NetIQ Identity Manager 4.5 Release Notes

April 2015

NetIQ Identity Manager 4.5 includes all features added to releases after Identity Manager 4.0.2. This release includes many other 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, our community Web site that also includes product notifications, blogs, and product user groups.

You can upgrade to Identity Manager 4.5 from Identity Manager 4.0.2 Advanced Edition, or perform a new installation. Identity Manager 4.5 includes all fixes and features addressed in Identity Manager 4.0.2 and later patches. For information about what's new in previous releases, see the "Previous Releases" section in the Identity Manager Documentation Web site.

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.

To download this product, see the Identity Manager Product Web site.

1 What's New and Changed?

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

1.1 New Features

- Section 1.1.4, “Permission Collection and Reconciliation Service (PCRS),” on page 3
- Section 1.1.5, “Self Service Password Reset as the Default Forgot Password Manager,” on page 3
- Section 1.1.6, “Providing Single Sign-on Access with One SSO Provider,” on page 3
- Section 1.1.7, “PostgreSQL and Apache Tomcat Support Identity Applications,” on page 3
- Section 1.1.8, “Identity Manager Engine Enhancements,” on page 3

For information about the new features in NetIQ Identity Manager Designer 4.5, see the *NetIQ Designer 4.5 Release Notes* (https://www.netiq.com/documentation/idm45/designer45_releasenotes/data/designer45_releasenotes.html). There are no new features for NetIQ Identity Manager Analyzer 4.5. For more information about NetIQ Identity Manager Analyzer, refer to the *NetIQ Analyzer 4.5 Release Notes* (https://www.netiq.com/documentation/idm45/analyzer45_releasenotes/data/analyzer45_releasenotes.html).

1.1.1 Centralized Access to the Identity Applications

Identity Manager 4.5 includes Identity Manager Home and the Identity Manager Provisioning Dashboard. Identity Manager Home provides a single access point for all Identity Manager users and administrators, including access to all existing Roles-Based Provisioning Module (RBPM) and User Application functionality. The Provisioning Dashboard provides user-specific content, such as password management and tasks. Users can log in with any supported Web browser on either a desktop computer or a tablet.

For more information, see the *NetIQ Identity Manager Home and Provisioning Dashboard User Guide* (https://www.netiq.com/documentation/idm45/idmhomepage/data/front.html).

1.1.2 Identity Approvals

The Identity Manager Approvals app allows managers and resource owners to approve or deny requests remotely, using an iPhone or iPad with the iOS operating system installed. Your users can see and work with the same approval tasks in the app that they would normally see in the User Application interface. All changes are synchronized between the Approvals app and the User Application.

For more information, see the *NetIQ User Application: User Guide* (https://www.netiq.com/documentation/idm45/ugpro/data/b13iylfy.html).

1.1.3 Catalog Administrator for Managing Roles and Resources

Identity Manager 4.5 includes a new Web-based tool called Catalog Administrator. Catalog Administrator simplifies the usage of entitlements from Identity Manager connected systems in the organization by associating them to Resources. You can manage Roles and Resources, associate Resources to Roles, and manage Separation of Duties conflicts between Roles. Catalog Administrator gets the Role and Resource information from the User Application driver.

For more information, see the *NetIQ Identity Manager Catalog Administration Guide* (https://www.netiq.com/documentation/idm45/catalog_administrator/).

NOTE: The Role Mapping Administrator (RMA) module is not supported in Identity Manager 4.5. Catalog Administrator replaces RMA.

1.1.4 Permission Collection and Reconciliation Service (PCRS)

PCRS enables entitlements for all Identity Manager drivers. It also makes it easy to on-board or reconcile the permissions from the connected systems in the Entitlement-Resource-Role format in the Identity Manager Catalog.

For more information, see the NetIQ Identity Manager Drivers Documentation Web site (https://www.netiq.com/documentation/idm45drivers/).

1.1.5 Self Service Password Reset as the Default Forgot Password Manager

Identity Manager 4.5 includes NetIQ Self Service Password Reset (SSPR) to help users reset their passwords without administrative intervention. In a new installation of Identity Manager 4.5, SSPR uses a proprietary protocol for managing authentication methods. When you upgrade Identity Manager to version 4.5, you can instruct SSPR to use the NetIQ Modular Authentication Services (NMAS) that Identity Manager has traditionally used for its legacy password management program.

For more information about SSPR, see the *NetIQ Identity Manager Setup Guide* (https://www.netiq.com/documentation/idm45/setup_guide/data/b1av7dg4.html).

1.1.6 Providing Single Sign-on Access with One SSO Provider

To provide single sign-on access to Identity Manager components, such as the User Application and Identity Manager Home, Identity Manager uses NetIQ One SSO Provider (OSP). When a user logs in, OSP verifies the user's credentials with the authentication server. OSP can work with more than one authentication source as long as the source uses OAuth protocol. For example, the Identity Vault, Kerberos, or SAML.

For more information about OSP, see the *NetIQ Identity Manager Setup Guide* (https://www.netiq.com/documentation/idm45/setup_guide/data/b1av7dg3.html).

1.1.7 PostgreSQL and Apache Tomcat Support Identity Applications

For your convenience, the Identity Manager 4.5 installation kit includes an installation program for the PostgreSQL database and the Apache Tomcat application server. Both of these programs provide the default framework for the identity applications, such as Catalog Administrator and Identity Reporting. Alternatively, you can use a different platform for your Identity Manager databases or application servers.

For more information about PostgreSQL and Tomcat, see the *NetIQ Identity Manager Setup Guide* (https://www.netiq.com/documentation/idm45/setup_guide/data/b1dfttbk.html).

1.1.8 Identity Manager Engine Enhancements

1.1.8.1 Out of Band Sync

Identity Manager 4.5 includes a new feature, Out of Band Sync. The Identity Manager drivers process events in the order they occur, which guarantees that all changes required for an event to successfully process are already applied. However, there are instances when you want a certain event to take precedence over others. For example, events that involve password changes, locking

an account, or disabling an account should take precedence over other events. Identity Manager Out of Band Sync feature allows you to assign a higher priority to these events, so that they are processed before other events in the queue.

For more information about this feature, see Enabling Out of Band Sync in the *NetIQ Identity Manager Driver Administration Guide*.

1.1.8.2 No Reference Association for Drivers

Identity Manager 4.5 includes a new feature called No Reference Association for Identity Manager drivers. You can use this feature along with the legacy association for an Identity Manager driver.

Identity Manager uses associations for identifying objects to which changes can be applied and maintains this information in an eDirectory attribute named DirXML-Associations. Using associations also results in a reference check when an object is updated, which can impact performance in large deployments. To improve performance in large deployments, a new feature, No-Reference Association, has been introduced in Identity Manager. For more information, see Managing Associations between Drivers and Objects in the NetIQ Identity Manager Driver Administration Guide

1.1.8.3 Relocating the Event Cache File

Every driver that is configured in Identity Manager has an associated event cache file. Events are cached in the TAO file before the driver processes them. By default, the TAO files are located in the `dib` directory.

Identity Manager 4.5 allows you to place the TAO files anywhere in the file system. Distributing the file I/O across multiple file systems improves the I/O throughput. Each driver can have an optional single-valued, server readable attribute `DirXML-CacheLocation`. The value of this attribute is an absolute path to the directory in the file system where the TAO files are created. When the engine is restarted, it looks for this attribute and the TAO files in the specified location.

For more information about relocating the event cache file, refer to Relocating the Event Cache File in the NetIQ Identity Manager Driver Administration Guide.

1.1.8.4 The Cache Flush Parameter

Identity Manager 4.5 provides an option to turn off the file system flush for each disk write. If you disable cache writes, they are not flushed immediately and instead, the underlying operating system will take care of the file system writes.

For more information about the cache flush parameter, see The Cache Flush Parameter in the NetIQ Identity Manager Driver Administration Guide.

1.2 What's Changed or Deprecated?

To streamline functionality, several items have changed or are no longer supported with Identity Manager 4.5. In many cases, alternative functionality replaces the items that are no longer supported.

1.2.1 Deprecated Functionality or Features

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

RIS.war File in the Identity applications

The REST Endpoints have been and, in this version, continue to be delivered in the `ris.war` file. However, the endpoints are transitioning to the main User Application WAR file. If you use the `ris.war` file version to create a client, you should expect to recreate that client with a future release of Identity Manager. `(Bug 874802)`

Password Self-Service and Forgot Password Features in the User Application

This release continues to support the Password Self-Service features in the User Application. However, that functionality is redundant, so it will be deprecated in the future. Use Self Service Password Reset (SSPR) instead. `(Bug 874800)`

For more information, see "Self Service Password Reset as the Default Forgot Password Manager" on page 3 and the *NetIQ Identity Manager Setup Guide*.

Portal Pages and Portlets in the User Application

This release does not support the portal functionality in the User Application. For more information about configuring the identity applications, see the *NetIQ Identity Manager Setup Guide*. `(Bugs 874794 and 874797)`

Guest and Single Sign-On Access for the User Application

This release no longer supports the guest access and guest shared pages for the identity applications. `(Bug 874789)`

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

For more information, see "Providing Single Sign-on Access with One SSO Provider" on page 3 and the *NetIQ Identity Manager Setup Guide*.

Starting Workflows with the Schema Mapping Editor

This release no longer supports the method for using the schema mapping policy editor. To start a workflow automatically when a user starts a provisioning request, use the `start workflow` policy action of Identity Manager. `(Bug 889793)`

Running Reports from the Roles and Resources Tab in the User Application

Starting with Identity Manager 4.0, you cannot use the reports provided under **Reports** on the **Roles and Resources** tab. However, the user interface does not label the reports as deprecated. `(Bug 628087)`

To generate reports, use the Identity Reporting Module. For more information, see the *NetIQ Identity Manager Setup Guide*.

Two drivers for Identity Manager

This release does not support the Avaya PBX and RSA SecurID drivers. For a list of supported drivers, see Section 3, "Identity Manager Component Versions," on page 8. `(Bug 911970)`

Telemetry Job

This release does not support the Telemetry job. Before upgrading Identity Manager, NetIQ recommends that you remove this predefined job. For more information, see the *NetIQ Identity Manager Setup Guide*. `(Bug 891224)`

JBoss Community Edition Application Server

Instead of using JBoss Community Edition, the installation kit for this release includes an program for installing the Apache Tomcat application server.

WebLogic

The identity applications and Identity Reporting cannot run on a Oracle WebLogic application server. Instead, use Apache Tomcat 7.0.55, IBM WebSphere 8.5.5.3, or JBoss Enterprise Application Platform 5.2.

MySQL and DB2

Components in this release cannot run on the Oracle MySQL or IBM DB2 database platforms. Instead, use Microsoft SQL Server 2014, Oracle 12c, or PostgreSQL 9.3.4.

Role Mapping Administrator

In this release, the Catalog Administrator component of the identity applications replaces most of the functionality previously provided by the Role Mapping Administrator. For more information, see "Catalog Administrator for Managing Roles and Resources" on page 2 and "Features Not Supported in Catalog Administrator" on page 7.

1.2.2 Name Change for RBPM and Related Components

In the installation program and Identity Manager documentation, this release combines the following components under the title of "identity applications":

- Catalog Administrator
- Home and Provisioning Dashboard
- Roles Based Provisioning Module (RBPM)
- User Application

1.2.3 Changes to Some Log Events

The changes to the log messages that Identity Manager generates for successful and failed login/logout attempts are as follows:

1.2.3.1 Event behavior before this release

Event	Behavior
0031550 Login Success	◆ Successful login to the User Application ◆ Successful SOAP call to the User Application
0031551 Login Failure	◆ Failed login attempt to the User Application ◆ Failed SOAP call to the User Application
0031700 Create Auth Token	◆ Successful login to Identity Reporting
0031701 Create Auth Token Failure	◆ Failed login attempt to Identity Reporting
0031702 Auth Token Revoked	◆ Successful logout of Identity Reporting

1.2.3.2 Event behavior with this release

In this release, Identity Manager sends some of the same events for the User Application. However, some events have been removed, such as for Identity Reporting. Instead, OSP generates a single event for both successful and failed attempts. XDAS taxonomy then interprets the OSP event either as a successful login/logout or SOAP call or as “other than success.”

Event	Behavior
0031550 Login Success	◆ Successful login to the User Application ◆ Successful SOAP call to the User Application
0031551 Login Failure	◆ Failed SOAP call to the User Application
003E0204	◆ OSP event for successful or failed login to the User Application and Identity Reporting ◆ OSP event for successful or failed SOAP call login to the User Application and Identity Reporting
003E0201	◆ OSP event for successful or failed logout from the User Application and Identity Reporting ◆ OSP event for successful or failed SOAP call logout of the User Application and Identity Reporting

Review your custom reports to ensure that they include the appropriate event codes. For more information about OSP, see the *NetIQ Identity Manager Setup Guide*.

1.2.4 Change to Compliance and Attestation Processes

For compliance and attestation processes, use NetIQ Access Review instead of the User Application. Access Review enables administrators and managers to easily collect all user and access information in one central location and certify that user have only the level of access that they need to do their jobs. Following the principle of least privilege, Access Review helps you ensure that your users have focused access to those applications and resources that they use and cannot access resources that they do not need to access. You can review all permissions assigned to your employees, either individually or as a group, and decide whether those permission assignments are appropriate.

For more information, see the NetIQ Access Review documentation.

1.2.5 Features Not Supported in Catalog Administrator

Catalog Administrator does not provide support for the following operations. To perform them, use the **Roles and Resource** tab in the User Application.

- Assigning and revoking roles or resources.
- Viewing the history of assignments of roles and resources.
- Creating, managing, or viewing resource request parameters.
- Assigning a parent role to a level 20 or level 10 role.
- Customizing text in the user interface.
- Changing languages for names and descriptions. The names and descriptions of roles, resources, and separation of duties definitions can only be created and viewed in the character set of the default language of the User Application.

- Managing Separation of Duties individually or as a group. To view a Separation of Duties definition, you must select one of the roles that uses the definition, then expand the Separation of Duties definition.
- Adding additional languages.
- Specifying a workflow to do extra work based on the grant or revoke setting for a resource.

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

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

2 System Requirements

You can install Identity Manager components on a variety of operating system platforms. For specific information about which component can be installed on which operating system, see Selecting an Operating System Platform for Identity Manager (https://www.netiq.com/documentation/idm45/setup_guide/data/b1bkyfvh.html) in the *NetIQ Identity Manager Setup Guide*. For information about prerequisites, computer requirements, installation, upgrade or migration, see Considerations and Prerequisites for Installation in the *NetIQ Identity Manager Setup Guide*.

3 Identity Manager Component Versions

Identity Manager 4.5 bundles the following components:

- NetIQ eDirectory 8.8.8 Patch 3
- NetIQ iManager 2.7.7 Patch 2
- NetIQ Identity Manager Designer 4.5
- NetIQ Identity Manager Analyzer 4.5
- NetIQ Identity Manager Engine 4.5
- NetIQ Identity Manager Remote Loader 4.5
- NetIQ Identity Manager RBPM/User Application 4.5
- NetIQ Identity Manager Catalog Administrator 4.5
- NetIQ Identity Manager Home and Provisioning Dashboard 4.5
- NetIQ Identity Manager Self Service Password Reset 3.2
- NetIQ Identity Manager Client Login Extension 3.8
- NetIQ Identity Manager Reporting Module 4.5
- NetIQ Identity Manager Identity Approvals (The installation package includes support for iOS.)
- For event auditing, one of the following:
  - NetIQ Event Auditing Service 6.1

    The installation package includes Event Auditing Service.
  - NetIQ Sentinel 7.0 and above

    This is available only for Identity Tracking. The Identity Manager installation package does not include Sentinel. You must install Sentinel separately.

- NetIQ Identity Manager drivers:
  - Active Directory Driver 4.0.0.4
  - Bidirectional eDirectory Driver 4.0.1.2
  - Blackboard Driver 4.0.2.0
  - Delimited Text Driver 4.0.0.3
  - Drivers for Linux and UNIX
    - Bidirectional 4.0.2.0
    - FanOut Driver 4.0.2.0
  - Drivers for Linux and UNIX Settings 4.0.2.0 (These drivers are available in a separate `.iso` file.)
  - Drivers for Mainframe (These drivers are available in a separate `.iso` file.)
    - ACF2 Driver 4.0.2.0
    - RACF Driver 4.0.2.0
    - Top Secret Driver 4.0.2.0
  - Drivers for Midrange (These drivers are available in a separate `.iso` file.)
    - i5os Driver 3.6.1.5
  - JDBC Driver 4.0.0.2
  - JMS Driver 4.0.0.2
  - eDirectory Driver 4.5.0.0
  - Entitlements Service Driver 4.0.0.0
  - Ellucian Banner Driver 4.0.2.2
  - GoogleApps Driver 4.0.2.2
  - GroupWise Driver 3.5.4
  - ID Provider Driver 4.0.0.0
  - Identity Tracking Driver for Sentinel 4.0.0.0
  - LDAP Driver 4.0.0.5
  - Lotus Notes Driver 4.0.0.2
  - Manual Task Service Driver 4.0.0.0
  - Null and Loopback Services 4.5.0.0
  - Oracle E-Business Suite HR Driver 4.0.0.2
  - Oracle E-Business Suite TCA Driver 4.0.0.2
  - Oracle E-Business Suite User Management Driver 4.0.0.2
  - Peoplesoft 5.2 Driver 5.2.3.7
  - Privileged User Management (PUM) Driver 4.0.2.1
  - Remedy Action Request System (ARS) Driver 4.0.2.0
  - SalesForce Driver 4.0.0.1
  - SAP HR Driver 4.0.0.1
  - SAP Portal Driver 4.0.0.0
  - SAP User Management Driver 4.0.0.2 (The User Management Fan-out driver uses the same shim.)
  - SharePoint Driver 4.0.0.0

- SOAP Driver 4.0.0.2
- WorkOrder Driver 4.0.0.0

4 Installing NetIQ Identity Manager 4.5

After you purchase Identity Manager 4.5, log in to the Identity Manager Product Web site and follow the link that allows you to download the software. The following `.iso` files contain the DVD image for installing the Identity Manager components:

- `Identity_Manager_4.5_Linux.iso`
- `Identity_Manager_4.5_Windows.iso`

Before installing Identity Manager 4.5, NetIQ recommends that you review the information in the following sections in the *NetIQ Identity Manager Setup Guide*:

- **Interaction among Identity Manager components**: "Introduction" (https://www.netiq.com/documentation/idm45/setup_guide/data/b16s52ia.html).

  This section describes the components that you might want to install for your identity management solution.
- **Planning your Identity Manager environment**: "Planning to Install Identity Manager" (https://www.netiq.com/documentation/idm45/setup_guide/data/b19fw3wm.html).

  This section provides a checklist and scenarios for installing Identity Manager. It also describes the prerequisites and system requirements for the computers where you want to install each Identity Manager component.
- **Deciding the type of installation for your environment**: "Understanding the Integrated and Standalone Installation Programs" (https://www.netiq.com/documentation/idm45/idm_integrated_install/data/front.html).

  The integrated installation program bundles Identity Manager components so you can avoid the need to separately install each component. This program bundles the latest versions of all necessary components for Identity Manager for your convenience. Use this process for a test environment or for evaluating Identity Manager.

5 Upgrading to Identity Manager 4.5

You can upgrade to Identity Manager 4.5 from Identity Manager 4.0.2 Advanced Edition. To upgrade or migrate your data to the latest version, use the individual installation programs for each component. You cannot perform an upgrade with the integrated installation program.

For the supported upgrade and migration paths, see "Understanding Upgrade and Migration" (https://www.netiq.com/documentation/idm45/setup_guide/data/b1abpvhy.html) in the *NetIQ Identity Manager Setup Guide*. To download the installation kits, see the NetIQ Downloads Web site.

After upgrading to this version, ensure that you perform the actions listed in the following sections:

- Section 5.1, "Delete Outdated Report Definitions," on page 10
- Section 5.2, "Delete Old .rpm Files," on page 11

5.1 Delete Outdated Report Definitions

This version replaces several report definitions in Identity Reporting. After you upgrade, delete the outdated report definitions from the **Repository** page.

Outdated definition	Replacement definition
Account IDs in the Managed System(s)	Account IDs in the Managed Systems
Account IDs in the Managed System(s) Current State	Account IDs in the Managed Systems Current State
Identity Vault Users with Access to Managed System(s)	Identity Vault Users with Access to Managed Systems
Identity Vault Users with Access to Managed System(s) Current State	Identity Vault Users with Access to Managed Systems Current State

5.2 Delete Old .rpm Files

The upgrade process leaves some `.rpm` files on the server where you upgrade the Identity Manager engine and Remote Loader. NetIQ Corporation recommends that you remove the unrequired files.

Linux:

- `novell-DXMLRSA-4.0.1-20120224`
- `novell-DXMLavpbx-3.5.4-20120601`
- `novell-DXMLnxdrv-4.0-0`
- `novell-DXMLnxpam-4.0-0`
- `novell-DXMLremedy-1.0.0.4-1`
- `novell-DXMLremedy71-1.0.0.3-1`
- `novell-DXMLsentl-3.6.1-20090721`

Windows (32-bit .NET Remote Loader):

- `dhutilj.dll`
- `dxevent.dll`
- `dxldap.dll`
- `jntls.dll`
- `novlactj.dll`

6 Known Issues

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

6.1 Installation Issues

6.1.1 Identity Manager Component Installation Issues

6.1.1.1 Cannot Specify Installation Paths on Windows that Include Spaces

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

6.1.1.2 Error Occurs when Installing Event Auditing Service on a Linux Server Set to Dutch

Issue: The Event Auditing Service standalone installation program reports errors on a Linux server with the locale set to Dutch. (Bug 896927)

Workaround: Change the following settings for locale:

- LANG=
- LC_ALL=

Do not include a value after the equal sign (=). This modification sets the type to POSIX instead of UTF-8 encoding.

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

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

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

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

Workaround: There is no workaround at this time.

6.1.1.4 A Copy of ConfigUpdate Utility is Created With a Standalone Installation of Self Service Password Reset

Issue: If you run the OSP Self Service Password Reset (SSPR) installation program and choose to install only SSPR, the installer places the ConfigUpdate utility and a few other files and folders in the OSP installation directory. For example, `/opt/netiq/idm/apps/osp`. (Bug 901293)

Workaround: Ignore the presence of the utility in the OSP installation directory because SSPR does not use it.

6.1.2 Identity Manager Integrated Installation Issues

- Section 6.1.2.8, “Configuring a Password Policy for Identity Applications on a Secondary Server Displays Error Messages,” on page 15
- Section 6.1.2.9, “Adding Rights to the User Container for Identity Applications on a Secondary Server Displays Error Messages,” on page 15

6.1.2.1 The Integrated Installation Program Fails to Install on Windows When You Use UNC Paths

Issue: You cannot use UNC paths for installation and configuration when you use the Identity Manager integrated installation program. For example, `\\myserver\share\Identity_Manager_4.5_Windows_Advanced`. `(Bug 627597)`

Workaround: Create an actual mapped drive.

6.1.2.2 No Server Health Check before Adding a Secondary Server On Windows

Issue: The integrated installation program does not perform a health check before the secondary server addition. `(Bug 677696)`

Workaround: Run the `ndscheck` command if you are adding a secondary server through integrated installer. Run the `ndscheck` command from the `<install location>\NDS` folder. Specify the mandatory parameters and run the following command:

```
ndscheck [-h <hostname port]>] [-a <admin FDN>] [[-w <password>]
```

NOTE: Running the `ndscheck` command on Windows displays the eMbox warnings. These warnings are not related to eDirectory health check failures. It is safe to ignore them.

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

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

Workaround: Complete the following steps:

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

   `cn=<Name of the SAML Object>`

   For example:

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

6.1.2.4 Integrated Installation Program Fails If the TMP or TEMP Directory Is Not Available On the C Drive

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

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

6.1.2.5 Cannot Restart Tomcat with Task Manager on Windows

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

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

- In the Services control panel, right-click **IDM Apps Tomcat Service** then click **Restart**.

- Use the command prompt to stop then start Tomcat:

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

  or

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

6.1.2.6 Integrated Installer Configuration Completion Page Does Not Close

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

Workaround: Terminate the installation program. (Bug 900241)

6.1.2.7 The Integrated Installer Conflicts with the iManager Default Port When the Computer Is Restarted Before Configuring Identity Manager

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

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

```
/etc/init.d/novell-tomcat7 stop
```

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

Proceed with the configuration using the integrated installer.

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

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

```
exitValue = 32
```

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

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

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

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

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

Issue: The following error messages are displayed:

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

  exitValue = 32
```

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

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

   ```
   LD_LIBRARY_PATH="/mnt/4.5/build/II/GMC1/147/install/utilities" "/mnt/4.5/
   build/
   II/GMC1/147/install/utilities/ldapmodify" -ZZ -h xxx.xx.xxx.16 -p 389 -D
   "cn=admin,ou=servers,o=system" -w ****** -a -c -f "/mnt/4.5/build/II/GMC1/147/
   install/utilities/sspr-edir-rights.ldif"
   LD_LIBRARY_PATH="/mnt/4.5/build/II/GMC1/147/install/utilities"  "/mnt/4.5/
   build/II/GMC1/147/install/utilities/ldapmodify" -ZZ -h xxx.xx.xxx.16 -p 389 -D
   "cn=admin,ou=servers,o=system" -w ****** -a -c -f "/mnt/4.5/build/II/GMC1/147/
   install/utilities/sspr-edir-rights.ldif"
   ```
3. (Optional) Verify whether you are able to add rights to the user container.

6.1.3 Incorrect Message Is Displayed During Uninstallation

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

Workaround: There is no workaround at this time.

6.1.4 End User License Agreement Is Not Available in All Supported Languages

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

- Danish
- Dutch
- Russian
- Swedish

Instead, the installation program displays the license agreement in English. For more information, see "Understanding Language Support" (https://www.netiq.com/documentation/idm45/setup_guide/data/bummf86.html) in the *Identity Manager Setup Guide*. `(Bug 896299)`

Workaround: There is no workaround at this time.

6.1.5 Installation Programs Provide Examples for Linux Instead of Windows

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

Workaround: There is no workaround at this time.

6.1.6 Navigation Panel Is Truncated in Identity Reporting Module Installer

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

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

6.1.7 Manually Adjust the Home Provisioning URL for Reporting on WebSphere

Issue: While installing the Identity Reporting Module on WebSphere, the installer does not ask where the Home Provisioning application is deployed. By default, the URL points to the Home Provisioning application page.(Bug 900184)

Workaround: If the URL points to a different location in your Identity Manager environment, ensure that you modify the `com.netiq.rpt.landing.url =` property with the correct value for your environment. This property is present in the `ism-configuration.properties` file in the `<Reporting-Install-Dir>/configuration` directory.

6.1.8 The Installer Does Not Create the master-key.txt File in the File System While Installing User Application on Tomcat and WebSphere

Issue: The Identity Applications installer prompts you to create a new master key or import it to the file system. If you create a new master key, the Identity Applications installer creates the `master-key.txt` file in the `<UserApp-install>` directory on JBoss. However, it fails to create the file on Tomcat and WebSphere. (Bug 900240)

Workaround: Use the master key value from `ism-configuration.properties` file if you are setting up a cluster and installing with Tomcat or WebSphere.

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

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

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

6.1.10 Restart the Operating System After Installing Identity Manager Using Integrated Installer on Linux

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

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

6.1.11 A Pop-up Window is Displayed During Framework Silent Installation

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

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

6.1.12 The Integrated Installer Might Set Up a Wrong Identity Manager Edition on Windows

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

Workaround: Run the following steps on your application server:

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

6.1.13 Installing Identity Manager with All Components Using the Integrated Installer in Silent Mode on Linux Fails to Create the Identity Applications

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

Workaround: There is no workaround at this time.

6.2 Remote Loader Issues

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

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

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

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

Issue: When a 32-bit Remote Loader 4.0.2 is upgraded to a 64-bit Remote Loader 4.5, the upgrade process does not clean the following 32-bit 4.0.2 packages:

- `novell-DXMLbase-4.0.0-20100929`
- `novell-DXMLedir-4.0.0-20100929`
- `novell-DXMLgw-3.5.3-20100405`
- `novell-DXMLrdxml-4.0.0-20100929`
- `novell-edirectory-expat-32bit-8.8.6-8`
- `novell-edirectory-xdaslog-32bit-8.8.6-8`
- `novell-NOVLjvml-4.0.0-20100929`

Workaround: There is no workaround at this time.

6.2.3 The Remote Loader Installation Creates Two Separate Directories And Includes Driver Files In Both of Them

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

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

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

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

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

6.3 Driver Issues

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

6.3.1 Cannot Configure the Role-Based Entitlements Driver on Identity Manager with eDirectory 8.8 SP8

Issue: You cannot create an entitlement policy in Identity Manager with eDirectory 8.8 SP8. (Bug 847632)

Workaround: Go to **LDAP Server > Connections > LDAP Interfaces** and change the existing values of the port to `ldap://IP:389` and `ldaps://IP:636`. Note that *IP* is appended to the existing port values.

6.3.2 InitiatorUserDomain is Set Incorrectly for Identity Manager Events

Issue: Identity tracking does not work properly if InitiatorUserDomain is not set correctly. (Bug 819675)

Workaround: To ensure that identity tracking works correctly, do the following:

- **For eDirectory drivers:** Ensure that the Sentinel driver is installed on both Identity Manager servers.
- **For Bidirectional eDirectory drivers:** Use `NOVLEDIR2ATR_2.2.0` or higher version for identity tracking.

6.3.3 TAO Files are Generated on the Cloned Server when Dibclone is Used

Issue: When the Dibclone utility is used on an Identity Manager server to clone another server, unnecessary TAO files are generated on the cloned server. (Bug 876418)

Workaround: Do not use the Dibclone utility on an Identity Manager server.

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

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

Workaround: There is no workaround at this time.

6.3.5 Links in Emails Might Not Work in Manual Task Driver

Issue: A conflict in the `javax.servlet.http.HttpServletRequest` class in the `j2eevalidate.jar` file affects links in emails for the Manual Task driver. (Bug 897240)

Workaround: Remove `j2eevalidate.jar` from the classpath if you do not require the User Application driver. Before removing it, ensure that the Manual Task driver and the User Application driver are not running on the same computer.

6.3.6 The Remote Loader Instance of the SharePoint Driver Might Fail to Start If the Default Width of Windows Command Prompt Window is Changed

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

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

6.4 Identity Reporting Module Issues

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

6.4.1 Removal of Extended Attributes Does Not Reflect in the Extended Attributes Table

Issue: If you remove an attribute that was added to the Data Collection Service driver filter policy, the attribute is not removed from the extended attributes table (`idmrpt_ext_attr`, which tracks the attributes) and no data is removed from the `idmrpt_ext_item_attr` table. (`Bug 633209`)

Workaround: There is no workaround.

6.4.2 Cannot Navigate to Today in the Calendar when the Display Option is Set to 1 Week

Issue: In Firefox, if the **Display Options** on the **Calendar** page are set to show 1 week, clicking **Today** displays a day one week ahead of today. This issue does not occur in Internet Explorer. (`Bug 635107`)

Workaround: To see today's schedule in the **Calendar** page, press the up-arrow to go back one week.

6.4.3 Installing Identity Reporting Might Overwrite the logevent.conf File

Issue: The Identity Reporting installation program overwrites `logevent.conf` without prompting under the following circumstances:

1. A `logevent.conf` file already exists in the `/etc/` directory.
2. EAS is installed on the same computer.
3. During the reporting installation, you replace the value of `localhost` and enter the computer's actual IP address for the EAS server.

(`Bug 642093`)

Workaround: After the installation is complete, manually update the `/etc/logevent.conf` file.

6.4.4 Reporting Module Installation Does Not Write the PostgreSQL JDBC JAR if EAS is Remotely Installed

Issue: If EAS is remotely installed and you want to test the connection to EAS during the Identity Reporting installation, the parent directory of your chosen installation directory must exist before you run the installation. Without an existing parent directory, the installation directory cannot be created in order to write the JDBC JAR file used for testing the connection. For example, if you are installing the Identity Reporting Module to `/opt/novell/IdentityReporting`, ensure that the `/opt/novell` directory exists before beginning the installation. (`Bug 642331`)

Workaround: Before running the installation, ensure that the parent directory of your chosen installation directory is present.

6.4.5 Reporting Module Does Not Convert a Valid Certificate when You Add an Application

Issue: When you add an application in the Reporting Module that runs on IBM WebSphere, you might notice that a valid certificate is not properly converted. The following sequence of events might cause this problem to occur:

1. Log in to the Identity Reporting Module with valid credentials.

2. On the Applications page, click **Add Application** and specify values for all mandatory fields.
3. To browse for the certificate, **SSL** and then click **Test**.

The certificate does not get converted. This issue occurs when you install Identity Reporting on an IBM WebSphere application server. (Bug 677645)

Workaround: Copy and paste the content of the certificate into the text area on the form.

6.4.6 Cannot Modify the Frequency of a Schedule

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

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

6.4.7 Downloading an RPZ File with Internet Explorer Might Change the File Extension to ZIP

Issue: When you access Identity Reporting in an Internet Explorer browser and download an `.rpz` file, the file extension might change from `.rpz` to `.zip`.

This issue does not occur with Firefox. (Bug 677436)

Workaround: There is no workaround needed because the file extension change does not cause any issues. The Reporting Module correctly handles the upload and import of the reports with the `.zip` file extension.

6.4.8 Internet Explorer Displays a Warning when Accessing Identity Reporting in HTTPS

Issue: If you use Internet Explorer in HTTPS to access Identity Reporting, the browser displays the following message:

```
Do you want to view only the webpage content that was delivered securely? This
webpage contains content that will not be delivered using a secure HTTPS
connection, which could compromise the security of the entire webpage.
```

If you select **Yes**, the browser does not display the login screen for Identity Reporting. This issue occurs because the download site for the new reports supports the HTTP protocol only. The link to that site is constructed if you use `http://`. This issue does not occur with Firefox. (Bug 685490)

Workaround: Select **No**.

6.4.9 Identity Reporting Leaves Entries in .xml Files for Tomcat after Uninstalling

Issue: When you uninstall Identity Reporting on Tomcat, the process leaves some entries in the Tomcat `server.xml` and `context.xml` files. You cannot reinstall Identity Reporting because the files contain duplicate entries for the connections pools. The entries might also expect different passwords than the ones that you specify in the second installation. (Bug 897505)

Workaround: After uninstalling Identity Reporting, manually remove the entries from the `server.xml` and `context.xml` files.

In the `server.xml` file, remove entries that resemble the following entries:

```
<Resource auth="Container" driverClassName="org.postgresql.Driver"
factory="com.netiq.iac.jdbc.pool.IacCustomDataSourceFactory" initialSize="10"
maxActive="50" maxIdle="10" maxWait="30000" minIdle="10"
name="shared/IDMRPTDataSource" password="" testOnBorrow="true"
type="javax.sql.DataSource" url="jdbc:postgresql://localhost:15432/SIEM"
username="idmrptsrv" validationInterval="120000" validationQuery="SELECT 1"/>

<Resource auth="Container" driverClassName="org.postgresql.Driver"
factory="com.netiq.iac.jdbc.pool.IacCustomDataSourceFactory" initialSize="10"
maxActive="50" maxIdle="10" maxWait="30000" minIdle="10"
name="shared/IDMRPTCfgDataSource" password="" testOnBorrow="true"
type="javax.sql.DataSource" url="jdbc:postgresql://localhost:15432/SIEM"
username="idmrptuser" validationInterval="120000" validationQuery="SELECT 1"/>
```

In the `context.xml` file, remove entries that resemble the following entries:

```
<ResourceLink global="shared/IDMRPTCfgDataSource"
name="jdbc/IDMRPTCfgDataSource" type="javax.sql.DataSource"/>

<ResourceLink global="shared/IDMRPTDataSource" name="jdbc/IDMRPTDataSource"
type="javax.sql.DataSource"/>
```

6.4.10 Console Mode Does Not Report a Successful Connection to the Database

Issue: When you install Identity Reporting, you can test the settings that you specify for the database. However, if you use the console mode for installation, the process does not report a successful connection. The process does report an error if the test connection fails. (Bug 899383)

Workaround: There is no workaround at this time.

6.4.11 Unable to Install Identity Applications in Console Mode on JBoss

Issue: The identity applications installation program does not allow you to specify values for all the parameters in the Java Install page. It displays the following message in the console:

```
For the JBoss Application server, you must use the Oracle Corporation jre
```

Workaround: Install identity applications silently or by using the GUI installation method. (Bug 917837)

6.4.12 Reporting Requires Additional Steps to Enable Auditing on Windows

Issue: If you installed Reporting and want to enable auditing, you need to run additional steps on your application server. (Bug 901336)

Workaround: This workaround uses Tomcat as an example. You can run these steps on other application servers where Reporting is deployed.

If Reporting is deployed without Identity Applications, perform the following actions:

1. Stop Tomcat.

   For example: **Go to Services > IDM Apps Tomcat Service > Stop**.

2. Stop the audit thread.

   2a Open Task Manager and find the Java process for jcache.

   2b Stop the jcache process.

3 Enable Reporting to utilize auditing.

3a (Optional) Update the ConfigUpdate utility to run in the GUI mode.

3b Launch the ConfigUpdate utility and select the **Reporting** tab.

3c Select the **Enable auditing to EAS** checkbox.

If it is already selected, de-select it and select it again.

3d Click **OK**.

4 Start Tomcat.

Go to **Services > IDM Apps Tomcat Service > Start**.

If Reporting is deployed with Identity Applications, perform the following actions:

1 Disable auditing in the Identity Applications.

1a Log in to the User Application as an administrator.

1b Go to **Administration > Application Configuration > Logging** and de-select the **Enable audit service** checkbox.

1b1 Select the **Persist the logging changes** checkbox.

1b2 Click **Submit**.

1c Log out from User Application.

2 Stop Tomcat.

For example: **Go to Services > IDM Apps Tomcat Service > Stop**.

3 Stop the audit thread.

3a Open Task Manager and find the Java process for jcache.

3b Stop the jcache process.

4 Enable Reporting to utilize auditing.

4a (Optional) Update the ConfigUpdate utility to run in GUI mode.

4b Launch the ConfigUpdate utility and select the **Reporting** tab.

4c Select the **Enable auditing to EAS** checkbox.

If it is already selected, de-select it and select it again.

4d Click **OK**.

5 Start Tomcat.

For example: **Go to Services > IDM Apps Tomcat Service > Start**.

6 Enable Auditing in the Identity Applications.

6a Log in to the User Application as an administrator.

6b Go to **Administration > Application Configuration > Logging** and select the **Enable audit service** checkbox.

6c Select the **Persist the logging changes** checkbox and click **Submit**.

6d Log out from User Application.

6.4.13 Reporting Requires Additional Steps to Enable Auditing on Linux

Issue: If you installed Reporting and want to enable auditing, you need to run additional steps on your application server. (`Bug 901325`)

Workaround: This workaround uses Tomcat as an example. You can run these steps on other application servers where Reporting is deployed.

1. Stop Tomcat.

   For example, `/etc/init.d/idmapps_tomcat_init stop`

2. Enable Reporting to utilize auditing.

   2a (Optional) Update the ConfigUpdate utility to run in GUI mode.

   2b Launch the ConfigUpdate utility and select the **Reporting** tab.

   2c Select the **Enable auditing to EAS** checkbox. If it is already selected, de-select it and then select it again.

   2d Click **OK**.

3. Start Tomcat.

   For example, `/etc/init.d/idmapps_tomcat_init start`

6.4.14 Setting Up Configupdate Utility When Identity Reporting Is Deployed Without Identity Applications

Issue: The standalone installation of Identity Reporting does not update the configuration file for the Configupdate utility on JBoss, Tomcat, or WebSphere application servers. (Bug 900846)

Woraround: To set up the Configupdate utility, perform the following additional steps for your application server where Identity Reporting is installed:

1. Navigate to the JBoss or Tomcat folder from your Reporting installation directory.

   For example, `/opt/netiq/idm/apps/IDMReporting/bin/linux/tomcat` or `/opt/netiq/idm/apps/IDMReporting/bin/linux/jboss`

2. From the Tomcat or JBoss folder, copy the Configupdate and Configupdate properties files and paste them in the `/IDMReporting/bin/lib` directory.

   For example, `/opt/netiq/idm/apps/IDMReporting/bin/lib`.

3. In a text editor, open the `configupdate.sh.properties` or `configupdate.bat.properties` file from the Tomcat or JBoss folder and change the below entries with the correct values for your application server where Identity Reporting is installed:

Existing Entries on Tomcat	New Entries on Tomcat	New Entries on WebSphere
`INSTALL_JAVA_BASE="$NOVL_JAVA_HOME$"`	`INSTALL_JAVA_BASE="/opt/netiq/idm/apps/jre"`	`INSTALL_JAVA_BASE="/opt/IBM/WebSphere/AppServer/java_1.7_64/jre"`
`CONTEXT_NAME="$NOVL_APPLICATION_NAME$"`	`CONTEXT_NAME="IDMRPT"`	`CONTEXT_NAME="IDMRPT"`
`CONTEXT_DIR="$NOVL_TOMCAT_BASE_FOLDER$"`	`CONTEXT_DIR="/opt/netiq/idm/apps/tomcat"`	`UA_DIR="/opt/netiq/idm/apps/IdentityReporting"`
`UA_DIR="$USER_INSTALL_DIR$"`	`UA_DIR="/opt/netiq/idm/apps/IdentityReporting"`	`USER_LANG="en"`
`USER_LANG="$NOVL_USER_LANGUAGE$"`	`USER_LANG="en"`	`USER_REGION=""`
`USER_REGION="$NOVL_USER_COUNTRY$"`	`USER_REGION=""`	`CONFIG_FILENAME="ism-configuration.properties"`
`CONFIG_FILENAME="$NOVL_UA_CONFIG_FILE_NAME$"`	`CONFIG_FILENAME="ism-configuration.properties"`	

Existing Entries on Tomcat	New Entries on Tomcat	New Entries on WebSphere
stop_deployer="false" use_ssl="true" use_console="$NOVL_CONFIGUPDATE_USE_CONSOLE_FLAG$" is_prov="true" read_pwd="true" #extFile extFile="$DOLLAR${UA_DIR}/IDMPwdMgt.war" edit_admin="$NOVL_UA_EDIT_ADMIN_FLAG$" debug="false" installDir="$USER_INSTALL_DIR$" provider_url="jnp://localhost:1099" file="$DOLLAR${CONTEXT_DIR}/webapps/$DOLLAR${CONTEXT_NAME}.war"	stop_deployer="false" use_ssl="true" use_console="false" is_prov="true" read_pwd="true" edit_admin="true" debug="true" installDir="/opt/netiq/idm/apps/IdentityReporting" provider_url="jnp://localhost:1099" file="${CONTEXT_DIR}/webapps/${CONTEXT_NAME}.war"	stop_deployer="false" use_ssl="true" use_console="false" is_prov="true" read_pwd="true" edit_admin="true" debug="false" installDir="/opt/netiq/idm/apps/IdentityReporting" provider_url="jnp://localhost:1099" file="${UA_DIR}/${CONTEXT_NAME}.war"

Existing Entries on JBoss	New Entries on JBoss	New Entries on WebSphere
INSTALL_JAVA_BASE=$NOVL_JAVA_HOME$ CONTEXT_NAME=$NOVL_APPLICATION_NAME$ CONTEXT_DIR=$NOVL_JBOSS_BASE_FOLDER$/server/$DOLLAR${CONTEXT_NAME} CONTAINER_CLIENT_DIR=client CONTAINER_CLIENT_JAR=jbossall-client.jar UA_DIR=$USER_INSTALL_DIR$ USER_LANG=$NOVL_USER_LANGUAGE$ USER_REGION=$NOVL_USER_COUNTRY$ CONFIG_FILENAME=$NOVL_UA_CONFIG_FILE_NAME$	INSTALL_JAVA_BASE=/opt/netiq/idm/jre CONTEXT_NAME="IDMRPT" CONTEXT_DIR="/opt/redhat/jboss-eap/jboss-as/server/Reporting" CONTAINER_CLIENT_DIR=client CONTAINER_CLIENT_JAR=jbossall-client.jar UA_DIR="/opt/netiq/idm/apps/IdentityReporting" USER_LANG="en" USER_REGION="" CONFIG_FILENAME="ism-configuration.properties"	INSTALL_JAVA_BASE="/opt/IBM/WebSphere/AppServer/java_1.7_64/jre" CONTEXT_NAME="IDMRPT" UA_DIR="/opt/netiq/idm/apps/IdentityReporting" USER_LANG="en" USER_REGION="" CONFIG_FILENAME="ism-configuration.properties"

Existing Entries on JBoss	New Entries on JBoss	New Entries on WebSphere
stop_deployer=false use_ssl=true use_console=$NOVL_CONFIGUPDATE_USE_CONSOLE_FLAG$ is_prov=true read_pwd=true extFile=$DOLLAR${UA_DIR}/IDMPwdMgt.war edit_admin=$NOVL_UA_EDIT_ADMIN_FLAG$ debug=false installDir=$USER_INSTALL_DIR$ provider_url=jnp://localhost:1099 file=$DOLLAR${CONTEXT_DIR}/deploy/$DOLLAR${CONTEXT_NAME}.war	stop_deployer=false use_ssl=true use_console="false" is_prov=true read_pwd=true #extFile=$DOLLAR${UA_DIR}/IDMPwdMgt.war edit_admin="true" debug="true" installDir="/opt/netiq/idm/apps/IdentityReporting" provider_url=jnp://localhost:1099 file="${CONTEXT_DIR}/deploy/${CONTEXT_NAME}.war"	stop_deployer="false" use_ssl="true" use_console="false" is_prov="true" read_pwd="true" edit_admin="true" debug="false" installDir="/opt/netiq/idm/apps/IdentityReporting" provider_url="jnp://localhost:1099" file="${UA_DIR}/${CONTEXT_NAME}.war"

4. Save and close the file.
5. Navigate to the Reporting installation folder and launch the Configupdate utility.

   You will now be able to launch the Configupdate utility. Be informed that values for some of the parameters are not populated. You need to specify values for them.
6. (Conditional) Take a back-up of the `configuration.properties` file on Tomcat and JBoss application servers.

   Navigate to the `JBossHome/server/${CONTEXT_DIR}/conf` directory and copy the `ism-configuration.properties` file to a different location on your filesystem.

   For example, copy the `ism-configuration.properties` file to the `/home/lab/restore` folder on your filesystem.

6.4.15 The Identity Reporting Installation Program Changes the Permission of the start-jboss.sh Script

Issue: If you install Identity Reporting after installing identity applications on JBoss, the installation process makes the `start-jboss.sh` script inexecutable. Attempts to start JBoss by using the `jboss_init` script logs a permission denied message is logged in the `jboss.log` file. `(Bug 919055)`

This issue does not occur when you install Identity Reporting separately on JBoss where identity applications are not already installed.

Workaround: Manually change the permissions of the `start-jboss.sh` file to enable this script to work.

6.4.16 The Identity Reporting Installation Program Does Not Create the jboss_init Script when It Is Separately Installed on JBoss

Issue: If you install Identity Reporting on a separate JBoss application server where identity applications are not already installed, JBoss does not automatically start with the system boot. This issue occurs because the Identity Reporting installation program fails to create the `jboss_init` script and the required mapping for JBoss to start automatically. `(Bug 919052)`

Workaround: Manually create the `jboss_init` script. For more information, see Preparing Your Application Server for the Identity Applications in the *NetIQ Identity Manager Setup Guide*.

6.4.17 The SystemErr.log File log4j Displays Warning Messages When Reporting Is Deployed on WebSphere

Issue: The following messages are displayed in the `SystemErr.log` file:

```
log4j:WARN No appenders could be found for logger
(com.sssw.fw.servlet.InitListener).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more
info.
```

Workaround: There is no functionality loss. It is safe to ignore the warning messages. `(Bug 900947)`

6.5 Roles Based Provisioning Module Issues

You might encounter the following issues when you use the Roles Based Provisioning Module:

6.5.1 Copying Text in the Detail Portlet Displays an Error Message

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

The following sequence of events cause this message to appear:

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

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

```
"Exception... "Access to XPConnect service
denied"  code: "1011" nsresult: "0x805303f3
(NS_ERROR_DOM_XPCONNECT_ACCESS_DENIED)"  location:
"http://172.16.1.99:8180/IDMProv/resource//portal-general/javascript/
html_editor.js
Line: 531" " when clicked on Copy button.
```

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

Workaround: There is no workaround at this time.

6.5.2 Newly Created User with Slashes in the Name Cannot Log In to the User Application on WebSphere

Issue: On WebSphere, if you create a new user with a slash (/) or backslash (\) in the name, the user cannot log in to the User Application. For example, if you create a user as /Test// from the **Create Users and Groups** page, an error is displayed when the new user tries to log in to the User Application. (Bug 636254, Bug 767345)

Workaround: There is no workaround at this time.

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

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

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

6.5.4 PostgreSQL Does Not Support Number Format of Simplified Chinese

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

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

6.5.5 Association Description is Required for the Default Language when Assigning Resources to Roles

Issue: When the User Application is accessed in a language other than the default language (for example, accessing in Spanish while the default language is set to English), if a resource is added to a role, ensure that a value is supplied for the default language in the **Association Description** field. If a value is not entered for the default language, you get an error and you cannot add the resource to the role. (Bug 687734)

Workaround: Click the **Localization** button after the **Association Description** field and enter a value in the language that is marked with the ***** (the default language).

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

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

Workaround: There is no workaround at this time.

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

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

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

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

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

Workaround: Ignore the error message. (Bug 896919)

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

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

Workaround: There is no workaround at this time.

6.5.10 Log File Reports Irrelevant Errors after a Successful Installation

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

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

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

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

6.5.11 The log4j.xml File is not Automatically Updated When Reporting is Installed on WebSphere

Issue: The `log4j.xml` file is not automatically updated when Reporting is installed on WebSphere. It displays the following error: (Bug 900590)

```
log4j:WARN No such property [datePattern] in org.apache.log4j.RollingFileAppender
```

Workaround: Manually update the `log4j.xml` file.

1. Go to *`Reporting-install-directory`*`/conf`. For example, `/opt/netiq/idm/apps/IdentityReporting/conf`.
2. Open the `log4j.xml` file in a text editor and find the following entry:

   ```
   <appender name="FILE" class="org.apache.log4j.RollingFileAppender">
   ```

   Change the class value `org.apache.log4j.RollingFileAppender` to `org.apache.log4j.DailyRollingFileAppender`, then save and close the file.
3. Restart WebSphere.

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

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

Workaround: There is no workaround at this time.

6.5.13 IDMProv.war File Path is Incorrect in the NetIQ-Custom-Install.log File for the liquibase Command for Tomcat and JBoss Installations

Issue: When User Application is installed on Tomcat or JBoss, the `IDMProv.war` file path for the `liquibase` command is not correctly set in the `NetIQ-Custom-Install.log` file. (Bug 900772)

Workaround: Manually change the `IDMProv.war` file path in the `NetIQ-Custom-Install.log` file.

6.5.14 The server.log File is Truncated on WebSphere

Issue: On 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. (Bug 900844)

Workaround: Ignore the issue because there is no loss of data as all the log data is available in the `SystemOut.log` file.

6.6 iManager Issues

You might encounter the following issues as you use iManager:

6.6.1 iManager Plug-in Dependency for the NDS-to-NDS Driver Certificates Wizard

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

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

6.6.2 Certificate Created During Identity Manager Installation is Invalid with Firefox 31

Issue: The certificate created during Identity Manager installation is invalid with Firefox 31. (Bug 896637)

Workaround: Change the Keytool self-signed certificate to an OpenSSL self-signed certificate in iManager.

1. Generate a private key for the host by running the following command:

   ```
   # openssl genrsa -out <HOSTNAME>-private.pem 2048
   ```

   Set HOSTNAME to the appropriate server name.
2. Use openSSL to derive the public key by running the following command:

   ```
   # openssl rsa -in HOSTNAME-private.pem -pubout > HOSTNAME-public.pem
   ```
3. Create a self-signed x509 certificate by running the following command:

   ```
   # openssl req -new -x509 -key HOSTNAME-private.pem -out HOSTNAME-
   certificate.pem -days 365
   ```
4. Convert the self-signed x509 certificate to the PKCS12 format by running the following command:

   ```
   # openssl pkcs12 -export -inkey HOSTNAME-private.pem -in HOSTNAME-
   certificate.pem -out HOSTNAME-certificate.p12 -name "iManager"
   ```

   4a Enter the export password, when prompted.

   4b Enter the export password again, when prompted for verifying.

   IMPORTANT: You must remember this password, because it is required later.
5. Copy the file to /var/opt/novell/novlwww by running the following command:

   ```
   # cp HOSTNAME-certificate.p12 /var/opt/novell/novlwww
   ```
6. Stop Tomcat by running the following command:

   ```
   # /etc/init.d/novell-tomcat5 stop
   ```

7 Edit the Tomcat configuration file, `server.xml`, from the `/etc/opt/novell/tomcat<5,6,7>` location.

Replace:

```
<!-- Define a SSL HTTP/1.1 Connector on port -->

   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

       maxThreads="150" maxHttpHeaderSize="8192" minSpareThreads="25"

       enableLookups="false" disableUploadTimeout="true"

       acceptCount="100" scheme="https" secure="true"

      clientAuth="false" sslProtocol="TLSv1.2"/>
```

with:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

    maxThreads="150" maxHttpHeaderSize="8192" minSpareThreads="25"

    enableLookups="false" disableUploadTimeout="true"

    acceptCount="100" scheme="https" secure="true"

    clientAuth="false"

    sslProtocol="TLS"

    keystoreFile="/var/opt/novell/novlwww/HOSTNAME-certificate.p12"

    keystorePass="<password from command in Step 4)>"

    keystoreType="PKCS12"/>
```

NOTE: You must specify the entire path when the keystore type is changed to PKCS12, because Tomcat no longer points to the default Tomcat home path.

---

8 Change the PKCS12 file ownership to `novlwww` and permissions to `user=rw`, `group=rx`, and `others=r` by running the following commands:

```
# chown novlwww:novlwww /var/opt/novell/novlwww/HOSTNAME-certificate.p12

# chmod 654 /var/opt/novell/novlwww/HOSTNAME-certificate.p12
```

9 Remove the existing keytool self-signed certificate by running the following command:

```
# mv /var/opt/novell/novlwww/.keystore /var/opt/novell/novlwww/orig.keystore
```

10 Restart Tomcat by running the following command:

```
# /etc/init.d/novell-tomcat<5,6,7> start
```

11 Open a Web browser and launch iManager.

6.6.3 iManager Does Not Send Audit Events to EAS

Issue: iManager does not send audit events to EAS even though a connection exists between EAS and iManager. This occurs in a standalone installation of iManager and the installation using integrated installer. (Bug 900283)

Workaround: Uncomment the following line from the /var/opt/novell/iManager/nps/WEB-INF/imanager_logging.xml file, and then restart Tomcat.

```
<appender-ref ref="NAUDIT_APPENDER"/>
```

6.7 Catalog Administrator Issues

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

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

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

6.7.2 Access Role and Resource Administration Requires Full Permissions

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

Workaround: There is no workaround at this time.

6.7.3 Cannot Change Revoke Process from Quorum to Serial

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

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

6.7.4 Dynamic Fields are not Displayed when a Resource is Mapped to a Role

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

Workaround: There is no workaround at this time.

6.7.5 Issues in iPad iOS 6 Safari Browser

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

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

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

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

6.7.5.2 The SoD Editor Fails to Load the SoD Form in the Right Panel

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

Workaround: There is no workaround at this time.

6.7.5.3 Map Resources Button does not Work

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

Workaround: There is no workaround at this time.

6.8 Home and Provisioning Dashboard Issues

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

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

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

6.8.2 Provisioning Dashboard Displays all Possible Values for Valued Entitlements

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

Workaround: There is no workaround at this time.

6.8.3 Workflows Report an Error when Using dateToString for Timestamp Control

Issue: Workflows that you created in the User Application and that use the form script method `dateToString` for a timestamp do not function appropriately in Identity Manager Home. The `dateToString` form script in the API includes seconds, while the new Date/Time control in Identity Manager Home does not. The new script uses a different format. To ensure that your forms function with Identity Manager Home, you must replace `dateToString` with the new script: `new Date ().toString ('M/d/yyyy h:mm tt')`.

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

```
document.getElementById('%Field-Name').value = new Date().toString('M/d/yyyy
h:mm tt');
```

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

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

```
document.getElementById('_startDate').value = new Date().toString('M/d/yyyy h:mm
tt');
```

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

```
var s = new Date().getTime();
  s = s + 3 * 1000 * 24 * 60 * 60;
  document.getElementById('_furDate').value = new Date(s).toString('M/d/yyyy
h:mm tt');
```

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

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

6.9 RHEL 6.5 Issues

- Section 6.9.1, “Identity Manager Installation Fails on RHEL 6.5,” on page 37

6.9.1 Identity Manager Installation Fails on RHEL 6.5

Issue: Identity Manager is not successfully installed on RHEL 6.5 because of the absence of some dependent libraries. (`Bug 693334`)

Workaround: Ensure that you install the dependant libraries before starting the Identity Manager installer on RHEL 6.5:

- **For GUI Install:** Manually install the dependent libraries.
  - **For a 64-bit RHEL:** Install the following libraries in the same order:
    1. `libXau-1.0.6-4.el6.i686.rpm`
    2. `libxcb-1.8.1-1.el6.i686.rpm`
    3. `libX11-1.5.0-4.el6.i686.rpm`
    4. `libXext-1.3.1-2.el6.i686.rpm`
    5. `libXi-1.6.1-3.el6.i686.rpm`
    6. `libXtst-1.2.1-2.el6.i686.rpm`
    7. `glibc-2.12-1.132.el6.i686.rpm`

8. `libstdc++-4.4.7-4.el6.i686.rpm`
9. `libgcc-4.4.7-4.el6.x86_64.rpm`
10. `compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm`
11. `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
12. `libXrender-0.9.7-2.el6.i686.rpm`

- **For a 32-bit RHEL:** Install the following library:
  - `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`

- **For Package Install on RHEL 6.x:** Manually set up a repository for the installation media.

1. (Conditional) If you are copying the ISO to the server, run the following command:

   ```
   #mount-o loop <path to iso>/mnt/rhes65
   ```

2. (Conditional) If you are copying to a CD or a DVD, and to the server, run the following command:

   ```
   #mount /dev/cdrom/mnt/rhes65
   ```

3. (Conditional) If you have mounted the ISO, create a repository file in the `/etc/yum.repos.d` location and perform the following configuration steps:

   ```
   #vi/etc/yum.repos.d/rhes.repo
     [redhat-enterprise]
     name=RedHat Enterprise  $releasever - $basearch
     baseurl=file:///mnt/rhes65/
     enabled=1
   ```

4. (Optional) If you are using an installation server, configure the following in `vi /etc/yum.repos.d/rhes.repo`:

   ```
   [redhat-enterprise]
   name=RedHat Enterprise  $releasever - $basearch
   baseurl=<url to the installation source>
    enabled=1
   ```

5. Run the following commands after setting up the repository:

   ```
   # yum clean all
   # yum repolist
   # yum makecache
   ```

6. To install the 32-bit packages, change “exactarch=1” to “exactarch=0” in the `/etc/yum.conf` file.
7. Install the GPG key by using the `rpm import <path / url> to RPM-GPG-KEY-redhat-release` command:

   ```
   # rpm --import /mnt/rhes65/RPM-GPG-KEY-redhat-release
   ```

   or

   ```
   # rpm --import http://<url>/RPM-GPG-KEY-redhat-release
   ```

8. (Optional) To install the required packages for Identity Manager 4.x, execute the following script:

```
#!/bin/bash

PKGS="libXau.i686 libxcb.i686 libX11.i686 libXext.i686  libXi.i686
libXtst.i686
glibc.i686 libstdc++.i686 libgcc.i686  compat-libstdc++-33.i686
compat-libstdc++-33.x86_64"
for PKG in $PKGS ; do
    yum -y install "$PKG"
done
```

NOTE: The script cannot locate the `compat-libstdc++-33.x86_64` library in the 32-bit repository unless you have modified the 64-bit repository and installed the RPM separately.

- **For Non-GUI Install:** Manually install the dependent libraries.
  - **For a 64-bit RHEL:** Install the following libraries in the same order:
    1. `glibc-2.12-1.7.el6.i686.rpm`
    2. `libstdc++-4.4.4-13.el6.i686.rpm`
    3. `libgcc-4.4.4-13.el6.i686.rpm`
    4. `compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm`
    5. `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
  - **For a 32-bit RHEL:** Install the following library:
    - `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`

NOTE: Ensure that the `unzip` rpm is installed before installing Identity Manager. This applies to all Linux platforms.

6.10 Identity Manager Upgrade Issues

6.10.1 Upgrading from Identity Manager 4.0.2 to 4.5 deletes CA certificates

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

Workaround: Complete the following steps:

1. Save the CA certificates in a custom location.
2. Upgrade Identity Manager 4.0.2 to 4.5.
3. Copy the certificates back to the JRE directory depending on your platform.

After the upgrade, verify the JRE version is 1.7.0_65.

6.11 Localization Issues

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

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

Workaround: Perform any one of the following actions:

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

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

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

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

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

1. Go to **Start > Run > Regedit > HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage** and change the value of **OEMCP** from *850* to *1252*.

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

6.11.3 Error Message Displays when Identity Manager is Installed on Russian Windows 2008 SP2

Issue: A Microsoft Visual C++ 2005 Redistributable error message displays when Identity Manager is installed on Russian Windows 2008 SP2. When you click **OK** in the error message, the installation completes successfully. (Bug 750992)

Workaround: To avoid this error, visit the Microsoft support site (http://support.microsoft.com/kb/952211) and run the steps specified in the Let me fix it myself (http://support.microsoft.com/kb/952211#LetMeFixItMyselfAlways) section of the online page.

6.12 Miscellaneous

6.12.1 Oracle 12c Database Creation Might take a Long Time

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

Workaround: There is no workaround at this time.

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

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

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

6.12.3 Manually Remove Old RPM Files After Upgrading to Identity Manager 4.5

Issue: When you upgrade to Identity Manager 4.5 from a previous version, the old RPM files for some drivers still exist. You must manually remove them. (Bug 888108)

Workaround: Manually remove the files listed in Table 1:

Table 1 Drivers and the RPM Files that Must be Removed

Drivers	Linux	Windows
RSA	◆ `novell-DXMLRSA-4.0.1-20120224`	◆ `ACEShim.jar`, `hsqldb.jar`, and `jace.jar` located in the `IDM_ENGINE_DIR\lib` and `IDM_REMOTELOADER_DIR\lib` folders ◆ `jace_api.dll` located in the `IDM_ENGINE_DIR\` and `IDM_REMOTELOADER_DIR\` folders
Remedy	◆ `novell-DXMLremedy-1.0.0.4-1` ◆ `novell-DXMLremedy71-1.0.0.3-1`	◆ `ARSDriver.jar` and `ARSDriver71.jar` located in the `IDM_REMOTELOADER_DIR\lib` folder ◆ `IDM_Notifier.xml` and `IDM_Notifier71.xml` located in the `IDM_REMOTELOADER_DIR\drivers\remedy\tools` folder
Avaya	◆ `novell-DXMLavpbx-3.5.4-20120601`	◆ `AvayaShim.jar` and `jta20.jar` located in `IDM_ENGINE_DIR\lib` ◆ `AvayaShim.jar` and `jta20.jar` located in `IDM_REMOTELOADER_DIR\lib`

6.12.4 The Identity Reporting Module Might Not Automatically Reconnect to the EAS Server

Issue: Sometimes the Identity Reporting Module does not automatically reconnect to the EAS server. `(Bug 900258)`

Workaround: Stop the application server where you deployed Identity Reporting and then start it again.

6.12.5 Internet Explorer 10 Displays an Error Message when Started Using Client Login Extension

Issue: A Stack Overflow message is displayed if you enter a wrong password on the SSPR Web page when you start SSPR (Self Service Password Reset) using Client Login Extension.

Workaround: Click **OK** and continue working. It is safe to ignore the message. `(Bug 833663)`

6.13 Uninstallation Issues

6.13.1 Identity Manager Framework Uninstallation Issues

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

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

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

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

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

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

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

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

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

- **For 32-bit computers:**

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

- **For 64-bit computers:**
  `\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Identity Manager`

6.13.2 Identity Manager Integrated Uninstallation Issues

6.13.2.1 The Identity Vault Uninstallation Hangs in Silent Mode on WIndows

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

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

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

6.13.2.2 The Integrated Uninstaller Does Not Completely Clean the Installation Folder on Windows

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

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

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

Workaround: Manually remove these folders.

7 Contact Information

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

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

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.

8 Legal Notice