Novell Identity Manager 3.5.1 Readme

Novell®

1 Documentation

This document contains the known issues for Identity Manager version 3.5.1.

These additional documentation resources are currently available:

- Novell Identity Manager 3.5 Product Documentation Web site (http://www.novell.com/documentation/idm35/).
- Identity Manager 3.0.1 Product Documentation (http://www.novell.com/documentation/idm/).

2 What's New

This section describes two more items that belong in the list of new features in the What's New section in the *Identity Manager 3.5.1 Installation Guide*.

2.1 Using SAML assertion for Single Sign-On to the User Application

The Identity Manager User Application supports single sign-on through Access Manager, using any third-party authentication service that can log into Access Manager. This capability enables using a non-password-based technology to log into the User Application through Access Manager. An

example is logging in through a user (client) certificate, for example with a smart card. For more information, refer to the Security section in "Designing the Production Environment" in the *Identity Manager 3.5.1 User Application: Administration Guide*.

2.2 Searching the Identity Manager Whitepages

You can now add Search parameters on a URL that references the Identity Manager Whitepages.

3 System Requirements for Identity Manager 3.5.1

This section describes system requirements for Identity Manager 3.5.1:

3.1 WebLogic Support

The IDM 3.5.1 User Application does not support running on a WebLogic application server. The System Requirements section in the Identity Manager 3.5.1 Installation Guide has been corrected to remove mention of WebLogic.

3.2 Java

The Identity Manager 3.5.1 Java* requirements are as follows:

- The User Application requires Java 5.0.10 to support digital signing and Cryptovision.
- On JBoss* Application Servers, use the following Sun* JDK*: Java 2 Platform Standard Edition Development Kit version 1.5.0_10.

  Use this version of the Sun JDK to start the User Application installer as follows:

  Linux/Solaris

  ```
  $ /opt/jdk1.5.0_10/bin/java -jar IdmUserApp.jar
  ```

  Windows

  ```
  C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.5.0_10\bin\java.exe"
  -jar IdmUserApp.jar
  ```

  When the installation procedure asks for the full path of your Java installation, provide the root path of the Sun JDK. For example, the root path on Linux could be `/opt/jkd1.5.0_10`.

  NOTE: SLES users: Do not use the IBM* JDK that comes with SLES. This version is incompatible with some aspects of the installation and can cause master key corruption errors.

- On WebSphere Application Servers, use the IBM JDK that comes with WebSphere* Application Server 6.1.0.9 or later, with the unrestricted policy files applied. Also, you must apply the WAS JDK fixpack for 6.1.0.9.
- The Metadirectory installer installs its own copy of the JVM on all platforms except NetWare. On NetWare, the Metadirectory uses whatever version of Java is installed on the system.

3.3 Novell Audit

Identity Manager 3.5.1 supports Novell Audit 2.0.2.

3.4 Required WebSphere Version and Fixpack

The following is an addendum to the system requirements listed in the *Identity Manager 3.5.1 Installation Guide*: The User Application requires WebSphere Application Server (WAS) 6.1.0.9 and the WAS SDK Fixpack 6.1.0.9.

3.5 Context Other than IDMProv Fails on WebSphere

During the installation of Novell User Application 3.5.1 using IBM WebSphere Application Server 6.1 as the Application Server, if the context is changed from IDMProv (for the Provisioning version) or IDM (for the Standard version) the new context name will not replace the default value through out the code in the User Application. The war will be created with the new context, but code will still use IDMProv or IDM and not the new context name. As a result, when a user tries to access the User Application in a browser using the context entered during the install they will receive an error similar to the following:

```
Error 404: No Target servlet configured for uri:/IDMProv/portal/cn/
GuestContainerPage/Welcome
```

or:

```
Error 404: No Target servlet configured for uri:/IDM/portal/cn/
GuestContainerPage/Welcome
```

Also, the URL in the browser will be changed to the default context of IDMProv or IDM instead of the context that was entered.

Here is an example:

During the installation of the Provisioning version of the User Application 3.5.1 with WebSphere as the Application Server, the context was set to 'MyPortal'. The war name would be 'MyPortal.war'. However, the code within the war would still be using 'IDMProv' instead of 'MyPortal'.

When trying to access the deployed war on WebSphere using the context specified during the installation:

```
HTTP://%server%:%port%/MyPortal
```

The following error will be presented in the browser:

```
Error 404: No Target servlet configured for uri:/IDMProv/portal/cn/
GuestContainerPage/Welcome
```

Also, the URL in the browser will now be:

```
HTTP://%server%:%port%/IDMProv/portal/cn/GuestContainerPage/Welcome
```

The behavior does not occur when you select Red Hat JBoss as the Application Server during the installation.

Solution:

This is a Bug with version 3.5.1 of the Novell User Application and it only occurs when selecting IBM WebSphere as the Application Server during the install. This bug has been fixed in version 3.6.0 of the Novell Identity Manager Roles Based Provisioning Module (User Application).

For version 3.5.1 of the Novell User Application, the default contexts of IDMProv (for the Provisioning version) or IDM (for the Standard version) that are presented during the installation must be used. The context names cannot be changed during the installation when using IBM WebSphere as the Application Server.

3.6 Database Platforms

3.6.1 Database Must Use character set with Unicode encoding

The User Application requires that the database character set use Unicode encoding. For example, UTF-8 is example of a character set that uses Unicode encoding, but Latin1 does not use Unicode encoding. Before installing the User Application, verify that your database is configured with a character set that has Unicode encoding.

3.6.2 Setting up a MySQL database for the User Application

Install your MySQL server. Optionally, set the UTF-8 character set for the whole server. Create your database and set the character set. Edit the mysql configuration file (`my.ini` on windows, or `my.cnf` on linux). Set the following values:

```
character_set_server=utf8
```

```
default-table-type=innodb
```

Create a user to log into the MySQL server and grant privileges to the user, for example

```
GRANT ALL PRIVILEGES ON <dbname.>* TO <username>@<host> IDENTIFIED BY
'password'
```

The minimum set of privileges is CREATE, INDEX, INSERT, UPDATE, DELETE, and LOCK TABLES. For documentation on the GRANT command, see http://www.mysql.org/doc/refman/5.0/en/grant.html (http://www.mysql.org/doc/refman/5.0/en/grant.html).

3.6.3 Setting up an Oracle database for the User Application

Create your Oracle server and use AL32UTF8 to specify a Unicode-encoded character set. (See AL32UTF8 (http://download-east.oracle.com/docs/cd/B19306_01/server.102/b14225/glossary.htm#sthref2039) .)

Create a user. (This automatically creates a database.) Issue the following statements using the SQL Plus utility. These statements create the user and set the user's privileges. Grant the user CONNECT and RESOURCE privileges, for example

```
CREATE USER idmuser IDENTIFIED BY password
```

```
GRANT CONNECT, RESOURCE to idmuser
```

3.6.4 Setting up an MS SQL Server database for the User Application

Set up your MS SQL Server database as follows:

1 Install the MS SQL server.

2 Connect to the server and open an application for creating the database and database user (typically the SQL Server Management Studio application).

3 Create a database. SQL Server does not allow users to select the character set for databases. The IDM User Application stores SQL Server character data in a NCHAR column type,which supports UTF-8.

4 Create a login.

5 Add the login as a user of the database.

6 Grant these privileges to the login: CREATE TABLE, CREATE INDEX, SELECT, INSERT, UPDATE, and DELETE.

The User Application requires version 1.0.809.102 of the Microsoft SQL Server 2005 JDBC Driver. Note that only the Sun Solaris, Red Hat Linux, and Windows 2000 or later operating systems are officially supported with this JDBC driver.

3.6.5 Tuning DB2 Databases to Prevent Deadlocks and Timeouts

When using DB2 if you see the error "The current transaction has been rolled back because of a deadlock or timeout," the problem may be caused by a high level of user and database concurrency.

DB2 provides many techniques for resolving lock conflicts including tuning of the cost-based optimizer. The *Performance Guide* included in the DB2 Administration documentation is an excellent source that contains much information on the topic of tuning.

There are no prescribed tuning values that can be used for all installations since the level of concurrency and size of data varies. However, here are some DB2 tuning tips that may be relevant for your installation:

- The `reorgchk update statistics` command will update the statistics used by the optimizer. Periodic updates of these statistics may be enough to alleviate the problem.

- Use of the DB2 registry parameter DB2_RR_TO_RS can improve concurrency by not locking the next key of the row that was inserted or updated.

- Increase the MAXLOCKS and LOCKLIST parameters on the database.

- Increase the currentLockTimeout property on the database connection pool.

- Use the Database Configuration Advisor and optimize for faster transactions.

- Alter all the User Application tables to be VOLATILE to indicate to the optimizer that cardinality of the table will vary significantly. For example, to make the AFACTIVITY table VOLATILE, you might issue the command: `ALTER TABLE AFACTIVITY VOLATILE`

The ALTER TABLE commands need to be run after the User Application has been started once and the database tables have been created. Refer to the ALTER TABLE documentation for more information on this statement. Here are the SQL statements for all the User Application tables:

```
ALTER TABLE AFACTIVITY VOLATILE
ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
ALTER TABLE AFBRANCH VOLATILE
ALTER TABLE AFCOMMENT VOLATILE
ALTER TABLE AFDOCUMENT VOLATILE
ALTER TABLE AFENGINE VOLATILE
ALTER TABLE AFENGINESTATE VOLATILE
ALTER TABLE AFMODEL VOLATILE
ALTER TABLE AFPROCESS VOLATILE
ALTER TABLE AFPROVISIONINGSTATUS VOLATILE
ALTER TABLE AFQUORUM VOLATILE
ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
ALTER TABLE AFWORKTASK VOLATILE
ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DSS_APPLET_BROWSER_TYPES VOLATILE
ALTER TABLE DSS_APPLET_CFG VOLATILE
ALTER TABLE DSS_APPLET_CFG_MAP VOLATILE
ALTER TABLE DSS_BROWSER_TYPE VOLATILE
ALTER TABLE DSS_CONFIG VOLATILE
ALTER TABLE DSS_EXT_KEY_USAGE_RESTRICTION VOLATILE
ALTER TABLE DSS_USR_POLICY_SET VOLATILE
ALTER TABLE PORTALCATEGORY VOLATILE
ALTER TABLE PORTALPORTLETHANDLES VOLATILE
ALTER TABLE PORTALPORTLETSETTINGS VOLATILE
ALTER TABLE PORTALPRODUCERREGISTRY VOLATILE
ALTER TABLE PORTALPRODUCERS VOLATILE
ALTER TABLE PORTALREGISTRY VOLATILE
ALTER TABLE PROFILEGROUPPREFERENCES VOLATILE
ALTER TABLE PROFILEUSERPREFERENCES VOLATILE
ALTER TABLE SCHEMAVERSION VOLATILE
ALTER TABLE SECURITYACCESSRIGHTS VOLATILE
ALTER TABLE SECURITYPERMISSIONMETA VOLATILE
ALTER TABLE SECURITYPERMISSIONS VOLATILE
ALTER TABLE SEC_DELPROXY_CFG VOLATILE
ALTER TABLE SEC_DELPROXY_SRV_CFG VOLATILE
ALTER TABLE SEC_SYNC_CLEANUP_QUEUE VOLATILE
```

3.6.6 Hibernate Exception

Using the Oracle* 9i driver creates the following exception:
```
org.hibernate.exception.GenericJDBCException: could not insert:
[com.sssw.fw.security.persist.EboPermissionMeta]
```

To avoid this problem, use the Oracle 10g drivers, `ojdbc14.jar` and `orai18n.jar`. These drivers are backward compatible to Oracle 9i.

4 Identity Manager Installation and Upgrade

The following sections describe installation and upgrade bugs and workarounds.

4.1 Upgrading Identity Manager requires correct Administrator account to avoid losing Challenge Response answers

When upgrading from an earlier version of Identity Manager on the Windows platform, you should use the same Administrator account that was used to install Novell eDirectory. For example, if a domain Administrator account was used to install eDirectory, you should use the domain Administrator account again when installing Identity Manager and not use a local Administrator account.

The result of not using the same Administrator account is that users' answers for their Challenge Response Questions are no longer accessible. This occurs because the tree key is recreated during the installation (because of the different Administrator account) and the new tree key does not provide the correct access to the stored answers. As a result, users will be prompted for new Challenge Response answers when they log in.

4.2   eDirectory upgrade from 8.7.3 SP 9 to 8.8.3 fails on Solaris, SUSE Linux Enterprise Server (SLES), and Red Hat Enterprise Linux (RHEL)

When you upgrade eDirectory 8.7.3 SP9 to eDirectory 8.8.3, it fails displaying the following warning message:

```
WARNING: The location and version of the current Novell Identity Manager
installation is not compatible with Novell eDirectory 8.8.3. Please install
Novell Identity Manager version 3.6 or above and then upgrade the Novell
eDirectory Server instances by running "ndsconfig upgrade --config-file
<nds.conf file path>.
```

Work around:

1. Open `ndsd` script.
2. Remove `/usr/lib/nds-modules` path from `LD_LIBRARY_PATH` of `/etc/init.d/ndsd`.
3. Start `ndsd`.
4. Reinstall Identity Manager 3.5.1.
5. Upgrade the Novell eDirectory server instances by running `ndsconfig upgrade --config-file <nds.conf file path>`.

4.3 eDirectory upgrade from 8.8.2 to 8.8.3 fails on Solaris

When you upgrade eDirectory 8.8.2 to eDirectory 8.8.3, it fails.

Work around: You should manually delete the following files before upgrading eDirectory.

```
/opt/novell/eDirectory/lib/libjclnt.so
/opt/novell/eDirectory/lib/libjclnt.so.0
```

4.4 Upgrade of eDirectory version earlier than 8.8.2 to eDirectory 8.8.3 on AIX 5.3 is not supported:

In place upgrade for eDirectory version earlier than 8.8.2 to eDirectory 8.8.3 on AIX 5.3 is not supported. For information on Migrating to eDirectory 8.8 SP3, refer to Migrating to eDirectory 8.8 SP3 (http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/b2f7k6c.html)

4.5 Error starting the Identity Manager User Application on JBoss running as Windows service

When starting the User Application on JBoss running as a Windows service, you might get the following error:

```
com.sssw.fw.exception.EboUnrecoverableSystemException: Failed to initialize
EboPortletContainer framework service. at
com.novell.afw.portlet.core.EboPortletContainer.<clinit>(EboPortletContainer.
java:100) at
com.sssw.portal.servlet.EboPortalBootServlet.init(EboPortalBootServlet.java:8
6) at
javax.servlet.GenericServlet.init(GenericServlet.java:211) at
org.apache.catalina.core.StandardWrapper.loadServlet(StandardWrapper.java:110
5) at
org.apache.catalina.core.StandardWrapper.load(StandardWrapper.java:932)  at
org.apache.catalina.core.StandardContext.loadOnStartup(StandardContext.java:3
951
.
.
```

```
.
Caused by: java.lang.ClassCastException:
.
.
.
```

This error happens if the JBoss service loaded a different `xalan.jar` file during start up from the one expected by Identity Manager. To work around this problem, append the path to the `xalan.jar` onto the -Djava.class.path entry for the service. The resulting registry entry for the service looks something like the following example:

```
-Djava.class.path=C:\Novell\IDM_35_FCS\jre\lib\tools.jar;C:\Novell\IDM_35_FCS
\jboss\bin\run.jar;C:\Novell\IDM_35_FCS\jboss\lib\endorsed\xalan.jar
```

Then, restart the service.

You can append the path when the service is created or afterward.

4.6 JBossMysql.bin throws exception on MySql installation

If you install the Identity Manager User Application on a 64-bit system, and choose to install JBoss and MySQL by using the `JBossMysql.bin`, you might encounter an error during the installation of the MySQL database. To work around this problem, run `setup-mysql.sh`, then `start-mysql.sh`.

4.7 Incorrect characters or Cancel button can display when installing the User Application on 64-bit SLES 10

Incorrect characters or the *Cancel* button can be displayed when attempting to access the root container DN while installing the User Application on 64-bit SLES 10. If this occurs, make sure that you have installed the correct JRE for your environment.

4.8 GUI install fails on Solaris 9 and 10 when using eDirectory 8.8.1

The GUI install fails on Solaris* 9 and 10 when using eDirectory™ 8.8.1. The workaround includes the following:

- Run the text-based installation program.
- Use eDirectory 8.8.2, which has the fix for this issue.

4.9 Configupdate script fails after adding files to the WAR

The `configupdate.sh` script fails after you manually add custom files to an `IDM.war`, if the WAR was created with the `jar` binary in `/usr/bin/jar` distributed in SLES 9. The error is:

```
DEBUG===WAR updating...java.util.zip.ZipException: invalid entry compressed
size (expected 16176 but got 16177 bytes) at
java.util.zip.ZipOutputStream.closeEntry(Unknown Source) at
java.util.zip.ZipOutputStream.putNextEntry(Unknown Source)
```

To solve or prevent the problem, use a newer version of the `jar` to create the WAR, as in this example: `/usr/lib/java/bin/jar -cvf IDM.war *`

4.10 Failed to set up clustering

The following warning message can appear when you start the User Application by using the default JBoss server configuration:

```
WARN  [TomcatDeployer] Failed to setup clustering, clustering disabled.
NoClassDefFoundError: org/jboss/cache/CacheException
```

If you chose the default configuration (single-node) during the User Application installation, you can disregard this message. This message comes from the JBoss application server. It indicates that although the Identity Manager User Application can support clustering, your chosen application server configuration does not support clustering.

4.11 Special characters in a password cause schema extension problem during install

If your Identity Manager installation account password contains special characters, you might see the schema extension fail. You should install using a different account or change your password.

4.12 User Application and Access Manager simultaneous logout

The most recent versions of Access Manager might not support the default URL path for the ICS Logout Page found under *iChain Settings* on the Show Advanced Options page when configuring the User Application. If the default URL path of `https://yourIChainServer/cmd/ICSLogout` doesn't work, try `https://yourAccessManagerServer/AGLogout`.

4.13 User Application install fails if a server already has an instance of MySQL running

The User Application install program will fail if the server already has MySQL running on port 3306 without presenting the opportunity to install MySQL on a different port. This problem is because of a limitation of the JbossMysql utility provided with the User Application, but can be overcome by using the standalone MySQL install program.

The workaround is to stop the existing MySQL instance, and run the install. The install program instalsl MySQL on port 3306, but asks which port you want to connect to. Specify a new port, then go to the `my.cnf` file, change it to this new port, and restart the User Application MySQL instance. Then restart your other MySQL instance and the application should run properly from then on.

The User Application installer should allow you to install on a different port and then start on that new port. At present, it appears that the User Application install program only works if 3306 is free.

4.14 Maintenance level 5300-04 required when installing on AIX 5L version 5.3

When installing the Java Remote Loader to AIX* 5L version 5.3 with eDirectory™ 8.8.3, the only supported AIX maintenance level is 5300-04. Newer or older maintenance levels are not supported.

5 User Application: User Interface

The following sections describe bugs and fixes affecting the user interface of the User Application.

5.1 NullPointerException in Forgot Password

The User Application does not support Password Policy names that contain leading or trailing spaces. If you have a password policy that does contain leading or trailing spaces, users will encounter the message "Challenge Response Failed" right after they enter their username on the Forgot Password page.

5.2 Space at end of a challenge set name causes an error when you try to use challenge questions

One or more spaces at the end of the name of a password challenge set cause an error when the User Application tries to return the password challenge questions.   To prevent this problem, do not append spaces at the end of your challenge set name.

5.3 Backslashes in entity names are multiplied

If you create an entity such as a user in the User Application and include a backslash in the name, the backslash is multiplied in the full DN. For example, `myusername\` becomes `mysusername\\\`. This is a known bug. To work around this bug, avoid using backslashes in entity names.

5.4 Deleting and adding groups for a user profile through the Detail Page

In the Identity Manager User Application, under the *Identity Self-Service* tab, editing the group attribute to delete and add groups should be done as separate operations. In removing and adding a group as a one-step process, the deleted group name reappears when the + (add) button is clicked.

5.5 Can't log in as two different users in Firefox at the same time

In the user application, if you log in as User A using a Mozilla-family browser (Firefox*, Netscape*, or Mozilla*), then open another browser instance of the same kind of browser and log in as User B, you might see information for User B when going back to the first browser instance. This is because browser instances are sharing (and overwriting) the same cookie. This behavior is specific to Mozilla-family browsers; it does not occur with Internet Explorer.

5.6 Using Organization Chart HTMLEditor in Firefox causes exceptions

Exceptions may occur in Firefox on cut, paste, and copy operations when using the HTMLEditor within Orgchart preferences. Mozilla doesn't allow scripts to access the clipboard for security reasons. Therefore, the cut, copy, and paste buttons aren't available in Firefox.

In Firefox, you can download an extension named Allow Clipboard Helper via tools > Extensions, which leads you to the extension download Web site (https://addons.mozilla.org/en-US/firefox/browse/type:1)

After the download, you will see *Allow Clipboard Helper* in *Firefox > tool*.

Open it, and enter the server address you want to grant the clipboard access, then click *Allow*. You can add as many Web sites as you like. Shut down all the Firefox browsers, restart Firefox, and cut, copy, and paste should be working in Firefox.

5.7 Users should have proper eDirectory rights to create users and groups

When logging into the Identity Manager User Application, there is a link on the left menu to create a user. In order to create users, you must have the necessary eDirectory rights to add entries to the directory. Because the Identity Manager User Application has existing eDirectory users, those users should already have the necessary rights.

1 In iManager, click *View Objects*.
2 Browse to the object that contains your user container (for example, MySample.novell.) and click *Modify Trustees*.
3 Add a trustee (for example, MySample.novell) and change the assigned rights.
4 Under *[Entry Rights]*, select *Create*. Leave other fields with the default values, then click *Save*.

Now all of the users in the users.MySample.novell container can create users or groups within that MySample entity.

5.8 Special characters in the User Application must be escaped

The User Application supports the same characters as iManager. For information on escaping special characters, go to http://www.novell.com/documentation/imanager26/index.html and refer to the *iManager 2.6 Administration Guide*, Chapter 3 "Navigating the iManager Interface," Section 3.2, "Special Characters," on page 20.

5.9 Logging in without first logging out can cause failure of the login

When a user is logged into the User Application, loads the login portlet or page from a Bookmark or History, and tries to log in again, the second login does not set up the new portal session correctly. This can cause the second login to fail. To work around this issue, always use the logout link before logging in.

5.10 Tab header text is now limited

The top-level tabs in the User Application now enforce a limit on the number of characters allowed. The limit is 22 characters. For languages other than English, the text will be truncated if it exceeds the limit, and ellipses (...) will appear to indicate that some text is not being shown. To display the full text, the user can hover over the tab name.

6 User Application: Administration

The following sections describe bugs and fixes affecting administration of the User Application.

6.1 Audit files are now copied to the install folder even if you do not enable auditing

The files required for auditing (`NAuditPA.jar` and `logevent.conf`) are now copied to the User Application install folder, even if you choose not to enable Audit at install time. However, the `logevent.conf` file contains some parameters that would need to edited by hand after installation if you disable auditing while running the install program. These parameters are explained in Chapter 3, "Setting Up Logging", in the Identity Manager User Application: Administration Guide.

6.2 Use string syntax when creating class attributes in iManager

You can get the following error message when trying to update with a single value attribute using stream format:

```
LDAP: error code 19 - NDS error: can't have multiple values (-612)
```

The workaround is to use String syntax, for example Case Ignore String, not Stream syntax, when you create class attributes in iManager. Stream syntax should be used sparingly because of performance overheads.

6.3 Port conflict on User Application on OES 2 Linux

By default, the User Application starts the JBoss Application Server on port 8009. This causes a conflict because OES 2 Linux already uses port 8009. To avoid this conflict, change the JBoss port in the service.xml file before starting the JBoss application server.

6.4 NotSerializableException when Forgot Password is clicked in a clustered User Application

When the Forgot Password functionality runs in a clustered environment, you might see a stack trace like the following:

```
java.io.NotSerializableException:
com.novell.pwdmgt.soap.PasswordManagementBinding_Stub (If using exteranl
forgot password war)
java.io.NotSerializableException: com.novell.pwdmgt.jsf.util.MyCallbackHdlr
```

This is informational and does not require action. This happens when users perform Forgot Password actions. These error messages don't affect users performing Forgot Password actions. Users don't see any issues and can finish their Forgot Password actions successfully.

6.5 Some portlets encounter javax.faces.application error

When you use WebSphere, some portlets that use JSF might encounter the following error:
```
java.io.NotSerializableException:
javax.faces.application.FacesMessage$Severity
```

This error is benign and does not affect JSF or the portlet operation. To suppress the error, add the following component in the WebSphere Change Log Detail Levels:
```
com.ibm.ws.webcontainer.httpsession.HttpSessDRSBuffWrapper=fatal
```

6.6 Limiting the rights of accounts

For security, it is advisable to limit the administrator and LDAP guest accounts to the minimum set of rights required to fulfill the intended roles. When assigning the following roles in the User Application (during installation, or with the configupdate utility after installation), specify a separate physical Identity Vault user account for each:

- ◆ LDAP Administrator
- ◆ LDAP Guest (if used)
- ◆ User Application Administrator
- ◆ Provisioning Application Administrator

6.7 Password policies are not inheritable

Password policies are not inheritable. The User Application Administrator must explicitly apply the password policy to a container in which users are created. Failure to do so can yield this error:

```
Invalid Secure Password Manager (SPM) request. If the problem persists,
contact your System Administrator.
```

6.8 Setting SSL configuration parameters

Setting the *Secure Administration Connection* and the *Secure User Connection* parameters in the configupdate utility allows operations that don't need SSL to operate without SSL. Operations that require SSL, such as password functionality, still use SSL.

6.9 Redirected user can bypass authentication checks

If a user is redirected after login to change the password or challenge response hint, the user can type a URL of the portal and bypass the authentication checks until the next login. This is a known bug without a workaround at this time.

6.10 Browse button crashes the configupdate utility on Windows

The *File Browse* button in the configupdate utility sometimes crashes the JVM on Windows XP SP2. To work around this problem, type the full file pathname rather than using the *File Browse* button.

6.11 User Application driver requires activation

When the Application Server is down and you restart the activated User Application driver, the driver activation status can display as requiring activation even though the activation credentials have been loaded against the driver. This is a known bug. To avoid or resolve this problem, start the User Application driver after the User Application server is started and available.

6.12 JGroups problem requires upgrade to JGroups 2.4.x

There is a problem in the version of JGroups (Version 2.2.7) that is included in JBoss 4.0.5 GA that can cause performance problems in a clustered environment. For details about the problem, see Deadlock - JBoss.org JIRA (http://jira.jboss.com/jira/browse/JGRP-292). The issue is resolved in JGroups 2.4. We recommend upgrading to JGroups 2.4 or higher to avoid the problem described in JGRP-292.

Before upgrading to JGroups 2.4.x (or before upgrading any other component in the JBoss install) consult the compatibility list provided by the JBoss Application Server, JBossCache and JGroups Compatibility Matrix (http://labs.jboss.com/portal/jbosscache/compatibility/index.html).

For downloads and information about JGroups see JGroups - The JGroups Project (http://www.jgroups.org).

6.13 java.util.NoSuchElementException exception

A java.util.NoSuchElementException exception can occur while the User Application is running in a cluster. This exception is a known issue in JBoss and has been fixed in a higher release. Refer to the JBoss Web site (http://jira.jboss.com/jira/browse/JBAS-4075) for more information.

Here is an example of the stack trace that occurs for this issue:

```
2007-02-06 14:23:58,231 ERROR
[org.jboss.web.tomcat.tc5.session.JBossCacheManager:processExpires]
processExpires: failed with exception: java.util.NoSuchElementException
java.util.NoSuchElementException
        at
EDU.oswego.cs.dl.util.concurrent.ConcurrentHashMap$HashIterator.next(Concurre
ntHashMap.java:1131)
        at java.util.AbstractCollection.toArray(AbstractCollection.java:176)
        at
org.jboss.web.tomcat.tc5.session.JBossCacheManager.findLocalSessions(JBossCac
heManager.java:851)
        at
org.jboss.web.tomcat.tc5.session.JBossCacheManager.processExpires(JBossCacheM
anager.java:1188)
        at
org.jboss.web.tomcat.tc5.session.JBossManager.backgroundProcess(JBossManager.
java:817)
        at
org.apache.catalina.core.ContainerBase.backgroundProcess(ContainerBase.java:1
284)
        at
org.apache.catalina.core.ContainerBase$ContainerBackgroundProcessor.processCh
ildren(ContainerBase.java:1569)
        at
org.apache.catalina.core.ContainerBase$ContainerBackgroundProcessor.processCh
ildren(ContainerBase.java:1578)
        at
org.apache.catalina.core.ContainerBase$ContainerBackgroundProcessor.processCh
ildren(ContainerBase.java:1578)
        at
org.apache.catalina.core.ContainerBase$ContainerBackgroundProcessor.run(Conta
inerBase.java:1558)
        at java.lang.Thread.run(Thread.java:595)
```

6.14 Sensitive data in a user session is not encrypted

Sensitive data (for example, a login password for single sign-on) in the user session is not encrypted in this release. This may expose sensitive data to network sniffers. To protect sensitive data that is temporarily stored in the user session and that might be transmitted over the network during session replication in a clustered environment, you need to perform one of the following:

- Enable encryption for JGroups. For information about enabling JGroups encryption, see JGroups Encrypt (http://wiki.jboss.org/wiki/Wiki.jsp?page=JGroupsENCRYPT).
- Make sure that the cluster is behind a firewall.

6.15 Initial password expiration for new users or groups is now configurable

Administrators can now configure the initial password expiration for new users. To do so, edit the Create Portlet Preferences as documented in the *Identity Manager User Application: Administration Guide*.

Specify an *Expire password on initial login* preference.

- *True* expires the password upon the new user's first login.
- *False* (the default) uses the eDirectory settings to determine when the password expires.

6.16 Using SOAP to override the default retention period for workflows

The default setting for retaining completed workflow information is 120 days. However, you can use the SOAP interface to the Workflow Engine to change this setting. To access the SOAP interface for the Workflow Engine, enter this URL in a browser:

```
http://server:host/IDMProv/provisioning/service?test
```

When you see the page that lists the Workflow Engine methods you can call, select the *setCompletedProcessTimeout* method. The parameter you pass to this method changes the retention period. The value you specify must be in milliseconds.

6.17 A workflow fails to trigger from an eDirectory event

A single quote in a workflow CN prevents an eDirectory event from triggering that workflow. Avoid using a single quote in a workflow Common Name (CN).

6.18 Coordinating Identity Manager user application passwords with iManager password policies

The *Identity Manager User Application: Administration Guide* is missing the following information to help you coordinate Identity Manager user application passwords with iManager password policies.

Sections 19.3.1 and 19.7.1, describing the Universal Password requirement:
"If Universal Password is enabled, open iManager and go to *Passwords > Password Policies > Universal Password > Configuration Options*. Make sure the following option is checked: *Verify whether existing passwords comply with the password policy (verification occurs on login).*"

Section 16.2.1, describing the Container for Create property:
"If you use the Create portlet to create users and want to assign the users to an iManager password policy, also assign the specified container to the same iManager password policy. This ensures that users created in the user application are automatically assigned to the default iManager password policy."

6.19 LDAP port must be set in ForgotPasswordPortlet

On your User Application Server (JBoss server), when using the User Application login page, if you click the *Forgotten Password* link and enter the user name, the portal might return the following error message on the JBoss console and not redirect:

```
08:59:17,962 ERROR [EboPortletProxyHelper] The portlet entity does not exist
com.novell.afw.portal.aggregation.EboPortletInfoBean: id [portal-general] iid
[-1] timeout [-1] multithread [false]
```

The error results from the ldap-sslport preference in the ForgotPasswordPortlet portlet using the standard default TLS (ldaps) port of 636 instead of the port configured for your LDAP server's secure connection. The eDirectory administrator has probably changed the default secure LDAP port on the eDirectory instance to a non-standard port. eDirectory administrators commonly change the LDAP ports when running eDirectory on the same physical hardware as other LDAP-enabled systems such as Active Directory*.

If your secure LDAP (TLS) configuration uses a port other than 636, change the ldap-sslport preference in the ForgotPasswordPortlet to the port configured for your secure LDAP as follows:

1 Open the User Application.

2 Open *Administration > Portlet Admin > ForgotPasswordPortlet > ForgotPasswordPortlet instance > Preferences*.

3 Change the value of ldap-sslport from the default port of 636 to the port configured for your LDAP server's secure LDAP connections.

6.20 Parallel approvals don't work when addressee for one step refers to another step

In a provisioning workflow that uses parallel processing, the addressee for one approval activity should not refer to the addressee for another approval activity in the flow. The reason for this is that the workflow engine does not have any way to know which step will be executed first, because the activities are being processed in parallel. Furthermore, the iManager plug-in for Provisioning Request Configuration is not able to determine which addressees should be allowed at any point in time. To restrict the list of possible addressees, the plug-in would need to be able to analyze the flow to get the list of upstream activities that have already been completed. This capability is not supported in the plug-in at this time.

6.21 JBoss directory browsing is enabled by default

By default, JBoss allows directory browsing. Therefore, if you type the URL http://server:8080/IDMProv/resources/, the list of resources under this URL is displayed.

If you do not want directory browsing to be enabled, go to `jboss-4.0.2\server\<IDM-Application Context>\deploy\jbossweb-tomcat55.sar\conf`, and edit the listings entry in the `web.xml` file:

```
<servlet>
   <servlet-name>default</servlet-name>
   <servlet-class>org.apache.catalina.servlets.DefaultServlet</servlet-class>
      <init-param>
            <param-name>debug</param-name>
                  <param-value>0</param-value>
                     </init-param>
                        <init-param>
                              <param-name>listings</param-name>
                                    <param-value>true</param-value>
                                       </init-param>
                                          <load-on-startup>1</load-on-startup>
                                          </servlet>
```

To suppress the display of resources, change the listings value from true to false.

6.22 Service config.xml files contain outdated version numbers

The services for various subsystems within the User Application might contain outdated version numbers. You do not need to modify these files to correct the versions.

For example, `IDMfw.jar` contains the `FrameworkService-conf\config.xml` file, which has the following entry for the version number:

```
<property>
    <key>FrameworkService.version</key>
          <value>040712, Version 5.2.1</value>
          </property>
```

6.23 Workflow activity escalation policy might result in workflow failure and process termination

In the Provisioning Request Configuration plug-in to iManager, you can define an escalation policy that redirects a workflow activity to the manager of the original addressee.

If the original addressee is a task group that has more than one manager, the escalation fails. The Provisioning Request Configuration plug-in does not prevent you from defining this type of escalation, so you need to be careful to avoid this type of configuration.

6.24 Starting workflows with the SOAP Web Service sometimes causes errors

On Linux*, the default open limit is not sufficient to support a large number of requests initiated through the SOAP Web Service. The User Application Driver might reach this limit when using the Web Service endpoints to trigger workflows in response to directory events.

Linux has a default open file limit of 1024 for each process. If you start the JBoss server with the default setting, you might see errors when more than 40 or 45 requests are started sequentially through the SOAP Web Service interface. After reaching the limit, you might be unable to initiate any more requests for several minutes. In some cases, you might need to restart the JBoss server.

To work around this problem, you can increase the open file limit from 1024 to 4096.

If you're using BASH, execute these commands to increase the open file limit:

```
su - root ulimit -n 4096 su - <user> start-jboss.sh
```

If you're using C Shell, execute these commands to increase the open file limit:

```
su - root limit descriptors 4096 su - user start-jboss.sh
```

6.25 Separate user applications should not share a single instance of the User Application driver

The User Application driver stores various kinds of information (such as workflow configuration and cluster information) that is application-specific. Therefore, a single instance of the User Application driver should be not shared among multiple applications.

The User Application stores application-specific data to control and configure the application environment. This includes the JBoss Application Server cluster information and the workflow engine configuration. The only user applications that should share a single User Application Driver instance are those applications that are part of the same JBoss cluster. You should not configure a set of user applications to share a single driver unless they are part of the same JBoss cluster. Otherwise, your configuration could lead to ambiguity and misconfiguration for one or more of the components running inside the User Application.

6.26 Root, user, and group container DNs do not support the root of the tree or allow multiple container DNs to be selected

In the install program for the Identity Manager User Application, you can specify the root container DN, user container DN, and group container DN for the application. In this release, you cannot specify the treeRoot in eDirectory as the root container. Also, you cannot specify more than one search root for any particular object type (container, user, or group). Instead, you must specify a single search scope.

An organization (o) could be contained in a Country (c) or locality (l), as shown below:

 c=US o=novell-provo o=novell-waltham

This type of configuration works.

6.27 Separate instances of the User Application driver should not share the same user container

If two separate instances of the User Application driver point to the same user container, the availability settings (on the Edit Availability page of the user application) show availability entries from both applications.

Suppose Server 1 is configured to use one driver (such as driver1,o=novell), and server 2 is configured to use another (such as driver2,o=novell). Both servers are configured to use the same containers for users, groups, and the root container (such as ou=users,o=novell). A user on server 1 creates a delegate definition for a user and provisioning request definition. The user is then marked as unavailable for that request definition. Server 2 shows the user as unavailable, but it is unable to resolve the friendly name for the request definition. If the user's delegate definitions on server 2 are examined, the definition from server 1 is not seen.

The reason for this behavior is that delegation information (created when users mark themselves available/unavailable) is stored on user records. This information includes the delegate/delegator information along with the provisioning request definition and start/stop time for delegation. The delegate definition, from which delegation information is derived is stored in the driver, along with the provisioning request definition.

We recommend not configuring two separate driver instances to point to the same user container.

6.28 The User Application driver must be restarted after creating a new provisioning request definition

The User Application driver reads the list of workflow attributes when the driver is started. If you create a new provisioning request definition, and if you immediately try to create a Schema Mapping policy, the attributes for the new provisioning request definition do not appear in the list of application attributes after you refresh the application schema. This is because the User Application driver needs to be restarted before the provisioning request definition is made available. After creating the new provisioning request definition, stop the User Application driver, then restart before attempting to use the provisioning request definition in policies. Alternatively, in the Schema Mapping policy editor, simply refresh the application schema twice.

6.29 Installing to a cluster does not prompt for the workflow engine ID

When running workflows in a cluster, each server's workflow engine must have a unique ID. The engine ID is identified by passing -Dcom.novell.afw.wf.engine-id to the Java VM. On Linux, the user needs to edit the jboss/bin/run.conf file and pass that property in the JAVA_OPTS line. For example:

```
if [ "x$JAVA_OPTS" = "x" ]; then JAVA_OPTS="-server -Xms800m -Xmx800m -
Dcom.novell.afw.wf.engine-id=echo"
```

The install program does not prompt you to specify the workflow engine ID. Therefore, you need to identify the engine by passing the JAVA_OPTS property, as shown above.

6.30 A server caching problem might occur with photos in the Detail portlet

If you change the way images are displayed in the Detail portlet header by specifying the $IMG: tag, you must flush the CompiledLayout cache for the changes to take effect. Follow these steps to flush the cache:

1 Go to the *Administration* tab of the user application.

2 Go to the *Caching* tab.

3 Select *CompiledLayout* from the *Flush Cache* drop-down list.

4 Click *Flush Cache*.

6.31 The Portal Data Import utility fails to import pages without descriptions

The Portal Data Import utility (*Administration > Tools > Portal Data Import*) uses the `shared-pages.xml` and `container-pages.xml` in the Portal Data Export ZIP file to generate container and shared pages, and portlets. If the `<description/>` element is blank, then pages cannot be imported.

To work around this, provide text for the `<description/>` element and perform the import again.

6.32 Additional JBoss setup documentation

The *Identity Manager User Application: Administration Guide* contains some information on configuring JBoss. If you need further information on JBoss setup, look at the sources listed below:

- For details on configuring JBoss as a service on SUSE, see the Novell Cool Solutions Web site (http://www.novell.com/coolsolutions/feature/14912.html).
- For Apache SSL setup, see the appropriate section on the JBoss Web site (http://www.jboss.org/wiki/Wiki.jsp?page=Tomcat).
- For information on IIS SSL setup, see the JBoss Forum: Installation, Configuration, and Deployment (http://jboss.org/index.html?module=bb&op=viewtopic&p=3816794#3816794).

6.33 Required Attribute rights for Provisioning Request objects

To use the iManager Provisioning Request Configuration plug-in, you must have read rights and write rights to the attributes associated with the Provisioning Request objects.

6.34 Character set encoding support and Tomcat

By default, the user application character encoding filter is set to enabled in the user application's `web.xml`. This setting typically does not require any specific configuration, but it might require changes if you have configured Tomcat for URI encoding. There are two attributes in the configuration of Tomcat HTTP/HTTPS connector that affect character set encoding and filter configuration.

--URIEncoding

This entry specifies the character encoding used to decode the URI bytes, after %xx decoding the URL. If not specified, ISO-8859-1 is used. The requirements for this include:

- Both HTTP and HTTPS connectors have the same configuration.
- The Charest encoding filter should be modified to include the uri-encoding init parameter. The value of this parameter should be the same as the value of the URIEncoding attribute in the Tomcat connector configuration.

```
<filter>
    <filter-name>AggregationServletEncFilter</filter-name>
    <display-name>AggregationServletEncFilter</display-name>
```

```
<filter-class>com.novell.afw.portal.l18n.CharacterEncodingFilter</filter-
class>
     <init-param>
             <param-name>uri-encoding</param-name>
             <param-value>UTF-8</param-value>
     </init-param>
</filter>
```

Also add `URIEncoding="UTF-8"` to `jboss-4.2.0.GA\server\IDMProv\deploy\jboss-web.deployer\server.xml`, for example:

```
<Connector port="8080" address="${jboss.bind.address}"
       maxThreads="250" maxHttpHeaderSize="8192"
       emptySessionPath="true" protocol="HTTP/1.1"
       URIEncoding="UTF-8" enableLookups="false" redirectPort="8443"
       acceptCount="100"
       connectionTimeout="20000" disableUploadTimeout="true" />
If SSL is enabled, make the same change for the SSL HTTP/1.1 Connector.
```

--useBodyEncodingForURI

This entry specifies whether the encoding specified in contentType should be used for URI query parameters instead of using the URIEncoding. This setting is present for compatibility with Tomcat 4.1.x, where the encoding is specified in the contentType, or explicitly set using Request.setCharacterEncoding method for the parameters from the URL. The default value is false.

If useBodyEncodingForURI is set to true, the filter configuration should include the use-body-encoding init parameter, for example:

```
<filter>
     <filter-name>AggregationServletEncFilter</filter-name>
    <display-name>AggregationServletEncFilter</display-name>
<filter-class>com.novell.afw.portal.l18n.CharacterEncodingFilter</filter-
class>
       <init-param>
             <param-name>use-body-encoding</param-name>
          <param-value>true</param-value>
       </init-param>
</filter>
```

For more details, see the Web site on Tomcat connector configuration information (http://tomcat.apache.org/tomcat-5.5-doc/config/http.html).

6.35 Change in behavior of the DirXML-EntitlementResult attribute

There has been a change to the way in which the DirXML-EntitlementResult multi-valued attribute is handled. Previously, entitlement results were not purged from this attribute. Now, the default behavior has been changed. Entitlement results are now purged after they are processed.

You can change the default behavior (specify whether entitlement results are purged or not, and how they are purged). To set the entitlement purge type:

1 In iManager, display the Identity Manager Driver Overview page for your user application driver.

2 Click *Event Transformation Policies*.

3 Click the Manage Modify policy for your user application driver, then click *Edit*.

4 Click *Set Entitlement Purge Type*.

5 For the *Do append XML text* action, type one of the following in the *Enter String* field:

- **current:** After notifying the user application driver, delete the entitlement result that caused the event. This is the default behavior. It is also used if no entitlement purge type is set, or if an invalid entitlement purge type is set.

- **none:** Do not purge the entitlement result.

- **previous:** Delete any previous entitlement results without deleting the one that caused the event.

- **notnewer:** Delete previous entitlement results including one that caused the event. This preserves any entitlement result that was created after the entitlement result that caused the event.

6.36 Network File accessory portlet has a new preference

The NetWork File accessory portlet has the following new preference: ShortcutsUseFullyQualifiedPath.

If this option is set to True,   any shortcuts you specify in the Shortcuts preference must have fully qualified paths.

If this optoin is set to False, any shortcuts you specify in the Shortcuts preference must have paths relative to the InitialDirectory. Select False only if users will navigate only to subdirectories within the path.

6.37 Configuring the Network File portlet for RMI access to NetWare

With the current release of JBoss, configuring the Network File portlet for accessing a NetWare server via RMI has changed.

Currently the documentation states to copy `njclv2r.jar` from `sys:\java\njclv2r\lib` on the NetWare/RMI server to the `$JAVA_HOME$/jre/lib/ext` directory on your portal platform.

With the current release of JBoss, you must copy `njclv2r.jar` to the `.../jboss/server/IDM/lib` directory where your User Application was initially deployed. Then, restart JBoss.

6.38 Exiting your Netstorage accessory portlet session

To end your NetStorage session and close access to the files you used, click the logout button in the NetStorage Web interface.

6.39 Enabling Single Sign-On in accessory portlets

In the *Identity Manager Accessory Portlet Reference Guide* (http://www.novell.com/documentation/idm35/index.html), replace each description of how to enable portlet SSO with this procedure:

To enable portlet Single Sign On, do the following:

1 In the User Application, open the *Administration* tab and choose *Application Configuration*.

2 Select *Password Module Setup > Login*.

3 Click the radio button that enables SSO.

6.40 Log file name changes

The log file `jboss/server/IDM/conf/extendlogging.xml` name has changed to `jboss/server/IDM/conf/idmuserapp_logging.xml`. The new log file name is used in the Identity Manager 3.5.1 User Application: Administration Guide (http://www.novell.com/documentation/idm35/index.html), Section 5.1.4 "Logging Configuration", in the subsection "Persisting Your Logging Settings."

6.41 Logging configuration does not allow removing a package

When you add a package to the log list, it immediately shows up in the Logging Configuration screen. To remove a package from the log list:

* Do not click *Persist the logging changes*. The new package will disappear from the log list the next time you start the server.

* If you click *Persist the logging changes*, you must manually remove the package from the `idmuserapp_logging.xml` file located in the `$JBOSS/servers/$seafang/conf` directory.

6.42 PermGen space error

In Identity Manager 3.5 or 3.5.1, you might encounter a `java.lang.OutOfMemoryError: PermGen space` error if you redeploy the User Application.

To avoid this error, do one of the following:

* Restart the JBoss server

* Increase the PermSpace value by passing `-XX:MaxPermSize` to the Java virtual machine by means of JAVA_OPTS in the `start-jboss` script.

  For 32-bit machines, specify 128 megabytes, for example `-XX:MaxPermSize=128m`.

  For 64-bit machines, specify 256 megabytes, for example `-XX:MaxPermSize=256m`.

6.43 Reassigning a workflow process from one workflow engine to another in a cluster

Workflow engines in a cluster now detect when a workflow engine in the cluster has failed, and automatically reassign any processes running on the failed workflow engine to another workflow engine.

However, there may be occasions when you want to manually reassign a workflow process from one workflow engine to another (for example, to distribute processes back to a failed workflow engine when it is brought back online). To do so, you use the iManager Workflow Administration plug-in, as follows:

1 Select the *Workflow Administration* category in *Roles and Tasks* in iManager.

2 Select *Workflows*.

3 If you have yet not accessed a workflow server, specify the driver name in the *User Application Driver* field and click *OK*.

iManager fills in the remaining fields on the screen for you.

4 (Optional) Override the user name in the *User* field and the password in the *Password* field.

The user must be the user application administrator (Provisioning Administrator). By default, the user name is set to the user who is currently logged in to iManager. If this user is not the user application administrator, you need to change the user name.

5 Click *Login*.

The Workflow Administration plug-in displays a page that allows you to specify a filter for finding workflows.

6 Click *Show all Workflows*, then click *OK*.

iManager displays the workflow processes running on the specified user application driver. The *Engine* column lists the engine ID of a workflow engine.

7 To reassign a workflow process from one engine to another, select the workflow in the Workflows panel by clicking the check box next to the workflow name, then click *Actions > Reassign*.

6.44 Workflow integration activity causes an error on shutdown

When using the Integration activity in a provisioning workflow, you may see this error in the JBoss console on shutdown.

```
15:26:51,031 INFO  [STDOUT] 173542 [JBoss Shutdown Hook] ERROR STDERR  -
Unable
to instantiate the config file null
15:26:51,032 ERROR [STDERR] java.lang.NullPointerException
15:26:51,033 INFO  [STDOUT] 173545 [JBoss Shutdown Hook] ERROR STDERR  -
java.lang.NullPointerException
15:26:51,034 ERROR [STDERR]     at
com.sssw.b2b.rt.xmlparser.GNVXMLFactory.createParser(GNVXMLFactory.java:112)
15:26:51,035 INFO  [STDOUT] 173547 [JBoss Shutdown Hook] ERROR STDERR  -
at
com.sssw.b2b.rt.xmlparser.GNVXMLFactory.createParser(GNVXMLFactory.java:112)
15:26:51,037 ERROR [STDERR]     at
com.sssw.b2b.rt.GNVConfig.<init>(GNVConfig.java:189)
15:26:51,038 INFO  [STDOUT] 173550 [JBoss Shutdown Hook] ERROR STDERR  -
at com.sssw.b2b.rt.GNVConfig.<init>(GNVConfig.java:189)
15:26:51,039 ERROR [STDERR]     at
com.sssw.b2b.rt.GNVConfig.<init>(GNVConfig.java:161)
15:26:51,040 INFO  [STDOUT] 173552 [JBoss Shutdown Hook] ERROR STDERR  -
at com.sssw.b2b.rt.GNVConfig.<init>(GNVConfig.java:161)
15:26:51,041 ERROR [STDERR]     at
com.sssw.b2b.ee.edi.rt.GNVEDIObject.<clinit>(GNVEDIObject.java:39)
15:26:51,042 INFO  [STDOUT] 173554 [JBoss Shutdown Hook] ERROR STDERR  -
```

```
at com.sssw.b2b.ee.edi.rt.GNVEDIObject.<clinit>(GNVEDIObject.java:39)
15:26:51,044 ERROR [STDERR]     at
com.sssw.b2b.ee.edi.rt.GNVEDIComponent.<clinit>(GNVEDIComponent.java:101)
15:26:51,045 INFO  [STDOUT] 173557 [JBoss Shutdown Hook] ERROR STDERR  -
at com.sssw.b2b.ee.edi.rt.GNVEDIComponent.<clinit>(GNVEDIComponent.java:101)
```

These error messages are not an indication of a serious problem. When you start up JBoss again, the server and the User Application should behave normally.

6.45 Unspecified e-mail notification server error

The following errors may appear in the log when the User Application is configured to use e-mail notification. You can ignore these errors. Users still receive email notifications.

```
[date  time EDT] 00000056 SystemOut    O 09:58:35,469 ERROR
[MailEngine] Notification email server host unspecified. Check eDirectory
setup.
com.novell.soa.notification.impl.NotificationException: Notification email
server host unspecified. Check eDirectory setup.
.
.
.
```

or

```
13:39:47,264 ERROR [MailEngine] Notification email default -from- unspecified.
Check eDirectory setup.
com.novell.soa.notification.impl.NotificationException: Notification email
default -from- unspecified. Check eDirectory setup.
        at
.
.
.
```

7 User Application: Performance

7.1 Session timeout should be tuned to improve server performance

By default, the session timeout for the server is 20 minutes. The session timeout should be tuned to match the server and usage environment in which the application will run. In general, it is advised that the session timeout be as small as practically possible. If business requirements can tolerate a five-minute session timeout, this allows the server to release unused resources sooner than the default, and make the server faster and more scalable.

* Longer session timeouts can potentially cause the JBoss server to run out of memory if many users log in. This is true of any application server that has too many open sessions.

◆ When a user logs in to the user application, an LDAP connection is created for the user, and bound to the session. Thus, if more sessions are open, more LDAP connections are held open and the longer the session timeout, the longer these connections are held open. Too many open connections to the LDAP server can cause system performance degradation, even if the connections are idle.

◆ If the server starts experiencing OutOfMemoryErrors, and the JVM heap and garbage collection tuning parameters have already been optimized for the server and usage environments, then you should consider lowering the session timeout.

The session timeout is set in the `web.xml` file.

7.2 Enabling e-mail notification for workflows without configuring the e-mail server results in memory consumption

If you enable e-mail notification in your provisioning request definitions, but you do not configure any e-mail servers, e-mail notifications pile up on the server and are never sent. This eventually uses up available memory.

If you turn on e-mail notification, be sure to configure the e-mail server so that the e-mails are actually sent. To configure the e-mail server, select *Email Server Options* under *Workflow Administration* in iManager.

8 Localization

8.1 E-mail Subject text display problem

The Windows GroupWise® Mail and Outlook* clients have a known bug when displaying the Subject text from an HTML `mailto:` command. This bug appears when the browser uses a double-byte character set language such as Chinese, Japanese, or Korean.

In this case, when you send identity information from the Detail page, the Subject line has invalid characters because these mail clients do not unescape the double-byte characters correctly.

8.2 Possible issue with character set encoding

You should ensure that the input and output character encodings match those used by the source or destination application. Any characters that are not representable in the selected output are changed to question marks ("?").

8.3 Locale must be set correctly to display localized characters on an English OS

If you run the User Application Configuration tool (for configuring LDAP settings) in a localized operating system environment, all the text input boxes are displayed correctly. For example, if there are any Chinese distinguished names in eDirectory, or you input any Chinese characters, these are displayed properly in a Chinese operating system environment. However, if you are in an English operating system environment, any Chinese characters entered or returned from eDirectory are displayed as non-readable characters (most likely squares). This is because the Locale is not properly set.

If you are in an English operating system environment and want to display localized characters, do the following:

 ◆ - In a Windows 2000 environment, go to the Control Panel and select *Regional Options*. Under the *General* tab, set *Your Locale* to the local language (for example, Chinese (PRC)).

 ◆ - In a Windows 2003 environment, go to the Control Panel and select *Regional Options*. Under the *Regional Options* tab, select *Chinese (PRC)* and apply the change.

 ◆ - In a SUSE Linux environment, set the environment variable LANG as follows: export LANG=zh_CN

The same basic procedure applies to all languages.

8.4 The Message accessory portlet has not been localized

The Message accessory portlet has not been localized.

8.5 OK and Cancel buttons on the Context Preferences dialog are not localized

In *Portal Administration > Page Administration*, the Content Preferences dialog box always displays the following text in English: "Changes have been made to your Selected Content. Click OK to save your changes or cancel to continue without saving."

8.6 E-mail has a problem displaying content in double-byte character-set languages

When Identity Manager sends an e-mail containing a double-byte character-set language such as Chinese or Japanese, the e-mail client has a problem reading it. Please contact Novell Technical Support if you encounter this problem.

9 iManager

The following sections list bugs, fixes, and workarounds for iManager.

9.1 Upgrading the iManager JClient if you are running iManager 2.6

The Identity Manager 3.5.1 plug-ins use the `JClient.readReference ( )` API. This API has been updated in iManager 2.7. If you are running iManager 2.6, Novell recommends upgrading the underlying JClient in iManager 2.6 to be the same version in iManager 2.7. The older version of the JClient can cause iManager to crash or not work.

9.2 Internet Explorer 7 prompts continually for access to the clipboard

When in iManager, particularly the Policy Builder, Internet Explorer 7 continually prompts you for access to the clipboard. To disable prompting:

1 Click *Tools > Internet Options*.
2 Select the *Security* tab, then click *Custom Level*.
3 Locate *Scripting > Allow programmatic clipboard access*, then select *Enable*.

After you restart Internet Explorer, the prompting stops.

9.3 Adding localized e-mail templates through iManager

To add localized e-mail templates through iManager:

1 Log in to iManager.
2 Under Roles and Tasks, expand *Passwords* or *Workflow Administration*.
3 Click *Edit Email Templates* (under Passwords plug-in) or *Email Templates* (under Workflow Administration).
4 Identify the e-mail template (without any locale in the name) you want to copy. Write down the template name to use in Step 5. Click the template subject to open the template and view its message subject, body, and replacement tags. Copy the message subject, body (to be translated) and replacement tags you want to use in your new template. Click *Cancel*.
5 Click *Create* and enter the template name with a locale extension. For example, to create a Forgot Hint template in German, enter the name Forgot Hint_de, where _de signifies Deutsch (German). Click *OK*.

   NOTE: If you use a two-letter language and two-letter country code, this works. If you attempt to use a locale with a variant such as en_US_TX, only the variant and language are considered. Do not use locale variants when naming e-mail templates in this release.

6 In the template list, click the newly created template, for example Forgot Hint_de, and enter the translated subject and message body, for example in German. Be sure to preserve the replacement tags surrounded by the dollar ($) sign in the message body.

7 Click *Add* to enter or paste replacement tags, then click *OK*.

8 Click *Apply*, then *OK*.

E-mail templates only send properly localized content if the preferred locale is set for the user to whom the mail is sent.

9.4 iManager plug-in error: The driver password could not be saved

This issue is fixed by upgrading to NMAS™ 2.3.9.

9.5 iManager plug-in dependency for the NDS-to-NDS Driver Certificates Wizard

If you want to use the NDS-to-NDS Driver Certificates Wizard, you must download and install the iManager plug-in for Certificate Server.

9.6 Problem creating a new password policy based on the default settings in Mobile iManager 2.6

When using the Identity Manager 3.5 plug-ins and Mobile iManager 2.6, iManager might quit unexpectedly when you select *Create a new Password Policy based on default settings*. This issue occurs because of an error in the JavaScript* handler of the embedded Mozilla browser that's delivered with Mobile iManager on Linux.

To work around this issue:

1 Start Mobile iManager, then minimize it.

2 Open your preferred browser, then access iManager at the following address: http:\\localhost:48080\nps\iManager.html.

10 Drivers

Ensure that the input and output character encodings configured in the delimited text driver match those used by the source or destination application. Mismatches cause errors or corrupted data in the Identity Vault or the application. Characters that are not representable in the selected output are changed to question marks (?).

11 Password Management

The following sections describe bugs, fixes, and workarounds related to password management.

11.1 Password Management JSF portlets lose state if the user application fails in a cluster

If a password management JSF portlet is running in a clustered environment and the server that runs the portlet fails, the user is automatically switched to another server. The portlet is displayed to the user with no message about whether the portlet operation on the original server succeeded or failed. The user can test to see if the operation succeeded before the server failure or rerun the portlet. The affected password management portlets are:

- Password Challenge Response
- Password Hint Change
- Change Password

11.2 Limited support of multi-language challenge sets

The User Application included with Identity Manager 3.5 supports the full use of multi-language challenge sets. You can configure this functionality through iManager and setting password policies.

If you are using the Novell Client™ 4.9.1 or older, or Password Management for Novell eDirectory, this multi-language feature is not yet supported. You should not assign password policies to users if you have defined challenge sets in more than one language. For example, you can define challenge sets for French, but not French and German.

11.3 Challenge Response Failure

A user might encounter a `Challenge Response Failed` error when they:

1. Type a username in the Forgot Password page.
2. Do not answer the challenge questions.
3. Click the browser's *Back* button and enter a different username in the Forgot Password page.

To work around this problem, the user should restart the Forgot Password process by accessing this URL:

`http://<servername>:<port>/<context-name>/jsps/pwdmgt/ForgotPassword.jsf`

12 Security

Downloads of Identity Manager 3.5 prior to April 9, 2007 contained a security issue. Under certain conditions, the iManager plug-ins were showing administrative users the values of hidden attributes. A fix has been made to the iManager plug-in to disallow the display of hidden attributes that have been synchronized by Identity Manager drivers. Because drivers often synchronize sensitive information, administrative rights to these drivers should be limited to prevent unauthorized access.

The md5sum hashes of the original affected media are:

Identity_Manager_3_5_DVD.iso	0c8c61364414c71fd81df11c1e23737b
Identity_Manager_3_5_Linux_NW_Win.iso	497f707b19ca5cc71e7623269175299e
Identity_Manager_3_5_Unix.iso	5850fea9187075f7e89a05802e80bb74

You can obtain the latest patches from the Novell Download Web site.

13 Documentation Changes

This section includes changes to the Identity Manager 3.5.1 documentation, including corrections and additional product information.

13.1 WebLogic Support

The System Requirements section in the Identity Manager 3.5.1 Installation Guide incorrectly lists WebLogic as being supported by Identity Manager 3.5.1. WebLogic has been removed from the System Requirements section.

13.2 User Application configuration iChain settings change

Please note the following changes to all Advanced Options tables of User Application configuration parameters in the *Identity Manager 3.5.1 Installation Guide (http://wwwstage.provo.novell.com/documentation/idm35/)*, Chapter 5, "Installing the User Application":

Obsolete Name	Replace With New:
iChain Settings	*Access Manager & iChain Settings*
ICS Logout Enabled and description	*Simultaneous Logout Enabled*
	If this option is selected, the User Application supports simultaneous logout from the User Application and either Novell Access Manager or iChain. The User Application checks for an Novell Access Manager or iChain cookie on logout and, if the cookie is present, reroutes the user to the simultaneous logout page.
ICS Logout Page and description	*Simultaneous Logout Page*
	The URL to the Novell Access Manager or iChain logout page, where the URL is a hostname that Novell Access Manager or iChain expects. If Simultaneous Logout is enabled and a user logs out of the User Application, the user is rerouted to this page. One of the two following URLs should direct the simultaneous logout feature to the correct page depending on your environment:
	Access Manager: https://yourAccessGatewayServer/AGLogout
	iChain: https://yourIChainServer/cmd/ICSLogout

13.3 Specifying JVM Custom Properties in WebSphere

Substitute the following for Section 5.6.12 of the *Identity Manager 3.5.1 Installation Guide*:

1 Copy the `sys-configuration-xmldata.xml` file from the User Application install directory to a directory on the machine hosting the WebSphere server, for example `/UserAppConfigFiles`. The User Application install directory is the directory in which you installed the User Application.

2 Set the path to the `sys-configuration-xmldata.xml` file in the JVM system properties. Log in to the WebSphere admin console as an admin user to do this.

3 From the left panel, go to *Servers > Application Servers*

4 Click on the server name in the server list, for example, server1.

5 In the list of settings on the right, go to *Java and Process Management* under *Server Infrastructure*.

6 Expand the link and select *Process Definition*.

7 Under the list of *Additional Properties*, select *Java Virtual Machine*.

8 Select *Custom Properties* under the *Additional Properties* heading for the JVM page.

9 Click *New* to add a new JVM Custom Property.

   9a For the *Name*, enter `extend.local.config.dir`.

   9b For the *Value*, enter the name of the install folder (directory) that you specified during installation. (The installer wrote the `sys-configuration-xmldata.xml` file to this folder.).

   9c For the *Description*, enter a description for the property, for example, `path to sys-configuration-xmldata.xml`.

   9d Click *OK* to save the property.

10 Click *New* to add another new JVM Custom Property.

   10a For the *Name*, enter `idmuserapp.logging.config.dir`

   10b For the *Value*, enter the name of the install folder (directory) that you specified during installation.

   10c For the *Description*, enter a description for the property, for example, `path to idmuserapp_logging.xml.`

   10d Click *OK* to save the property.

> **NOTE:** The `idmuserapp-logging.xml` file does not exist until you persist the changes through *User Application > Administration > Application Configuration > Logging*.

14 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 ($^®$, ^{TM}, etc.) denotes a Novell$^®$ trademark; an asterisk (*) denotes a third-party trademark.

15 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.

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.