analyzer for Identity Manager 4.7
- 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.

Third-Party Component Versions

This release adds support for the following dependent components:

- Java 8 Update 162
- OpenSSL 1.0.2n-fips
- Apache Tomcat 8.5.27
- PostgreSQL 9.6.6
- Apache ActiveMQ 5.15.2
- MapDB 3.0.5

  When you upgrade to Identity Manager engine 4.7, some of the existing MapDB cache files remain uncleaned in the Identity Vault’s DIB directory. You must manually remove these files for your driver after upgrading the driver. For more information, see “Working with MapDB 3.0.5” on page 28.

Database

In addition to PostgreSQL 9.6.6, this release adds support for the following databases:

- Oracle 12.2.0.1
- MS SQL 2016 (only for Identity Applications)

Web Browser

Any of the following browsers, at a minimum:

- Google Chrome 61
- Mozilla Firefox 51
- Apple Safari 9
- Microsoft Edge 20.10240.17146.0
- Microsoft Internet Explorer 11.0.10240.17443

NOTE: The Compatibility View option is not supported in the Internet Explorer browser.

System Requirements

For information about hardware requirements and supported operating systems, see the Technical Information for Identity Manager page.

Installing NetIQ Identity Manager 4.7

Identity Manager 4.7 provides Advanced Edition and Standard Edition in a single ISO file. Before downloading the installation files, you must understand what features are contained in each edition and the options for downloading the Identity Manager components.

- "Features Supported with Identity Manager Advanced and Standard Editions" on page 18
- "Downloading Identity Manager" on page 20
- "Locating the Executables and Default Installation Paths" on page 21
- "Installing NetIQ Identity Manager 4.7" on page 23

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	Components to Install
Rule-based automated user provisioning	Yes	Yes	◆ Identity Manager ◆ Engine and Designer
Real-time identity synchronization	Yes	Yes	◆ Identity Manager ◆ Engine and Designer
Password management and password self-service	Yes	Yes	◆ Identity Manager ◆ Engine and SSPR
Uniform identity information tool (Analyzer)	Yes	Yes	Analyzer
REST APIs and single sign-on support	Yes	Yes (limited support)	◆ Identity Manager ◆ Engine, OSP, and Identity Reporting
Current state reporting	Yes	Yes	◆ Identity Manager ◆ Engine and Identity Reporting
Role-based enterprise-level provisioning	Yes	No	◆ Identity Manager ◆ Engine and Identity Applications
Automated approval workflows for business policy enforcement	Yes	No	◆ Identity Manager ◆ Engine, Designer, and Identity Applications
Advanced self-service in the identity applications	Yes	No	◆ Identity Manager ◆ Engine and Identity Applications

Feature	Advanced Edition	Standard Edition	Components to Install
Resource model and catalog for easy resource provisioning	Yes	No	- Identity Manager - Engine and Identity Applications
Historical state reporting	Yes	No	- Identity Manager - Engine and Identity Applications
Connected systems reporting	Yes	No	- Identity Manager - Engine and Identity Application
Role and resource administration	Yes	No	- Identity Manager - Engine and Identity Applications

Downloading Identity Manager

After you purchase Identity Manager 4.7, log in to the Identity Manager Product Web site and follow the link that allows you to download the software. The following files contain the Identity Manager components:

File Name	Description
Identity_Manager_4.7_Linux.iso	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration), Identity Applications, Identity Reporting, Designer, and Analyzer **NOTE:** This download file has been updated to include the OES 2018 support and software fixes to the Linux installer. For more information, see TID 7023435.
Identity_Manager_4.7_Windows.iso	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration), Identity Applications, Identity Reporting, Designer, and Analyzer
Identity_Manager_4.7_Linux_Designer.tar.gz	Contains Designer
Identity_Manager_4.7_Windows_Designer.zip	Contains Designer
Identity_Manager_4.7_MacOSX_Designer.dmg	Contains Designer files for macOS 10.13 (High Sierra)
Identity_Manager_4.7_Linux_Analyzer.tar.gz	Contains Analyzer
Identity_Manager_4.7_Windows_Analyzer.zip	Contains Analyzer
SentinelLogManagementForIGA8.1.1.0.tar.gz	Contains Sentinel Log Management for Identity Governance and Administration This installation is supported only on Linux.

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 file that you want to download.
4. Follow the on-screen prompts to download the file to a directory on your computer.

Locating the Executables and Default Installation Paths

- Executables and Default Installation Paths on Linux
- Executables and Default Installation Paths on Windows

Executables and Default Installation Paths on Linux

Identity Manager Component	Location of the Executable within ISO	Default Installation Path
Identity Manager Server (Contains Identity Manager Engine, Remote Loader, Fan-Out Agent, iManager Web Administration)	`install.sh` in the mounted location	◆ **Engine:** `/opt/novell/eDirectory/lib/dirxml` ◆ **Remote Loader:** `/opt/novell/dirxml/bin/x86_64` ◆ **Fanout Agent:** `/opt/novell/dirxml/fanoutagent` ◆ **iManager:** `var/opt/novell/iManager`
Identity Applications (Identity Manager Dashboard, Identity Manager Administration Interface, User Application, Role and Resource Service driver, User Application driver, Configuration Update Utility)	`install.sh` in the mounted location	◆ **Identity Applications:** `/opt/netiq/idm/apps` ◆ **User Application:** `/opt/netiq/idm/apps/UserApplication` ◆ **Configuration Update Utility:** `/opt/netiq/idm/apps/configupdate`
Designer for Identity Manager	`/designer/packages`	`/root/designer`
Identity Reporting	`install.sh` in the mounted location	`/opt/netiq/idm/apps/IDMReporting`
Password Management Component (Standard Edition)	`./install.sh` in the `/sspr` directory in the mounted location	`/opt/netiq/idm/apps/sspr`
Analyzer for Identity Manager	`/analyzer/packages`	`/root/analyzer`
Sentinel Log Management for IGA	`./install.sh` in the `/SentinelLogManagementforIGA` directory if the `SentinelLogManagementForIGA8.1.1.0.tar.gz` file	`/opt/novell/sentinel`

Executables and Default Installation Paths on Windows

Identity Manager Component	Location of the Executable within ISO	Default Installation Path
Identity Vault	`Setup.exe` located in `\products\eDirectory\x64\`	`C:\netiq\eDirectory`

Identity Manager Component	Location of the Executable within ISO	Default Installation Path
iManager	- **Server installation:** iManagerInstall.exe located in \products\iManager\installs\win\ - **Workstation installation:** iManager.bat located in imanager\bin	- **Server installation:** C:\Program Files\Novell - **Workstation installation:** C:\Program Files\Novell
Remote Loader	idm_install.exe located in \products\IDM\windows\setup	C:\Novell
PostgreSQL and Tomcat (supported database and application server)	TomcatPostgreSQL.exe located in products\CommonApplication\postgre_tomcat_install\	C:\netiq\idm\apps\tomcat
Single Sign-on (OSP)	osp-install.exe located in \products\CommonApplication\osp_install	C:\netiq\idm\apps\osp
Self Service Password Reset (SSPR)	sspr-install.exe located in \products\CommonApplication\sspr_install	C:\netiq\idm\apps\sspr
Identity applications	IdmUserApp.exe located in products\UserApplication	C:\netiq\idm\apps\UserApplication
Designer for Identity Manager	install.exe located in \products\Designer\	c:\netiq\idm\apps\Designer
Identity Reporting	rpt-install-win.exe located in \products\Reporting	C:\netiq\idm\apps\IdentityReporting
Analyzer for Identity Manager	install.exe located in \products\Analyzer\	C:\netiq\idm\apps\Analyzer

Installing NetIQ Identity Manager 4.7

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

- Advanced Edition: *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*
- Standard Edition: *Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.7 Standard Edition*

Upgrading to NetIQ Identity Manager 4.7

You can upgrade to Identity Manager 4.7 from Identity Manager 4.6.x and 4.5.6 versions. Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your current version.

- Upgrading from Identity Manager 4.6.x
- Upgrading from Identity Manager 4.5.6
- Upgrading to Advanced Edition
- Upgrading to Standard Edition

For more information about upgrading Identity Manager, see “Upgrading Identity Manager” in the *NetIQ Identity Manager Setup Guide for Linux* or Upgrading Identity Manager in *NetIQ Identity Manager Setup Guide for Windows*.

Upgrading from Identity Manager 4.6.x

The following table lists the upgrade paths for Identity Manager components:

Component	Base Version	Notes
Identity Manager Engine	4.6.x	1. Upgrade the operating system to a supported version. 2. Upgrade Identity Manager engine to 4.7. **NOTE:** Before upgrading the engine, ensure that Identity Vault is upgraded to 9.1.
Remote Loader	4.6.x	Install Remote Loader 4.7
Fanout Agent	4.6.x	Install Fanout Agent 4.7
Designer	4.6.x	1. Install Designer 4.7. 2. Convert your workspace to work with LDAP-based Designer. Before using this version, see *NetIQ Identity Manager Designer 4.6 Release Notes*.

Component	Base Version	Notes
Identity Applications	4.6.x	Before you upgrade Identity Applications, ensure that Identity Vault and Identity Manager engine are upgraded to 9.1 and 4.7 versions respectively. 1. Upgrade the operating system to a supported version. 2. Update User Application driver and Role and Resource Service driver packages. 3. Upgrade the database to a supported version (PostgreSQL, Oracle, or MS SQL). 4. (Conditional) If SSPR is installed on a separate computer, upgrade the component to 4.7 version. 5. Stop Tomcat. 6. Upgrade Identity Applications to 4.7. **NOTE:** Identity Manager 4.7 does not support a remotely installed OSP for Identity Applications on Linux platforms. The installer installs OSP when Identity Applications are installed. After competing the installation, you must copy the OSP settings from your existing OSP server to the new server where Identity Applications and OSP are installed. For more information, see Upgrading the Identity Applications Components in the *NetIQ Identity Manager Setup Guide for Linux*.
Identity Reporting	4.6.x	1. Upgrade the operating system to a supported version. 2. Upgrade your database to a supported version (PostgreSQL or Oracle). 3. Upgrade SLM for IGA. 4. Install Identity Reporting 4.7. 5. Update Data Collection Services driver and Managed System Gateway driver packages.

Upgrading from Identity Manager 4.5.6

The following table lists the upgrade paths for Identity Manager components:

Component	Base Version	Intermediate Step	Notes
Identity Manager Engine	Identity Manager 4.5.x (where x is 0 to 5) with eDirectory 8.8.8.x (where x is 3 to 9)	Apply Identity Manager 4.5.6 service pack	1. Upgrade the operating system to a supported version. 2. Upgrade Identity Manager engine to 4.7. **NOTE:** Before upgrading Identity Manager engine, ensure that Identity Vault is upgraded to 9.1 version.
Remote Loader	4.5.x		Install Remote Loader 4.7
Fanout Agent	4.5.x		Install Fanout Agent 4.7

Component	Base Version	Intermediate Step	Notes
Designer	4.5.x		1. Install Designer 4.7. 2. Convert your workspace work with LDAP-based Designer. Before using this version, see *NetIQ Identity Manager LDAP Designer Release Notes*.
Identity Applications	4.5.x	If you are using JBoss or WebSphere as your application server, migrate to Tomcat application server	Before upgrading Identity Applications, ensure that the Identity Vault and Identity Manager engine are upgraded to 9.1 and 4.7 version respectively. 1. Upgrade the operating system to a supported version. 2. Update User Application driver and Role and Resource Service driver packages. 3. Upgrade the database to a supported version (PostgreSQL, Oracle, or MS SQL). 4. (Conditional) If SSPR is installed on a separate computer, upgrade the component to 4.7 version. 5. Stop Tomcat. 6. Upgrade Identity Applications to 4.7. **NOTE:** Identity Manager 4.7 does not support a remotely installed OSP for Identity Applications on Linux platforms. The installer installs OSP when Identity Applications are installed. After competing the installation, you must copy the OSP settings from your existing OSP server to the new server where Identity Applications and OSP are installed. For more information, see Upgrading the Identity Applications Components in the *NetIQ Identity Manager Setup Guide for Linux*.

Component	Base Version	Intermediate Step	Notes
Identity Reporting	4.5.x	If you are using JBoss or WebSphere as your application server, migrate to Tomcat application server	1. Upgrade the operating system to a supported version. 2. Upgrade the database to a supported version. 3. Migrate Event Auditing Service data to a supported version of PostgreSQL or Oracle database. 4. Install SLM for IGA. 5. Install Identity Reporting 4.7. 6. Run the Data Synchronization utility. 7. Update Data Collection Services driver and Managed System Gateway driver packages.

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 4.7 Advanced Edition
    - From Identity Manager 4.5 Standard Edition to 4.6 Advanced Edition and then to 4.7 Advanced Edition

Upgrading to Standard Edition

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

The Identity Manager 4.7 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.

Working with MapDB 3.0.5

Identity Manager 4.7 adds support for MapDB 3.0.5. In addition to Identity Manager Engine, MapDB is used by the following Identity Manager drivers:

- Data Collection Services
- JDBC
- LDAP
- Managed System Gateway
- Office 365 and Azure Active Directory
- Salesforce

If you are using any of these drivers, you must review the following sections before upgrading the driver:

- "Understanding Identity Manager 4.7 Engine Support for Driver Versions" on page 28
- "Manually Removing the MapDB Cache Files" on page 28

Understanding Identity Manager 4.7 Engine Support for Driver Versions

Review the following considerations before upgrading an Identity Manager driver that uses MapDB:

- Drivers shipped with Identity Manager 4.7 are compatible with Identity Manager 4.7 Engine or Remote Loader. You must perform the following actions to complete the driver upgrade:
  1. Upgrade the Identity Manager Engine.
  2. (Conditional) Upgrade the Remote Loader.
  3. Upgrade the driver.
  4. Manually remove the MapDB state cache files from the Identity Vault's DIB directory. For more information, see "Manually Removing the MapDB Cache Files" on page 28.
- Drivers shipped before Identity Manager 4.7 are not compatible with Identity Manager 4.7 Engine or Remote Loader.
- Drivers shipped with Identity Manager 4.7 are not backward compatible with Identity Manager 4.6.x Engine or Remote Loader.
- Drivers shipped with Identity Manager 4.7 are not backward compatible with Identity Manager 4.5.x Engine or Remote Loader.

Manually Removing the MapDB Cache Files

The Identity Manager Engine upgrade process leaves some of the existing MapDB state cache files (`dx*`) in the Identity Vault's DIB directory (`/var/opt/novell/eDirectory/data/dib` or `C:\Novell\NDS\`). You must manually remove these files for your driver after upgrading the driver. This action ensures that your driver works correctly with Identity Manager 4.7 engine.

The following table lists the MapDB state cache files that must be removed:

Identity Manager Driver	MapDB State Cache File To Remove
Data Collection Services	DCSDriver_<driver instance guid>-* <driver instance guid>-*
JDBC	jdbc_<driver instance guid>_*
LDAP	ldap_<driver instance guid>*
Managed System Gateway	MSGW-<driver-instance-guid>.*
Office 365 and Azure Active Directory	<Azure driver name>_obj.db.*
Salesforce	<Salesforce driver name>.* <Salesforce driver name>

where ***** represents the name of the MapDB state cache file for a driver. In case of Salesforce driver, the MapDB state cache files are also represented by the driver name. Below are some examples of these files.

- `DCSDriver_<driver instance guid>-0.t`, `<driver instance guid>-1.p`
- `jdbc_<driver instance guid>_0.t`, `jdbc_<driver instance guid>_1`
- `ldap_<driver instance guid>b`, `ldap_<driver instance guid>b.p`
- `MSGW-<driver instance guid>.p`, `MSGW-<driver instance guid>.t`
- `<Azure driver name>_obj.db.t`, `<Azure driver name>_obj.db.p`
- `<Salesforce driver name>.p, <Salesforce driver name>.t, Salesforce driver1`

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.

- "Installation Issues" on page 30
- "Identity Manager Engine Issues" on page 34
- "Remote Loader Issues" on page 34
- "Driver Issues" on page 35
- "Identity Applications Issues" on page 37
- "Identity Reporting Issues" on page 44
- "iManager Plug-In Issues" on page 46
- "Identity Manager Upgrade Issues" on page 47
- "Localization Issues" on page 50
- "Uninstallation Issues" on page 51

Installation Issues

Exception Caused by Missing Reporting Database Startup Key After Configuration on Linux

Issue: If you are installing Identity Reporting on the same server that has Identity Applications installed, and you choose the database creation option as **Startup** during the Identity Reporting installation, the configuration script reports some exceptions in the log. (Bug 1082959)

Workaround: Clear the exceptions by manually restarting Tomcat.This does not cause any impact on the installation. It is safe to ignore the exception.

User Application Driver Fails to Deploy When the Driver Set Context Contains an Organizational Unit on Linux

Issue: If Identity Manager engine is installed and configured with a custom driver set and the driver set's deploy context contains at least one `Organizational Unit`, the User Application driver fails to completely deploy to the Identity Vault. For example, the driver partially deploys if the deploy context is `ou=drivers,o=novell`. (Bug 1104606)

Below is a snippet of the error message logged to the `idmconfigure.log` file:

```
Couldn't write all values for nrfRequestDef. The object with DN cn=Attestation
Report,cn=RequestDefs,cn=AppConfig,cn=User Application
Driver,cn=appsdriverset,cn=driversets,o=novell doesn't exist in the directory.
Failure deploying cn=SoD Violation-
Default,cn=Attestations,cn=RoleConfig,cn=AppConfig,cn=User Application
Driver,cn=appsdriverset,ou=driversets,o=novell.
Deployment of cn=SoD Violation-
Default,cn=Attestations,cn=RoleConfig,cn=AppConfig,cn=User Application
Driver,cn=appsdriverset,ou=driversets,o=novell failed.
```

Workaround: Perform the following actions:

1. Delete User Application and Role and Resource Service drivers that are automatically deployed by the installer.
2. Manually deploy User Application and Role and Resource Service drivers.
3. Verify that the User Application driver's dn is valid by using the configupdate utility.

Datasource Not Added to the Reporting Application Page When Database Schema Is Created During Identity Reporting Installation with Oracle Database on Windows

Issue: After installing and configuring Identity Reporting, when you log in to the reporting application, the datasource is not available in the application. (Bug 1082990)

The following error is logged to the `catalina.out` file:

```
com.netiq.persist.PersistenceException: javax.naming.NameNotFoundException: Name
[IDMDCSDataSource] is not bound in this Context. Unable to find
[IDMDCSDataSource].
```

Workaround: After completing the Identity Reporting configuration, manually add the datasource to the reporting application.

1. Log in to Identity Reporting.
2. Click **Data Sources > Add**.
3. In **Add Data Source**, click **Select from predefined list**.
4. Select **IDMDCSDataSource** and name it `IDMDCSDataSource`.

   The Save button is activated only when a name is specified.
5. Click **Save**.

Cannot Specify Installation Paths on Windows that Include Spaces

The installation programs for Identity Manager components 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)

Cannot Restart Tomcat with Task Manager on Windows

Issue: You cannot use the Task Manager to restart Tomcat on a Windows server. (Bug 893155)

Workaround: Use one of the following methods to restart Tomcat:

- In the Services control panel, right-click **IDM Apps Tomcat Service** then click **Restart**.
- Use the command prompt to stop and 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"
  ```

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.

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.

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.

Navigation Panel is Truncated in Identity Reporting Installer on Windows

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.

Designer Fails to Authenticate With Identity Manager Server on Windows When the Connection Uses Proxy Configuration

Issue: When Designer is configured to use a proxy server to access the Identity Manager server, Designer fails to authenticate with the Identity Manager server.

Workaround: Perform the following actions:

1. Click **Window > Preferences General > Network Connections**.
2. Change the **Active Provider** setting from `Direct` to `Manual`.
3. Select HTTP or HTTPS protocol under the **Proxy entries** section. Do not select SOCKS protocol.
4. In the Edit Proxy Entry window, provide the IP address of the Identity Vault for your connection `(HTTP or HTTPS)`, then click **OK**.
5. Click **Add Host** under the **Proxy bypass** section.
6. In the Proxy bypass hosts window that opens, provide the IP address of the Identity Vault, then click **OK**.

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.

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**.

Drivers Do Not Start When Identity Manager Engine Is Installed as a Non-root User

Issue: This issue occurs because the Java files are not installed during the installation process.

Workaround: Perform the steps from TID 7023354.

Cannot Configure Multiple Instances of Identity Vault on Linux

Issue: The Identity Manager Linux installer does not support configuring multiple instances of Identity Vault.

Workaround: Perform the following actions:

1. Manually configure an additional instance of Identity Vault on which you want to install Identity Manager by using the ndsconfig utility.

   You can configure multiple instances of the Identity Vault on a single host. The method to configure multiple instances with the ndsconfig utility is similar to configuring a single instance multiple times. Each instance must have unique instance identifiers, such as the following:

   - Different data and log file locations. Use the `--config-file`, `-d`, and `-D` options.
   - A unique port number for the instance. Use the `-b` and `-B` options.
   - A unique server name for the instance. Use the `-S` server name option.
2. Verify that all Identity Vault instances are stopped. To stop an Identity Vault instance, run `ndsmanage stopall`.
3. Navigate to `/etc/opt/novell/eDirectory/conf/.edir/` and take a backup of the `instances.0` file.
4. Edit the `instances.0` file to keep only the Identity Vault instance entry on which you want to install Identity Manager.
5. Create an empty file named `IDM` in `/etc/opt/netiq/idm/configure/`.

   ```
   #cd /etc/opt/netiq/idm/configure/
   ```

   ```
   # touch IDM
   ```
6. Run the `configure.sh` script.
7. Restore the `instances.0` file to `/etc/opt/novell/eDirectory/conf/.edir/` that you backed up in Step 2.
8. Restart the additional Identity Vault instances.

Identity Manager Engine Issues

- "Unable to Execute Large ECMAScripts" on page 34
- "Adding Multiple Entitlement Values to a Static Resource Fails" on page 34

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*.

Adding Multiple Entitlement Values to a Static Resource Fails

Issue: When you create a static resource with multiple entitlement values by using `do-create-resource` token, Identity Manager engine creates only one nrfEntitlementRef object for the resource. Therefore, you cannot create static resources with multiple assignment values by using this token. `(Bug 995486)`

Workaround: There is no workaround at this time.

Remote Loader Issues

- "Cannot Generate Novell Audit Events for 32-Bit and 64-Bit Remote Loaders on the Same Server" on page 34
- "Key Password Specified at the Remote Loader Side is Not Validated Using Mutual Authentication" on page 34
- ".NET Remote Loader Driver Instance Configured for Mutual Authentication Does Not Start" on page 35

Cannot Generate Novell 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 Novell 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.

Key Password Specified at the Remote Loader Side is Not Validated Using Mutual Authentication

Issue: The dxcmd tool generates the PEM file for a private key without an encryption password. Therefore, Identity Manager establishes the connection between remote loader and engine without validating the encryption password (key password). `(Bug 1077147)`

Workaround: You must create a client KMO using iManager with a encrypted password. Generate `keyfile.pem` from this KMO and replace the existing `keyfile.pem` using following steps:

1 Log in to iManager.

2 Create a KMO for a client authentication in `.pfx` format:

2a Go to **Roles and Tasks > NetIQ Certificate Access > Server Certificates**.

2b Click **New**, specify the **Nickname** for your certificate.

2c Select **Custom** as creation method and click **Next**.

This option allows you to define certificate parameters.

2d Select **Organizational certificate authority** and click **Next**.

2e In **Enable extended key usage**, select **User** and click **Next**.

2f Select the **Validity Period** from the list and click **Next**.

2g Select **Your organization's certificate** and click **Next**.

2h Click **Finish**.

3 Select the newly created certificate and click **Validate**.

4 Select the client KMO and click **Export**.

NOTE: In iManager, KMO is exported in `.pfx` format.

5 Convert the exported client KMO from `.pfx` to `.pem` format using the following command:

```
openssl pkcs12 -in <exported_certificate_name>.pfx -out
<converted_certificate_name>.pem
```

For example,

```
openssl pkcs12 -in cert.pfx -out client_cert.pem
```

6 Replace `keyfile.pem` with `client_cert.pem`

.NET Remote Loader Driver Instance Configured for Mutual Authentication Does Not Start

Issue: After upgrading 32-bit or 64-bit .NET Remote Loader, a driver configured with mutual authentication enabled fails to start the .NET Remote Loader instance. (`Bug 1082989`)

Workaround: After upgrading .NET Remote Loader, perform the following steps:

1 Edit the .NET Remote Loader instance, specify the same key password that is set prior to upgrading the .NET Remote Loader.

The default key password is `dirxml`.

2 Save the configuration.

3 Start the .NET Remote Loader driver instance.

Driver Issues

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

- "ClassNotFoundException Reported When tmp Directory is Full" on page 36
- "Statistics Report Shows Zero for Role and License Values for an Office 365 Driver" on page 36

- “Remote Loader Instance of a Driver Might Fail to Start If the Default Width of Windows Command Prompt Window is Changed” on page 36
- “dxcmd Query with Huge Output is Executed Twice” on page 36
- “Issue with Adding DirXML Accounts Entry When a User is Migrated” on page 36
- “Driver Cache Inspector is Unable to Display the Last Entry in the Cache List” on page 37
- “Remedy Driver Does Not Start When Run Locally with the Identity Manager Engine” on page 37

ClassNotFoundException Reported When tmp Directory is Full

Issue: Sometimes a driver fails to start and reports a `java.lang.ClassNotFoundException` exception although the driver shim is present in the `classes` directory. This can occur if the temporary directory used by the Java environment has no free space. In most cases, the location of the temporary directory is `/tmp`. `(Bug 683259)`

Workaround: Provide sufficient space in the temporary directory.

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.

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.

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.

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.

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.

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-5.15.2.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-5.15.2.jar` file from the `lib` folder of the Remote Loader installation directory.
3. Start the driver.

Identity Applications Issues

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

- “Unable to Change Password using Identity Manager Dashboard” on page 42
- “Default Dashboard Widgets Fail to Load Widget Information on the Dashboard After Upgrade” on page 42
- “Dashboard Logout Button Might Not Work ” on page 43
- “Click Description Or Mapping Description of a Child Role to Select It For Deletion” on page 43
- “Increased Length of the OSP Attribute Value Causes Login Issues” on page 43
- “Role and Resource Service Driver Does Not Support Recalculation of Roles, Resources, and DirXML-EntitlementRef Attribute for a User” on page 43
- “catalina.out File Does Not Rotate the Log” on page 44

Error Reported if Different Databases Are Configured for Identity Applications and Identity Reporting Installed on the Same Server

Issue: Identity Manager does not support using different databases for the identity applications and Identity Reporting components installed on the same server. For example, you cannot use a PostgreSQL database installed on the same server for the identity applications and point Identity Reporting to a remote Oracle database. This causes exceptions in the `catalina_<date>.log` file. `(Bug 1079738)`

Workaround: To use different databases for the identity applications and Identity Reporting, install the components on separate servers.

Zero File Size Shown for Archived Logs From catalina.out File Despite Log RollOver

Issue: The archived file size shows zero file size. `(Bug 1044488)`

Workaround: Perform the following actions:

1. Stop the Tomcat service. For example, run the following command from a command prompt:

   ```
   systemctl stop netiq-tomcat.service
   ```

2. Navigate to the `Tomcat/conf` directory. For example, `/opt/netiq/idm/apps/tomcat/conf`.
3. Modify the `userapp-log4j.xml` file in a text editor.

   3a Add the following entries for log appenders after the `Catalina Appender` section.

   ```
   <!-- catalina.out logrollover -->
       <appender name="CATALINALOG"
   class="org.apache.log4j.DailyRollingFileAppender">
           <param name="Append" value="true"/>
           <param name="DatePattern" value="'.'yyyy-MM-dd'.log'"/>
           <param name="Encoding" value="UTF-8"/>
           <param name="File" value="${catalina.base}/logs/catalina.out"/>
           <param name="Threshold" value="ALL"/>
           <layout class="org.apache.log4j.PatternLayout">
               <param name="ConversionPattern" value="%d [%p] %c{1} %m%n"/>
           </layout>
       </appender>
   ```

   3b Add `<appender-ref ref="CATALINALOG"/>` entry under the `<root>` section before `</log4j:configuration>` section.

The section should look similar to this:

```
<!-- ====================== -->
    <!-- Setup the Root category -->
    <!-- ====================== -->
    <root>
        <level value="INFO"/>
        <appender-ref ref="CONSOLE"/>
        <appender-ref ref="IDAPPS"/>
        <appender-ref ref="CATALINALOG"/>
    </root>
```

4 Start the Tomcat service.

Revoke Permissions Page Incorrectly Lists Others Permissions for Role Administrator and Delegated Role Administrator

Issue: If you log in to the Dashboard as a Role Administrator or a Delegated Role Administrator, the Others page (**Access > Permissions > Revoke Permissions > Others**) lists the user permissions that are outside of your domain or scope.

- For a Role Administrator, the Dashboard lists resources of users that are not part of the administrator's domain.
- For a Delegated Role Administrator, the Dashboard lists all resources and roles of users that are not delegated. (Bug 1079043)

Workaround: There is no workaround at this time.

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.

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.

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");
```

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.

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.

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.

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.

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');
```

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.

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
```

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.

Unable to Change Password using Identity Manager Dashboard

Issue: If you installed SSPR and identity applications on separate servers, and try to change the password on the **Applications** page, the identity applications display `Page not found` error. (Bug 1077395)

Workaround: Specify the network IP address of the SSPR server in **Change My Password** in the **Applications** page.

1. Log in to your Identity Manager Dashboard as an administrator.

   ```
   https://<Identity Applications IP address:Port>/idmdash
   ```
2. Go to **Applications**, click ⚙.
3. On **Change My Password**, click ✎.
4. In **Link**, specify the SSPR server address.

   ```
   https://<SSPR-IP-address:port>//sspr/private/ChangePassword
   ```
5. Click **Save**.

Default Dashboard Widgets Fail to Load Widget Information on the Dashboard After Upgrade

Issue: If you defined a different context name than `IDMProv`, the default dashboard widgets that use REST APIs fail to obtain the widget information from the identity applications. `(Bug 1080591)`

Workaround: Change the context name for the widgets that are using REST APIs:

1. In **Dashboard**, click ○○○ and select **Widgets**.
2. Click ⚙ on a widget that you want to change the context name.
3. In **URL**, change `/IDMProv` to `/<defined context name>`.

   For example, in the following URL,

   ```
   /IDMProv/rest/access/assignments/
   advanced?nextIndex=1&sortBy=name&sortOrder=ASC&forceRefresh=true&searchScope=r
   ole&size=20
   ```

   change `/IDMProv` to `/IDMProv_new`.

Dashboard Logout Button Might Not Work

Issue: Sometimes identity applications do not take you to the Login page when you click the Logout button in the Dashboard. (Bug 1082178)

Workaround: Perform one of the following actions:

1. Refresh the Dashboard page.
2. Navigate to a different application (for example, Role Administration or IDMProv) and log out from that application page.

Click Description Or Mapping Description of a Child Role to Select It For Deletion

Issue: The new Identity Applications user interface displays the parent and child role list in the Role Details page. The page does not allow you to select a child role by selecting the name, instead it shows child role quick information. (Bug 1082533)

Workaround: To delete a child role, click the description or mapping description of the child role. For deleting multiple child roles, use keyboard's Ctrl key and click the description or mapping description of the selected roles.

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 actions:

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 using the ConfigUpdate utility:

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

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

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.

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.

Identity Reporting Issues

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

- "Cannot Modify the Frequency of a Schedule" on page 45
- "Identity Reporting and Identity Data Collection Services Pages Are Unable to Launch Identity Applications" on page 45
- "Data Collection Page Help for Non-English Locales Redirects to English Help" on page 46
- "Identity Manager Data Collection Services Page is Not Displayed in Standard Edition on Linux" on page 46
- "OSP Events Are Not Forwarded to the sentinel_events Table When CEF Is Enabled" on page 46
- "Identity Reporting Creates Tables With Incorrect Data Type When Startup Option Is Selected" on page 46

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.

Identity Reporting and Identity Data Collection Services Pages Are Unable to Launch Identity Applications

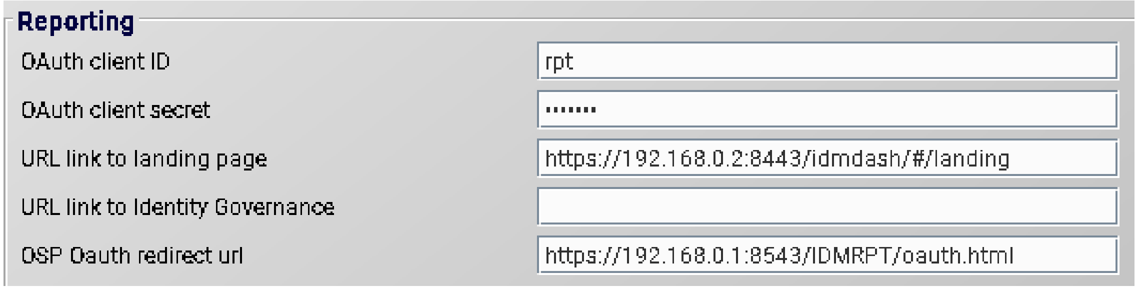
Issue: This issue occurs after upgrading Identity Manager to the latest version. When you click **Home** from Identity Reporting or Identity Data Collection Services user interface that are installed on separate servers than the identity applications, the identity applications are not launched. Instead, the `Page Not Found` error is displayed. (`Bug 1080514`)

Workaround: To change the landing URL for Identity Reporting, manually update the `configupdate` utility with Identity Manager Dashboard URL:

1. Launch `configupdate` utility.

   By default, this utility is located in `/opt/netiq/idm/apps/configupdate`
2. Navigate to **SSO clients > Reporting**.
3. In **URL link to landing page**, specify the URL of the Identity Manager Dashboard.

   For example, `https://<Identity Applications network IP address:Port>/idmdash/#/landing`



Reporting

OAuth client ID	rpt
OAuth client secret	•••••••
URL link to landing page	https://192.168.0.2:8443/idmdash/#/landing
URL link to Identity Governance	
OSP Oauth redirect url	https://192.168.0.1:8543/IDMRPT/oauth.html

To change the landing URL for Identity Manager Data Collection Services:

1. Open the `ism-configuration.properties` in the text editor from `/opt/netiq/idm/apps/tomcat/conf`.
2. Append the landing URL to the following text:

   ```
   com.netiq.idmdcs.landing.url = https://<Identity Applications network IP
   address:Port>/idmdash/#/landing
   ```

   For example,

   ```
   com.netiq.idmdcs.landing.url = https://192.168.0.2:8443/idmdash/#/landing
   ```
3. Restart Tomcat.

You can ignore the issue if you are using Standard Edition that does not include identity applications. This issue does not cause any functionality loss for Standard Edition installations.

Data Collection Page Help for Non-English Locales Redirects to English Help

Issue: When you install Data Collection Services in a non-English locale and click the **Help** icon from the Data Collection Services page, it takes you to the English version of the Help. (`Bug 1082987`)

Workaround: There is no workaround at this time.

Identity Manager Data Collection Services Page is Not Displayed in Standard Edition on Linux

Issue: After installing and configuring Identity Reporting in Standard Edition, the Identity Manager Data Collection Services page is not displayed. (`Bug 1082564`)

Workaround: While configuring Identity Reporting, select **No (N)** for the following prompt:

Do you want to connect to an external One SSO Server (Y/N)?

OSP Events Are Not Forwarded to the sentinel_events Table When CEF Is Enabled

Issue: When CEF is enabled, the product name for OSP events is changed to `MicroFocus One SSO Provider`. The changed product name is not present in the data synchronization policy criteria. Therefore, OSP events are not forwarded to the sentinel_events table after reaching SLM for IGA. (`Bug 1087435`)

Workaround: Perform the following actions:

1. In SLM for IGA, click **storage** > **data synchronization**
2. Edit the policy created by idmdcs
3. In criteria, append `pn:"MicroFocus One SSO Provider"`
4. Click **Save** and resynchronize

Identity Reporting Creates Tables With Incorrect Data Type When Startup Option Is Selected

Issue: When Identity Reporting is used with Oracle database and the **Startup** option is selected during the database schema creation, the database tables incorrectly create the `varchar2` data type as `nvarchar2`. (`Defect 288170`)

Workaround: There is no workaround at this time.

iManager Plug-In Issues

You might encounter the following issues as you use iManager:

- "Exception on Windows 2016 When Using KMO" on page 46
- "Dependency on NDS-to-NDS Driver Certificates Wizard" on page 47
- "Some Actions Are Not Available in Policy Builder Plug-In" on page 47

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.

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.

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.

Identity Manager Upgrade Issues

Existing Data Sync Policy Is Not Shown in the Data Collection Services Page after Upgrading from Identity Manager 4.6.x to 4.7

Issue: If you upgrade to Sentinel 8.1.1 and Identity Reporting 4.7, the new Data Collection Services page does not display the existing Data Sync policy. (Bug 1080081)

Workaround: Complete the following steps after upgrading Sentinel:

1. Delete your Data Synchronization policy.
   - If you upgraded from Sentinel 8.0.1 or prior versions, delete the Data Synchronization policy from Sentinel and delete the sentinel_events table from the reporting database. Log in to the PostgreSQL database and delete the sentinel_events table under public schema. Updating Sentinel removes data

from the sentinel_events table. Log in to **Sentinel > Storage > Data Synchronization**, select your policy and click **Delete**. Log in to the reporting database and delete the sentinel_events table under public schema.

- If you upgraded from versions later than Sentinel 8.1, delete only the Data Synchronization policy. Log in to **Sentinel > Storage > Data Synchronization**, select your policy and click **Delete**.

2. Launch the Data Collection Services page and navigate to **Settings > Data Sync > Data Sync Policies**.
3. To add a new policy, click **New Policy**.
4. In the New Data Sync Policy page, specify the Sentinel and database server details.
5. Click **Show Advanced** to configure the payload for the policy you are creating.
6. Click **Create**.

Upgrading Identity Manager Components in a Distributed Environment

Issue 1: If OSP and SSPR are installed on a separate server in your distributed environment.

The upgrade process replaces the non-default file, `oauth-keystore.file` (for example, `idmnew.jks`) with the default file name (`osp.jks`). `(Bug 1081968)`

Workaround: Perform the following steps to replace the default file with the non-default file after completing the upgrade:

1. Launch the **Configuration Update** utility.
2. In **Authentication** tab, scroll to the **Authentication Configuration** section.
3. In **OAuth keystore** file, replace the path to the JKS keystore file with the non-default file (for example, `idmnew.jks`). This file is located in the back-up folder of OSP.
4. In **OAuth keystore file password**, specify the password to load the non-default OAuth keystore file.

Issue 2: If Identity Manager is configured to authenticate with NetIQ Access Manager and you imported third-party certificates into Tomcat's `cacerts` directory.

Workaround: Reimport the third-party certificates into the `idm.jks` key-store. This is required because Tomcat of Identity Manager 4.7 uses `idm.jks` key-store. For example, if Identity Manager is configured to use Access Manager server for authentication, import the Access Manager certificate into `idm.jks`.

Progress Indicator Shows Truncated Directory Names for Some Components During Upgrade on Windows

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.

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`

Identity Applications Upgrade Fails to Preserve Branding Settings in the Database

Issue: Identity Manager Dashboard's **Branding** page settings are lost after Identity Applications are upgraded. This issue is only observed when the **com.netiq.idmdash.client.settings.store.preference** parameter is set to **Database** in the `ism.configuration.properties` file.

Workaround: Take a backup of the CSS file, located at the `<home>` directory of the `novlua` user, before upgrading Identity Applications. Use the CSS file to rework on the customization settings.

Unable To Save the Configuration Update Utility After Upgrading Identity Reporting in Standard Edition

Issue: On Linux, after upgrading Identity Reporting in a standard edition, you cannot save the configuration update utility because it prompts for User Application parameters. This issue is observed because the **is_prov** parameter in the `configupdate.properties.sh` file is set to **True**.

Workaround: Perform the following steps after upgrading Identity Reporting:

1. Log in to the server where Identity Reporting is upgraded.
2. Navigate to the `/opt/netiq/idm/apps/configupdate` directory.
3. Edit the `configupdate.sh.properties` file.

   ```
   vi configupdate.sh.properties
   ```
4. Set the **is_prov** parameter to **false**.

Upgrading Tomcat Results in Loss of SSL Certificates

Issue: While upgrading to Identity Manager 4.7, the Tomcat upgrade process does not persist the certificate used for SSL communication between Tomcat and PostgreSQL.

Workaround: Perform the following steps after upgrading Identity Manager 4.7:

1. Import the certificate to the `idm.jks` keystore.

   For example, on Linux, run the following command:

   ```
   /opt/netiq/idm/apps/jre/bin/keytool -import -trustcacerts -alias postgres -
   file server.crt -keystore /opt/netiq/idm/apps/tomcat/conf/idm.jks
   ```
2. Restart Tomcat.

Upgrading PostgreSQL Using the Upgrade Script Defaults to Non-SSL Configuration

Issue: When PostgreSQL is upgraded through the `pg_upgrade.sh` script, the upgrade process does not preserve the SSL configuration settings.

Workaround: Perform the following steps after upgrading PostgreSQL:

1. Locate the `postgresql.conf` file:

   Linux: `/opt/netiq/idm/postgres/data`

   Windows: `C:\NetIQ\idm\apps\postgres\data`
2. Open the file in a text editor and modify the following properties:
   - Set the **SSL** parameter to **On.**
   - Provide the `server.crt` and `server.key` certificate details in the **ssl_cert_file** and **ssl_key_file** parameters.

Localization Issues

- "Identity Manager Fails to Install Specific Drivers in Non-English Locales" on page 50
- "Identity Manager Installers Contain Corrupt Characters in the Console Mode On Windows" on page 50
- "Some Component Installers Are Not Localized" on page 51
- "PostgreSQL Installation Fails If postgres User Password Is Provided in Russian on Windows" on page 51

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>`

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.

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. (`Bug 1008039`)

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

PostgreSQL Installation Fails If postgres User Password Is Provided in Russian on Windows

Issue: The PostgreSQL installer does not accept password for the database administrator (**Password for admin user)** in Russian. (`Bug 1075752`)

Workaround: Specify the password in English.

Uninstallation Issues

Identity Manager Engine Uninstallation Script Incorrectly Removes Identity Vault RPMs on Linux

Issue: The Identity Manager engine uninstallation script removes Identity Manager engine RPMs and Identity Vault RPMs. The script also deconfigures the Identity Vault. (`Bug 1088416`)

Workaround: There is no workaround at this time.

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

Issue: The uninstallation program does not remove the JAR files from the `lib` directory. (`Bug 643077`)

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

Identity Manager Framework Uninstallation Log Files Are Not Created in the Uninstallation Folder on Windows

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

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

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
  ```

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.

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).

For general corporate and product information, see the NetIQ Corporate website (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/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

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/.