Banner Enterprise Identity Services Release Guide and Upgrade Guide

Release 8.1.1
February 2010

SUNGARD HIGHER EDUCATION

Prepared by: SunGard Higher Education

4 Country View Road
Malvern, Pennsylvania 19355
United States of America
(800) 522 - 4827

Customer Support Center Website

http://connect.sungardhe.com

Documentation Feedback

http://education.sungardhe.com/survey/documentation.html

Distribution Services E-mail Address

distserv@sungardhe.com

Revision History Log

Publication Date	Summary
February 2010	New version that supports Banner Enterprise Identity Services 8.1.1 software.

Think Before You Print.

Banner Enterprise Identity Services 8.1.1 Release Guide and Upgrade Guide

Contents

Introduction

This document summarizes the following enhancements that are being delivered in Banner® Enterprise Identity Services 8.1.1:

- Generation of Internet-native Banner (INB) passwords for Single Sign-On (SSO)
- Exclusion of tax ID from UDCIdentity messages (requires Banner General patch p1-8pw6xj_gen80300)
- Performance enhancement

This document also summarizes the problem resolutions that are being delivered in Banner Enterprise Identity Services 8.1.1.

Banner General dependency

Banner General 8.2, plus patch p1-41h1lh_gen80200, is the *minimum* version that supports Banner Enterprise Identity Services 8.1.1.

Banner General 8.3, plus patch p1-8pw6xj_gen80300, is the *recommended* version to support Banner Enterprise Identity Services 8.1.1. This Banner General patch provides the new tax ID functionality and defect corrections for Banner Enterprise Identity Services.

Note

Patch p1-8pw6xj_gen80300 can be applied to Banner General 8.2. However, the patch must be reapplied when you upgrade from Banner General 8.2 to Banner General 8.3.

Generation of INB passwords for SSO

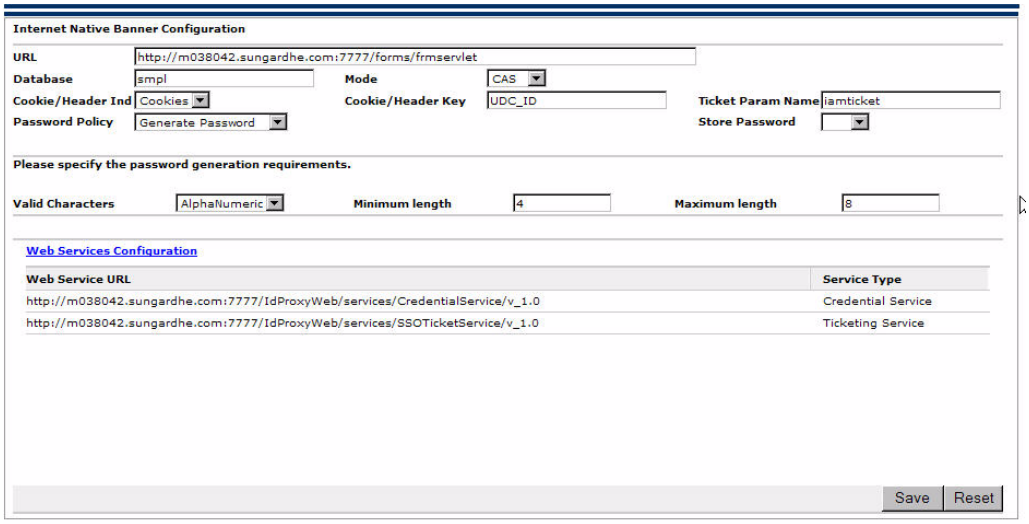
The Credential Web service stores credential information for Single Sign-On (SSO) between Internet-native Banner (INB) and other applications. Before this release, if the Credential Web service did not know the INB Oracle password for an end user, the user was prompted for the password. This behavior detracted from the SSO experience.

You can now configure the Banner Identity Gateway to automatically generate a password if the Credential Web service does not know the password. Configuration settings ensure that the password generation process conforms to Oracle password policy rules. If password generation is configured, users are never prompted for INB Oracle passwords, thus enhancing the SSO experience.

Use the following steps to configure the automatic generation of Oracle INB passwords.

1. Log in to the Banner Identity Gateway administrative interface (`http://<host>:<port>/bnigWeb`).

2. Select Application Config>Internet Native Banner from the menu bar. The following page is displayed:



3. In the **Password Policy** drop-down list, select *Generate Password*.

4. In the **Store Password** field, choose one of the following values:

YES	Store generated passwords for future SSO requests.
NO	Do not store generated passwords for future SSO requests.

5. Enter the following settings for your institution's password requirements:

Setting	Description
Valid characters	Valid characters for generated passwords: *AlphaNumeric* Both alphabetic and numeric characters *Numbers* Numeric characters only *Characters* Alphabetic characters only
Minimum length	Minimum length of generated passwords. Must be numeric.
Maximum length	Maximum length of generated passwords. Must be numeric.

6. Click **Save**.

Optional exclusion of tax ID

Before this release, UDCIdentity messages always included a tax ID. The tax ID (`SPBPERS_SSN`) stores a person's Social Security Number (U.S.), Social Insurance Number (Canada), or Tax Identification Number (other countries).

You can now optionally exclude tax IDs from UDCIdentity messages. The following new record on the Crosswalk Validation Form (GTVSDAX) controls the publication of tax IDs in UDCIdentity messages:

Internal Code	*IDM*
Internal Group	*TAXID*
External Code	*Y* - Publish tax IDs in UDCIdentity messages (default). Any other value - Do not publish tax IDs in UDCIdentity messages.
Description	*UDC IDM Person Tax ID*

If this GTVSDAX record is missing, UDCIdentity messages include tax IDs.

This enhancement requires Banner General patch p1-8pw6xj_gen80300. This patch includes a script that creates the new GTVSDAX record with the external code equal to *Y* (publish tax IDs). To exclude tax IDs from UDCIdentity messages, you must change the external code to another value.

This enhancement fulfills RPE 1-70XFV5.

Performance enhancement

The batch process that extracts UDCIdentity information from the database was updated to improve performance. Oracle database set based processing capabilities are used by invoking the `gp_udc_user_provisioning.f_lookup` function inside a select statement. Identities are now fetched in batches rather than one at a time. As a result, the database engine retrieves data more efficiently and the extract runs nearly ten times faster.

Problem resolutions

Banner Enterprise Identity Services 8.1.1 includes the following problem resolutions. Detailed description, impact, and resolution information for the problem resolutions is delivered in a separate file named `beis80101resolutions.txt`.

Component	Defect #	Summary
Enterprise Identity Proxy Services	1-6RYUHH	When the SPML Provisioning>View Messages menu option was selected, the first set of results was failures. However, the Message Status filter at the top of the page displayed 'Select.' It should have displayed 'FAILURE.'
Enterprise Identity Proxy Services	1-754A1F	Updates to the xpath expression in the Proxy Services were not being picked up.
Identity Data Export Utilities	1-8RR2CF	An XML parsing issue occurred when the XML contained special characters.
Identity Data Export Utilities	1-8RR2CH	JDBC URL validation was limited, and the validation did not allow URLs for Oracle RAC (Real Application Cluster).

Additional problem resolutions in Banner General patch p1-8pw6xj_gen80300 support Banner Enterprise Identity Services. Refer to the patch documentation for details about these problem resolutions.

Upgrade instructions

Upgrading Banner Enterprise Identity Services from version 8.1 to version 8.1.1 includes the following steps:

- Step 1, "Download upgrade files"
- Step 2, "Modify database schema"
- Step 3, "Define a new data source for generating INB Oracle passwords"
- Step 4, "Check for lock files"
- Step 5, "Redeploy Banner Identity Gateway"
- Step 6, "Redeploy Enterprise Identity Proxy Services"
- Step 7, "Redeploy Identity Data Export Utilities"

Step 1 Download upgrade files

Download and unzip `BEIS_8_1_1.zip` from the Customer Support Software Download Center. Download instructions are contained in `BEIS_8.1.1_readme.txt`, located on the download center.

Step 2 Modify database schema

The following modifications must be made to the database schema:

- Create the password specification parameters table
- Update the dependent packages that use the columns in the password specification parameters table
- Grant select privileges to `integmgr` on the tables that the Identity Data Export Utilities application uses during the batch extract process

Use the following steps to modify the database schema.

1. Extract the `BEIS_8_1_1.zip` archive file.
2. Change your working directory to `db-scripts/tables`.

```
cd <upgrade directory>/db-scripts/tables
```

3. Execute SQL*Plus and connect as user `bnixmgr`.
4. Execute the following script:

```
sql> @ db_upgrade_8_1_to_8_1_1.sql
sql> exit
```

5. Change your working directory to `db-scripts/packages`.

```
cd <upgrade directory>/db-scripts/packages
```

6. Execute SQL*Plus and connect as user `bnixmgr`.
7. Execute the following script:

```
sql> @ db_upgrade_8_1_to_8_1_1.sql
sql> exit
```

8. Change your working directory to `db-scripts/privileges`.
9. Execute SQL*Plus and connect as user `baninst1`.
10. Execute the following script:

```
sql> @ db_upgrade_8_1_to_8_1_1.sql
sql> exit
```

Step 3 Define a new data source for generating INB Oracle passwords

You need a new data source to dynamically generate or reset INB Oracle passwords during Single Sign-On. Use the following steps to define the Banner security user data source.

1. Connect to the Oracle Application Server Web application: `http://servername:adminport`. The system displays the Oracle Enterprise Manager console.
2. Click the name of the OC4J instance that hosts the components of Banner Enterprise Identity Services. The console displays the Home page for the selected instance.
3. Select the **Administration** tab.
4. Select Data Sources from the **Application Defaults** section. The console displays a list of data sources for the instance.
5. Click **Create** to create the data source. The console displays the Create Data Source page.
6. Use information in the following tables to set up the data source.

General	
Name	*Banner_security*
Data Source Class	*com.evermind.sql.DriverManagerDataSource*
JDBC URL	*jdbc:oracle:thin:@host:port:SID* where *host* = database host *port* = database listener port (usually *1521* or *1549*) *SID* = database instance
JDBC Driver	*oracle.jdbc.driver.OracleDriver*

Datasource Username and Password	
Username	Banner security user name (*bansecr*)
Use Clear Text Password	Select the **Use Cleartext Password** button and provide the password for the `bansecr` user.

JNDI Locations	
Location	*jdbc/inbadmin*
Transactional(XA) Location	*jdbc/xa/inbadmin*
EJB Location	*jdbc/ejb/inbadmin*

7. Click **Create**. The console displays a confirmation message.

8. Click **Yes** to restart the server.

9. When the server confirms that the instance was restarted, click **OK**. The console displays a list of all data sources.

Step 4 Check for lock files

Lock files can cause problems when you redeploy Banner Enterprise Identity Services. Use the following steps to check for lock files and remove any that exist.

1. Connect to the Oracle Application Server Web application: `http://servername:adminport/`. The system displays the Oracle Enterprise Manager console.

2. Stop the OC4J instance where the Banner Enterprise Identity Services components are deployed:

   2.1. Select the OC4J instance where the components are deployed.

   2.2. Click **Stop**. The console displays the Confirmation page.

   2.3. Click **Yes**. The system redisplays the console once the application stops.

3. Navigate to `OAS_HOME/j2ee/<instance_name>/persistence/<instance_name>_default_island_1`.

4. Remove any .lock files that exist.

5. Re-start the OC4J instance:

   5.1. Select the OC4J instance where the components are deployed.

   5.2. Click **Start**. The system displays the Processing: Start page, then redisplays the console once the application starts.

Step 5 Redeploy Banner Identity Gateway

Use the following steps to redeploy the Banner Identity Gateway.

1. Connect to the Oracle Application Server Web application: `http://servername:adminport/`. The system displays the Oracle Enterprise Manager console.

2. Click the name of the OC4J instance where the Banner Identity Gateway is deployed. The console displays the Home page for the selected instance.

3. Select the **Applications** tab. The console displays a list of deployed applications.

4. Select Banner Identity Gateway.

5. Click **Redeploy**. The console displays the Redeploy page.

6. Click **Browse** and navigate to the `bnig.ear` file in the `jee-apps` folder in the unzipped `BEIS_8_1_1.zip` file.

7. Click **Redeploy**. The console displays a confirmation message, after successful redeployment.

8. Click **OK**.

Step 6 Redeploy Enterprise Identity Proxy Services

Use the following steps to redeploy the Enterprise Identity Proxy Services.

1. Connect to the Oracle Application Server Web application: `http://servername:adminport/`. The system displays the Oracle Enterprise Manager console.

2. Click the name of the OC4J instance where the Enterprise Identity Proxy Services is deployed. The console displays the Home page for the selected instance.

3. Select the **Applications** tab. The console displays a list of deployed applications.

4. Select Enterprise Identity Proxy Services.

5. Click **Redeploy**. The console displays the Redeploy page.

6. Click **Browse** and navigate to the `IdProxy.ear` file in the `jee-apps` folder in the unzipped `BEIS_8_1_1.zip` file.

7. Click **Redeploy**. The console displays a confirmation message, after successful redeployment.

8. Click **OK**.

Step 7 Redeploy Identity Data Export Utilities

Use the following steps to redeploy the Identity Data Export Utilities. Be sure to back up the indicated files so they are not lost when the application is redeployed.

1. Copy and save the following properties files to a backup folder outside the application server's root directory.

Note

The properties files are located in the home directory of the OC4J instance where the Identity Data Export Utilities application is deployed.

Within the home directory, the files are located in `applications\<ideu_application_name>\IdentityDataExportUtilities\WEB-INF`.

```
properties\BannerLDIF.properties
properties\ldif_xpath_mapping.properties
properties\spml_endpoints.properties
properties\spml_publisher_config.properties
properties\UdcIdAssignmentConfig.properties
properties\UDCIdentityExtractor.properties
classes\udcBatchApp.properties
```

2. If you are using the default location of the working directory as specified in the `udcBatchApp.properties` file, back up the generated XML and LDIF files.

3. Connect to the Oracle Application Server Web application: `http://servername:adminport/`. The system displays the Oracle Enterprise Manager console.

4. Click the name of the OC4J instance where the Identity Data Export Utilities application is deployed. The console displays the Home page for the selected instance.

5. Select the **Applications** tab. The console displays a list of deployed applications.

6. Select Identity Data Export Utilities.

7. Click **Redeploy**. The console displays the Redeploy page.

8. Click **Browse** and navigate to the `IdentityDataExportUtilities.ear` file in the `jee-apps` folder in the unzipped `BEIS_8_1_1.zip` file.

9. Click **Redeploy**. The console displays a confirmation message, after successful redeployment.

10. Click **OK**.

11. Replace the properties files in the home directory with the backup files that were created in steps 1 and 2.

12. Restart the OC4J instance for the original properties to take effect.