

NetIQ Identity Manager 4.5 Service Pack 1 Release Notes

May 2015



NetIQ Identity Manager 4.5 Service Pack 1 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](#).

- ♦ [Section 1, "What's New?," on page 1](#)
- ♦ [Section 2, "System Requirements," on page 8](#)
- ♦ [Section 3, "Installing This Service Pack," on page 8](#)
- ♦ [Section 4, "Known Issues," on page 19](#)
- ♦ [Section 5, "Contact Information," on page 19](#)
- ♦ [Section 6, "Legal Notice," on page 19](#)

1 What's New?

This service pack provides improvements to and resolves several previous issues for the following Identity Manager components:

- ♦ Identity Manager engine
- ♦ Remote Loader
- ♦ Designer for Identity Manager
- ♦ Identity applications, including the underlying framework
- ♦ Identity Reporting

For the list of software fixes and enhancements in previous releases, see the Release Notes for that version on the [Identity Manager Documentation page](#).

- ♦ [Section 1.1, "Enhancements to Identity Manager," on page 2](#)
- ♦ [Section 1.2, "Enhancements to Designer for Identity Manager," on page 2](#)
- ♦ [Section 1.3, "Enhancements to the Identity Applications and Identity Reporting," on page 4](#)
- ♦ [Section 1.4, "Software Fixes for the Identity Manager Framework," on page 4](#)
- ♦ [Section 1.5, "Software Fixes for Designer for Identity Manager," on page 6](#)
- ♦ [Section 1.6, "Software Fixes for the Identity Applications and Identity Reporting," on page 7](#)

1.1 Enhancements to Identity Manager

This release provides the following enhancements:

- ♦ [Section 1.1.1, “New Names for Installation Log Files on Linux Servers,” on page 2](#)
- ♦ [Section 1.1.2, “Improved Patch Installer for the Identity Manager Engine and Remote Loader,” on page 2](#)

1.1.1 New Names for Installation Log Files on Linux Servers

The installation log files now indicate whether you updated Identity Manager components on a Linux server as a root or non-root user:

- ♦ **Linux root:** `idmPatchInstall-root.log`
- ♦ **Linux non-root:** `idmPatchInstall-nonroot.log`

The installation process also changes the permission of the `/tmp/logs` file on a Linux server:

```
chown root:users /tmp/logs
chmod +t /tmp/logs
```

The log file for a Windows server continues to be `idmPatchInstall.log`. Permissions for the file have not been changed. (Bug 943808)

1.1.2 Improved Patch Installer for the Identity Manager Engine and Remote Loader

This service pack improves the content in the NetIQ Identity Manager Patch Installer program for the Identity Manager engine and Remote Loader. For example, the program accurately identifies the operating system on which you run the update. (Bug 873938)

Also, when updating Remote Loader, you can now specify the path where you want to perform the update. The NetIQ Identity Manager Patch Installer allows you to browse to the installed version of Remote Loader. Previously, the patch installer might incorrectly detect the location of the installed Remote Loader 64-bit and would use a default path as if installing the 32-bit version. (Bug 921959)

1.2 Enhancements to Designer for Identity Manager

- ♦ [Section 1.2.1, “Creating the deprecated.properties file On Custom Package Update Site,” on page 2](#)
- ♦ [Section 1.2.2, “Improved Ability to Upgrade Installed Packages,” on page 3](#)
- ♦ [Section 1.2.3, “Designer Maintains Parameter Value after Conversion to GCV,” on page 3](#)
- ♦ [Section 1.2.4, “Enhances Ability to Perform Comparisons,” on page 3](#)
- ♦ [Section 1.2.5, “Designer Update Site Has Changed,” on page 3](#)

1.2.1 Creating the deprecated.properties file On Custom Package Update Site

Designer automatically generates the `deprecated.properties` file if the update site is created by using the Designer package build and publish mechanism. This file contains the required instructions for building the list of deprecated packages.

If you have created your own update site, create a `deprecations` folder on the site and include a `deprecated.properties` file in this folder.

1.2.2 Improved Ability to Upgrade Installed Packages

Designer now allows you view and upgrade the already installed packages in your Identity Manager environment in a single consolidated view. The provision of a single view removes the need for you to separately go to each driver, driver set, or Identity Vault in your project to view or upgrade the packages that they contain. For more information, see [“Upgrading Installed Packages”](#) in the *NetIQ Designer for Identity Manager Administration Guide*. (Bug 912257)

1.2.3 Designer Maintains Parameter Value after Conversion to GCV

You can convert a parameter for driver configuration to a Global Configuration Value (GCV). In this release, Designer preserves the specified value of the parameter during the conversion process. (Bug 808304)

1.2.4 Enhances Ability to Perform Comparisons

This service pack improves your ability to perform the following types of comparisons:

Resource Objects

You can compare any pair of resource objects in the same manner that you might compare two policies. For example, you can compare resources, mapping tables, or ecma scripts. (Bug 916906)

Driver Set Packages

You can compare the customization capability of driver set packages, similar to comparisons for a driver. You can compare the package folder items from the package to the one in driver set for the following library items: policy, ECMA script, mapping table, DS object, resource, and GCV. (Bug 916912)

Identity Vault Packages

You can compare the customization capability of policy packages in the Identity Vault, similar to comparisons for a driver. You can compare the package folder items from the tree-level package to the one in the Identity Vault for the following library items: schema map, policy, ECMA script, mapping table, DS object, resource, and notification templates. (Bug 916913)

1.2.5 Designer Update Site Has Changed

NetIQ provides a new update site for downloading the Designer updates and packages. NetIQ recommends that you start using the new update site even though it continues to support the existing update site for updating the older versions of Designer. To receive notifications from the new update site, include the new URLs in your Designer. (Bug 905397)

To include the new URL of the Designer update site in Designer, do the following actions:

- 1 Launch Designer.
- 2 From Designer's main menu, click **Windows > Preferences > NetIQ > Identity Manager > Updates** tab and change the value of the **URL** field to `https://nu.novell.com/designer/updatesite4_5_0/`.
- 3 Click **Apply**, then click **OK**.

To verify whether the new URL is working,

- 1 Launch Designer.
- 2 From Designer's main menu, click **Help > Check for Designer Updates**.

If your version of Designer is up-to-date, a prompt informs you that no updates are available. If an update is available, a prompt lists components that you can update.

- 3 If the updates are available, select the updates and then click **OK**.

To include the new URL of the package update site, do the following actions:

- 1 Launch Designer.
- 2 From Designer's main menu, click **Windows > Preferences > NetIQ > Package Manager > Online Updates** and click the **plus** icon to add the new URL as `https://nu.novell.com//designer/packages/idm/updatesite2_0_0/`.
- 3 Click **OK**.
- 4 Select the required check boxes for the update sites in the Preferences window.
- 5 Click **Apply**, then click **OK**.

To verify whether the new URL is working,

- 1 Launch Designer.
- 2 From Designer's main menu, click **Help > Check for Package Updates**.
If there are no package updates, Designer returns a message stating that no updates are available. If an update is available, a prompt lists the packages with newer versions.
- 3 From the list of available packages, select the required version for update and click **Yes**.

1.3 Enhancements to the Identity Applications and Identity Reporting

- ♦ [Section 1.3.1, "Can Specify the Timezone for a Report," on page 4](#)
- ♦ [Section 1.3.2, "Reports Include the Name of the Reporter," on page 4](#)

1.3.1 Can Specify the Timezone for a Report

When configuring a report, you can specify the timezone for which you want to run the report. This change ensures that you can gather data from a source at the time appropriate for that source rather than the time on the reporting server.

For example, the data source resides on a server in Houston and the reporting server is in Delhi. You can configure the report to run at 2 AM Houston time. If the report runs at 2 AM in Delhi, which is 12:30 PM in Houston, it cannot capture all the changes that occur at the Houston office that day. (Bug 902453)

1.3.2 Reports Include the Name of the Reporter

Identity Reporting now includes the name of user who generated the report. The name appears in the report header. (Bug 911849)

1.4 Software Fixes for the Identity Manager Framework

This release resolves the following major customer issues for the Identity Manager engine, Remote Loader, and the Identity Vault:

- ♦ [Section 1.4.1, "Events from the Identity Vault Display Full Domain Name in NetIQ Sentinel," on page 5](#)
- ♦ [Section 1.4.2, "Identity Vault Now Displays Special Characters," on page 5](#)
- ♦ [Section 1.4.3, "Can Run the Update Regardless of Spaces in the Installation Path," on page 5](#)

- [Section 1.4.4, “Email Policy Does Not Require SMTP Authentication,” on page 5](#)
- [Section 1.4.5, “Set and Clear SSO Credentials for Accounts Configured with an Older Version of NetIQ SecureLogin,” on page 5](#)
- [Section 1.4.6, “Password Expiration Job Runs Successfully after an NDSrepair,” on page 6](#)
- [Section 1.4.7, “ndsd.log File Does Not List an Erroneous Warning Message,” on page 6](#)
- [Section 1.4.8, “Resolves an Issue with Adding Event Information,” on page 6](#)

1.4.1 Events from the Identity Vault Display Full Domain Name in NetIQ Sentinel

When you use NetIQ Sentinel to collect Add Group Member events from the Identity Vault, the **TargetTrustDomain** and **TargetUserDomain** fields now include the full domain name, such as `\org\groups\test`. Previously, the fields failed to include the name of the top-level container, such as `\org`. This change allows you to create more precise correlation rules within Sentinel. (Bug 914242)

1.4.2 Identity Vault Now Displays Special Characters

This service pack resolves an issue where the Identity Vault might synchronize a `?` character instead of a special character such as an umlaut for user-specified fields. For example, it synchronizes `j?ppel` instead of `jäppel` for a user's name. This issue usually occurred after you rebooted the server that hosts the Identity Vault and the environment variable reverted to a non-UTF-8 character set. Now Identity Manager ensures that the JVM option `file.encoding` is set to UTF-8 before launching the JVM. (Bug 909406)

1.4.3 Can Run the Update Regardless of Spaces in the Installation Path

You can now update Identity Manager even when path of the installation program includes a space. Previous updates would fail if the installation path contained a space. (Bug 887378)

1.4.4 Email Policy Does Not Require SMTP Authentication

Identity Manager can now communicate with an SMTP server that does not require authentication while executing the policy `do-send-mail-with-template`. For example, you can now use the policy to send notifications from the Identity Manager engine without configuring SMTP authentication. (Bug 875033)

1.4.5 Set and Clear SSO Credentials for Accounts Configured with an Older Version of NetIQ SecureLogin

This service pack resolves an issue where you could not clear and set the SSO credential of an account that uses `clear-sso-credentials` actions. This issue occurred for accounts where you previously set the credential using NetIQ SecureLogin 6 or older. The `clear-sso-credentials` action failed with the following message:

```
Couldn't perform SSO operation <do-set-sso-credential>: '4444:ERROR
(provisionNSLAccount): General Exception: java.lang.NullPointerException'
```

(Bug 904822)

1.4.6 Password Expiration Job Runs Successfully after an NDSrepair

This service pack resolves an issue where the Password Expiration Job fails after you run the NDSrepair utility on the same server that processes the job. The job would fail with the following error:

```
no object DCH for MIME type multipart/mixed
```

This issue occurred only if the Password Expiration Job used HTML format and you did not restart eDirectory after running the NDSrepair utility. (Bug 890229)

NOTE: NetIQ recommends running the NDSrepair utility only when you need to correct problems in the Identity Vault (eDirectory database), rather than running the utility as a scheduled activity. Corrections usually require a restart of eDirectory and Identity Manager, which can adversely affect user operations.

1.4.7 ndsd.log File Does Not List an Erroneous Warning Message

This service pack resolves an issue where eDirectory 8.8.8 Patch 3 generates the following warning in the ndsd.log when you load libvrdim:

```
Java HotSpot(TM) 64-Bit Server VM warning: You have loaded library /opt/novell/
eDirectory/lib64/libdhutilj.so.3.0.500 which might have disabled stack guard
(Bug 907240)
```

1.4.8 Resolves an Issue with Adding Event Information

This service pack resolves an issue where the Identity Manager engine incorrectly adds extra event information to operation data. (Bug 906276)

1.5 Software Fixes for Designer for Identity Manager

This release resolves the following major customer issues for Designer:

- [Section 1.5.1, "Designer Appropriately Launches ECMAScript Editor for New Workflow Scripts," on page 6](#)
- [Section 1.5.2, "Email Addresses Can Include Numeric Characters," on page 7](#)
- [Section 1.5.3, "Resolves an Issue with Changing a Driver Icon," on page 7](#)
- [Section 1.5.4, "Designer Help Has Been Updated," on page 7](#)
- [Section 1.5.5, "Adds the Ability to Download the Deprecated.properties File," on page 7](#)
- [Section 1.5.6, "Add Resource Action No Longer Needs instanceGUID," on page 7](#)
- [Section 1.5.7, "Correction to Documentation," on page 7](#)

1.5.1 Designer Appropriately Launches ECMAScript Editor for New Workflow Scripts

This service pack updates Designer so you can use the ECMAScript editor when you add a new script for a form in a workflow in Designer. In previous releases, you might have received an unhandled event loop exception error when attempting to launch the script editor. The launch failed because the JSEditor plugin was not initialized. (Bug 901510)

1.5.2 Email Addresses Can Include Numeric Characters

With this service pack, you can specify email addresses that begin with a numeric character. For example, when you specify the From address for Default Notification Collection. (Bug 907783)

1.5.3 Resolves an Issue with Changing a Driver Icon

Changing the icon for a driver is no longer causes high CPU utilization and Designer does not initiate a loop while trying to display the icon. (Bug 911470)

1.5.4 Designer Help Has Been Updated

This service pack updates the Help to ensure that all appropriate content gets displayed upon request on Windows-based computers. In the previous release, some Help pages were not displayed as expected. (Bug 902975)

1.5.5 Adds the Ability to Download the Deprecated.properties File

If you create the update site with the Designer package build and publish mechanism, Designer automatically generates the deprecated.properties file. This file contains the required instructions for building the list of deprecated packages.

If you have created your own update site, create a deprecations folder on the site and include a deprecated.properties file in this folder. (Bug 903087)

1.5.6 Add Resource Action No Longer Needs instanceGUID

This service pack resolves an issue where you use attempt to add and remove one resource assignment in the Policy Builder using the remove resource action but Designer removes all resource assignments. This is occurred because Designer expected an instanceGUID to be associated with each remove resource action. Designer now prompts you to specify a value for instanceGUID when you perform the remove resource action. (Bug 902428)

1.5.7 Correction to Documentation

The online documentation for Designer erroneously stated that you can browse to objects in an application for Source DN (if on publisher) or Destination DN (if on subscriber). However, Designer allows you to browse to the Identity Vault, not an application. The online help has been improved to reflect Designer behavior. (Bug 890716)

1.6 Software Fixes for the Identity Applications and Identity Reporting

This release resolves the following major customer issues for the identity applications and Identity Reporting:

- ♦ [Section 1.6.1, "Role Service Now Provides a "Cancelled" Message," on page 8](#)
- ♦ [Section 1.6.2, "Resolves an Issue with Using the Resource Request Portlet," on page 8](#)
- ♦ [Section 1.6.3, "Resolves an Issue with Form Displays in Internet Explorer 11," on page 8](#)
- ♦ [Section 1.6.4, "The server.log File is Truncated on WebSphere," on page 8](#)

1.6.1 Role Service Now Provides a “Cancelled” Message

The Role Service now reports a “Cancelled” message when you search for role assignments for a user and the service attempts to return a retracted role assignment request. Previously, the service responded with an error. (Bug 895501)

1.6.2 Resolves an Issue with Using the Resource Request Portlet

This service pack resolves an issue where you use the Resource Request Portlet on a Shared Page to provide a form for a workflow. The browser responded with an unrecoverable error. (Bug 920641)

1.6.3 Resolves an Issue with Form Displays in Internet Explorer 11

This service pack resolves an issue where fields in forms do not display appropriately in Internet Explorer 11 on a Windows computer. (Bug 920853)

1.6.4 The server.log File is Truncated on WebSphere

This service pack resolves an issues where in WebSphere, the server . log file located in the *WebSphere-install-dir/AppServer/profiles/profile-name* (for example, /opt/IBM/WebSphere/AppServer/profiles/AppSrv01) might be truncated. (Bugs 900844, 899981)

2 System Requirements

This service pack requires the following product versions:

- NetIQ Identity Manager 4.5
- NetIQ One SSO Provider 4.5.0.2
- NetIQ Self Service Password Reset 3.2.0.3
- NetIQ eDirectory 8.8.SP8 Patch 5

3 Installing This Service Pack

To install this service pack, complete the installation steps in the following sections:

- [Section 3.1, “Updating the Identity Manager Engine,” on page 8](#)
- [Section 3.2, “Updating the Remote Loader,” on page 9](#)
- [Section 3.3, “Updating Designer Offline,” on page 9](#)
- [Section 3.4, “Updating One SSO Provider and Self Service Password Reset,” on page 11](#)
- [Section 3.5, “Updating the Identity Applications,” on page 11](#)
- [Section 3.6, “Updating Identity Reporting,” on page 15](#)

3.1 Updating the Identity Manager Engine

This service pack includes a `IDM_engine_r1_IDM4.5SP1.zip` for updating the Identity Manager engine and Remote Loader. Install this package on the Identity Manager engine server. For more information, see [“Installing the Identity Manager Engine and Remote Loader Patch”](#) in the *NetIQ Identity Manager Setup Guide*.

3.2 Updating the Remote Loader

This service pack provides updates for the Remote Loader, Remote Loader .NET, and the Java Remote Loader. When you install the Remote Loader on supported platforms, the installation program includes all versions of the Remote Loader for the operating system.

3.2.1 Updating the Remote Loader Files

Install the contents of IDM_engine_rl_IDM4.5SP1.zip package on each server where you have installed the Remote Loader, .Net Remote Loader, and the Java Remote Loader. For more information, see [“Installing the Identity Manager Engine and Remote Loader Patch”](#) in the *NetIQ Identity Manager Setup Guide*.

NOTE: If you previously used a manual process to install the Java Remote Loader, you must perform the procedure in [“Updating the Java Remote Loader Manually”](#) on page 9.

3.2.2 Updating the Java Remote Loader Manually

If you installed the Java Remote Loader manually on a server, you must manually upgrade the Java Remote Loader.

- 1 Shut down the Java Remote Loader:

```
../dirxml_jremote -config fileName -u
```

- 2 Extract the contents of the IDM_engine_rl_IDM4.5SP1.zip file to a temporary location.
- 3 Replace the following files in the lib folder of your Java Remote Loader installation with the files extracted from the .zip file:
 - ♦ dirxml.jar
 - ♦ dirxml_misc.jar
 - ♦ dirxml_remote.jar

By default, the files are located in the /cd-image/patch/OS_platform/<architecture>/RL/lib folder of the installation package.

- 4 Restart the Java Remote Loader:

```
../dirxml_jremote -config fileName &
```

3.3 Updating Designer Offline

Designer provides an in-built auto-update feature that notifies you of new features available at the Online Update Web site. This feature allows you to download Designer package and patch updates when the computer that has Designer installed and is connected to the Internet.

You also can perform an offline update of Designer when the computer that has Designer installed and is not connected to the Internet. To perform an offline update, first download the required contents from the Designer and Package Update Web sites on a local or remote computer and then point Designer to the directory containing the downloaded files.

- ♦ [Section 3.3.1, “Updating Designer in An Offline Mode,”](#) on page 10
- ♦ [Section 3.3.2, “Updating the Designer Packages Offline,”](#) on page 10

3.3.1 Updating Designer in An Offline Mode

To do this, create an offline copy of the Designer update files and then configure Designer to read the patch updates from the files copied to the local computer.

To create an offline copy of the Designer update files on Linux, perform the following actions:

- 1 Log in to the computer that has Designer installed and create a local directory.
- 2 Download the latest patch zip file for Designer version from the [specified location \(http://cdn.novell.com/cached/designer/AUPatches/\)](http://cdn.novell.com/cached/designer/AUPatches/) and unzip the files into the local directory.

To configure Designer to read the patch updates from the files copied to the local computer, perform the following actions:

- 1 Launch Designer.
- 2 From Designer's main menu, click **Windows > Preferences**.
- 3 Click **NetIQ > Identity Manager** and select **Updates**.
- 4 Select **Do not check for updates** and deselect all the other check boxes.
- 5 For **URL**, specify `file:///path_to_files/updatesite4_5_0`.
For a Linux mounted ISO, use the following URL format: `file:///media/designer450offline/updatesite4_5_0`.
- 6 Click **Apply**, then click **OK**.
- 7 From Designer's main menu, click **Help > Check for Designer Updates**.
- 8 Select the required updates and click **Yes** to accept and update the Designer patch updates.
You need to launch Designer again for the changes to take effect.

3.3.2 Updating the Designer Packages Offline

To do this, create an offline copy of the package update files and then configure Designer to read the package updates from the files copied to the local computer.

To create an offline copy of the package update files on Linux:

- 1 Log in to the computer that has Designer installed and create a local directory.
- 2 In a shell, change to this directory and run the following commands to copy the Designer package update files:

```
wget -r -nH -np http://nu.novell.com/cached/designer/packages/idm/updatesite1_0_0/
```

```
wget -r -nH -np http://nu.novell.com/cached/designer/packages/idm/updatesite2_0_0/
```

To configure Designer to read the package updates from the files copied to the local computer:

- 1 Launch Designer.
- 2 From Designer's main menu, click **Windows > Preferences**.
- 3 Click **NetIQ > Package Manager > Online Updates**.
- 4 To add a new URL, click the **plus** icon.

5 Provide information for the following fields:

5a Vendor: Specifies the vendor name for package update.

5b URL: Specifies the URL as `file:///path_to_files/packages/idm/updatesite1_0_0`.

For Linux mounted ISO, use the following URL format:

`file:///media/designer450offline/packages/idm/updatesite1_0_0`

`file:///media/designer450offline/packages/idm/updatesite2_0_0`

NOTE: If you have multiple package sites, repeat Step 5 and add multiple sites and URLs.

6 Click **OK**.

7 In the **Preferences** window, select the required check boxes for the sites.

NOTE: The new sites are selected by default.

8 Click **Apply**, then click **OK**.

9 From Designer's main menu, click **Help > Check for Package Updates**.

10 Select the required updates and click **Yes** to accept and update the Designer package updates.

You need to launch Designer again for the changes to take effect.

3.4 Updating One SSO Provider and Self Service Password Reset

This service pack requires the latest versions of NetIQ One SSO Provider and NetIQ Self Service Password Reset. To install these updates, download the following packages and perform the steps listed in the readme files:

- ♦ [IDM 4.5 One SSO Provider \(OSP\) 4.5.0.2](#)
- ♦ [Self Service Password Reset 3.2.0.3](#)

3.5 Updating the Identity Applications

This service pack includes an update to the identity applications. The process for installing the update depends on the web server that you use to support the applications. Also, ensure that you complete the post-installation steps.

- ♦ [Section 3.5.1, "Updating the Identity Applications on a JBoss Server," on page 11](#)
- ♦ [Section 3.5.2, "Updating the Identity Applications on a Tomcat Server," on page 12](#)
- ♦ [Section 3.5.3, "Updating the Identity Applications on a WebSphere Server," on page 14](#)
- ♦ [Section 3.5.4, "Post-installation Steps for Updating the Identity Applications," on page 15](#)

NOTE: The identity applications require the latest versions of NetIQ One SSO Provider and NetIQ Self Service Password Reset. For more information, see [Section 3.4, "Updating One SSO Provider and Self Service Password Reset," on page 11](#).

3.5.1 Updating the Identity Applications on a JBoss Server

- 1 Copy the `IDM45-Apps-SP-1.zip` file to the server where you deployed the identity applications on JBoss.
- 2 Extract the contents of the `.zip` file for the identity applications to a temporary location on the server.

- 3 Stop JBoss.
- 4 Create a backup folder outside of the JBoss installation path.
- 5 Move the following files from the `jboss/server/%context%/deploy` folder to the backup folder:
 - ♦ `dash.war`
 - ♦ `IDMProv.war`
 - ♦ `IDMPwdMgt.war` (if it applies)
 - ♦ `landing.war`
- 6 Move the `homepagelogging.xml` file from the `jboss/server/%context%/conf` folder to the backup folder.
- 7 Delete all files and folders from the following locations:
 - ♦ `jboss/server/%context%/tmp`
 - ♦ `jboss/server/%context%/work/jboss.web`
- 8 Delete the `permindex` folder from the `/tmp` folder.
- 9 Move the following files from the JBoss/deploy folder of the extracted files to the `jboss/server/%context%/deploy` folder:
 - ♦ `dash.war`
 - ♦ `IDMProv.war`
 - ♦ `IDMPwdMgt.war` (if it applies)
 - ♦ `landing.war`
- 10 Move the `homepagelogging.xml` file from the JBoss/conf folder of the extracted files to the `jboss/server/%context%/conf` folder.
- 11 (Conditional) On a Linux server, change the ownership of the `.war` and `homepagelogging.xml` files to the user `novlua` and the group `users`. For example:


```
chown novlua:users ./IDMProv.war
```
- 12 Start JBoss.
- 13 Ensure that users remove all cookies and cache from their browsers before accessing the deployed identity applications.

3.5.2 Updating the Identity Applications on a Tomcat Server

NetIQ provides Apache Tomcat as a convenience for Identity Manager users. By default, NetIQ installs Tomcat in the following locations:

- ♦ **Linux:** `/opt/netiq/idm/apps/tomcat`
- ♦ **Windows:** `C:\NetIQ\IdentityManager\apps\tomcat`

To update the identity applications on a Tomcat server:

- 1 Copy the `IDM45-Apps-SP-1.zip` file to the server where you deployed the identity applications on Tomcat.
- 2 Extract the contents of the `.zip` file for the identity applications to a temporary location on the server.
- 3 Stop Tomcat.
- 4 Create a backup folder outside of the Tomcat installation path.

- 5 Move the following files from the tomcat/webapps folder to the backup folder:
 - ♦ dash.war
 - ♦ IDMPProv.war
 - ♦ IDMPwdMgt.war (if it applies)
 - ♦ landing.war
- 6 Move the homepagelogging.xml file from the tomcat/conf folder to the backup folder.
- 7 Move the iac-datasource-factory-1.0.0.jar or iac-datasource-factory.jar file from the tomcat/lib folder to the backup folder.

If both files exist in the tomcat/lib folder, move them both.
- 8 Delete the following files and folders from the following locations:
 - ♦ dash folder from the tomcat/webapps folder
 - ♦ IDMPProv folder from the tomcat/webapps folder
 - ♦ IDMPwdMgt folder (if it applies) from the tomcat/webapps folder
 - ♦ landing folder from the tomcat/webapps folder
 - ♦ localhost folder from the tomcat/work/Catalina folder
 - ♦ all files and folders from the tomcat/temp folder, including the permindex file if it exists
- 9 Move the following files from the Tomcat/webapps folder of the extracted files to the tomcat/webapps folder:
 - ♦ dash.war
 - ♦ IDMPProv.war
 - ♦ IDMPwdMgt.war (if it applies)
 - ♦ landing.war
- 10 Move the homepagelogging.xml file from the Tomcat/conf folder of the extracted files to the tomcat/conf folder.
- 11 Move the iac-datasource-factory.jar file from the Tomcat/lib folder of the extracted files to the tomcat/lib folder.
- 12 (Conditional) On a Linux server, change the ownership of the following files to the user novlua and the group users:
 - ♦ .war
 - ♦ homepagelogging.xml
 - ♦ iac-datasource-factory.jar

For example:

```
chown novlua:users ./IDMPProv.war
```
- 13 (Optional) Delete or move all of the existing logs in the tomcat/logs folder.
- 14 Start Tomcat.
- 15 Ensure that users remove all cookies and cache from their browsers before accessing the deployed identity applications.

3.5.3 Updating the Identity Applications on a WebSphere Server

You can apply this service pack to the identity applications deployed to a WebSphere server.

- 1 Copy the IDM45-Apps-SP-1.zip file to the server where you deployed the identity applications on WebSphere.
- 2 Extract the contents of the .zip file for the identity applications to a temporary location on the server.
- 3 Create a backup folder outside of the WebSphere installation path.
- 4 Move the following files from the identity applications folder to the backup folder:

- ♦ dash.war
- ♦ IDMPProv.war
- ♦ IDMPwdMgt.war (if it applies)
- ♦ landing.war
- ♦ log4j.xml
- ♦ homepagelogging.xml

By default, the identity applications are installed in the following locations:

- ♦ **Linux:** /opt/netiq/idm/apps/UserApplication
- ♦ **Windows:** C:\NetIQ\IdentityManager\apps\UserApplication

- 5 Move the following files from the WebSphere folder of the extracted files to the identity applications folder:

- ♦ dash.war
- ♦ IDMPProv.war
- ♦ IDMPwdMgt.war (if it applies)
- ♦ landing.war
- ♦ log4j.xml
- ♦ homepagelogging.xml

- 6 To add the log4j.configuration JVM system property, complete the following steps:

6a For **Name**, specify log4j.configuration.

6b For **Value**, specify the full path including the filename to the log4j.xml file that you updated in [Step 5 on page 14](#). For example:

file:///opt/netiq/idm/apps/UserApplication/log4j.xml

6c For **Description**, specify a description for the property. For example:

log4j configuration file

For more information about adding a JVM system property, see [“Adding User Application Configuration Files and JVM System Properties”](#) in the *NetIQ Identity Manager Setup Guide*.

- 7 Remove the IDMselector.jar from the shared library that you created when you installed the identity applications.

For more information, see [“Creating and Applying a Shared Library”](#) in the *NetIQ Identity Manager Setup Guide*.

- 8 Stop and then uninstall the following files:

- ♦ dash.war
- ♦ IDMPProv.war

- ♦ IDMPwdMgt.war (if it applies)
 - ♦ landing.war
- 9 Install, but do not start, the following files:
 - ♦ dash.war
 - ♦ IDMPProv.war
 - ♦ IDMPwdMgt.war (if it applies)
 - ♦ landing.war
 - 10 Stop WebSphere.
 - 11 Restart WebSphere.
 - 12 Ensure that users remove all cookies and cache from their browsers before accessing the deployed identity applications.

3.5.4 Post-installation Steps for Updating the Identity Applications

This section provides the final steps for updating for the identity applications where you remove the `j2eevalidate.jar` from the Identity Vault. (Bug 907429)

- 1 Stop eDirectory.
- 2 Move the `j2eevalidate.jar` to a backup folder from its current location, by default:
 - ♦ **Linux:** `/opt/novell/eDirectory/lib/dirxml/classes`
 - ♦ **Windows:** `C:\Novell\IdentityManager\NDS\lib`
- 3 Start eDirectory.

3.6 Updating Identity Reporting

This service pack includes an update to Identity Reporting and a new Report Packaging Tool. The process for installing the updates depends on the web server that you use to support reporting.

- ♦ [Section 3.6.1, “Updating the Report Packaging Tool,” on page 15](#)
- ♦ [Section 3.6.2, “Updating Identity Reporting on a JBoss Server,” on page 16](#)
- ♦ [Section 3.6.3, “Updating Identity Reporting on a Tomcat Server,” on page 16](#)
- ♦ [Section 3.6.4, “Updating Identity Reporting on a WebSphere Server,” on page 18](#)

NOTE: Identity Reporting requires the latest versions of NetIQ One SSO Provider and NetIQ Self Service Password Reset. For more information, see [Section 3.4, “Updating One SSO Provider and Self Service Password Reset,” on page 11](#).

3.6.1 Updating the Report Packaging Tool

This service pack includes an update to the Report Packaging Tool.

- 1 Copy the `IDM45-Reporting-SP-1.zip` file to the server where you installed Identity Reporting.
- 2 Extract the contents of the `.zip` file for Identity Reporting to a temporary location on the server.
- 3 Create a backup folder.
- 4 Move the existing `reportpkg.jar` file from the original installation to the backup folder.
- 5 Copy the `reportpkg.jar` file from root folder of the extracted files to your installation for Identity Reporting.

3.6.2 Updating Identity Reporting on a JBoss Server

- 1 (Conditional) If you use the identity applications, apply the service pack to the identity applications.
For more information, see [Section 3.5, “Updating the Identity Applications,” on page 11](#).
- 2 Copy the IDM45-Reporting-SP-1.zip file to the server where you deployed Identity Reporting on JBoss.
- 3 Extract the contents of the .zip file for Identity Reporting to a temporary location on the server.
- 4 Stop JBoss.
- 5 Create a backup folder outside of the JBoss installation path.
- 6 Move the following files from the `jboss/server/%context%/deploy` folder to the backup folder:
 - ♦ `IDMRPT.war`
 - ♦ `IDMRPT-CORE.war`
 - ♦ `easrestapi.war`
- 7 Move the `homepagelogging.xml` file from the `jboss/server/%context%/conf` folder to the backup folder.
- 8 Delete all files and folders from the following locations:
 - ♦ `jboss/server/%context%/tmp`
 - ♦ `jboss/server/%context%/work/jboss.web`
- 9 Move the following files from the `JBoss/deploy` folder of the extracted files to the `jboss/server/%context%/deploy` folder:
 - ♦ `IDMRPT.war`
 - ♦ `IDMRPT-CORE.war`
 - ♦ `easrestapi.war`
- 10 (Conditional) On a Linux server, change the ownership of the .war files to the user `novlua` and the group users. For example:

```
chown novlua:users ./IDMRPT.war
```
- 11 Start JBoss.
- 12 Ensure that users remove all cookies and cache from their browsers before accessing the deployed Identity Reporting.

3.6.3 Updating Identity Reporting on a Tomcat Server

NetIQ provides Apache Tomcat as a convenience for Identity Manager users. By default, NetIQ installs Tomcat in the following locations:

- ♦ **Linux:** `/opt/netiq/idm/apps/tomcat`
- ♦ **Windows:** `C:\NetIQ\IdentityManager\apps\tomcat`

To update Identity Reporting on a Tomcat server:

- 1 (Conditional) If you use the identity applications, apply the service pack to the identity applications.
For more information, see [Section 3.5, “Updating the Identity Applications,” on page 11](#).
- 2 Copy the IDM45-Reporting-SP-1.zip file to the server where you deployed the Identity Reporting on Tomcat.

- 3 Extract the contents of the .zip file for the Identity Reporting to a temporary location on the server.
- 4 Stop Tomcat.
- 5 Create a backup folder outside of the Tomcat installation path.
- 6 Move the following files from the tomcat/webapps folder to the backup folder:
 - ♦ IDMRPT.war
 - ♦ IDMRPT-CORE.war
 - ♦ easrestapi.war
- 7 Delete the following files and folders from the following locations:
 - ♦ IDMRPT folder from the tomcat/webapps folder
 - ♦ IDMRPT-CORE folder from the tomcat/webapps folder
 - ♦ easrestapi folder from the tomcat/webapps folder
 - ♦ localhost folder from the tomcat/work/Catalina folder
 - ♦ all files and folders, **except** the permindex folder if it exists, from the tomcat/temp folder
- 8 Move the following files from the Tomcat/webapps folder of the extracted files to the tomcat/webapps folder:
 - ♦ IDMRPT.war
 - ♦ IDMRPT-CORE.war
 - ♦ easrestapi.war
- 9 (Conditional) On a Linux server, change the ownership of the .war files to the user novlua and the group users:
For example:

```
chown novlua:users ./IDMRPT.war
```
- 10 (Conditional) If you use Identity Reporting without the identity applications, complete the following steps:
 - 10a Move the iac-datasource-factory-1.0.0.jar or iac-datasource-factory.jar file from the tomcat/lib folder to the backup folder.
If both files exist in the tomcat/lib folder, move them both.
 - 10b Move the iac-datasource-factory.jar file from the Tomcat/lib folder of the extracted files to the tomcat/lib folder.
 - 10c (Conditional) On a Linux server, change the ownership of the iac-datasource-factory.jar files to the user novlua and the group users. For example:

```
chown novlua:users ./iac-datasource-factory.jar
```
- 11 (Optional) Delete or move all of the existing logs in the tomcat/logs folder.
- 12 Start Tomcat.
- 13 Ensure that users remove all cookies and cache from their browsers before accessing the deployed Identity Reporting.

3.6.4 Updating Identity Reporting on a WebSphere Server

You can apply this service pack to Identity Reporting deployed to a WebSphere server.

- 1 (Conditional) If you use the identity applications, apply the service pack to the identity applications.

For more information, see [Section 3.5, “Updating the Identity Applications,” on page 11](#).

- 2 Copy the IDM45-Reporting-SP-1.zip file to the server where you deploy Identity Reporting on WebSphere.
- 3 Extract the contents of the .zip file for Identity Reporting to a temporary location on the server.
- 4 Create a backup folder outside of the WebSphere installation path.
- 5 Move the following files from the IdentityReporting folder to the backup folder:
 - ♦ IDMRPT.war
 - ♦ IDMRPT-CORE.war
 - ♦ easrestapi.war

By default, the Identity Manager installation process installs Identity Reporting in the following locations:

- ♦ **Linux:** /opt/netiq/idm/apps/IdentityReporting
 - ♦ **Windows:** C:\NetIQ\IdentityManager\apps\IdentityReporting
- 6 Move the log4j.xml file from the IdentityReporting/conf folder to the backup folder.
 - 7 Move the following files from the WebSphere folder of the extracted files to the IdentityReporting folder:
 - ♦ IDMRPT.war
 - ♦ IDMRPT-CORE.war
 - ♦ easrestapi.war
 - 8 Move the log4j.xml file from the WebSphere folder of the extracted files to the IdentityReporting/conf folder.

- 9 (Conditional) If you use Identity Reporting without the identity applications, complete the following steps:

- 9a Add log4j.configuration to the JVM system properties, using the following information:

- ♦ For **Name**, specify log4j.configuration.
- ♦ For **Value**, specify the full path including the filename to the log4j.xml file that you updated in [Step 7 on page 18](#). For example:

file:///opt/netiq/idm/apps/IdentityReporting/log4j.xml

- ♦ For **Description**, specify a description for the property. For example:

log4j configuration file

For more information about adding a JVM system property, see [“Adding User Application Configuration Files and JVM System Properties”](#) in the *NetIQ Identity Manager Setup Guide*.

- 9b Remove the IDMselector.jar from the shared library that you created when you installed Identity Reporting.

For more information, see [“Creating and Applying a Shared Library”](#) in the *NetIQ Identity Manager Setup Guide*.

10 Stop and then uninstall the following files:

- ♦ IDMRPT.war
- ♦ IDMRPT-CORE.war
- ♦ easrestapi.war

11 Install, but do not start, the following files:

- ♦ IDMRPT.war
- ♦ IDMRPT-CORE.war
- ♦ easrestapi.war

12 Stop WebSphere.

13 Restart WebSphere.

14 Ensure that users remove all cookies and cache from their browsers before accessing the deployed Identity Reporting.

4 Known Issues

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

For the list of the known issues in Identity Manager 4.5 and Identity Manager Standard Edition 4.5, see the Release Notes for each version on the [Identity Manager Documentation page](#).

5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (<mailto:Documentation-Feedback@netiq.com>). We value your input and look forward to hearing from you.

For detailed contact information, see the [Support Contact Information website](http://www.netiq.com/support/process.asp#phone) (<http://www.netiq.com/support/process.asp#phone>).

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

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

6 Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR

PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2015 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see <http://www.netiq.com/company/legal/> (<http://www.netiq.com/company/legal/>).