ellucian™

Banner Enterprise Identity Services
Release and Upgrade Guide

Release 8.1.5
October 2011

Prepared by: Ellucian
4375 Fair Lakes Court
Fairfax, Virginia 22033
United States of America

Revision History

Publication Date	Summary
October 2011	New version that supports Banner Enterprise Identity Services 8.1.5 software.

Contents

Introduction

Banner® Enterprise Identity Services (BEIS) 8.1.5 introduces the SSO Manager, a new component that consolidates BEIS single sign on (SSO) functionality. This release guide provides an overview of the SSO Manage, describes other changes in BEIS 8.1.5, and provides upgrade instructions.

Note

Luminis® Platform 5.0, 5.0.1 and 5.0.2 are not compatible with BEIS 8.1.5. If you are running these versions of Luminis Platform, you must run BEIS 8.1.4 or earlier. This incompatibility is related to the way Luminis Platform 5.x handles deep-linking to Self-Service Banner.

SSO Manager

Banner Enterprise Identity Services (BEIS) 8.1.5 introduces the SSO Manager, a new component that consolidates BEIS single sign on (SSO) functionality. This consolidation allows you to install and manage SSO features separately from the account provisioning features of BEIS.

The SSO Manager provides a SSO gateway for Self-Service Banner (SSB) and Internet-native Banner (INB), allowing these applications to participate in a claims-based authentication environment. The SSO Manager also provides services that other Ellucian applications can use to facilitate claims-based authentication based on the UDCIdentifier.

This release guide provides an overview of the SSO Manager. Refer to Chapter 11, "SSO Manager," in the *Banner Enterprise Identity Services Handbook* (version 8.1.5) for details on the components, processing flow, and implementation of the SSO Manager.

SSO for Self-Service Banner (SSB)

The SSO Manager acts as a front-end to SSB, bypassing native SSB authentication. A central access manager handles authentication, protecting the SSB access URLs that are exposed by the SSO Manager. Once the central access manager authenticates the user, the SSO Manager collaborates with Banner Web Tailor to provide access to the user.

The following processing occurs when using the SSO Manager for single sign on to SSB:

1. The user opens a Web browser and requests access to SSB through a protected SSB URL.
2. Because the URL is protected by a central access manager, the user is redirected to the central access manager login page.
3. The user logs in to the central access manager.
4. The central access manager issues an SSO token to the user and forwards the request to the SSO Manager.
5. The SSO Manager uses the SSO token to retrieve the required user information (UDCIdentifier) from the identity vault and stores the UDCIdentifier in a cookie that it creates in the browser session.
6. Banner Web Tailor uses the UDCIdentifier to look up the Banner PIDM that is associated with the UDCIdentifier and creates a session for the user.

7. The SSO Manager redirects the user's browser to SSB.

8. Banner Web Tailor verifies that the session was started after authentication.

SSO for Internet-native Banner (INB)

The SSO Manager acts as a front-end to INB, bypassing native Banner authentication. A central access manager handles authentication, protecting the INB access URLs that are exposed by the SSO Manager. Once the central access manager authenticates the user, the SSO Manager collaborates with Oracle Forms runtime components to provide access to Banner.

The following processing occurs when using the SSO Manager for single sign on to INB:

1. The user opens a Web browser and requests access to INB through a protected INB URL.

2. Because the URL is protected by a central access manager, the user is redirected to the central access manager login page.

3. The user logs in to the central access manager.

4. The central access manager issues an SSO token to the user and forwards the request to the SSO Manager.

5. The SSO Manager uses the SSO token to obtain the required user information (UDCIdentifier) and creates a request scope INB ticket.

6. The baniam.jar obtains the user's credentials that are required to log the user into Oracle Forms and start the user session.

Application development with the SSO Manager

The SSO Manager contains services and features that can be used to develop single sign on capabilities for your institution's digital campus. The following features support single sign on, which may or may not involve Banner.

Deep-linking

Deep-linking is the ability to bypass a menu page and hyperlink directly to a specific page in Self-Service Banner or to a specific form in Internet-native Banner. The SSO Manager

supports deep-linking in both SSB and INB through the protected URLs that it exposes for accessing these applications. Applications that need to deep-link into either SSB or INB need to supply the appropriate URL parameters that identify the page or form to which the user should be transferred. Refer to Chapter 11, “SSO Manager,” in the *Banner Enterprise Identity Services Handbook* (version 8.1.5) for more details.

Ticketing and Credential Web services

The following services work together to provide credential information to Internet-native Banner:

- The Ticketing Web service provides an operation that generates a ticket (a globally unique identifier) for a given credential or credential identifier.
- The Credential Web service provides operations that store and retrieve credential information based on a ticket generated by the Ticketing Web service. The credential information is encrypted before being stored and decrypted when retrieved.

These services were previously exposed by the Enterprise Identity Proxy Services component. These services are now exposed by the SSO Manager.

These services can be used to develop SSO support for applications that require the user’s actual credentials for authentication. They provide a secure mechanism for requesting and retrieving application-specific credentials. Refer to Chapter 11, “SSO Manager,” in the *Banner Enterprise Identity Services Handbook* (version 8.1.5) for more details.

Validation services

The SSO Manager requires that the UDCIdentifier be retrieved to identify the user. If you are using CAS as your central access manager for BEIS 8.1.5, either the /bannerValidate service or the /samlValidate service must be used to retrieve the UDCIdentifier of an authenticated user. When you configure the SSO Manager, you must choose to use one of these services.

Before BEIS 8.1.5, /bannerValidate was required to retrieve the UDCIdentifier. Starting with BEIS 8.1.5, either /bannerValidate or /samlValidate is required to retrieve the UDCIdentifier. The /bannerValidate service is being phased out in the SSO Manager and other Ellucian applications. The /samlValidate service is recommended for any new applications that use CAS.

/bannerValidate

This service validates the CAS service ticket and returns a UDCIdentity XML fragment response to the calling application. This is a proprietary validation service. Ellucian provides CAS version-specific extensions that implement /bannerValidate.

/samlValidate

This service can be configured to retrieve the UDCIdentifier of the authenticated NetID via SAML (Security Assertion Markup Language). This service is provided natively in JA-SIG CAS starting with version 3.1.

The saml/Validate service is a feature of CAS, not a feature of the SSO Manager or any other BEIS component. Any applications that are being developed to use CAS should use the /samlValidate service rather than the /bannerValidate service.

SSO Manager without BEIS account provisioning

One of the fundamental principles of BEIS is the assignment of the UDCIdentifier to persons in the enterprise. BEIS account provisioning stores a person's UDCIdentifier in Banner and in the central identity vault. Correlating the UDCIdentifier in Banner and in the central identity vault facilitates single sign on.

To use the SSO Manager without BEIS account provisioning, you must correlate the globally unique identifier (GUID) that is stored in Banner with the GUID that is stored in the central identity vault. In Banner, a person's GUID is stored in the GOBUMAP table (`GOBUMAP_UDC_ID`). Although this column is designed to store the UDCIdentifier, any unique identifier for the person can be stored in this column. The same GUID must be stored in the central identity vault so it can be retrieved by the validation service (/bannerValidate or /samlValidate). As long as the GUIDs stored in these two repositories are correlated and retrievable as the UDCIdentifier, SSB and INB can be accessed through the SSO Manager.

Changes to Other BEIS Components

BEIS 8.1.5 includes the following changes to existing BEIS components.

Changes that support the SSO Manager

Before BEIS 8.1.5, SSO functionality was distributed among the BEIS components. The SSO Manager now consolidates SSO functionality into one component. This consolidation affects the following BEIS components:

- Banner Identity Gateway - The bnSSOWeb component and its configuration screens are disabled. The SSO Manager now performs proxy functionality that was previously performed by bnSSOWeb.
- Enterprise Identity Proxy Services - Previously, Proxy Services exposed the Ticketing and Credential Web services. The SSO Manager now exposes these Web services, which work together to provide credential information to Internet-native Banner.
- Banner CAS Client - This component is disabled. It is no longer needed due to the consolidation of SSO functionality in the SSO Manager.

Changes to the SPML LDAP Adapter

The SPML LDAP Adapter creates user accounts in an LDAP V3 compliant directory. Data elements in the UDCIdentity XML structure are mapped to LDAP attributes. Several elements in the UDCIdentity XML structure have recurring child attributes (for example, the institutionrole element). The adapter now recognizes recurring elements in a UDCIdentity message and populates multi-valued LDAP attributes. This enhancement allows an institution to populate its LDAP repository with role information as a child of the user attribute.

This enhancement addresses RPE 1-SDNW22.

Upgrade Instructions

This section provides instructions for upgrading to BEIS 8.1.5.

Note

Installation of BEIS 8.1.5 on Oracle WebLogic 11g was tested on versions 10.3.2 and 10.3.5. Documentation is based on version 10.3.2. There are minor documentation differences between installation on versions 10.3.2 and 10.3.5.

If your current BEIS is earlier than 8.1.3

If your current BEIS installation is earlier than BEIS 8.1.3, you must first upgrade to BEIS 8.1.3. Refer to the *Banner Enterprise Identity Services 8.1.3 Release and Upgrade Guide* for upgrade instructions.

After you upgrade to BEIS 8.1.3, you can use the following instructions to upgrade to BEIS 8.1.5.

If your current BEIS is 8.1.3 or 8.1.4

If your current BEIS installation is BEIS 8.1.3 or BEIS 8.1.4, the upgrade steps are almost identical. Minor differences are identified in the following instructions.

BEIS 8.1.5 includes changes to the Banner Identity Gateway, Enterprise Identity Proxy Services, and SPML LDAP Adapter. All three components should be upgraded. In addition, the new SSO Manager must be deployed.

Upgrade the Banner Identity Gateway

The following zip files are used to upgrade the Banner Identity Gateway:

- `Banner_IdentityGateway_full_release_Oracle.zip` is used for upgrading the Gateway on Oracle Application Server 10.1.3.4/5.
- `Banner_IdentityGateway_full_release_Weblogic.zip` is used for upgrading the Gateway on Oracle WebLogic Server 11g.

Use the following steps to deploy the 8.1.5 version of the Banner Identity Gateway.

Step 1 Configure the integmgr user password

To ensure optimal performance, the Gateway should refresh its database connection periodically. This requires that the Gateway be configured for the password of the `integmgr` user in your environment. Use the following steps to configure the password.

1. Extract the contents of the applicable zip file:

   ```
   jar xvf Banner_IdentityGateway_full_release_Oracle.zip
   ```
   or
   ```
   jar xvf Banner_IdentityGateway_full_release_Weblogic.zip
   ```

   The extract contains a directory named `jee-app`.

2. Navigate to the `jee-app` directory and execute the following command:

   ```
   jar xvf bnig.ear
   ```

   The extract contains a directory named `lib`.

3. Navigate to the `lib` directory and execute the following command:

   ```
   jar xvf bnigCore.jar BnigResources.properties
   ```

4. Open `BnigResources.properties`, which is extracted under the `lib` directory.

5. Modify the last two properties in the file:

`integmgr.pwd`	Password for the `integmgr` schema for your environment. Required.
`connection.refresh.count`	Frequency for creating a new connection. A new connection is created each time this number of message sets is processed. Default is 10000.

6. Save and close the file.

7. From the `lib` directory, execute the following command to rebuild `bnigCore.jar`:

   ```
   jar uvf bnigCore.jar BnigResources.properties
   ```

8. After this command runs successfully, delete `BnigResorces.properties` under the `lib` directory.

9. From the `jee-app` directory, execute the following command to rebuild the enterprise archive file:

   ```
   jar cvf bnig.ear *.war *.jar META-INF/* lib/*
   ```

   The rebuilt `bnig.ear` file is used for installation.

Step 2 Undeploy the current Gateway

Use the Enterprise Manager in Oracle Application Server 10.1.3.4/5 or the Oracle WebLogic Server 11g to undeploy the current Gateway.

Step 3 Recompile triggers for the Gateway

BEIS 8.1.5 includes an upgrade script that recompiles the triggers used in the Gateway error logging component. Use the following steps to apply this script.

1. Extract the contents of the applicable zip file:

   ```
   jar xvf Banner_IdentityGateway_full_release_Oracle.zip
   ```
   or
   ```
   jar xvf Banner_IdentityGateway_full_release_Weblogic.zip
   ```

2. Navigate to the `db-scripts\packages` directory.

3. Run SQL*Plus and connect as the `bnixmgr` user.

4. Execute the `db_upgrade_8_1_4_to_8_1_5.sql` script:

   ```
   sqlplus> @db_upgrade_8_1_4_to_8_1_5.sql
   ```

5. Exit SQL*Plus.

Step 4 Validate the application server configuration (OC4J only)

Installation instructions in previous versions of the *Banner Enterprise Identity Services Handbook* did not specify the creation of the `UDC_IDENTITY_SUBSCRIBER` connection factory as XA-enabled. On OC4J, this caused messages to be held in the UDCIdentity Topic after they were processed, resulting in the following problems:

- Previously processed messages were reprocessed when the OC4J container was restarted.
- Restart of the OC4J container was unreliable.
- Performance was degraded when the Proxy Services produced messages.

Check the configuration of the `UDC_IDENTITY_SUBSCRIBER` connection factory to determine whether it is XA-enabled. If it is not XA-enabled, use the following steps to remove and recreate the necessary connection factory.

1. On the Oracle Enterprise Manager console, click the name of the OC4J instance where the Gateway will be redeployed. The home page for the selected instance is displayed.

2. Click the **Administration** tab. A list of tasks is displayed.

3. Select **JMS Connection Factories** in the Enterprise Messaging Service section. The JMS Connection Factories page is displayed.

4. Delete the existing configuration for `jms/UDC_IDENTITY_TCF`.

5. Click **Create New**. The Add Connection Factory page is displayed.

6. Enter the following information to create a connection factory:

Connection Factory Type	*Topic*
JNDI Location	*jms/UDC_IDENTITY_TCF*
Host	*[ALL]*
Client Identifier	Leave blank
XA Enabled	checked (yes)

7. Click **OK**. The JMS Connection Factories page is redisplayed.

8. Restart the OC4J container for the changes to take effect.

Step 5 Deploy the new Gateway

You can reuse all previously configured data sources, JMS queues and topics, and security users. All that is needed is to deploy the new `bnig.ear` to your application server.

Refer to Chapter 7, "Banner Identity Gateway," of the *Banner Enterprise Identity Services Handbook* (version 8.1.5) for instructions. The specific step depends on your application server:

- Oracle Application Server 10.1.3.4/5 - Use "Step 9 - Deploy the Banner Identity Gateway" in the instructions for Oracle Application Server 10.1.3.4/5.
- Oracle WebLogic Server 11g - Use "Step 12 - Deploy the Banner Identity Gateway" in the instructions for Oracle WebLogic Server 11g.

Upgrade the Enterprise Identity Proxy Services

The following zip files are used to upgrade the Enterprise Identity Proxy Services:

- `Banner_IdentityProxy_full_release_Oracle.zip` is used for upgrading the Identity Proxy on Oracle Application Server 10.1.3.4/5.
- `Banner_IdentityProxy_full_release_Weblogic.zip` is used for upgrading the Identity Proxy on Oracle WebLogic Server 11g.

Use the following steps to update processing properties (if needed) and deploy the 8.1.5 version of the Enterprise Identity Proxy Services.

Step 1 Update processing properties (if needed)

The Proxy Services component is delivered with default values in the `spml.properties` file. Most installations should not change these properties. Some installations, however, can change these properties to improve performance, depending on the capabilities of the adapter(s) to which the Proxy Services application provisions.

If processing properties were changed for your current installation, use the following steps to update the properties in the 8.1.5 version of the Proxy Services.

1. Extract the contents of the applicable zip file:

   ```
   jar xvf Banner_IdentityProxy_full_release_Oracle.zip
   ```
   or
   ```
   jar xvf Banner_IdentityProxy_full_release_Weblogic.zip
   ```

   The extract contains a directory named `jee-apps`.

2. Navigate to the `jee-apps` directory and execute the following command:

   ```
   jar xvf IdProxy.ear
   ```

   The extract contains an archive named `IdProxyEJB.jar`.

3. From the `jee-apps` directory, execute the following command:

   ```
   jar xvf IdProxyEJB.jar spml.properties
   ```

4. Open `spml.properties`, which is extracted under the `jee-apps` directory.

5. Modify any default values to meet your requirements.

6. Save and close the file.

7. From the `jee-apps` directory, execute the following command to rebuild `IdProxyEJB.jar`:

   ```
   jar uvf IdProxyEJB.jar spml.properties
   ```

8. After this command runs successfully, delete `spml.properties` under the `jee-apps` directory.

9. From the `jee-apps` directory, execute the following command to rebuild the enterprise archive file:

   ```
   jar cvf IdProxy.ear *.war *.jar lib/* META-INF/*
   ```

   The rebuilt `IdProxy.ear` file is used for installation.

Step 2 Undeploy current Proxy Services

Use the Enterprise Manager in Oracle Application Server 10.1.3.4/5 or Oracle WebLogic Server 11g to undeploy the current Proxy Services.

Step 3 Create an index on the T_UDC_SPML_MSG_LOG table

Note

If you are upgrading from BEIS 8.1.4, you can skip this step. If you are upgrading from BEIS 8.1.3, you must do this step. ■

BEIS 8.1.4 included an update script to create an index on the `T_UDC_SPML_MSG_LOG` table to improve performance. Use the following steps to apply this script.

1. Extract the contents of the applicable zip file:

   ```
   jar xvf Banner_IdentityProxy_full_release_Oracle.zip
   ```
   or
   ```
   jar xvf Banner_IdentityProxy_full_release_Weblogic.zip
   ```

2. Navigate to the `db-scripts\upgrade-scripts` folder.

3. Run SQL*Plus and connect as the `identmgr` user.

4. Execute the `db_upgrade_8_1_3_to_8_1_4.sql` script:

   ```
   sqlplus> @db_upgrade_8_1_3_to_8_1_4
   ```

5. Exit SQL*Plus.

Step 4 Deploy the new Proxy Services

You can reuse all previously configured data sources, JMS queues and topics, and security users. All that is needed is to deploy the new `idproxy.ear` file to your application server.

Refer to Chapter 8, “Enterprise Identity Proxy Services,” of the *Banner Enterprise Identity Services Handbook* (version 8.1.5) for instructions. The specific step depends on your application server:

- Oracle Application Server 10.1.3.4/5 - “Use Step 6 - Install the Proxy Services” in the instructions for Oracle Application Server 10.1.3.4/5.
- Oracle WebLogic Server 11g - Use “Step 9 - Install the Proxy Services” in the instructions for Oracle WebLogic Server 11g.

Upgrade the SPML LDAP Adapter

The `ldap_spml_psp_full_release.zip` file is used for upgrading the SPML LDAP Adapter on both Oracle Application Server 10.1.3.4/5 and on Oracle WebLogic Server

11g. Use the following steps to configure and deploy the 8.1.5 version of the SPML LDAP Adapter.

1. Extract the contents of the `ldap_spml_psp_full_release.zip` file.

2. Extract the `ldap-spml-psp.ear` file, configure the SPML LDAP Adapter, and rebuild the ear file.

   Refer to Chapter 10, "SPML LDAP Adapter," of the *Banner Enterprise Identity Services Handbook* (version 8.1.5) for instructions. The specific steps depend on your application server (Oracle Application Server 10.1.3.4/5 or Oracle WebLogic Server 11g).

3. Use the Enterprise Manager in Oracle Application Server 10.1.3.4/5 or Oracle WebLogic Server 11g to undeploy the current SPML LDAP Adapter.

4. Deploy the new `ldap-spml-psp.ear` file to your application server.

   Refer to Chapter 10, "SPML LDAP Adapter," of the *Banner Enterprise Identity Services Handbook* (version 8.1.5) for instructions. The specific steps depend on your application serve (Oracle Application Server 10.1.3.4/5 or Oracle WebLogic Server 11g).

Deploy the SSO Manager

Use the following steps to deploy the SSO Manager.

Prerequisites

- JDK 1.6 must be installed.
- The environment variable `'JAVA_HOME'` must be set.
- A user account that has privileges to create users must be identified or created. This account is needed when you run the SSO Manager installation utility.

Step 1 Implement the SSO Manager

Use the steps in Chapter 11, "SSO Manager," in the *Banner Enterprise Identity Services Handbook* (version 8.1.5) to implement the SSO Manager.

Note

If you are using self-signed certificates (not recommended for anything other than a test or development environment), ensure that the certificate from your CAS server is imported into the keystore of the JVM where the SSO Manager is deployed (if using SSL).

Step 2 Protect the SSO Manager URL

If you are using CAS as your central access manager, configure the CAS server to protect the SSO Manager URL. Refer to Appendix D, "CAS Installation and Configuration," in the *Banner Enterprise Identity Services Handbook* (version 8.1.5) for details on using the CAS server management tool to protect the SSO Manager.

Step 3 Verify the configuration of baniam.jar

The baniam.jar component is delivered with Banner General. For previous BEIS releases, the baniam.jar component was configured to communicate with the Credential Web service that was exposed by the Enterprise Identity Proxy Services. The jar file must be reconfigured to communicate with the Credential Web service that is now exposed by the SSO Manager. Verify that baniam.jar was reconfigured when the SSO Manager was implemented in step 1.

Step 4 Reconfigure applications to access Banner via the SSO Manager

Reconfigure applications that access Banner via links to the Banner CAS Client (CAS mode) or the Banner Identity Gateway (third-party mode) to link through the SSO Manager instead.

In a CAS-based environment, the following URLs are exposed by the SSO Manager:

SSB	`http(s)://<host>:<port>/ssomanager/c/SSB`
INB	`http(s)://<host>:<port>/ssomanager/c/INB`

In a third-party-based environment, the following URLs are exposed by the SSO Manager:

SSB	`http(s)://<host>:<port>/ssomanager/c/auth/SSB`
INB	`http(s)://<host>:<port>/ssomanager/c/auth/INB`