Novell Identity Manager Roles Based Provisioning Module 3.7 Readme

Novell®

February 10, 2012

This document contains the known issues for the Identity Manager Roles Based Provisioning Module, Version 3.7. See Section 3, "Issues Fixed in 3.7," on page 19 for a list of the IDM Roles Based Provisioning Module 3.6.1 issues that were fixed in this release.

The documentation resources are refreshed regularly. Corrections and enhancements are made as needed. Please check the Roles Based Provisioning Module 3.7 Product Documentation Web site (http://www.novell.com/documentation/idmrbpm37/index.html) for updates. For Designer 3.5 Readme notes, see Designer 3.5 Readme (http://www.novell.com/documentation/designer35/readme/readme.html).

1 What's New in 3.7

The following features have been added in the 3.7 release:

- The *Work Dashboard* provides a single, consolidated user interface for all end-user functions within the Identity Manager User Application. The *Work Dashboard* provides a convenient way to manage tasks, resources, and roles. In addition, it allows you to review the status of requests, and change settings within the User Application. The *Work Dashboard* presents only the most relevant features of the application, allowing you to focus on your work.

- The new *resource model* enables you to:
  - Request resource assignments and manage the approval process for resource assignment requests
  - Check the status of your resource requests
  - A *resource* is any digital entity such as a user account, computer, or database that a business user needs to be able to access. The User Application provides a convenient way for end users to request the resources they need. In addition, it provides tools that administrators can use to define resources. Resources are mapped to entitlements.

- The new *security model* provides support for three general categories of administrators and managers:
  - The *Domain Administrator* is an administrator who has the full range of capabilities within a particular domain, which gives a user assigned to be this type of administrator the ability to perform all operations on all objects within the domain for all users.

- The *Domain Manager* is a delegated administrator who has the ability to perform selected operations for a subset of authorized objects within the domain for all users.
- The *Team Manager* is a business line manager who can perform selected operations for a subset of authorized objects within the domain, but only for a designated set of users (team members).

- *REST support* includes the following services:
  - Identities service
  - Password Management and SSO services
  - Roles service
  - Work Items service
  - Workflow Process and Definitions service

- *Single Sign-On (SSO) support* provides these features:
  - Easy way to integrate single sign on functionality into the User Application
  - Support for Kerberos and SAP

2 Known Issues in 3.7

The following sections describe known issues in Version 3.7 of the Roles Based Provisioning Module:

2.1 Theme Support

The following themes are supported in Version 3.7:

- BlueGloss
- Neptune (new theme introduced in this release)

Several of the themes introduced in earlier versions of the User Application have been deprecated in this release. The following themes have been deprecated:

- Manilla
- Linen
- Medico
- IDMStandard

These themes are no longer supported with the current release. You cannot select any of these themes on the *Theme Administration* page on the *Administration* tab.

The Manilla, Linen, Medico, and IDMStandard themes will most likely be removed in a future release. If you use any of these themes, you should migrate them to Version 3.7 of the User Application. If you use a custom theme that is based on one of the deprecated themes, you need to follow these steps to migrate the theme:

1 Look inside the theme.css for your custom theme and copy any custom selectors (new or edited) from this theme into either the BlueGloss or Neptune theme.

2 Save a new custom theme, which now includes your customizations as well as selectors from the BlueGloss or Neptune theme.

2.2 Steps to Allow a User to Modify Their Own Information

This section provides the steps required to allow a typical user to perform self-modification procedures within the Detail Portlet on the Novell User Application 3.0.x.

To allow a user to perform self modification:

1 In iManager go to Configure -> iManager Server -> Configure iManager -> Misc Tab.

   1a Check the Checkbox next to 'Enable "[this]".

   1b Press Save.

2 In iManager go to View Objects and navigate to the container of interest (i.e.: support-idm.novell).

   2a Select the container where the users are (i.e.: users.support-idm.novell) and choose Modify Trustees.

      2a1 Press the Add Trustee button and select [This].

      2a2 Press OK.

   2b Select the 'Assigned Rights' link to the right of [This].

      2b1 Do not make any changes to [All Attribute Rights] or [Entity Rights]

      2b2 Add the attribute 'Object Class', select the Write and Self Assigned Rights, and then enable Inherit.

      2b3 Add the attribute(s) you are interested in (i.e. Title), select the Write and Self Assigned Rights, and then enable Inherit.

      2b4 Press Done.

      2b5 Press Apply.

      2b6 Press OK.

3 In the Designer for Novell Identity Manager, make sure that the attribute(s)that were added in Step II. B.3. above have 'Edit' enabled in the Directory Abstraction Layer in the Entity that is to be modified. If the attribute was not editable, please enable Edit and deploy.

4 Restart the JBoss Application Server.

5 Test the application.

2.3 NVDA Reader Reads Password on IE7

In Internet Explorer 7, if a user enters their password in the login screen, and presses the Backspace key while still in the Password field, the NVDA reader will read out the characters entered in the password, which reveals the password. This behavior does not occur on FireFox.

This is a known problem with the NVDA Reader software.

2.4 User Unable to Change Password on Firefox 2.0

On Firefox 2.0.0.2 and 2.0.0.11, the user is unable to change his own password by using Change Password link under password management.

This problem is reproducible by performing these steps on Firefox 2.0.0.2 and 2.0.0.11:

1 Login to the User Application with valid user credentials.

2 Click on Identity Self-Service.

3 Click on Change Password link under password Management.

4 Provide the details in the fields Old password, New password and Retype password and click on the Submit button.

After performing these steps, the user should see a message confirming the password change. Instead, no message is displayed and the password is not changed. The page remains the same. If the user then clicks on any other link in the User Application (such as Organization Chart) the user is redirected to the login page.

2.5 Clicking in the Browse field launches the browse functionality with FireFox 3

When running a FireFox 3 browser, if you access the SSO Configuration page on the Administration tab and click in the browse fields, the user interface will pop-up the browse functionality. This is a known issue in GWT. For more information, see https://bugzilla.mozilla.org/show_bug.cgi?id=258875 (https://bugzilla.mozilla.org/show_bug.cgi?id=258875).

2.6 Error Page Displayed When Saving Locale on FireFox 2

On FireFox 2.0.0.11, if you attempt to save a locale, you may see an error message instead of a confirmation message. After the error message has been displayed, if you click on any link, or tab within the User Application, the login page is displayed. If you are planning to use FireFox 2, you need to use the last version (2.0.0.20), since FireFox stopped supporting version 2 of their browser.

2.7 Novell GroupWise Portlets Have Been Removed

In version 3.7.0 of the Novell Identity Manager Roles Based Provisioning Module (RBPM), the proprietary Novell GroupWise Portlets have been completely removed. If you are upgrading from a previous version of the RBPM, the Novell GroupWise Portlets will be removed during the upgrade process.

There are open source JSR-168 Novell GroupWise Portlets available. To learn more about these portlets please go to http://developer.novell.com/wiki/index.php/Novell_Collaboration_Portlets (http://developer.novell.com/wiki/index.php/Novell_Collaboration_Portlets).

The Novell Collaboration Portlets have instructions on how to deploy them to the JBoss portal and to the Liferay portal.

The Novell Collaboration GroupWise Portlets will not run in the RBPM portal, at this time. We have logged Bug 476982 with the Developers responsible for these portlets to have this issue resolved. If you require the use of the GroupWise Portlets with RBPM portal, you will need to use both the RPBM portal and one of the two portals listed above until a blocking issue has been resolved. Alternatively, you might try using the RPBM version 3.7.0 and a previous version that still contains the proprietary Novell GroupWise Portlets.

2.8 External Forgot Password WAR File Name Must Be Manually Renamed in configupdate Batch File

When running configupdate standalone mode, if user checks "Use External Password WAR" checkbox, the external war name will be renamed to the name specified in Forgot Password Link field. For example, if the Forgot Password Link is entered as: `http://localhost:8080/NewExtWar/jsps/pwdmgt/ForgotPassword.jsp`, then the external forgot password war name will be renamed to `NewExtWar.war`.

After the above step is done, at the end of configupdate process, if the rename is successful, the following message is displayed:

```
Renaming external war file from
/data/novell/trunk/runtime/build-library/ExtPwdMgt.war to
/data/novell/trunk/runtime/build-library/NewExtWar.war is successful, please
update configupdate.sh or configupdate.bat parameter -extFile to reflect
renamed war name.
```

Renaming the WAR file name is a manual process. To complete this process, you need to edit configupdate.sh or configupdate.bat to modify the `-extFile` parameter to reflect new external forgot password war file name. To complete the example shown above, you would you need to change the parameter as follows:

```
-extFile /data/novell/trunk/runtime/build-library/NewExtWar.war in above case.
```

2.9 Error Displayed While Retrieving Roles List Report for Business Role on IE 7 with Adobe Reader 8.0

On Internet Explorer 7, if you attempt to generate a Roles List Report with Business level specified as the role level, the following error message appears if you're using Adobe Reader 8.0:

```
Internet Explorer cannot display the page
```

This is a known issue with Adobe Reader 8.0. To correct this problem, you need to update your reader.

2.10 Case-Sensitivity Setting Must Be Consistent in MySQL Databases When Migrating from 3.6 to 3.7

When migrating from RBPM 3.6 to 3.7, you need to ensure that the case sensitivity setting is consistent between the 3.6 database and the 3.7 database. In addition, you need to use ansi mode, and use the same characterset & collation values.

To set the case sensitivity, you need to make sure the value of lower_case_table_names is consistent between database versions while migrating. Here is an example showing how this value is set:

```
set-variable=lower_case_table_names=0
```

2.11 Caching Issue with Newly Removed Assignments

If you create a role or resource assignment, and then remove it, you will see a message indicating that the assignment has been removed, but the assignment is still listed. If you refresh the page, you will likely see that the assignment has been removed. This is caused by a caching issue.

2.12 SOAP Resource Service Link Missing on Administration Tab

The Administration tab in the User Application does not include a left navigation link to the new Resource service. This functionality is not available in this release. This feature may be added in a future release.

2.13 Some Text Fields in Role and Resource Assignments Have No Cursor on Firefox 2

On Firefox 2, some of the fields in the *Filter* dialog for Role and Resource Assignments do not show a cursor when you click on the fields. This is a known Firefox 2 bug.

2.14 Unprocessed Role Requests Never Reevaluated Upon Driver Restart

Role requests that have not been processed (that have a status of 0) are sometimes not reevaluated after the Role Service driver has been restarted. For example, suppose a Role Service driver (TestRoleDriver) points to a User Application A (misconfiguration). The User Application pointing at the driver B submits the request to assign a role to a user. Since no Role driver has been configured for User Application driver B, the request is never picked up. The TestRoleDriver is reconfigured to point at User App driver B and restarted. However, the status of existing role requests never changes from 0 and the requests are not processed.

2.15 Refresh of the Browser Drops You Out of Manage Mode

If you are in Manage mode and refresh the browser, you are taken out of Manage mode. This occurs because the state of Manage mode is stored in JavaScript.

This behavior can be seen in Internet Explorer and FireFox.

2.16 Need to set NDSD_TRY_NMASLOGIN_FIRST to true on eDirectory

If you perform a default eDirectory installation and apply a password policy (that has email password to user action) to an existing user, then login as this user and perform a forgot password procedure, you may see a message that says *Univeral Password is not set* after answering the challenge response questions.

To fix this issue, perform these two steps:

1. Add the following two lines to the pre_ndsd_start script located at in /etc/init.d:

    ```
    NDSD_TRY_NMASLOGIN_FIRST=true
    export NDSD_TRY_NMASLOGIN_FIRST
    ```

    This should be done on any server that may handle NMAS logins via LDAP.

2. Restart eDirectory to apply the change.

For more information, see "How to Make Your Password Case-Sensitive" (http://www.novell.com/documentation/edir88/edir88new/?page=/documentation/edir88/edir88new/data/brvwgsv.html).

2.17 Some Characters Are Not Supported in Role and SoD Names

When you create a role or separation of duties (SoD) constraint, you need to be sure not to include certain characters. The following characters are not supported in role and separation of duties (SoD) constraint names:

```
< > , ; \ " + # = / | & *
```

Spaces at the beginning or end of the name are automatically stripped out.

2.18 Attesters in Request Details Are Not Filtered Based on Attestation Results

In the Compliance Tab > View Attestation Request Status > Request Details, the Filter by Attestation Result does not always work when also changing the Status filter criteria. Some attester rows will still appear that do not match the filter criteria. As a workaround, choose Status and click Filter, then choose Attestation Result and click Filter again.

2.19 Novell Secure Login 6.1 and 7.0 are Incompatible with RBPM

Issues have been encountered using Novell Secure Login 6.1 and 7.0 with the Role Based Provisioning Module in the area of password management. These issues will be addressed in a future release of Novell Secure Login.

2.20 In Manage Mode, User Selected Role is not Selected through Look Ahead Feature

In the lookahead support for Roles or Resources, there may be a problem with selecting the last item in the lookahead list, if the list shows the last value as the one with the fewest letters and there is only one word. For example, suppose you type `Test`, and the following values appear in the list in the following order:

```
Test2
Test
```

If you select `Test`, when you click elsewhere, `Test2` will be selected. The end user can get around this by instead of typing `Test` search for `Test` by clicking the Finder icon. The Role Administrator can try adding temporary roles that start with `Test`, then deleting them, to make the issue go away.

If the list is sorted properly (as shown below), this problem will not occur:

```
Test
Test2
```

2.21 Filter by Attestation Result Does Not Work When Changing Status Filter Criteria

In *View Attestation Request>Request Details* screen on the *Compliance* Tab, the *Filter by Attestation Result* function does not always work when the user also changes the *Status* filter criteria. Some attester rows will still appear that do not match the filter criteria. As a workaround, choose *Status* and click *Filter*, then choose *Attestation Result* and click *Filter* again.

2.22 Timeout Filtering Does Not Work in Task Notifications for End User

The timeout filter is not working in the *Task Notifications* list on the *Work Dashboard* when an end user logs in. When a provisioning Team Manager logs in, and is not managing someone else, the timeout filter does not work either. When he is managing another user, the timeout filter works as expected. When a Provisioning Administrator or Provisioning Manager logs in, the time out filter also works as expected.

2.23 User Interface May Generate Unnecessary Error Messages on Firefox 3.0.5

While using Firefox 3.0.5 to browse the Work Dashboard and interact with other parts of the application, you may see an error message appear with the following text "Permission denied to get property Window.JUICE". The message is not indicative of a real error or an issue with the application. To correct this behavior, upgrade to the latest version of Firefox 3.0.

2.24 Double Clicking a Link May Open Multiple Instances of a Dialog

It is possible to open more than one dialog when double clicking links within the Roles, Resources, and SoD sections of the User Application. For example, if you select a role and double click the edit link, you may see two instances of the dialog appear. To workaround this issue, simply close the extra dialog.

2.25 A blank page is displayed when login name contains * or +

If the cn for a user includes a * or +, the User Application displays a blank page at login time. Do not use these characters in a login name.

2.26 Role and Resource Driver May Not Process Existing Requests on First Startup

Role requests that are created by the User Application before a Role and Resource Driver has been started for the first time will not be processed. These requests will have a status of *Running: New Request* in the User Application. If your User Application has requests in this state, they can be processed by performing a synchronize on the Role and Resource Driver. Be aware that the synchronization process may take some time depending on the size of the tree.

2.27 Enable Browser Caching for Best Client-Side Performance

RBPM 3.7 uses GWT (Google Web Toolkit), which stores application code in a file that is intended to be cached by the user's browser rather than be loaded for each user session. It is therefore recommended that you enable caching on the browser in order to obtain the best performance.

2.28 Object Selectors Don't Always Display in Password Sync Status Admin UI on IE 7 or 8

An administrator, using Internet Explorer 7 or 8, who attempts to add or update a *Password Sync Status Application* within the *Administration>Application Configuration >Password Sync Status* page of the User Application, should fill out the details for the *Application DirXML-PasswordSyncStatus GUID* or the *Dependent Driver* before editing the localized values for the application name, using the expanded language list. Once the language list has been expanded, the Object Selectors used in the detail settings will no longer display.

To correct the display problems associated with the Object Selectors, close the settings window by canceling the edit, or save the incomplete details, then reopen the settings and the Object Selectors should function correctly.

2.29 Some Fields Do Not Display Validation Messages

A validation message should appear for invalid values but does not in some cases for fields within the Resource Assignment window or Approval Quorum Percentage. This is the case, for example, after the user clicks Clear then Submit or enters the %, $, or - characters.

2.30 Browse Buttons Are Not Localized in SSO Admin UI

In the *Administration -> Single Sign On (SSO)* section of the User Application, the Browse buttons for *Signing Certificate* and *Signing Key* in the *SSO Controller Configuration* and *SSO Providers* area are not localized. These buttons always appear in English as *Browse...*

A fully localized version of the browser must be installed (meaning full version of Spanish Firefox or Internet Explorer must be installed). Simply changing the language in the browser from English to another language will not cause these HTML controls to translate. These HTML controls are controlled not by the UA, but rather by the browser. This is the default HTML control behavior.

2.31 Quick Clicking Causes Display Errors

When navigating quickly, the user may see occasional data loading errors in the User Application. This behavior is expected because the AJAX control cannot complete its server calls.

2.32 Report Administrator Not Yet Implemented

The Report Administrator system role introduced in this release has not been implemented yet. The role is available for assignment in the Role Catalog, however, attempts to assign this role generate a runtime exception. In the user interface, nothing appears to happen when the assignment is requested.

The Report Administrator role functionality will be implemented in a future release.

2.33 Team Managers Cannot Create Delegate Assignments with Assign By Relationship

It is not possible for a Team Manager to create team delegate assignments by using the assignment type of *Assign by relationship.*

Only Provisioning Managers who have been assigned explicit permissions to perform delegate assignments for a PRD can create a delegate assignment for that PRD using the assignment type of *Assign by relationship.*

2.34 PDF Plug-In Needed to Run Roles Reports

Running a Roles Report generates a PDF. If the browser does not have a PDF plugin installed, you are prompted to save a file, and you need to specify the filename. To avoid this situation, please ensure that you have the Adobe PDF plug-in installed before running the report.

2.35 Org Chart View Does Not Show Images in Print View

The Organization Chart does not show images in print view. If the Print icon is selected on the Organization Chart portlet, the printable view displays the chart appropriately but does not include the user images.

2.36 User Application Does Not Display Results When Default Number of Results is Zero

If the configuration administrator changes the value of *Default number of results displayed per page* to zero on the *Provisioning UI Display Settings* page under the *Administration* tab, the *Work Dashboard* page fails to display Task Notifications, Resource Assignments, Role Assignments, and Requests Status details. In addition, the Role Catalog, Resource Catalog and SOD Catalog pages on the Roles and Resources tab, as well as the Administrator Assignments page on the Administration tab, fail to display any results.

When the *Default number of results displayed per page* is set to zero, the pages listed above should be displayed with all the results, and the default number of results displayed per page should be zero. Instead, the pages do not display any results, and the browser hangs when you expand the Request Status section on the Work Dashboard.

2.37 User Application Throws SSO Compatibility Error During Startup

If you set the JAASManager Log level to TRACE on the *Administration>Caching* page and then restart the User Application, the following error message is displayed in the Stack Trace:

```
com.novell.common.auth.saml.ConfigureException: Failed to initialize SSO due
to
improper environment.
    at
com.novell.common.auth.saml.AuthTokenGenerator.<init>(AuthTokenGenerator.java
:82)
    at
com.novell.common.auth.saml.AuthTokenGeneratorFilter.init(AuthTokenGeneratorF
ilter.java:281)
```

The following steps outline the solution to this problem:

1 Remove conflicting opensaml jars from the Weblogic system folder:

```
./bea/modules/com.bea.core.bea.opensaml_1.0.0.0_5-0-2-0.jar
../bea/modules/com.bea.core.bea.opensaml2_1.0.0.0_5-0-2-0.jar
```

2 Endorse Apache JAXP implementation:

```
../bea/jrockit_160_05/jre/lib/endorsed

-rw-r--r-- 1 lab lab   84091 May 21 10:24 resolver-2.9.1.jar
-rw-r--r-- 1 lab lab  278286 May 21 10:24 serializer-2.9.1.jar
-rw-r--r-- 1 lab lab 3176148 May 21 10:24 xalan-2.7.1.jar
-rw-r--r-- 1 lab lab 1229289 May 21 10:24 xercesImpl-2.9.1.jar
-rw-r--r-- 1 lab lab  194354 May 21 10:24 xml-apis-2.9.1.jar
```

You can either download the jars listed above from Apache, or get them from the "endorsed" folder inside `http://shibboleth.internet2.edu/downloads/opensaml/java/2.2.0/opensaml-2.2.0-bin.zip`.

2.38 Screen Reader Support

NVDA v. 0.6p3 screen reader was used during accessibility testing.

2.39 EboClusterManager Error May Be Observed in Clusters

An EboClusterManager error may be observed in cluster environments. The error occurs because a cache notification is sent to servers in the cluster to remove a key, but the key does not exist in the remote cache.

2.40 NrfCaseUpdate Cannot Use an IP Address

The *Installation Guide* outlines steps for using an IP address to connect to the eDirectory server when running the NrfCaseUpdate utility. However, using IP address will not work. The NrCaseUpdate utility specifically asks for the DNS name of the eDirectory server:

```
Specify the DNS address of the Identity Vault (e.g acme.com)
```

The NrfCaseUpdate process will proceed if an IP address is provided and will report back that the update was successful. However, if you look at the schema.log (on Linux or Solaris) or the Modschema.log (on Windows), you will see that the schema actually was not updated. Also, if you look at the two attributes (nrfLocalizedNames and nrfLocalizedDescrs) with iManager or ConsoleOne, you will see that they are still marked *Case Exact String* instead of *Case Ignore String*.

If the schema had been updated, an entry similar to the following would appear:

```
Windows:

Begin schema update for: C:\Program Files\Novell\Identity
Manager\update-nrf-case.sch
(Note: Successfully resolved to server: .myserver-NDS.novell.myTREE)
Modifying schema attributes...
(Note: Successfully resolved to server: .myserver-NDS.novell.myTREE)
  : Different from existing definition, will attempt to modify
    Syntax: Modified OK
  : Different from existing definition, will attempt to modify
    Syntax: Modified OK
Schema update summary: 0 warnings and 0 errors

Linux:

Starting schema update for: update-nrf-case.sch...
Modified schema attribute nrfLocalizedNames.Modified schema attribute
nrfLocalizedDescrs.
```

Only the machine name (for example: myserver) or the fully qualified name (for example:
myserver.novell.com) can be used with the Nrf CaseUpdate utility.

2.41 NrfCaseUpdate issue with Windows 2003 Server SP1

In some instances on a Windows 2003 Server SP1, the schema for nrfLocalizedNames and
nrfLocalizedDescrs is not modified at the conclusion of running the NrfCaseUpate utility. The
utility reports that the process completed successfully. However, there is not an entry in the
Modschema.log outlining that the schema was modified. If the update had modified the schema, an
entry similar to the following would be in the Modschema.log:

```
Begin schema update for: C:\Program Files\Novell\Identity
Manager\update-nrf-case.sch
(Note: Successfully resolved to server: .myserver-NDS.novell.myTREE)
Modifying schema attributes...
(Note: Successfully resolved to server: .myserver-NDS.novell.myTREE)
  : Different from existing definition, will attempt to modify
    Syntax: Modified OK
  : Different from existing definition, will attempt to modify
    Syntax: Modified OK
Schema update summary: 0 warnings and 0 errors
```

Also, if you look at the two attributes (nrfLocalizedNames and nrfLocalizedDescrs) with iManager
or ConsoleOne, you will see that they are still marked *Case Exact String* instead of *Case Ignore
String*.

There are two work arounds for this issue:

 ◆ Upgrade to Windows 2003 Server SP2.
 ◆ If the NrfCaseUpdate process outlined above does not succeed, and the two attributes have not
   been modified, you need to import the schema change using the install.dim before proceeding
   with importing the ldif file (if that applies) or proceeding with the installation:

   1. Select *Start -> Control Panel -> Novell eDirectory Services -> install.dlm*.
   2. Select *Install additional schema files* and press *Next*.
   3. Provide the information to connect to your eDir server and press *OK*.
   4. Navigate and select the update-nrf-case.sch file an then press *Finish*.

2.42 Installation Fails to Create Database Schema in Console Mode for French Locale and MS SQL

The database tables will not be created when installing in console mode with French as the language and Microsoft SQL Server 2005. An error similar to following will be seen in the db.out file:

```
SEVERE: null
liquibase.exception.JDBCException: java.lang.ClassNotFoundException: null
    at
liquibase.commandline.CommandLineUtils.createDatabaseObject(CommandLineUtils.
java:97)
    at liquibase.commandline.Main.doMigration(Main.java:578)
    at liquibase.commandline.Main.main(Main.java:97)
Caused by: java.lang.ClassNotFoundException: null
```

There are two work arounds for this issue:

   ◆ Run the installer in Graphical mode instead of console mode.

   ◆ If console mode was used during the installation, the following steps must be performed:

      1. Create the database tables:

         a. Open the Novell-Custom-Install.log file, which is located in the at the "root" of the User Application install directory. For example: `/home/lab/IDM370/idm`

         b. Search for an entry similar to the following:

            ```
            **************************************************
            If a failure is encountered while creating the tables, verify that
            this string
            is correct
            If not , you can modify this string and copy/paste to a command
            line to run
            **************************************************
            ```

         c. Copy the command outlined and paste it into a terminal on the machine where the User Application is installed.

              i. Replace the null value for --databaseClass= with the correct value of:

                 `--databaseClass=com.novell.soa.persist.MSSQLUnicodeDatabase`

             ii. Replace the null value for --driver= with the correct value of:

                 `--driver=com.microsoft.sqlserver.jdbc.SQLServerDriver`

                 Replace the null value for --url= with the correct value. For example:

                 `--url=jdbc:sqlserver://`
                 `myserver.novell.com:1433;DatabaseName=mydatabase`

            iii. You will have to replace the the stars (*) that appear for the database username and password with the actual values.

         d. Press Enter. Depending on the option selected during the install, the tables or a sql file will created.

      2. Edit the JBoss JDBC connection pool file (if it applies):

         a. Open the %context%-ds.xml (For Example: IDM-ds.xml) located in the deploy directory. For example:

            `/home/lab/IDM370/idm/jboss/server/IDM/deploy`

         b. The connection URL will appear similar to the following:

```
                    <connection-url>myserver.novell.com:1433mydatabase</connection-
                    url>
```

c. Modify the connection-url to have the correct information. For example:

```
                    <connection-url>jdbc:sqlserver://
                    myserver.novell.com:1433;DatabaseName=mydatabase</connection-url>
```

d. Save and close the file.

2.43 Grace Login Counter Is Incorrect with Auth Headers for SSO

If Access Gateway is placed in front of the User Application and SSO is enabled, the available grace login amount might decrease by 2 for each login (instead of by 1 without Access Gateway). In the event that a password expires for a user, the user interface prompts the user to change the password. The user should follow the instructions presented and change the password accordingly.

2.44 Association Report Is Not Working for Team Managers

The Association report page works only for administrators and typical users. It does not work for team managers. If the administrator configures the Associate Report page security settings and opens it to public access, a typical user can log in and view his or her association report without a problem. However, when a team manager logs in, this user cannot use the lookup icon to search for a team member and view the team member's association report.

2.45 Greater Than and Less Than Symbols Are Not Supported in User CNs

The User Application does not support using the < and > symbols in a user's CN (or any other login attribute, such as workforceID) in this release. Using the < or > symbols will cause the password self-service feature to work incorrectly.

2.46 Server Start Fails if OpenXDAS is Enabled and xdasd is Not Started

If the User Application is configured for Audit logging using OpenXDAS, the application will not deploy properly if the xdasd process is not running.

The error message will appear in the server console and log as shown below:

```
2008-05-03 13:46:48,308 ERROR [com.sssw.fw.servlet.Boot:contextInitialized]
Un>com.novell.srvprv.spi.util.servlet.LogConfiguratorException: Error
Initialize >          at
com.novell.srvprv.spi.util.servlet.LogConfigurator.init(LogConfigur>        at
com.sssw.fw.servlet.InitListener.contextInitialized(InitListener.ja>        at
org.apache.catalina.core.StandardContext.listenerStart(StandardCont>        at
org.apache.catalina.core.StandardContext.start(StandardContext.java>        at
org.apache.catalina.core.ContainerBase.addChildInternal(ContainerBa>        at
org.apache.catalina.core.ContainerBase.addChild(ContainerBase.java:>        at
org.apache.catalina.core.StandardHost.addChild(StandardHost.java:55>        at
sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
```

```
        at java.lang.reflect.Method.invoke(Unknown Source)
        at org.apache.tomcat.util.modeler.BaseModelMBean.invoke(BaseModelMB
```

Then hundreds of:

```
2008-05-03 13:46:53,072 WARN  [com.novell.soa.af.impl.core.EngineImpl:run]
Fai>java.lang.NullPointerException
        at
com.novell.soa.af.impl.persist.EngineStateDAO.updateHeartbeat(Engin>
      at com.novell.soa.af.impl.core.EngineImpl$HeartbeatTimer.run(EngineImp>
      at java.lang.Thread.run(Unknown Source)
2008-05-03 13:46:53,072 INFO  [STDOUT:warn] XDas was not enabled
```

There may also be an infinite loop caused by the Workflow heartbeat thread throwing a null pointer exception.

On WebSphere, the User Application will start even if OpenXDAS throws an exception.

To work around this problem, perform either of these steps:

 - Start the xdasd process and restart the application server.
 - Remove the OpenXDAS appender-ref from idmuserapp_logging.xml (`<appender-ref ref="OpenXDas"/>`).

2.47 Text Following Less-Than Symbol is Truncated in a Shared or Container Page Name

The user interface does not restrict the use of the less-than symbol (<). However, if a page name includes the < character, the page name does not display properly in the Page Administration console. The name of the page in the page list and in the page name field will be truncated at the < character. For example, the name `<Page` displays an empty row in the page list and nothing in the page name field. The name `Pa<ge` displays `Pa` in the page list and `Pa` in the page name field.

The page name does display properly in the navigation portlet.

2.48 Protected Mode Must Be Disabled on Internet Explorer 7.0 for Digital Signature Support

If you are running the digital signature applet with the Windows Vista version of Internet Explorer 7.0, you may see the following error message:

```
"The application's Digital Signature has an Error. Do you want to run the
Application?"
```

To fix this problem, you need to turn off Protected Mode in Internet Explorer.

2.49 Colon Not Supported in IDVault.globalQuery() Method

Using a colon (:) character in a call to the IDVault.globalQuery() method will cause scripting errors. Novell does not support using the colon (:) character at this time.

2.50 Heap Size for IDM Process Should Be Increased in Large Environments

More heap memory is needed for the IDM Java process in situations where a role has many role assignments (tens of thousands) associated with it. There are two ways to increase the Java heap memory allocated to IDM:

- In iManager, navigate to the Driver Set Properties and select the *Misc* tab. Then, specify values in the *Initial heap size* and *Max heap size* fields.

- Define the DHOST_JVM_INITIAL_HEAP and DHOST_JVM_INITIAL_HEAP variables in the ndsd start script. Note that these values take precedence over the values configured via iManager. In this example, the minimum and maximum heap size values are set to 500 megabytes.

  ```
  export DHOST_JVM_INITIAL_HEAP=500M
  export DHOST_JVM_MAX_HEAP=500M
  ```

For more information about configuring Java environment parameters, see the IDM Common Driver Administration Guide (http://www.novell.com/documentation/idm36/idm_common_driver/?page=/documentation/idm36/idm_common_driver/data/bg24txl.html).

2.51 User Application Does Not Locate Entitlement-Based Drivers in Multiple Driversets

Currently, the User Application is not able to find entitlement-based drivers on servers other than the one where the User Application Driver is located. For Entitlement mapping to work in the 3.7.0 release, the Drivers with the Entitlements must be running on the same DriverSet as the User Application Driver.

2.52 Entity Names with a Dash Are Not Supported in Search within Org Chart

The search feature from the Orch Chart Portlet will not work if the Entity type being displayed has a dash (-) in the name. At this time, the product does not support Entities with dashes in their names.

2.53 Novell Does Not Provide Support for Components Installed by JBossMySQL Utility

Novell provides the JBossMySQL utility as a convenience. If your company does not already provide an application server and a database server, you can use the JBossMySQL utility to install an Open Source version of these components. By running this utility, you can install these components without having to download them separately. If you need support, go to the third party provider of the component. Novell does not provide updates for these components, or administration, configuration, or tuning information for these components, beyond what it is outlined in the Roles Based Provisioning Module documentation.

2.54 srvprvUserPrefs Attribute Must Be Cleaned Up Manually

Values that are saved into the srvprvUserPrefs attribute are not fully removed when a user removes or change their filters or customization entries.

The attribute srvprvUserPrefs is a single values, synchronize immediately, string in eDirectory. It is limited to about 33,000 total characters. Once the attribute reaches the maximum size, users will not be able to save filter and customization entries into this attribute. To work around this issue, an Administrator would need to clean up the attribute manually with iManager or an LDAP Browser.

2.55 Need to Manually Enter a Four Digit Year When Using a Year Past 2030

When using the Effective or Expiration dates for a role assignment in the User Application, you need to manually enter the date if the year you want to use is after 2030. For example, if you want to set the Effective Date for a role to be assigned on January 01, 2031, the Calendar picker will display it as 1/1/31. If you leave this as is, the role will be immediately assigned. You must make the year a four digit year if the year is greater than 2030. For this example, you would need to use 1/1/2031.

2.56 A Resource Might Be Removed Unexpectedly When an Associated Role is Removed

If a user has been assigned to multiple roles, and these roles are associated with a resource that is dynamically bound (meaning that the value for the entitlement is set at assignment time), the user may lose all of the resource assignments for these roles if only one of the roles is removed. This will only happen if the option *Allow user to request multiple assignments by selecting more than on value* (which maps to nrfAllowMulti) is not selected when mapping the entitlement to a resource.

For example, suppose you have a resource that is dynamically bound to an entitlement, and the resource is mapped to two different roles, and the option *Allow user to request multiple assignments by selecting more than one value* is not set for the resource. In this case, if a user has been assigned to both roles, and later is removed from one of the roles, the user will lose both resources. This behavior occurs because the option *Allow user to request multiple assignments by selecting more than one value* was not selected when the entitlement was mapped to the resource.

3 Issues Fixed in 3.7

This section includes the list of issues described in the IDM 3.6.1 Roles Based Provisioning Module Readme that were fixed in the IDM 3.7 Roles Based Provisioning Module.

- 1.1.4 Setting up an MS SQL Server database for the User Application
- 1.2 Cryptovision Installer Refers to Incorrect Version of User Application
- 1.11 Special Characters in a Role Name Produce a Blank Role Report
- 1.12 XSS Error Messages are Not Informative
- 1.14 Accesing External Password WAR Causes Exception When log4j.jar Is Not Included
- 1.16 User Application on WebSphere Cannot Find Trusted Store Path
- 1.17 Digital Signature Verification Fails When Using xmlsigner 1.4

4 Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell® trademark; an asterisk (*) denotes a third-party trademark.

5 Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

All third-party trademarks are the property of their respective owners.