NetIQ Identity Manager 4.7 Service Pack 1 Release Notes

July 2018

NetIQ Identity Manager 4.7 Service Pack 1 provides new features, improves usability, and resolves several previous issues. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Identity Manager Community Forums on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

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

1 What’s New?

Identity Manager 4.7.1 provides the following key features, enhancements, and fixes in this release:

1.1 New Features

This release provides the following key features:

1.1.1 New Features in Identity Applications

To facilitate administrators in configuring the Identity Applications settings, the **Configuration** tab is added to Identity Manager Dashboard. This tab also allows you to create and edit administrator assignments for the Identity Applications domain types. This tab provides an interface to configure logging, caching, provisioning display, workflow engine, and cluster settings. For more information, see Configuring Identity Applications Default Settings in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

The following table lists the features that were earlier part of the User Application interface and have now been added to Identity Manager Dashboard.

Feature	User Application User Interface (Discontinued)	Identity Manager Dashboard
Proxy Settings: Allow you to configure the retention time for proxy assignments and notification templates that are used to generate alerts for respective users. For more information, see Configuring Delegation and Proxy Settings.	In the **Administration** tab, select **RBPM Provisioning & Security > Delegation and Proxy**.	**Configuration > Delegation and Proxy**
Logging: Helps you to debug the identity applications configuration. For more information, see Configuring Logging Settings.	In the **Administration** tab, select **Application Configuration > Logging**.	**Configuration > Logging**
Caching and Cluster: Helps you to manage the caches that are maintained by Identity Applications. For more information, see Configuring Caching and Cluster Settings.	In the **Administration** tab, select **Application Configuration > Caching**.	**Configuration > Caching and Cluster**
Administrator Assignments: Helps you assign administrators for Identity Applications supported domain types. For more information, see Assigning Administrators in Identity Applications.	In the **Administration** tab, select **RBPM Provisioning & Security > Administrator Assignments**.	**Configuration > Administrator Assignments**
Workflow Engine and Cluster Settings: Help you configure the Workflow Engine and cluster settings. These settings apply to all the workflow engines in the cluster. For more information, see Configuring Workflow Engines and Cluster Settings.	In the **Administration** tab, select **RBPM Provisioning & Security > Engine and Cluster Settings**.	**Configuration > Workflow Engine and Cluster**
Driver Status: Displays the User Application driver details. For more information, see Viewing User Application Driver Status.	In the **Administration** tab, select **Application Configuration > Driver Status**.	**Configuration > Driver Status**
Provisioning Display Settings: Help you control the behavior of general search results in Identity Manager Dashboard. Also, allows you to modify the appearance of **Tasks** and **Request History** page. For more information, see Configuring the Default Provisioning Display Settings.	In the **Administration** tab, select **RBPM Provisioning & Security > Provisioning UI Display Settings**.	**Configuration > Provisioning Display**

Feature	User Application User Interface (Discontinued)	Identity Manager Dashboard
Client Access Settings: allow you to set the access permissions for all the navigation items within the Identity Manager Dashboard. For more information, see Managing User Access.	In the **Administration** tab, select **RBPM Provisioning & Security > Navigation Access Permissions**.	1. Click **YourID** and select **Settings**. 2. Select **Access**.
Groups: Identity Manager Dashboard allows you to create or manage groups. For more information, see the *inline* help in Identity Manager Dashboard or Manage Groups.	In the **Identity Self-Service** tab, select **Create User or Group**.	**People > Groups**

1.1.2 Extended Support of Controlled Permission Reconciliation Services for New Drivers

The Controlled Permission Reconciliation Services (CPRS) support that was introduced in Identity Manager 4.7 has been extended to the following drivers in this release: Delimited Text, Loopback, and REST.

CPRS is integrated with Identity Manager Dashboard to assist you reconcile connected system 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.

1.1.3 Support for ZoomDB 1.0.0.0

This release replaces MapDB 3.0.5 with ZoomDB 1.0.0.0 for the following components:

- Identity Manager Engine
- Managed System Gateway (MSGW) Driver
- Data Collection Service (DCS) Driver

IMPORTANT: This change does not impact other Identity Manager drivers that use MapDB for caching requirements at the driver level.

The Engine update process installs ZoomDB files in the following locations:

File	Linux	Windows
zoomdb.jar	`/opt/novell/eDirectory/lib/dirxml/classes/zoomdb.jar`	`C:\NetIQ\eDirectory\lib\ zoomdb.jar` or `C:\novell\remoteloader\64bit\lib`
ZoomDB library	`/opt/novell/eDirectory/lib64/nds-modules/libzoomdb.so`	`C:\NetIQ\eDirectory\zoomdb.dll` or `C:\novell\remoteloader\64bit\zoomdb.dll`

If you installed Identity Manager as a non-root user, the ZoomDB files are located under the extracted eDirectory directory. For example, if the extracted eDirectory location is `/home/user/eDirectory`, then the files are located at `/home/user/eDirectory/opt/novell/eDirectory/lib/dirxml/classes/zoomdb.jar` and `/home/user/eDirectory/opt/novell/eDirectory/lib64/nds-modules/libzoomdb.so`.

Perform the following actions before working with ZoomDB:

- You must install the 64-bit NICI. The installer does not install the appropriate NICI.
- The Engine update process automatically updates the MSGW driver for use with ZoomDB. However, you must manually update the DCS driver from the NetIQ Downloads website (https://dl.netiq.com/index.jsp). To update the driver, follow the instructions from Section 2.6, “Updating the DCS Driver,” on page 18.
- After installing ZoomDB, you can optionally remove the existing MapDB cache files from your environment. For more information, see Section 2.7, “Manually Removing the MapDB Cache Files,” on page 19.

1.1.4 Extended Support of Uniform Auditing for Identity Reporting

Uniform auditing for Identity Manager components was introduced in Identity Manager 4.7. This support has been extended to the Identity Reporting component in this release.

Identity Manager uses Common Event Format (CEF) for uniform auditing. CEF is an extensible, text-based format designed to support multiple device types by offering the most relevant information. CEF defines a syntax for log records comprised of a standard header and a variable extension, formatted as key-value pairs. For information about enabling CEF for Identity Reporting, see Section 2.8, “Enabling CEF for Identity Reporting,” on page 19.

1.2 Enhancements

This release introduces the following enhancements:

- Section 1.2.1, “Enhancements in Identity Manager Engine,” on page 4
- Section 1.2.2, “Enhancements in Identity Applications,” on page 5
- Section 1.2.3, “Enhancements in Designer,” on page 5

1.2.1 Enhancements in Identity Manager Engine

This release provides the following enhancement in Identity Manager Engine:

- Section 1.2.1.1, “Support for Recalculation of Roles, Resources, and DirXML-EntitlementRef Attribute for a User in the Roles and Resource Service Driver,” on page 4

1.2.1.1 Support for Recalculation of Roles, Resources, and DirXML-EntitlementRef Attribute for a User in the Roles and Resource Service Driver

Identity Manager allows you to resynchronize roles, resources, and Dir-XML EntitlementRef of a user by using the following methods. This requires the 4.7.1 Roles and Resource Service driver with the following driver package (`NOVLRSERVB_4.7.1.20180514123552.jar` OR later). `(Bug 1093450)`

REST API

REST Endpoint: `https://host:port/IDMProv/rest/admin/identityResync`

Permission Required: A user who issues the API must be a Provisioning Administrator.

```
HTTP Method: POST
              Body:
              {
                "dn": dn of the identity
             }
```

iManager

1. Log in to iManager.
2. Click **Driver Sets** in **Identity Manager Overview**.
3. Click the driver set containing your driver, then click the Role and Resource Service driver.
4. Locate the driver icon, then click the upper right corner of the driver icon to display the **Actions** menu.
5. Click **Open Driver Overview** to display the driver overview page.
6. Click **Migrate > Migrate from Identity Vault**.
7. In Migrate data from Identity Vault page, click **Add**, then select the identities to resynchronize.
8. Click **Start**.

When you send a resynchronization request through any of these methods, Identity Manager generates a Resynchronization event for the driver and pushes the event to the engine cache. The driver resynchronizes roles, resources, and Dir-XML EntitlmentRef attribute for the user as part of processing the event.

NOTE: Both the methods add the event to the driver's cache and do not submit the command directly to the driver. Therefore, resynchronization occurs depending on the load of the driver.

1.2.2 Enhancements in Identity Applications

This release provides the following enhancements in Identity Applications:

- Section 1.2.2.1, "Improved Client Access Settings Page," on page 5
- Section 1.2.2.2, "Simplified Confirmation Number Format for Requests," on page 5

1.2.2.1 Improved Client Access Settings Page

The Client Access settings help you to provision the page access to a user, group, role, or a container. The **Settings > Access** page is restructured based on the look and accessibility of the pages in Identity Manager Dashboard. For more information, see Managing User Access.

1.2.2.2 Simplified Confirmation Number Format for Requests

Identity Applications generate a unique confirmation number for each request in the dashboard. In this release, the format of the confirmation number is simplified and is displayed in the `YYYYMMDD-<`*`Sequence_number`*`>` format. For example: **20180529-12**.

1.2.3 Enhancements in Designer

This release provides the following enhancements in Designer:

- Section 1.2.3.1, "Support for eDirectory-to-eDirectory Certificate Creation on Mac Operating Systems," on page 6
- Section 1.2.3.2, "Support for query-ex Action in the Entitlement Editor," on page 6
- Section 1.2.3.3, "Support for token-map-source-col token in Policy Builder," on page 6
- Section 1.2.3.4, "New Option to Overwrite the Driver Startup Value Set in the Driver Packages," on page 6

1.2.3.1 Support for eDirectory-to-eDirectory Certificate Creation on Mac Operating Systems

An eDirectory-to-eDirectory connection helps you configure two eDirectory drivers to communicate directly with each other. If SSL/TLS are enabled, Designer creates the certificates in the eDirectory tree when you deploy the drivers.

IMPORTANT: To create an edirectory-to-edirectory certificate using Designer 4.7.1, ensure that the engine is updated to 4.7.1 version.

1.2.3.2 Support for query-ex Action in the Entitlement Editor

The Entitlement editor of Designer extends support for building the `<query-ex>` action. `<query-ex>` is a query variant used to limit the number of search results returned at one time. It specifies whether an Identity Manager driver supports `query-ex` action for a particular entitlement. For more information about `<query-ex>`, see the Identity Manager Developer Documentation (https://www.netiq.com/documentation/identity-manager-developer/dtd-documentation/ndsdtd/query-ex.html).

1.2.3.3 Support for token-map-source-col token in Policy Builder

Identity Manager uses `<token-map-source-col>` for specifying multiple source columns in `token-map`. This cannot be used in any other token other than token-map. Designer's Policy Builder adds support for `<token-map-source-col>` in this release. For more information about `<token-map-source-col>`, see the Identity Manager Developer Documentation (https://www.netiq.com/documentation/identity-manager-developer/dtd-documentation/dirxmlscript/token-map-source-col.html).

1.2.3.4 New Option to Overwrite the Driver Startup Value Set in the Driver Packages

Value for driver startup option is set in the driver packages when the driver is created. This release provides support for overwriting the startup value through a new option, **Overwrite the driver option...**, in the **Preferences** page.

1. Open Designer 4.7.1.
2. Click **Window** > **Preferences**.
3. On the **Preference** page, click **NetIQ** > **Identity Manager** > **Configuration**.
4. On the **General** tab, select a value for **Default driver startup driver value**. For example, `Manual`.
5. Select **Overwrite the driver Startup option...**.
6. Click **OK**.

The default value set in the driver packages is **Auto-Start**. When you click **Overwrite the driver option...**, **Auto-Start** is overwritten with **Manual**.

1.3 Platform Support

In addition to the existing platforms, this service pack extends support for the following platforms:

- Red Hat Enterprise Linux (RHEL) 7.5 for all Identity Manager components
- Open Enterprise Server (OES) 2018 for Designer

1.4 Component Updates

1.4.1 Identity Manager Component Versions

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

- Identity Manager Engine 4.7.1
- Identity Manager Remote Loader 4.7.1
- Identity Manager Fanout Agent 1.2.1
- Identity Applications 4.7.1
- Identity Reporting 6.0.1
- Identity Manager Designer 4.7.1
- Managed System Gateway Driver 4.2.0.0
- Data Collection Services Driver 4.2.0.0

1.4.2 Updates for Dependent Components

This release adds support for the following dependent components:

- NetIQ eDirectory 9.1.1
- NetIQ iManager 3.1.1

  You must install iManager 3.1.1 to support eDirectory 9.1.1. Ensure that you update your existing plug-ins to the latest versions for the iManager version you are using.
- NetIQ Self Service Password Reset (SSPR) 4.3.0
- NetIQ One SSO Provider (OSP) 6.2.2
- Sentinel Log Management for Identity Governance and Administration 8.2

1.4.3 Third-Party Component Versions

- Java Development Kit 8 Update 172 (jdk8u172) or Java Runtime Environment 1.8 Update 172 (jre8u172)
- Apache Tomcat 8.5.30
- PostgreSQL 9.6.9

1.5 What’s Discontinued?

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

- The User Application interface and the following features are discontinued:
  - Availability based Delegation
  - Portlets
  - Shared and Container pages
  - Password Management

- Compliance, Configuration, and Reporting domains within the User Application are discontinued. This change does not remove the existing assignments that have been previously made to these domain types. However, you cannot edit those assignments.

  Compliance: For compliance and attestation processes, NetIQ recommends you to use NetIQ Identity Governance (formerly Access Review) instead of the identity applications. For more information, see the NetIQ Identity Access Governance documentation.

  Configuration: Identity Applications include Client Settings in the Identity Applications administration interface. You must use it to configure the User Application. For more information, see “Client Access Settings:” on page 3.

  Reporting: Identity Manager includes Identity Reporting. Identity Reporting is accessible to Reporting Administrators. You must use this Reporting Administrator role for all reporting needs. For more information, see Assigning the Identity Applications Administrators.

To see the details about features or functionalities discontinued in Identity Manager 4.7, see the Identity Manager 4.7 Release Notes (https://www.netiq.com/documentation/identity-manager-47/releasenotes_idm47/data/releasenotes_idm47.html#discontinued-features-functions-identity-manager-47).

1.6 What’s Deprecated for Removal?

Permission Collection Reconciliation Services (PCRS) is deprecated from this release. Controlled Permissions Reconciliation Services (CPRS) now extends support for all PCRS-supported drivers. For more information about CPRS, see Using Controlled Permission Reconciliation Services in the *NetIQ Identity Manager - Administrator’s Guide to the Identity Applications*.

To see the details about features or functionalities deprecated in Identity Manager 4.7, see the Identity Manager 4.7 Release Notes (https://www.netiq.com/documentation/identity-manager-47/releasenotes_idm47/data/releasenotes_idm47.html#deprecated-features-functions-identity-manager-47).

1.7 Software Fixes

This release includes the following software fixes that resolve several previous issues in the Identity Manager.

- Section 1.7.1, “Identity Manager Engine,” on page 8
- Section 1.7.2, “Identity Applications,” on page 10
- Section 1.7.3, “Designer for Identity Manager,” on page 14

1.7.1 Identity Manager Engine

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

- Section 1.7.1.1, “Identity Manager Engine Supports Policies Containing Queries,” on page 9
- Section 1.7.1.2, “Ability to Migrate a Named Password Without Specifying its Description,” on page 9
- Section 1.7.1.3, “No Strict Order to Specify the localaddress Parameter in the Remote Loader Configuration,” on page 9
- Section 1.7.1.4, “Start and Stop Icons Do Not Overlap in the Remote Loader Console on German Locale,” on page 9

1.7.1.1 Identity Manager Engine Supports Policies Containing Queries

Identity Manager Engine is updated to support policies that contain queries. The Policy Simulator no longer reports any issues while running such policies. `(Bug 1096036)`

1.7.1.2 Ability to Migrate a Named Password Without Specifying its Description

Identity Manager removes the dependency of providing a description for a named password when migrating the password. Migration succeeds without specifying the description of the password. `(Bug 1086158)`

1.7.1.3 No Strict Order to Specify the localaddress Parameter in the Remote Loader Configuration

The `localaddress` parameter no longer needs to be the first parameter in the Remote Loader configuration. Remote Loader is successfully connected to the Identity Manager engine if `localaddress` is specified in any order in the configuration. `(Bug 642123)`

1.7.1.4 Start and Stop Icons Do Not Overlap in the Remote Loader Console on German Locale

The Remote Loader Console has been enhanced to restrict the Start and Stop buttons from overlapping. Also, the buttons now have the same size for consistency. `(Bug 1080971)`

1.7.1.5 Issue with Starting or Stopping Trace in Multiple Remote Loader Sessions Connected Remotely to the Same Windows Server

The Trace window correctly opens in the session from which it has been opened. `(Bug 1092067)`

1.7.1.6 Issue with Regenerating Identity Manager Server Keys

When you instruct Identity Manager to regenerate all Identity Manager server keys, eDirectory no longer crashes during startup or while loading dirxml.dlm or vrdim modules. `(Bug 1071778)`

1.7.1.7 Data Collection Service Driver Correctly Handles Synchronization Events

The Data Collection Service driver correctly handles synchronization events such as resynchronization, migration, enabling the driver after disabling it, and cache recovery. `(Bug 941637)`

1.7.1.8 Identity Manager Treats SYN_TIME values as Signed Integers Instead of Unsigned Integers

Identity Manager Engine 4.7.1 treats timestamps as unsigned integer (like eDirectory treats LDAP). This allows you to specify the time between 1970 until 2106. `(Bug 1092478)`

1.7.1.9 Issue with Running the Sentinel Log Management for IGA Installer

The Sentinel Log Management for IGA installation program no longer generates errors just before a language is selected for installation during the installation process. `(Bug 1088859)`

1.7.1.10 Symbolic Link Issue While Installing or Upgrading Identity Manager Engine as a Non-Root User

The symbolic link to JRE now points to a valid directory. `(Bug 1092023)`

1.7.2 Identity Applications

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

- Section 1.7.2.1, “Ability to Log In and Log Out of Identity Applications Simultaneously,” on page 11
- Section 1.7.2.2, “Dashboard Shows Same Results When Searching for Permissions for Self and Others,” on page 11
- Section 1.7.2.3, “Identity Manager Schema Includes pwmOtpSecret Attribute,” on page 11
- Section 1.7.2.4, “Ability to Handle Duplicate Permissions While Building the Index and During Searches,” on page 11
- Section 1.7.2.5, “Can Specify a Negative Integer in Workflow Forms,” on page 11
- Section 1.7.2.6, “Updated Struts Library,” on page 11
- Section 1.7.2.7, “Workflow Initiator Field Is Correctly Displaced in Dashboard,” on page 11
- Section 1.7.2.8, “catalina.out File Correctly Rotates the Logs on Linux,” on page 11
- Section 1.7.2.9, “Ability to Create a Team with Dynamic Group as a Manager,” on page 11
- Section 1.7.2.10, “User Look Up Search Displays the Placeholder Based on Customized User Search Lookup Attributes,” on page 11
- Section 1.7.2.11, “Workflow for Role Request is Not Terminated in Non-English Locales When the Request is Later Retracted,” on page 12
- Section 1.7.2.12, “Correct WorkID for Group Approver Type,” on page 12
- Section 1.7.2.13, “Restricted View of PRDs of Different Users,” on page 12
- Section 1.7.2.14, “Entitlement Value Parameter Is Not Displayed for Valueless Entitlements,” on page 12
- Section 1.7.2.15, “Ability to Control Granular Navigation Permissions in Identity Applications,” on page 12
- Section 1.7.2.16, “Task Page Responds Properly When the Page Size Has a High Value,” on page 13
- Section 1.7.2.17, “Objectclass Is Included in the Search Filter when Kerberos or SAML Authentication Methods Are Used with OSP,” on page 13
- Section 1.7.2.18, “ECMA Script Does Not Display Errors When a PRD is Deployed,” on page 13
- Section 1.7.2.19, “Consistency in Styles on the Request and Approval Forms,” on page 13
- Section 1.7.2.20, “Improved Performance for Proxy assignments that Contain Users Only,” on page 13
- Section 1.7.2.21, “Improved Performance When you Access the Dashboard Without Internet Connectivity,” on page 13
- Section 1.7.2.22, “E-mail Based Approval Support for Role and Resource Approval Workflows,” on page 13
- Section 1.7.2.23, “Null Pointer Errors are Not Displayed on the User Interface,” on page 14
- Section 1.7.2.24, “Ability to Delete Direct Assignments Only,” on page 14

1.7.2.1 Ability to Log In and Log Out of Identity Applications Simultaneously

Identity Applications are updated to support simultaneous login and logout actions when the applications are accessed using multiple browsers by same or different users at the same time. (Bug 1090511)

1.7.2.2 Dashboard Shows Same Results When Searching for Permissions for Self and Others

The permission search functionality now shows the same permissions for yourself or others based on the search string. For example, when you search permissions for yourself in the dashboard, it shows all the permissions name or description that match the search string. Similarly, **Others** show the same permissions that are seen in **Self**. (Bug 1071957)

1.7.2.3 Identity Manager Schema Includes pwmOtpSecret Attribute

Identity Manager uses the `pwmOtpSecret` attribute to extend the Self Service Password Reset component schema. This attribute is now included in the `edirectory-schema.sch` file. (Bug 1094665)

1.7.2.4 Ability to Handle Duplicate Permissions While Building the Index and During Searches

Permission Indexing can now handle duplicate permissions when it is building the index. Duplicate permissions are also properly handled when searching for permissions. (Bug 1083074)

1.7.2.5 Can Specify a Negative Integer in Workflow Forms

You can now specify a negative integer in a workflow form when the data type is set to integer. (Bug 1092563)

1.7.2.6 Updated Struts Library

The Struts library has been replaced with Spring MVC 5.0.4. (Bug 1071143)

1.7.2.7 Workflow Initiator Field Is Correctly Displaced in Dashboard

The Workflow form correctly displays the Recipient field instead of the Workflow Initator field. (Bug 1093382)

1.7.2.8 catalina.out File Correctly Rotates the Logs on Linux

The `catalina.out` file correctly rotates the logs in Linux using the LogRotate service. It creates a new log file every day with daily `cron` service. (Bug 1047148)

1.7.2.9 Ability to Create a Team with Dynamic Group as a Manager

You can now create a team and assign a dynamic group as the manager of the team. Also, it is possible for a member of the dynamic group to obtain information about other members of that group. (Bug 1088079)

1.7.2.10 User Look Up Search Displays the Placeholder Based on Customized User Search Lookup Attributes

The User Look up Search functionality is enhanced to display the placeholder based on customized user search lookup attributes. (Bug 1080794)

1.7.2.11 Workflow for Role Request is Not Terminated in Non-English Locales When the Request is Later Retracted

When using a locale other than English, if you request for a role and later retract the request, the dashboard correctly terminates the workflow for the requested role. `(Bug 1069960)`

1.7.2.12 Correct WorkID for Group Approver Type

The My Tasks page displays the same workID that is shown in the deeplink URL. `(Bug 955680)`

1.7.2.13 Restricted View of PRDs of Different Users

Identity Applications shows the PRD information of users only for the following users: `(Bug 1069960)`

- Recipient or initiator of a task
- Provisioning Administrator or a Delegated Team Manager can obtain the data. No other user can view this information.

1.7.2.14 Entitlement Value Parameter Is Not Displayed for Valueless Entitlements

You can now successfully create and map a valueless entitlement to a resource. Identity Applications no longer display the Entitlement Value parameter for valueless entitlements.`(Bug 1093705)`

1.7.2.15 Ability to Control Granular Navigation Permissions in Identity Applications

You can now configure Provisioning Dashboard to control what a user can view and access in the dashboard user interface. For example, you can control the following permissions in Access Settings for your users: `(Bug 1064143)`

- Tasks
- Settings
  - Manage Clients
- Users
  - Manage User
  - Edit User
  - Display Roles
  - Display Resources
  - Display Groups
  - Create User
- Password Sync Status
- Organization Chart
- Groups
  - Manage Group
  - Delete Group
  - Create Group
- Manage Dashboard
  - Edit Dashboard
- Workflow Engine Cluster Configuration
- Provisioning Display
- Task Settings

- Request History Settings
- Permission Reconciliation
- Logging
- Driver Status
- Delegation and Proxy Configuration
- Caching and Cluster Configuration
  - Flush Cache
  - Cache Configuration
- Email Based Approval
- New Request
- Request History
- Permissions
  - Revoke Permission

1.7.2.16 Task Page Responds Properly When the Page Size Has a High Value

While building task overview, the dashboard performance is no longer impacted when the page size preference is set to 100 or more. `(Bug 1067071)`

1.7.2.17 Objectclass Is Included in the Search Filter when Kerberos or SAML Authentication Methods Are Used with OSP

Identity Applications append objectclass to the search filter when Kerberos or SAML Authentication Methods are used. This restricts OSP to search only for objectclasess for that user or inetorgperson.`(Bug 1019811)`

1.7.2.18 ECMA Script Does Not Display Errors When a PRD is Deployed

The issue is fixed. The Workflow engine works as expected when a PRD is deployed. `(Bug 1092261)`

1.7.2.19 Consistency in Styles on the Request and Approval Forms

The issue is fixed. The fonts, style, space between buttons, confirmation messages, and the length of combo box in Request and Approval forms are consistent with Identity Manager 4.6.`(Bug 1096225)`

1.7.2.20 Improved Performance for Proxy assignments that Contain Users Only

When a proxy assignment contains users only, the filter is applied based on the proxy assignment. It does not fetch groups and containers. `(Bug 1099444)`

1.7.2.21 Improved Performance When you Access the Dashboard Without Internet Connectivity

The performance is improved when you try to access the Dashboard from a server which is not connected to the internet.`(Bug 1094133)`

1.7.2.22 E-mail Based Approval Support for Role and Resource Approval Workflows

The default notification template is updated to add e-mail based approval support for role and resource approval workflows. Ensure that you have imported the Provisioning notification templates package (`NOVLPROVNOTF_2.1.2.20180624233150` OR later). `(Bug 1056889)`

1.7.2.23 Null Pointer Errors are Not Displayed on the User Interface

The utility is updated to handle runtime exceptions. The exceptions are not displayed on the UI anymore.`(Bug 1079522)`

1.7.2.24 Ability to Delete Direct Assignments Only

The issue is fixed. You can now revoke direct assignments only. Revoking of inherited assignments are disabled.`(Bug 1096229)`

1.7.2.25 Ability to Enable permission Index for Clustering from the Dashboard

The dashboard is updated to enable the permission index for clustering. `(Bug 1025450)`

1.7.2.26 Modifications to the Confirmation Number in the Request History Page

The confirmation number in the request history page is updated to display in `YYMMDD` format followed by a unique number for each request.`(Bug 1063052)`

1.7.3 Designer for Identity Manager

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

1.7.3.1 Policy Simulator allows you to expand the dirxml.auto.driverdn GCV details

The Policy Simulator is updated to print the details for the `dirxml.auto.localserverdn` GCV. `(Bug 1071532)`

1.7.3.2 Ability to Establish a Role to Role Relationship in Workflows

You can now establish a role to role relationship in workflows. `(Bug 1079305)`

1.7.3.3 Schema Comparison Shows Correct Results With Identity Vault 9.1.1 for a Converted Project for SYN_CLASS_NAME, SYN_HOLD, and SYN_INTERVAL Syntax Types

Issue: Identity Vault (eDirectory 9.1.1) is enhanced to correctly map SYN_HOLD, SYN_CLASS_NAME, and SYN_INETRVAL syntax types. After a project is converted, Designer correctly maps these syntax types for the following attributes: `(Bug 1099973)`

- cACertificate
- crossCertificatePair
- userCertificate
- Login Allowed Time Map
- Printer Configuration
- certificateRevocationList
- deltaRevocationList
- authorityRevocationList

1.7.3.4 Successfully Deploys Additional Server to the Identity Vault

When a new server is added to a driverset, Designer can now successfully deploy the new server to the Identity Vault. `(Bug 1089523)`

1.7.3.5 Successfully Imports Projects with Driversets of Mixed Versions of Identity Manager

Designer now supports importing projects with driversets containing mixed versions of Identity Manager 4.6 and 4.7 servers. `(Bug 1089534)`

1.7.3.6 Selected Outline View is Consistent with the Fishbone View

When you select the Outline view, Designer displays it consistently with the Fishbone view. `(Bug 1078773)`

1.7.3.7 Designer Correctly Displays the Identity Manager Version

This issue is fixed. In a multi-server setup, Designer is updated to display the correct Identity Manager version. `(Bug 1089958)`

1.7.3.8 Ability to Deploy SoD objects in the Attestations Context

This issue is fixed. Designer is updated to handle the conversion of provision attribute values correctly in LDAP Format. `(Bug 1090177)`

1.7.3.9 Allows Deploying a Workflow That Includes a Target Expression Containing An ‘@’ character

The NCP Designer is now able to deploy a workflow when the target expression includes a @ character. `(Bug 1055213)`

1.7.3.10 Allows Dynamic Groups as Workflow Trustee Rights

This issue is fixed. When a PRD, Role, and Resource are deployed, the dynamic groups are correctly displayed in trustee rights. `(Bug 420043)`

1.7.3.11 Schema Comparison Shows Correct Results After Converting a Project

This issue is fixed. Converting a designer project from NCP to LDAP format converts and displays the schema correctly. `(Bug 1052404)`

1.7.3.12 Policy Token editor adds UTC (Coordinated Universal Time) As the Default Time Zone for New Tokens

This issue is fixed. The policy editor now adds UTC as the default time zone for new time tokens. `(Bug 1088817)`

1.7.3.13 Supports Standard E-Mail Port in the Identity Manager Configuration

This issue is fixed. A new option is introduced in Designer to prompt users to specify the server and port details, when the port is not specified with a URL. `(Bug 1076364)`

1.7.3.14 Policy Simulator Extends Support for Simulating Policies With Mapping Tables

Simulator now correctly simulates the policies containing mapping table objects.`(Bug 1088822)`

1.7.3.15 Correctly Configures the Startup Option of Drivers

This issue is fixed. Modifying the Startup option in LDAP designer and deploying it updates the Identity Vault correctly.`(Bug 1089528)`

1.7.3.16 Ability to Select Custom Tokens from send email from Template

Policy Builder is enhanced to allow you to select custom tokens from "send email from template" policy action. `(Bug 1088824)`

1.7.3.17 ECMAScript Editor Is Not Automatically Closed with Escape Key

The default behavior of Escape key action is disabled for ECMAScript Editor and ECMA Expression Builder pop-up windows. If you press the Escape key while the cursor is in these windows, Designer does not close these windows. `(Bug 1080333)`

1.7.3.18 Correct Display of LDAP Connection Preference User Page

The LDAP Connection Preferences user interface has been resized. Now the parameters are correctly displayed on this page. `(Bug 1083833)`

1.7.3.19 Resized Save Dialog for Committing Changes to the Subversion Server

The Save dialog that Designer prompts for saving your changes before committing the changes to the Subversion sever has been resized to sufficiently accommodate the displayed text. `(Bug 1089425)`

1.7.3.20 Correctly Displays Dirxml-pkgLinkage Comparison Details

When comparing two drivers with differences in the DirXML-pkgLinkage attribute, the earlier versions of Designer displayed only the first line the XML file of each driver. Now Designer displays the complete XML data. (Bug 1088718)

1.7.3.21 MacOS Keyboard Shortcuts Work Properly in Actions Builder

Designer is enhanced to allow working with MacOS keyboard shortcuts such as Command-C, Command-V in Actions Builder. (Bug 1088812)

1.7.3.22 Driverset Deployment Context Containing Organization Unit and Organization Fails

This issue is fixed. Designer is enhanced to deploy context with different combinations such as `ou="<value>",o=<value>`. (Bug 1092514)

2 Installing or Updating to This Service Pack

Log in to the NetIQ Downloads page and follow the link that allows you to download the software.

The following files are available:

Filename	Description
`Identity_Manager_4.7.1_Linux.zip`	Contains files for Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent), Identity Applications, and Identity Reporting for Linux platform. **NOTE:** This file also contains JDBC Fanout and Managed System Gateway driver files.
`Identity_Manager_4.7.1_Windows.zip`	Contains files for Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent), Identity Applications, and Identity Reporting for Windows platform. **NOTE:** This file also contains JDBC Fanout and Managed System Gateway driver files.
`Identity_Manager_4.7.1_Designer.zip`	Contains files for Designer.
`SentinelLogManagementForIGA8.2.0.0.tar.gz`	Contains Sentinel Log Management for Identity Governance and Administration (IGA) files. **NOTE:** This installation is supported only on Linux.

For more information about the order of upgrading the components, see Section 2.1, “Update Order,” on page 18.

2.1 Update Order

You must update the components in the following order:

1. Identity Vault (Optional)
2. Identity Manager Engine
3. Remote Loader
4. Fanout Agent
5. Designer
6. Identity Applications (for Advanced Edition)
7. Sentinel Log Management for IGA
8. Identity Reporting
9. One SSO Provider (OSP)

   NOTE: Standalone update of OSP is supported only on Windows.

10. Self-Service Password Reset

2.2 Updating the Identity Manager Components on Linux

This service pack includes a `Identity_Manager_4.7.1_Linux.zip` for updating the Identity Manager components on Linux platforms. For update instructions, see the steps listed in the Linux Readme file.

2.3 Updating the Identity Manager Components on Windows

This service pack includes a `Identity_Manager_4.7.1_Windows.zip` for updating the Identity Manager components on Windows platforms. For update instructions, see the steps listed in the Windows Readme file.

2.4 Updating Designer

This service pack includes a `Identity_Manager_4.7.1_Designer.zip` for updating the Identity Manager Designer. For update instructions, see the steps listed in the Designer Readme file.

2.5 Updating Sentinel Log Management for IGA

This service pack includes a `SentinelLogManagementForIGA8.2.0.0.tar.gz` file for updating the Sentinel Log Management for Identity Governance and Administration (IGA) component. For update instructions, see the steps listed in the Sentinel Readme file.

2.6 Updating the DCS Driver

1 Stop the driver instance by using iManager, Designer, or dxcmd by performing one of the following actions:

- If the driver is running locally, stop the driver instance and the Identity Vault.
- If the driver is running with a Remote Loader instance, stop the driver and the Remote Loader instance.

For example, go to a command prompt on Linux and run `ndsmanage stopall`.

2. Download the driver patch file (IDM_DCS_4200.zip) to a temporary folder on your server.
3. Extract the contents of the driver patch file.
4. Update the driver files.
    - **Linux:** Open a command prompt and run the following command to update the existing RPM:

      ```
      rpm -U (IDM_DCS_4200.zip)/novell-DXMLdcs.rpm
      ```

    - **Windows:** Navigate to the `<Extracted Driver Patch File Temporary Location>\windows` folder and copy the `dcsshim.jar` file to `<IdentityManager installation>\NDS\lib` or `<IdentityManager installation>\RemoteLoader\lib` folder.
5. (Conditional) If the driver is running locally, start the Identity Vault and the driver instance.

   For example, open a command prompt on Linux and run `ndsmanage startall`.
6. (Conditional) If the driver is running with a Remote Loader, start the Remote Loader and the driver instance.

   Ensure that the ZoomDB library is included in the Remote Loader’s library path. The ZoomDB cache files are created when the driver runs.

2.7 Manually Removing the MapDB Cache Files

After the Identity Manager engine is updated, the existing MapDB driver cache files (dx*) are no longer used by the Identity Manager engine and DCS and MSGW drivers. Instead, the new cache directories (dx*) created with the `.zoomdb` suffix are used. After completing the update, you can optionally remove the existing MapDB state cache files as described in the following table:

Identity Manager Component	MapDB Driver Cache File To Remove	Examples of MapDB Driver Cache Files
Identity Manager Engine	`dx<driver_entry_id>`	`dx32876`, `dx33474`
DCS Driver	`<driver_guid>`	`98E8DE83-AE91-4eaa-8084-83DEE89891AE-1`, `98E8DE83-AE91-4eaa-8084-83DEE89891AE-state-0`, `98E8DE83-AE91-4eaa-8084-83DEE89891AE-status-0`
MSGW Driver	`MSGW-{<driver_guid>}`	`MSGW-{75394052-4338-4332-9E58-524039753843}`

2.8 Enabling CEF for Identity Reporting

Perform the following steps to enable CEF for Identity Reporting:

NOTE: Ensure that you have enabled CEF in the configupdate utility. For more information, see CEF Auditing Parameters in the *NetIQ Identity Manager Setup Guide for Linux*.

1. Navigate to the `idmrptcore_logging.xml` file.

   Linux: `/opt/netiq/idm/apps/tomcat/conf`

   Windows: `C:\netiq\idm\apps\tomcat\conf`
2. Edit the `idmrptcore_logging.xml` file and provide the auditing server details:

```
<audit>
        <syslog>
            <enabled>true</enabled>
            <protocol>TCP</protocol>>
            <host>IP Address of your auditing server</host>
            <port>Audting server port</port>
            <cache-dir>name of the cache directory</cache-dir>
            <cache-file>name of the cache file within the cache directory</
cache-file>
       <application>Reporting Core</application>
       <vendor>Micro Focus</vendor>
           <version>6.0</version>
        </syslog>
    </audit>
```

3 Restart Tomcat.

3 Known Issues

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

- Section 3.1, “Designer Fails to Authenticate With Identity Manager Server on Windows When the Connection Uses Proxy Configuration,” on page 20
- Section 3.2, “Designer Does Not Respond If The Project Name Contains a Space,” on page 21
- Section 3.3, “TCP Channel Fails to Send Messages When Cache Settings Are Modified in Identity Application Cluster Nodes,” on page 21
- Section 3.4, “The getValueForNamedPassword Function in Designer Refers to the Wrong Attribute Name,” on page 21
- Section 3.5, “Permissions Are Not Synchronized on Identity Applications Cluster Nodes That Are Temporarily Disconnected From the Network,” on page 22
- Section 3.6, “Unable to Add a Featured Item on the Request Page,” on page 22
- Section 3.7, “Group Count Is Not Correctly Updated When a Group Is Deleted From the Group Catalog Page,” on page 22
- Section 3.8, “Cannot Create a Resource If the Resource Name Contains Special Characters,” on page 22
- Section 3.9, “Filter Resource Changes Are Not Automatically Applied to the Package,” on page 22
- Section 3.10, “Different Engine Control Values Are Set for Drivers Associated with Multiple Servers,” on page 23
- Section 3.11, “custom.css File Settings Are Overwritten by form-renderer.css File Settings,” on page 23

3.1 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.(Bug 1100070)

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**.

3.2 Designer Does Not Respond If The Project Name Contains a Space

Issue: Designer does not respond if the project name contains a space in it.`(Bug 1094152)`

Workaround: Do not use spaces while naming a project.

If your existing project name contains a space, perform the following actions to rename the project:

1. Close all the projects, including the files of projects outside Designer.
2. Go to Project view, and right click on the project name and click **Rename**.
3. Rename the project without any spaces in it and click **OK**.

3.3 TCP Channel Fails to Send Messages When Cache Settings Are Modified in Identity Application Cluster Nodes

Issue: In a cluster environment, when Identity Applications are restarted on cluster nodes after modifying the cache settings, Java exceptions are logged to the catalina.out file. It is safe to ignore these exceptions. They do not impact the cluster activities. For more information about these exceptions, see TID 7018506. `(Bug 1093442)`

Workaround: To clear the exceptions, restart the database server.

3.4 The getValueForNamedPassword Function in Designer Refers to the Wrong Attribute Name

Issue: When driver uses ECMA editor to fetch the defined named passwords, it populates the wrong attribute (named-password) instead of the GCV attribute.

For example, using the ECMA editor, if the GCV on the User Application driver is named `gcv.user.password` with the named-password reference as `np.user.password`, it populates GCV.getValueForNamedPassword (`np.user.password`) instead of GCV.getValueForNamedPassword (`gcv.user.password`).`(Bug 1092215)`

Workaround: Replace the named-password attribute with the GCV attribute name. In the above example, replace GCV.getValueForNamedPassword (`np.user.password`) with GCV.getValueForNamedPassword (`gcv.user.password`).

3.5 Permissions Are Not Synchronized on Identity Applications Cluster Nodes That Are Temporarily Disconnected From the Network

Issue: Permission changes from an active node of a cluster are not synchronized to any other node of the cluster when the node is reconnected to the network. `(Bug 1100166)`

Workaround: Restart Tomcat on the node that reconnected to the network after a temporary disconnection.

3.6 Unable to Add a Featured Item on the Request Page

Issue: A user with Provisioning or Security administrator rights fails to add a featured item on the **Request** page. `(Bug 1099815)`

Workaround: To add the featured item on the **Request** page, make sure that the user has the administrator rights for all the supported domain types.

3.7 Group Count Is Not Correctly Updated When a Group Is Deleted From the Group Catalog Page

Issue: When you delete a group from the **Group Catalog** page, the change is reflected on the page. However, the page does not show the correct number of available groups. `(Bug 1095879)`

Workaround: Refresh the page for the changes to take effect.

3.8 Cannot Create a Resource If the Resource Name Contains Special Characters

Issue: While creating a resource with an entitlement, you cannot use the following special characters in the resource name:

[< > , ; \ " + # = / | & * ' ! @ $ %] or a blank space

Identity Applications detect these characters and disable the **Apply** button in the **Create Resource** page. (`Bug 1101369`)

Workaround: Do not use special characters in the resource name.

3.9 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**.

3.10 Different Engine Control Values Are Set for Drivers Associated with Multiple Servers

Issue: When you create a driver in a driverset that is associated with multiple servers, different ECVs (Engine Control Value) are set for the driver for different servers. For example, the “Qualified form for DN-syntax attribute values” ECV shows different values (true and false) for the driver for each server it is associated with.

Workaround: There is no workaround at this time.

3.11 custom.css File Settings Are Overwritten by form-renderer.css File Settings

Issue: By default, the `form-renderer.css` file takes precedence over the custom.css file and overwrites the settings written in the `custom.css` file. If you have any customized forms, you must rework them to prevent discrepancies in the appearance of the forms.

Workaround: Rename the `form-renderer.css` file. For example, rename the file to `form-renderer-renamed.css`. This action will ensure that the `custom.css` file takes precedence over the `form-renderer.css` file.

4 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.

5 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/.