



# **Banner Enterprise Identity Services** Release and Upgrade Guide

Release 8.2.1  
March 2015



Without limitation: Ellucian®, Banner®, Colleague®, and Luminis® are trademarks of the Ellucian group of companies that are registered in the U.S. and certain other countries; and Ellucian Advance™, Ellucian Course Signals™, Ellucian Degree Works™, Ellucian PowerCampus™, Ellucian Recruiter™, Ellucian SmartCall™, are also trademarks of the Ellucian group of companies. Other names may be trademarks of their respective owners.

©2015 Ellucian.

Contains confidential and proprietary information of Ellucian and its subsidiaries. Use of these materials is limited to Ellucian licensees, and is subject to the terms and conditions of one or more written license agreements between Ellucian and the licensee in question.

In preparing and providing this publication, Ellucian is not rendering legal, accounting, or other similar professional services. Ellucian makes no claims that an institution's use of this publication or the software for which it is provided will guarantee compliance with applicable federal or state laws, rules, or regulations. Each organization should seek legal, accounting, and other similar professional services from competent providers of the organization's own choosing.

Ellucian  
4375 Fair Lakes Court  
Fairfax, VA 22033  
United States of America

# Contents

---

<b>Introduction</b> .....	<b>4</b>
<b>Enhancements to SSO Manager</b> .....	<b>5</b>
<b>Resolutions</b> .....	<b>6</b>
<b>Upgrade Instructions</b> .....	<b>7</b>
<b>Download BEIS 8.2.1</b> .....	<b>8</b>
<b>Upgrade Banner Identity Gateway and Banner Identity Proxy to 8.2.1</b> .....	<b>8</b>
Automated upgrade for Banner Identity Gateway and Banner Identity Proxy .....	<b>8</b>
Manual upgrade for Banner Identity Gateway and Banner Identity Proxy .....	<b>24</b>
<b>Upgrade SSO Manager to 8.2.1</b> .....	<b>46</b>
Automated upgrade for SSO Manager.....	<b>46</b>
Manual upgrade for SSO Manager.....	<b>55</b>

# Introduction

---

Banner® Enterprise Identity Services (BEIS) is a collection of Banner components that support your institution's identity and access management architecture. This document describes the enhancements, resolutions, and upgrade instructions for BEIS 8.2.1.

You must be on BEIS 8.2 before you upgrade to BEIS 8.2.1.

BEIS 8.2.1 is supported on Oracle WebLogic Server 11g. BEIS 8.2.1 is not supported on previous Oracle application servers.

All BEIS 8.2.1 components were tested and certified on Java 7.

# Enhancements to SSO Manager

---

The SSO Manager acts as a single sign on gateway for Internet-Native Banner (INB) and Self-Service Banner (SSB).

BEIS 8.2.1 updates the SSO Manager to allow multiple login sessions for a Banner user. This feature supports performance testing for SSO to INB with a single user account.

# Resolutions

---

The Banner Enterprise Identity Services 8.2.1 Resolutions Report is a companion to this document. The Resolutions Report provides summary information about the change requests that are resolved in Banner Enterprise Identity Services 8.2.1. Use the following steps to access the Resolutions Report on the Ellucian Support Center:

1. Go to <https://ellucian.force.com/clients/home/home.jsp>.
2. Sign in to the Ellucian Support Center.
3. Select the **Documentation Libraries** tab.
4. Search for the Banner Enterprise Identity Services Resolutions 8.2.1 Report.

# Upgrade Instructions

---

This section provides instructions for upgrading from BEIS 8.2 to BEIS 8.2.1. You must be on BEIS 8.2 before you upgrade to BEIS 8.2.1. If you are on an earlier version, you must upgrade to BEIS 8.2 before you upgrade to BEIS 8.2.1.

The upgrade from BEIS 8.2 to BEIS 8.2.1 involves the following tasks:

1. Download BEIS 8.2.1.
2. Upgrade the Banner Identity Gateway and the Banner Identity Proxy. These components must be upgraded together. You can choose an automated upgrade process or a manual upgrade process.
3. Upgrade the SSO Manager. You can choose an automated upgrade process or a manual upgrade process.

The upgrade process updates the following database components and application server components:

Database Components	Application Server Components
Banner Identity Gateway schema - BNIXMGR	JEE applications
Banner Identity Proxy schema - IDENTMGR	
SSO Manager schema - SSOMGR	

Database components must be upgraded with a manual process. Some application server components can be upgraded with a manual process or an automated process. Where applicable, both automated upgrade instructions and manual upgrade instructions are provided. You can choose which method you wish to use.

## Download BEIS 8.2.1

---

Use the following steps to download BEIS 8.2.1:

1. Download `BEIS_8.2.1.zip` from the Ellucian Download Center. The file is located under the Banner General product.
2. Extract `BEIS_8.2.1.zip`.
3. Navigate to the `Deployables` directory.
4. Identify the BEIS components that will be upgraded:

Component	Zip file name	Function
Banner Identity Gateway	<code>IdGtwyPrxy_8.2.zip</code>	Creates and publishes identity messages based on changes to identity data in the Banner database
Banner Identity Proxy	<code>IdGtwyPrxy_8.2.zip</code>	Propagates identity messages to SPML-enabled applications
SSO Manager	<code>SSOManager_8.2.zip</code>	Provides a single sign on (SSO) gateway for Internet-Native Banner (INB) and Self-Service Banner (SSB)

## Upgrade Banner Identity Gateway and Banner Identity Proxy to 8.2.1

---

You can choose an automated upgrade process or a manual upgrade process.

### Automated upgrade for Banner Identity Gateway and Banner Identity Proxy

The Banner Identity Gateway and the Banner Identity Proxy must be upgraded together. Use the following steps if you choose an automated upgrade process:

- [Step 1 - Verify the BEP installation](#)
- [Step 2 - Enable cross domain security](#)
- [Step 3 - Delete deprecated objects](#)

- [Step 4 - Upgrade the database schema](#)
- [Step 5 - Run the automated installer](#)
- [Step 6 - Evaluate the environment](#)
- [Step 7 - Verify that messaging is working](#)
- [Step 8 - Confirm access to the Banner Identity Gateway and the Banner Identity Proxy](#)
- [Step 9 - Configure the Banner Identity Gateway and the Banner Identity Proxy](#)

The following sections provide details for each step.

## Step 1 - Verify the BEP installation

Verify that the Banner Event Publisher (BEP) is installed and configured. Refer to Chapter 2, "Preinstallation," in the *Banner Enterprise Identity Services 8.2. Installation Guide* for details.

## Step 2 - Enable cross domain security



**Note:** This step is required only if BEIS and BEP are deployed on separate Oracle WebLogic Server domains. Skip this step if BEIS and BEP are deployed on the same Oracle WebLogic Server domain.

Skip this step if cross domain security was previously enabled during the BEIS 8.2 deployment.

Cross domain security establishes trust between two Oracle WebLogic Server domains. A trust relationship is established when the domain credential for one domain matches the domain credential for the other domain.

By default, the domain credential is randomly created the first time an Oracle WebLogic Server domain is started. This process ensures that each Oracle WebLogic Server domain has a unique credential.

To enable trust between the BEIS and BEP Oracle WebLogic Server domains, you must update the credential of each domain so they match. Use the following steps to enable cross domain security for the BEIS and BEP Oracle WebLogic Server domains.

1. Connect to the Oracle WebLogic Server administration console:

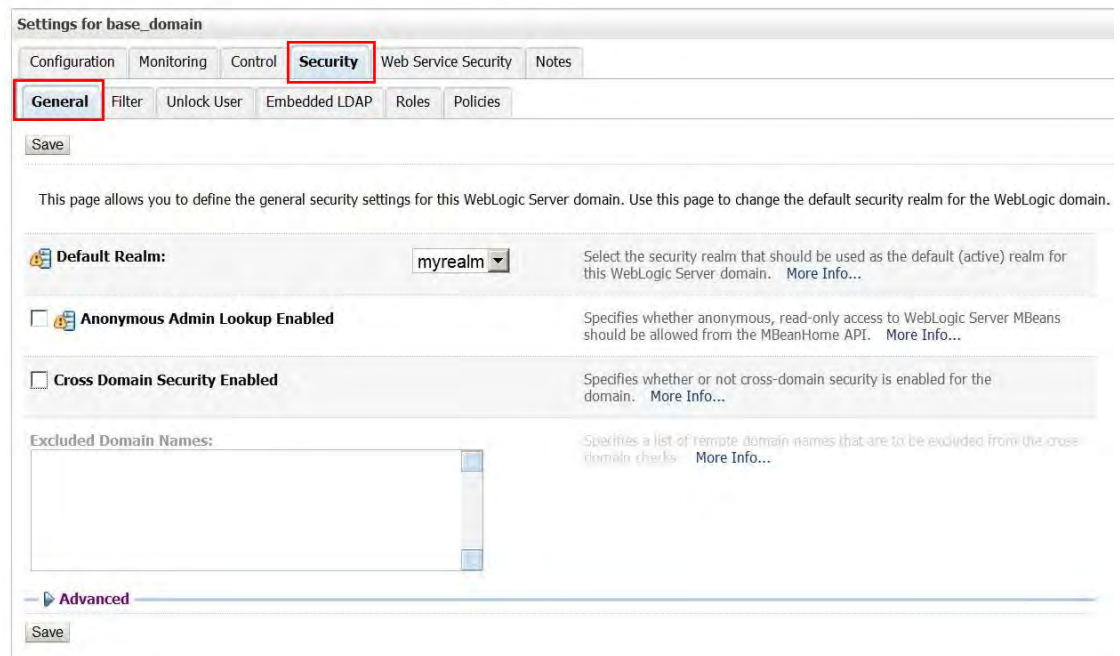
```
http://<host>:<port>/console
```

2. In the Change Center pane, click **Lock & Edit**.

3. In the Domain Structure pane, click the name of the BEIS domain. (When you repeat this step for the BEP domain, click the name of the BEP domain.)



4. Select the **Security > General** tab.



5. Select the **Cross Domain Security Enabled** check box.

Settings for base\_domain

Configuration Monitoring Control **Security** Web Service Security Notes

General Filter Unlock User Embedded LDAP Roles Policies

Save

This page allows you to define the general security settings for this WebLogic Server domain. Use this page to change the default security realm for the WebLogic domain.

**Default Realm:** myrealm Select the security realm that should be used as the default (active) realm for this WebLogic Server domain. [More Info...](#)

**Anonymous Admin Lookup Enabled** Specifies whether anonymous, read-only access to WebLogic Server MBeans should be allowed from the MBeanHome API. [More Info...](#)

**Cross Domain Security Enabled** Specifies whether or not cross-domain security is enabled for the domain. [More Info...](#)

**Excluded Domain Names:** Specifies a list of remote domain names that are to be excluded from the cross-domain checks. [More Info...](#)

Advanced

Save

6. Click **Save**.

7. Click **Advanced**.

Settings for base\_domain

Configuration Monitoring Control **Security** Web Service Security Notes

General Filter Unlock User Embedded LDAP Roles Policies

Save

This page allows you to define the general security settings for this WebLogic Server domain. Use this page to change the default security realm for the WebLogic domain.

**Default Realm:** myrealm Select the security realm that should be used as the default (active) realm for this WebLogic Server domain. [More Info...](#)

**Anonymous Admin Lookup Enabled** Specifies whether anonymous, read-only access to WebLogic Server MBeans should be allowed from the MBeanHome API. [More Info...](#)

**Cross Domain Security Enabled** Specifies whether or not cross-domain security is enabled for the domain. [More Info...](#)

**Excluded Domain Names:** Specifies a list of remote domain names that are to be excluded from the cross-domain checks. [More Info...](#)

Advanced

Save

8. Update the following information:

**Credential** Credential for the Oracle WebLogic Server domain. Use a credential that can be shared by the BEIS and the BEP Oracle WebLogic Server domains.

**Confirm Credential** Confirmation of the credential for the Oracle WebLogic Server domain

The screenshot shows the 'Settings for base\_domain' page in the Oracle WebLogic Administration Console. The 'Security' tab is selected, and the 'General' sub-tab is active. The 'Credential' and 'Confirm Credential' fields are highlighted with a red box. The 'NodeManager Username' field is set to 'weblogic'.

Settings for base\_domain

Configuration Monitoring Control **Security** Web Service Security Notes

General Filter Unlock User Embedded LDAP Roles Policies

Save

This page allows you to define the general security settings for this WebLogic Server domain. Use this page to change the default security realm for the WebLogic domain.

**Default Realm:** myrealm Select the security realm that should be used as the default (active) realm for this WebLogic Server domain. [More Info...](#)

**Anonymous Admin Lookup Enabled** Specifies whether anonymous, read-only access to WebLogic Server MBeans should be allowed from the MBeanHome API. [More Info...](#)

**Cross Domain Security Enabled** Specifies whether or not cross-domain security is enabled for the domain. [More Info...](#)

**Excluded Domain Names:** Specifies a list of remote domain names that are to be excluded from the cross-domain checks. [More Info...](#)

**Advanced**

**Security Interoperability Mode:** default Specifies the security mode of the communication channel used for XA calls between servers that participate in a global transaction. All server instances in a domain must have the same security mode setting. [More Info...](#)

**Credential:** The credential for this WebLogic Server domain. When a domain is created, a unique credential is generated for the domain. If you want to establish trust between two or more domains, decide on a credential that will be shared by the domains, then specify it here and in the other domains. [More Info...](#)

**Confirm Credential:**

**NodeManager Username:** weblogic The user name that the Administration Server uses to communicate with Node Manager when starting, stopping, or restarting Managed Servers. [More Info...](#)

9. Click **Save**.

10. In the Change Center pane, click **Activate Changes**.

11. Shut down all Managed Servers in the domain.

12. Shut down the Admin Server.

13. Start the Admin Server.

14. Start all Managed Servers in the domain.

15. Repeat steps 1 through 14 for the BEP Oracle WebLogic Server domain. Enter the same credential that was used for the BEIS Oracle WebLogic Server domain.

### Step 3 - Delete deprecated objects

Use the Oracle WebLogic Server administration console to delete the Banner Identity Gateway 8.2 and Banner Identity Proxy 8.2 applications.

### Step 4 - Upgrade the database schema

Use the following steps to upgrade the database packages that are required by the Banner Identity Gateway and the Banner Identity Proxy.

1. Extract `IdGtwyPrxy_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/bnig/packages`.
3. Connect to the database instance where BEIS is installed as the `BNIXMGR` user.
4. Execute `iokp_build.sql` to upgrade the database packages:  

```
sqlplus> @iokp_build
```
5. Execute the following command to reset the package variables:  

```
sqlplus> exec DBMS_SESSION.RESET_PACKAGE;
```
6. Exit SQL\*Plus.
7. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/idproxy/packages`.
8. Connect to the database instance where BEIS is installed as the `IDENTMGR` user.
9. Execute `iokp_build.sql` to upgrade the database packages:  

```
sqlplus> @iokp_build
```
10. Execute the following command to reset the package variables:  

```
sqlplus> exec DBMS_SESSION.RESET_PACKAGE;
```
11. Exit SQL\*Plus.

### Step 5 - Run the automated installer

The automated installer *must* be run on the Oracle WebLogic Server to configure the following files:

<code>bnig.ear</code>	Banner Identity Gateway
<code>IdProxy.ear</code>	Banner Identity Proxy

Use the following steps to run the automated installer.

1. Extract `IdGtwyPrxy_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.

2. Open a command prompt and navigate to `<ZIP_HOME>/ant-installer`.
3. Execute the following command:

```
java -jar gtwy-prxy-weblogic-installer.jar
```

The automated installer is launched. The user interface depends on whether you are running in a windowing (GUI) or non-windowing (command-line) environment. The remaining instructions are based on using the GUI for configuration. Configuration options are identical for a command-line interface.



**Note:** In command-line mode, each configuration option is displayed with the default value in brackets. To accept the default value, press Enter on your keyboard. To enter a different value, enter the correct value and press Enter on your keyboard. Valid values for the configuration options are *true* and *false*. All values must be entered without leading and trailing spaces.



4. Click **Next**.

5. Select the following check boxes:

**Configure and Save EAR Files**

**Deploy Banner Identity Gateway**

**Deploy Banner Identity Proxy**



6. Click **Next**.

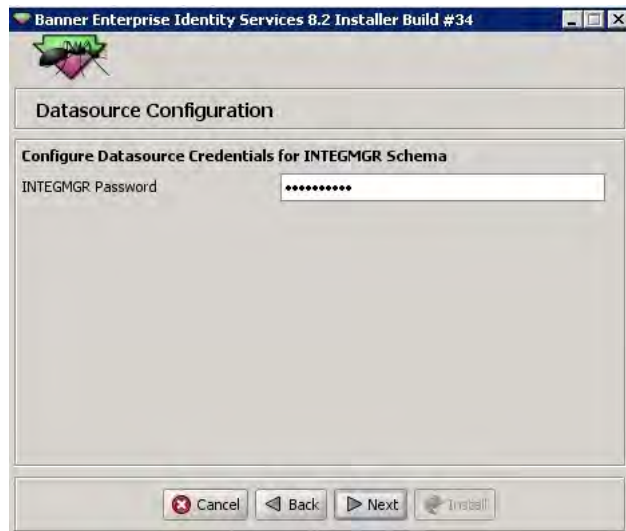
7. Enter the following Banner Event Publisher (BEP) information:

<b>BEP Server Host</b>	BEP server host name
<b>BEP Server Port</b>	Port number where BEP is running
<b>BEP Server Username</b>	User name for the administrator of the application server where BEP is deployed
<b>BEP Server Password</b>	Password for the administrator of the application server where BEP is deployed



8. Click **Next**.

9. Enter the password for the INTEGMR account.



10. Click **Next**.

- Click **Select Folder** and browse to the location where you want to save `bnig.ear` and `IdProxy.ear`.



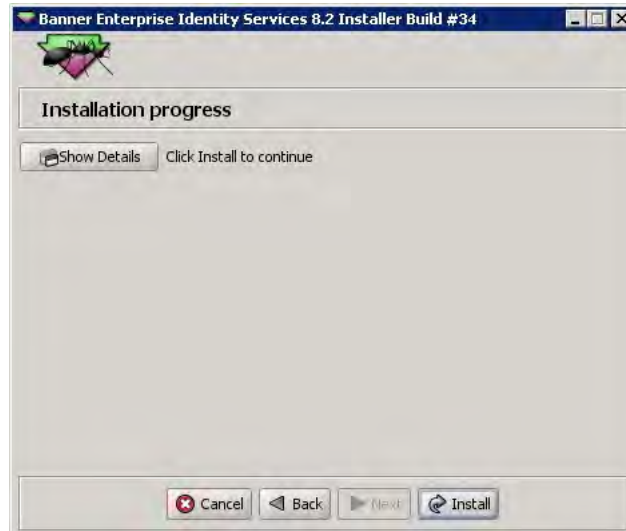
- Click **Next**.

- Enter the following application server information:

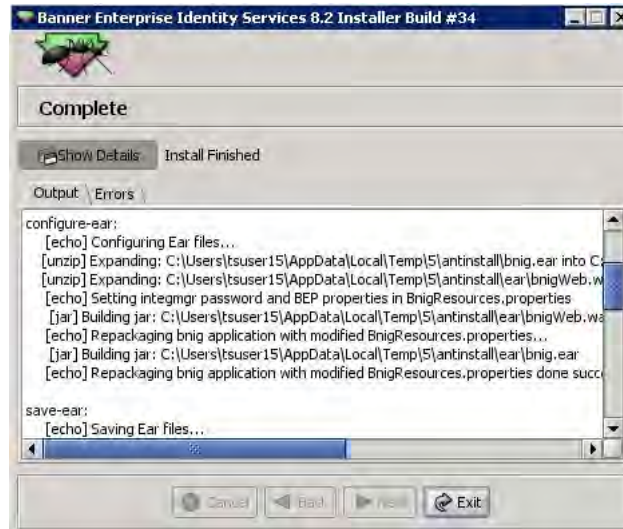
<b>WebLogic Server Home Directory</b>	Path of the Oracle WebLogic Server home directory (for example, <code>C:\Oracle\Middleware\wlserver_10.3</code> )
<b>Weblogic Admin Username</b>	User name for the application server administrator
<b>Weblogic Admin Password</b>	Password for the application server administrator
<b>Weblogic Server Host</b>	IP address or host name of the machine where the Oracle WebLogic Server is installed
<b>Weblogic Admin Sever Port</b>	Port where the Oracle WebLogic Server is running
<b>Weblogic Managed Server Name</b>	Name of the Oracle WebLogic Managed Server where the data sources are created, the JMS artifacts are created, and the applications are deployed



- 14. Click **Next**.
- 15. Click **Show Details**.
- 16. Click **Install**.



Installation details are displayed as the installation progresses.



The message *Install Finished* is displayed when the installation is complete. The `bnig.ear` and `IdProxy.ear` files are saved in the selected folder.

## Step 6 - Evaluate the environment

After you upgrade the Banner Identity Gateway and the Banner Identity Proxy, you should run `post_install_beis_checksript.sql` to evaluate your environment and identify potential problems. This script reports on several criteria that are essential for a fully functioning BEIS environment. You can use the script to evaluate both new installations and upgrades. Depending on the current state of your Banner/Oracle RDBMS environment, you might need to make changes based on the output of the script.

Use the following steps to run the check script and evaluate the results.

1. Extract `IdGtwyPrxy_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/util`.
3. Ensure that `post_install_beis_checksript.sql` has read permission.
4. Connect to SQL\*Plus as the `BANINST1` user.
5. Execute `post_install_beis_checksript.sql`:  

```
sqlplus> @post_install_beis_checksript
```
6. When prompted, enter the following information:
  - Username for the `BNIXMGR` schema (for example, `BNIXMGR`)
  - Username for the `IDENTMGR` schema (for example, `IDENTMGR`)
7. Exit SQL\*Plus.

8. Evaluate the results as follows:

Result	Evaluation
BNIXMGR schema	The BNIXMGR schema must exist.
Roles assigned to BNIXMGR	The following roles must be assigned to BNIXMGR: <ul style="list-style-type: none"> <li>• RESOURCE</li> <li>• CONNECT</li> </ul>
Privileges granted to BNIXMGR	The following privileges must be granted to BNIXMGR: <ul style="list-style-type: none"> <li>• DROP PUBLIC SYNONYM</li> <li>• CREATE PUBLIC SYNONYM</li> <li>• UNLIMITED TABLESPACE</li> <li>• CREATE SESSION</li> <li>• CREATE SYNONYM</li> <li>• CREATE VIEW</li> </ul>
Database objects in BNIXMGR database schema	The BNIXMGR schema should have the following tables: <ul style="list-style-type: none"> <li>• BNIXVAL</li> <li>• GTWMETA</li> <li>• PSPALOG</li> <li>• T_UDC_ERROR_LOG</li> <li>• T_UDC_ERROR_LOG_H</li> </ul>
Sequences that belong to BNIXMGR	The BNIXMGR schema should have the following sequences: <ul style="list-style-type: none"> <li>• T_UDC_ERROR_LOG_SEQ</li> <li>• T_UDC_ERROR_LOG_H_SEQ</li> <li>• PSPALOG_SEQ</li> </ul>
Views that belong to BNIXMGR	The BNIXMGR schema should have the VW_UDC_ERROR_LOG view.
Triggers that belong to BNIXMGR	The BNIXMGR schema should have the following triggers: <ul style="list-style-type: none"> <li>• TRG_UDC_ERROR_LOG_BUS</li> <li>• TRG_UDC_ERROR_LOG_BUR</li> <li>• TRG_UDC_ERROR_LOG_AUS</li> </ul>
Packages that belong to BNIXMGR	The BNIXMGR schema should have the following packages: <ul style="list-style-type: none"> <li>• IOKP_GTW_METADATA</li> <li>• IOKP_UDC_ERROR_LOG</li> <li>• IOKP_PSPALOG</li> <li>• IOKP_UDC_ERROR_LOG_H</li> </ul>
IDENTMGR schema	The IDENTMGR schema must exist.

<b>Result</b>	<b>Evaluation</b>
Roles assigned to IDENTMGR	The following roles must be assigned to IDENTMGR: <ul style="list-style-type: none"> <li>• RESOURCE</li> <li>• CONNECT</li> </ul>
Privileges granted to IDENTMGR	The following privileges must be granted to IDENTMGR: <ul style="list-style-type: none"> <li>• CREATE VIEW</li> <li>• UNLIMITED TABLESPACE</li> <li>• DROP PUBLIC SYNONYM</li> <li>• CREATE PUBLIC SYNONYM</li> <li>• CREATE SYNONYM</li> <li>• CREATE SESSION</li> </ul>
Database objects in IDENTMGR database schema	The IDENTMGR schema should have the following tables: <ul style="list-style-type: none"> <li>• T_UDC_PST_LIST</li> <li>• T_UDC_SPML_MSG_BALANCER</li> <li>• T_UDC_SPML_MSG_LOG</li> <li>• T_UDC_SPML_RES_ERROR_LOG</li> </ul>
Sequences that belong to IDENTMGR	The IDENTMGR schema should have the following sequences: <ul style="list-style-type: none"> <li>• T_UDC_PST_LIST_SEQ</li> <li>• T_UDC_SPML_MSG_LOG_SEQ</li> <li>• T_UDC_SPML_RES_ERROR_LOG_SEQ</li> </ul>
Packages that belong to IDENTMGR	The IDENTMGR schema should have the following packages: <ul style="list-style-type: none"> <li>• IOKP_UDC_SPML_MSG_LOG</li> <li>• IOKP_UDC_PST</li> </ul>

### Step 7 - Verify that messaging is working

During the BEIS 8.2 installation, seed data for BEISIdentityEvent was loaded into the Banner Event Publisher (BEP). BEP uses this event to capture identity data changes in Banner, evaluate the changes, and publish XML messages for BEIS processing.

Use the following steps to verify that the seed data was loaded and that BEP is publishing XML messages properly.

1. Log in to Internet-Native Banner (INB).
2. Access the Identification (SPAIDEN) form.
3. Change the first name of a person.
4. Save the change.

- Connect to the Oracle WebLogic Server administration console:  
`http://<host>:<port>/console`
- In the Domain Structure pane, expand and click **Services > Messaging > JMS Servers**.



- Click the name of the JMS server that was created for BEP.

**Summary of JMS Servers**

JMS servers act as management containers for the queues and topics in JMS modules that are targeted to them. This page summarizes the JMS servers that have been created in the current WebLogic Server domain.

[Customize this table](#)

**JMS Servers (Filtered - More Columns Exist)**

New Delete Previous | Next

<input type="checkbox"/>	Name ^	Persistent Store	Target	Current Server	Health
<input type="checkbox"/>	bepJMSServer	BEPFileStore	BEPmanagedServer	BEPmanagedServer	

New Delete Previous | Next

- Select the **Monitoring > Monitoring** tab on the Settings page.

**Settings for bepJMSServer**

Configuration Logging Targets **Monitoring** Control Notes

**Monitoring** Paging Store Active Destinations Active Transactions Active Connections Active Session Pools Active Pooled Connections

Use this page to view runtime statistics for all of the active JMS servers, active destinations, active transactions, active connections, and session pools in the current domain.

[Customize this table](#)

**Statistics (Filtered - More Columns Exist)**

Showing 1 to 1 of 1 Previous | Next

Name ^	Destinations Current	Messages Current	Messages Pending	Messages Received	Messages Pageable Current	Messages Paged Out Total	Bytes Current
bepJMSServer	1	0	0	1	0	0	0

Showing 1 to 1 of 1 Previous | Next

- Verify that the **Messages Received** count increased by 1.
- Return to SPAIDEN and update the person's first name to the original value. This should trigger another event.
- Refresh the Settings page for the JMS server.

12. Verify that the **Messages Received** increased by 1. If the message count increased, BEP consumed the message from the queue and posted it to the JMS topic.

## Step 8 - Confirm access to the Banner Identity Gateway and the Banner Identity Proxy

Use the following steps to confirm that you can successfully access the Banner Identity Gateway administrative interface and the Banner Identity Proxy administrative interface.

1. Connect to the Banner Identity Gateway:

```
http://<host>:<port>/bnigweb
```

2. Log in with the user name and password for the Banner Identity Gateway.

If the login fails, verify that the credentials are correct and that the Oracle WebLogic Server is configured correctly to assign the appropriate users and roles to the application. Repeat these steps until login is successful.

3. Connect to the Banner Identity Proxy:

```
http://<host>:<port>/idproxyweb
```

4. Log in with the user name and password for the Banner Identity Proxy.

If the login fails, verify that the credentials are correct and that the Oracle WebLogic Server is configured correctly to assign the appropriate users and roles to the application. Repeat these steps until login is successful.

## Step 9 - Configure the Banner Identity Gateway and the Banner Identity Proxy

Refer to the *Banner Enterprise Identity Services 8.2 User Guide* for instructions on configuring the Banner Identity Gateway and the Banner Identity Proxy as follows.

If...	Then...
<p>You are implementing outbound account provisioning</p>	<p>Refer to chapter 2 of the user guide to configure Banner:</p> <ul style="list-style-type: none"> <li>• Declare the PIDM as a bind variable.</li> <li>• Configure email, address, and telephone number content.</li> <li>• Configure the display of tax IDs.</li> <li>• Customize the UDCIdentity XML structure.</li> <li>• Define extension attributes for the LDAP user name and password (if you are integrating with an LDAP directory).</li> <li>• Define capture data for monitoring the LDAP user name and password (if you are integrating with an LDAP directory).</li> </ul> <p>Refer to chapter 4 of the user guide to configure BEIS:</p> <ul style="list-style-type: none"> <li>• Identify the Banner instance that provides identity data.</li> <li>• Configure the location of each Provisioning Service Provider (PSP).</li> </ul>
<p>You are implementing inbound account provisioning</p>	<p>Refer to chapter 2 of the user guide to configure Banner:</p> <ul style="list-style-type: none"> <li>• Configure email, address, and telephone number content.</li> <li>• Configure a GTVSDAX rule for Common Matching.</li> </ul> <p>Refer to chapter 5 of the user guide to update the default user profile for new INB users.</p>

## Manual upgrade for Banner Identity Gateway and Banner Identity Proxy

The Banner Identity Gateway and the Banner Identity Proxy must be upgraded together. Use the following steps if you choose a manual upgrade process:

- [Step 1 - Verify the BEP installation](#)
- [Step 2 - Enable cross domain security](#)
- [Step 3 - Delete deprecated objects](#)
- [Step 4 - Upgrade the database schema](#)
- [Step 5 - Configure the Banner Identity Gateway and Banner Identity Proxy .ear files](#)
- [Step 6 - Deploy the Banner Identity Gateway](#)
- [Step 7 - Deploy the Banner Identity Proxy](#)

- [Step 8 - Evaluate the environment](#)
- [Step 9 - Verify that messaging is working](#)
- [Step 10 - Confirm access to the Banner Identity Gateway and the Banner Identity Proxy](#)
- [Step 11 - Configure the Banner Identity Gateway and the Banner Identity Proxy](#)

The following sections provide details for each step.

## Step 1 - Verify the BEP installation

Verify that the Banner Event Publisher (BEP) is installed and configured. Refer to Chapter 2, "Preinstallation," in the *Banner Enterprise Identity Services 8.2. Installation Guide* for details.

## Step 2 - Enable cross domain security



**Note:** This step is required only if BEIS and BEP are deployed on separate Oracle WebLogic Server domains. Skip this step if BEIS and BEP are deployed on the same Oracle WebLogic Server domain.

Skip this step if cross domain security was previously enabled during the BEIS 8.2 deployment.

Cross domain security establishes trust between two Oracle WebLogic Server domains. A trust relationship is established when the domain credential for one domain matches the domain credential for the other domain.

By default, the domain credential is randomly created the first time an Oracle WebLogic Server domain is started. This process ensures that each Oracle WebLogic Server domain has a unique credential.

To enable trust between the BEIS and BEP Oracle WebLogic Server domains, you must update the credential of each domain so they match. Use the following steps to enable cross domain security for the BEIS and BEP Oracle WebLogic Server domains.

1. Connect to the Oracle WebLogic Server administration console:

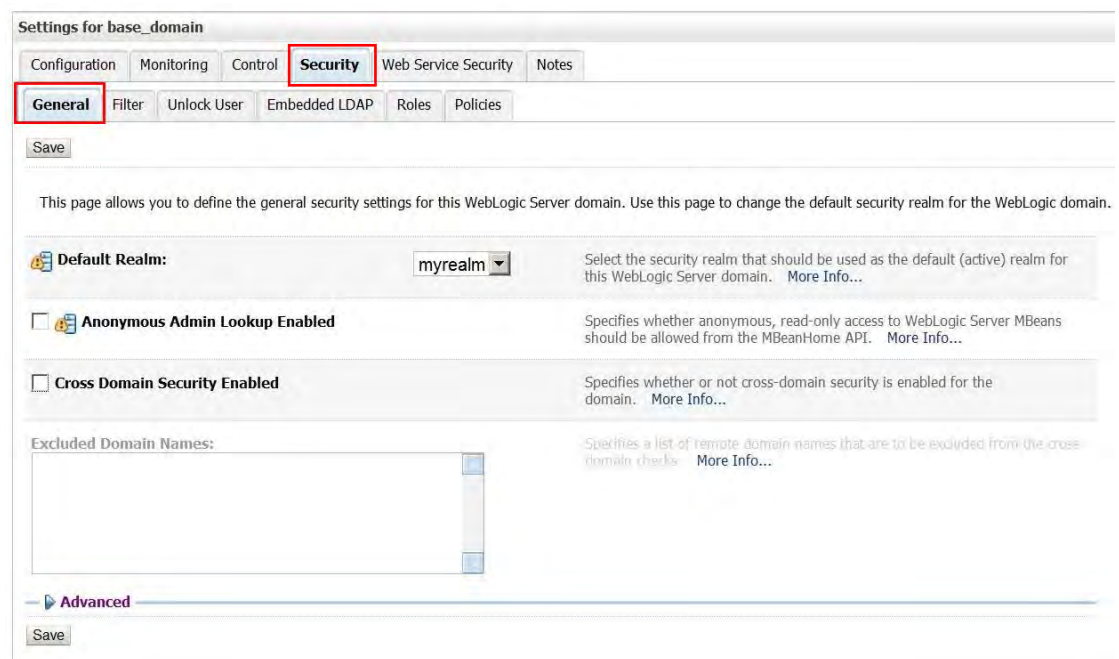
```
http://<host>:<port>/console
```

2. In the Change Center pane, click **Lock & Edit**.

3. In the Domain Structure pane, click the name of the BEIS domain. (When you repeat this step for the BEP domain, click the name of the BEP domain.)



4. Select the **Security > General** tab.



5. Select the **Cross Domain Security Enabled** check box.

Settings for base\_domain

Configuration Monitoring Control **Security** Web Service Security Notes

General Filter Unlock User Embedded LDAP Roles Policies

Save

This page allows you to define the general security settings for this WebLogic Server domain. Use this page to change the default security realm for the WebLogic domain.

**Default Realm:** myrealm Select the security realm that should be used as the default (active) realm for this WebLogic Server domain. [More Info...](#)

**Anonymous Admin Lookup Enabled** Specifies whether anonymous, read-only access to WebLogic Server MBeans should be allowed from the MBeanHome API. [More Info...](#)

**Cross Domain Security Enabled** Specifies whether or not cross-domain security is enabled for the domain. [More Info...](#)

**Excluded Domain Names:** Specifies a list of remote domain names that are to be excluded from the cross-domain checks. [More Info...](#)

Advanced

Save

6. Click **Save**.

7. Click **Advanced**.

Settings for base\_domain

Configuration Monitoring Control **Security** Web Service Security Notes

General Filter Unlock User Embedded LDAP Roles Policies

Save

This page allows you to define the general security settings for this WebLogic Server domain. Use this page to change the default security realm for the WebLogic domain.

**Default Realm:** myrealm Select the security realm that should be used as the default (active) realm for this WebLogic Server domain. [More Info...](#)

**Anonymous Admin Lookup Enabled** Specifies whether anonymous, read-only access to WebLogic Server MBeans should be allowed from the MBeanHome API. [More Info...](#)

**Cross Domain Security Enabled** Specifies whether or not cross-domain security is enabled for the domain. [More Info...](#)

**Excluded Domain Names:** Specifies a list of remote domain names that are to be excluded from the cross-domain checks. [More Info...](#)

Advanced

Save

8. Update the following information:

**Credential** Credential for the Oracle WebLogic Server domain. Use a credential that can be shared by both the BEIS and the BEP Oracle WebLogic Server domains.

**Confirm Credential** Confirmation of the credential for the Oracle WebLogic Server domain

The screenshot shows the 'Settings for base\_domain' page in the Oracle WebLogic Server Administration Console. The 'Security' tab is selected, and the 'General' sub-tab is active. The 'Credential' and 'Confirm Credential' fields are highlighted with a red box. The 'NodeManager Username' field is set to 'weblogic'.

Settings for base\_domain

Configuration Monitoring Control **Security** Web Service Security Notes

General Filter Unlock User Embedded LDAP Roles Policies

Save

This page allows you to define the general security settings for this WebLogic Server domain. Use this page to change the default security realm for the WebLogic domain.

**Default Realm:** myrealm Select the security realm that should be used as the default (active) realm for this WebLogic Server domain. [More Info...](#)

**Anonymous Admin Lookup Enabled** Specifies whether anonymous, read-only access to WebLogic Server MBeans should be allowed from the MBeanHome API. [More Info...](#)

**Cross Domain Security Enabled** Specifies whether or not cross-domain security is enabled for the domain. [More Info...](#)

**Excluded Domain Names:** Specifies a list of remote domain names that are to be excluded from the cross-domain checks. [More Info...](#)

Advanced

**Security Interoperability Mode:** default Specifies the security mode of the communication channel used for XA calls between servers that participate in a global transaction. All server instances in a domain must have the same security mode setting. [More Info...](#)

**Credential:** The credential for this WebLogic Server domain. When a domain is created, a unique credential is generated for the domain. If you want to establish trust between two or more domains, decide on a credential that will be shared by the domains, then specify it here and in the other domains. [More Info...](#)

**Confirm Credential:**

**NodeManager Username:** weblogic The user name that the Administration Server uses to communicate with Node Manager when starting, stopping, or restarting Managed Servers. [More Info...](#)

9. Click **Save**.

10. In the Change Center pane, click **Activate Changes**.

11. Shut down all Managed Servers in the domain.

12. Shut down the Admin Server.

13. Start the Admin Server.

14. Start all Managed Servers in the domain.

15. Repeat steps 1 through 14 for the BEP Oracle WebLogic Server domain. Enter the same credential that was used for the BEIS Oracle WebLogic Server domain.

### Step 3 - Delete deprecated objects

Use the Oracle WebLogic Server administration console to delete the Banner Identity Gateway 8.2 and Banner Identity Proxy 8.2 applications.

### Step 4 - Upgrade the database schema

Use the following steps to upgrade the database packages that are required by the Banner Identity Gateway and the Banner Identity Proxy.

1. Extract `IdGtwyPrxy_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/bnig/packages`.
3. Connect to the database instance where BEIS is installed as the `BNIXMGR` user.
4. Execute `iokp_build.sql` to upgrade the database packages:  

```
sqlplus> @iokp_build
```
5. Execute the following command to reset the package variables:  

```
sqlplus> exec DBMS_SESSION.RESET_PACKAGE;
```
6. Exit SQL\*Plus.
7. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/idproxy/packages`.
8. Connect to the database instance where BEIS is installed as the `IDENTMGR` user.
9. Execute `iokp_build.sql` to upgrade the database packages:  

```
sqlplus> @iokp_build
```
10. Execute the following command to reset the package variables:  

```
sqlplus> exec DBMS_SESSION.RESET_PACKAGE;
```
11. Exit SQL\*Plus.

### Step 5 - Configure the Banner Identity Gateway and Banner Identity Proxy .ear files

The automated installer *must* be run on the Oracle WebLogic Server to configure the following files:

<code>bnig.ear</code>	Banner Identity Gateway
<code>IdProxy.ear</code>	Banner Identity Proxy

Use the following steps to run the automated installer and configure the .ear files.

1. Extract `IdGtwyPrxy_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.

2. Open a command prompt and navigate to `<ZIP_HOME>/ant-installer`.
3. Execute the following command:

```
java -jar gtwy-prxy-weblogic-installer.jar
```

The automated installer is launched. The user interface depends on whether you are running in a windowing (GUI) or non-windowing (command-line) environment. The remaining instructions are based on using the GUI for configuration. Configuration options are identical for a command-line interface.



**Note:** In command-line mode, each configuration option is displayed with the default value in brackets. To accept the default value, press Enter on your keyboard. To enter a different value, enter the correct value and press Enter on your keyboard. Valid values for the configuration options are *true* and *false*. All values must be entered without leading and trailing spaces.



4. Click **Next**.

5. Select the **Configure and Save EAR Files** check box.



6. Click **Next**.
7. Enter the following Banner Event Publisher (BEP) information:

<b>BEP Server Host</b>	BEP server host name
<b>BEP Server Port</b>	Port number where BEP is running
<b>BEP Server Username</b>	User name for the administrator of the application server where BEP is deployed
<b>BEP Server Password</b>	Password for the administrator of the application server where BEP is deployed



8. Click **Next**.

9. Enter the password for the INTEGMR account.



10. Click **Next**.

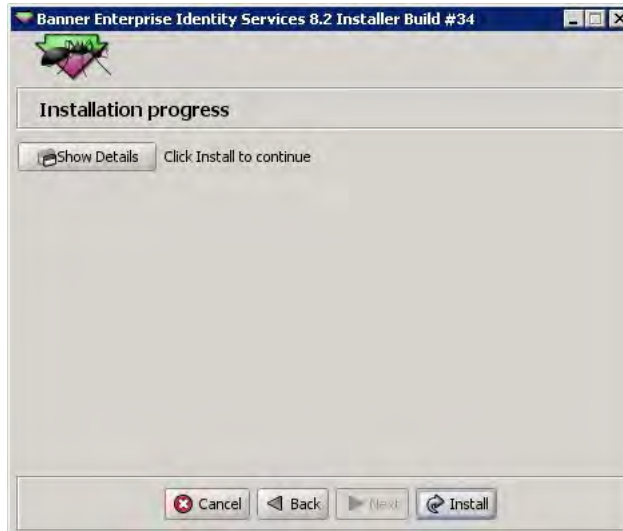
11. Click **Select Folder** and browse to the location where you want to save `bnig.ear` and `IdProxy.ear` for manual deployment.



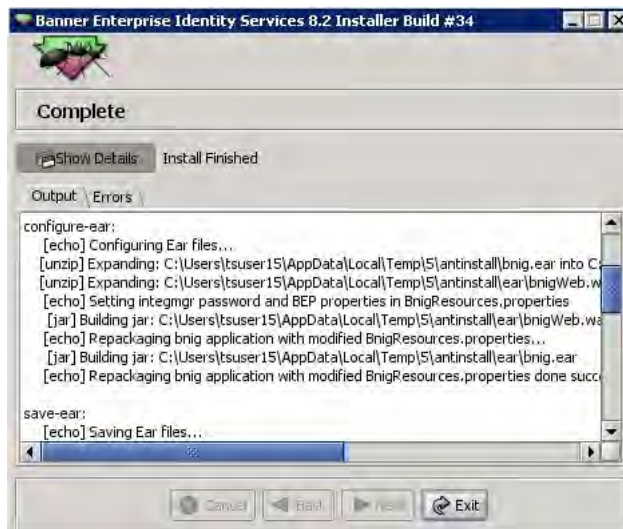
12. Click **Next**.

13. Click **Show Details**.

#### 14. Click **Install**.



Installation details are displayed as the installation progresses.



The message *Install Finished* is displayed when the installation is complete. The `bnig.ear` and `IdProxy.ear` files are saved in the selected folder.

### Step 6 - Deploy the Banner Identity Gateway

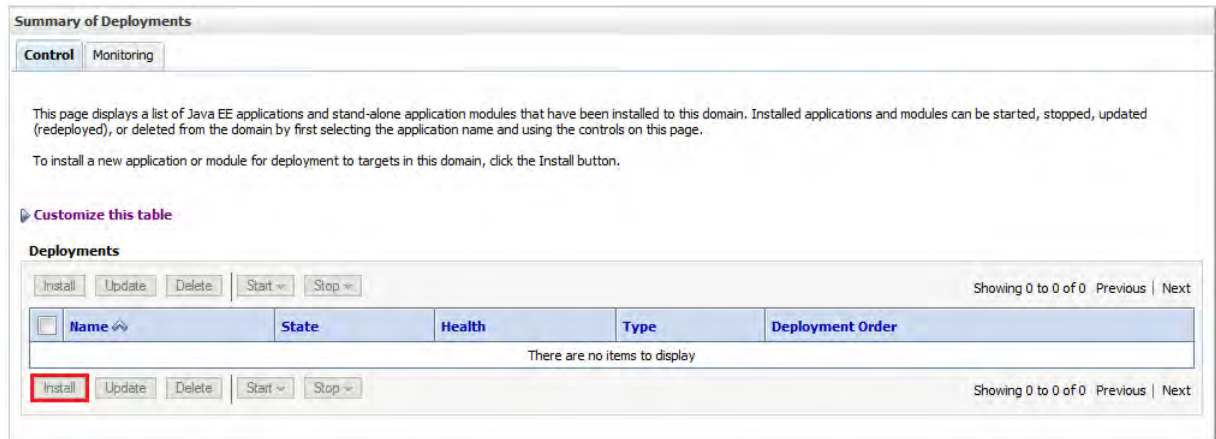
Use the following steps to deploy the Banner Identity Gateway.

1. In the Change Center pane, click **Lock & Edit**.

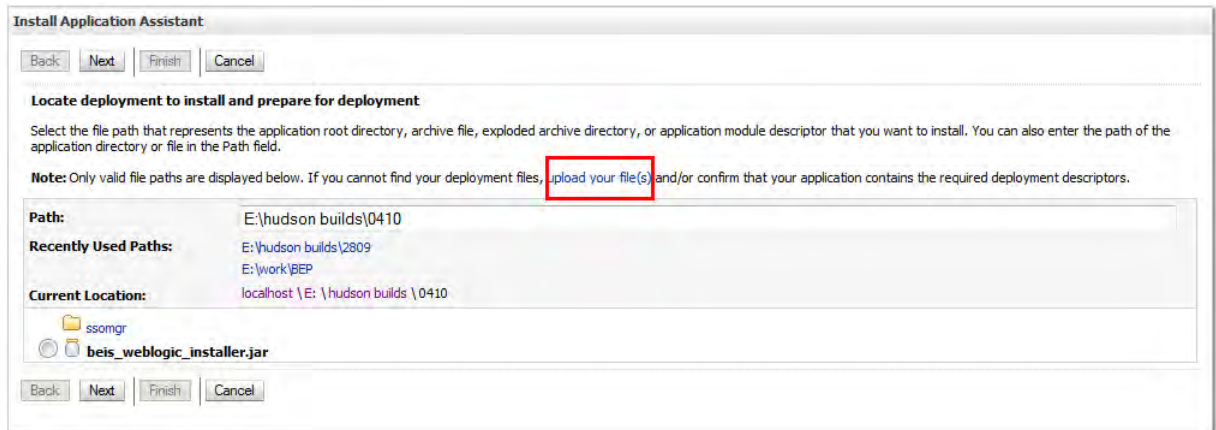
- In the Domain Structure pane, click **Deployments**.



- Click **Install**.

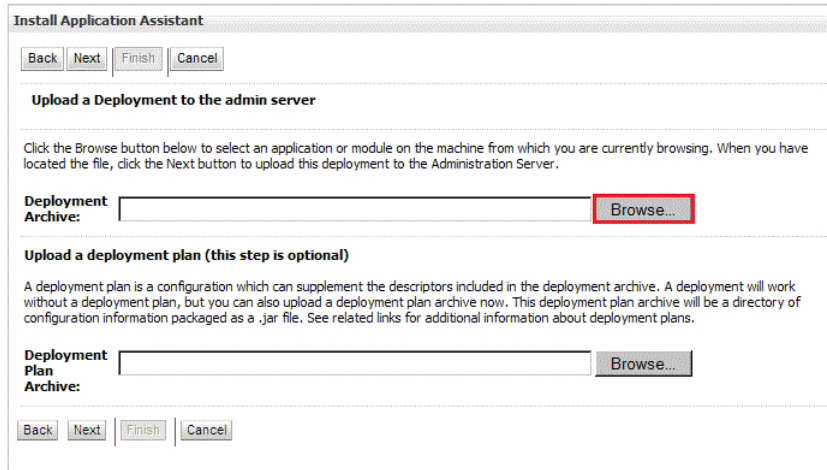


- Click **upload your file(s)**.



5. Select the file to be uploaded as follows:

5.1. In the **Deployment Archive** field, click **Browse**.

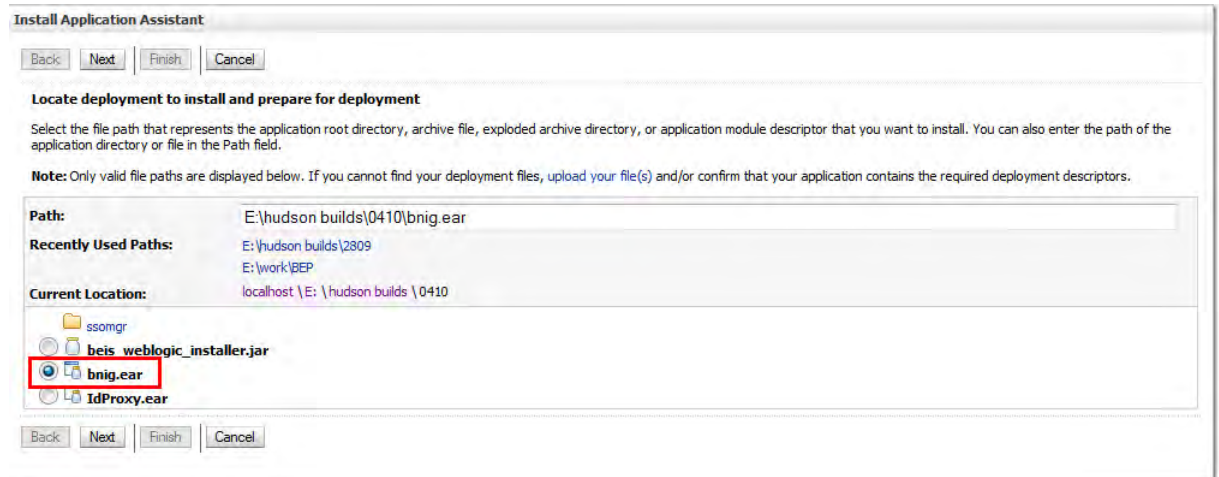


5.2. Navigate to `bnig.ear`. This file was copied to a specified location when the automated installer was run in [Step 5 - Configure the Banner Identity Gateway and Banner Identity Proxy .ear files](#).

5.3. Select the file and click **Open**.

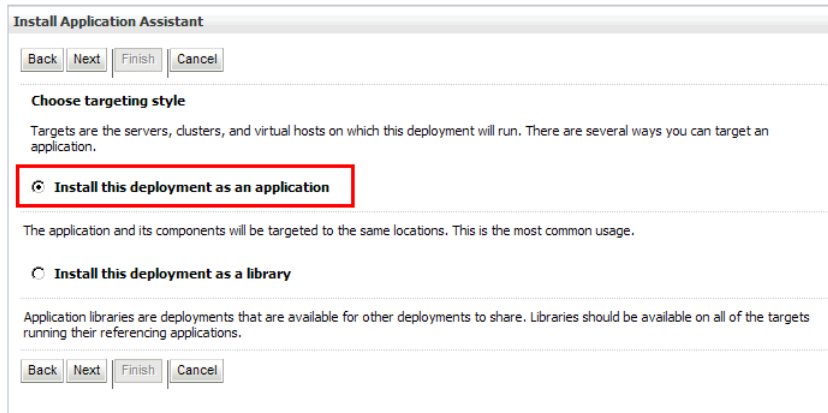
6. Click **Next**.

7. Select `bnig.ear` from the list at the bottom of the page.



8. Click **Next**.

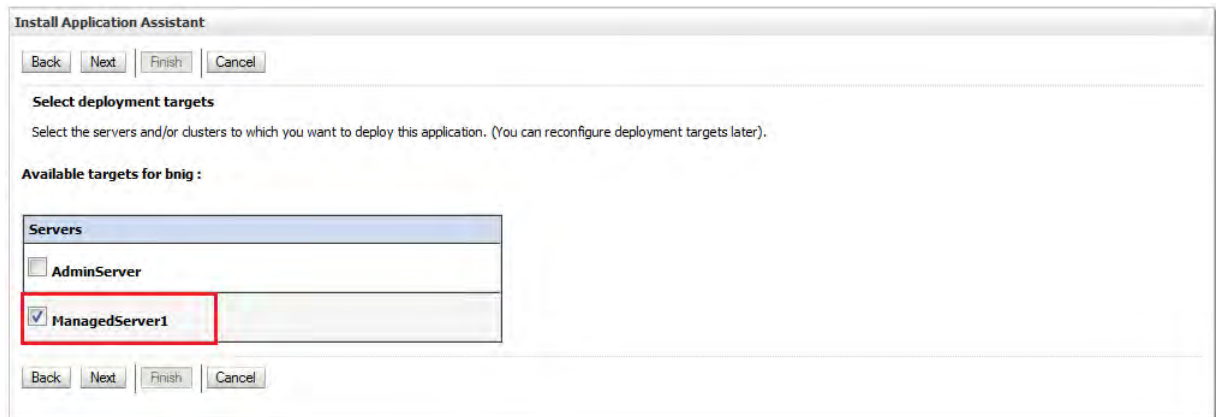
9. Select **Install this deployment as an application.**



10. Click **Next**.

11. The next page is either an optional settings page or a deployment targets page, depending on the domain.

- If an optional settings page is displayed, check your Oracle WebLogic Server configuration before you continue. Make sure that a Managed Server is available for deployment of applications. If a Managed Server is not available, the application will be deployed to the Admin Server, which is not a recommended configuration. For more information, consult the Oracle WebLogic Server Documentation Library. Then go to step 12.
- If a select deployment targets page is displayed, select the server where the application should be deployed. The application can be deployed to an existing server. The application should be installed to a Managed Server, not to the Admin Server. The application must be installed on the same server with the Banner Identity Proxy. Then click **Next** and go to step 12.



12. Enter the following settings:

- |  |   |
|--|---|
| <b>Name</b>  | Name for the application (for example, <i>BannerIdentityGateway</i> ) |
| <b>Advanced: Use a custom model that you have configured on the realm's configuration page</b> | Select the radio button.  |
| <b>Copy this application onto every target for me</b>  | Select the radio button.  |

The screenshot shows the 'Install Application Assistant' dialog box with the following settings:

- Optional Settings**
  - General**
    - What do you want to name this deployment?
      - Name:** BannerIdentityGateway
  - Security**
    - What security model do you want to use with this application?
      - DD Only: Use only roles and policies that are defined in the deployment descriptors.
      - Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.
      - Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.
      - Advanced: Use a custom model that you have configured on the realm's configuration page.**
  - Source accessibility**
    - How should the source files be made accessible?
      - Use the defaults defined by the deployment's targets
      - Copy this application onto every target for me**
    - Recommended selection:
      - Copy this application onto every target for me**
    - During deployment, the files will be copied automatically to the managed servers to which the application is targeted.
      - I will make the deployment accessible from the following location
    - Location:** C:\test\bnig.ear
    - Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.

13. Click **Next**.

14. Select **No, I will review the configuration later.**

**Install Application Assistant**

Back Next Finish Cancel

**Review your choices and click Finish**

Click Finish to complete the deployment. This may take a few moments to complete.

**Additional configuration**

In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?

Yes, take me to the deployment's configuration screen.

**No, I will review the configuration later.**

**Summary**

**Deployment:** C:\test\bnig.ear

**Name:** BannerIdentityGateway

**Staging mode:** Copy this application to every target for me

**Security Model:** Advanced: Use a custom model that you have configured on the realm's configuration page.

**Target Summary**

Components	Targets
bnig.ear	ManagedServer1

Back Next Finish Cancel

15. Click **Finish** to start the deployment. When deployment is completed, the Summary of Deployments page is redisplayed with the newly deployed application.

**Summary of Deployments**

Control Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page. To install a new application or module for deployment to targets in this domain, click the Install button.

[Customize this table](#)

**Deployments**

Install Update Delete Start Stop Showing 1 to 3 of 3 Previous Next

Name	State	Health	Type	Deployment Order
BannerEventPublisher	Active	OK	Enterprise Application	100
<b>BannerIdentityGateway</b>	<b>deploy Initializing</b>	OK	Enterprise Application	100
BannerIdentityProxy	Active	OK	Enterprise Application	100

Install Update Delete Start Stop Showing 1 to 3 of 3 Previous Next

16. In the Change Center pane, click **Activate Changes.**

17. Start the newly deployed application as follows:
  - 17.1. Make sure the Summary of Deployments page is displayed.
  - 17.2. Select the newly deployed application.
  - 17.3. Click **Start > Servicing all requests**.



- 17.4. Click **Yes** to start the application.



## Step 7 - Deploy the Banner Identity Proxy

Use the following steps to deploy the Banner Identity Proxy.

1. In the Change Center pane, click **Lock & Edit**.
2. In the Domain Structure pane, click **Deployments**.
3. Click **Install**.
4. Click **upload your file(s)**.
5. Select the file to be uploaded as follows:
  - 5.1. In the **Deployment Archive** field, click **Browse**.
  - 5.2. Navigate to `IdProxy.ear`. This file was copied to a specified location when the automated installer was run in [Step 5 - Configure the Banner Identity Gateway and Banner Identity Proxy .ear files](#).
  - 5.3. Select the file and click **Open**.
6. Click **Next**.

7. Select `IdProxy.ear` from the list at the bottom of the page.
8. Click **Next**.
9. Select **Install this deployment as an application**.
10. Click **Next**.
11. The next page is either an optional settings page *or* a deployment targets page, depending on the domain.
  - If an optional settings page is displayed, check your Oracle WebLogic server configuration before you continue. Make sure that a Managed Server is available for deployment of applications. If a Managed Server is not available, the application will be deployed to the Admin Server, which is not a recommended configuration. For more information, consult the Oracle WebLogic Server Documentation Library. Then go to step 12.
  - If a select deployment targets page is displayed, select the server where the application should be deployed. The application can be deployed to an existing server. The application should be installed to a Managed Server, not to the Admin Server. The application must be installed on the same server with the Banner Identity Gateway. Then click **Next** and go to step 12.
12. Enter the following settings:

<b>Name</b>	Name for the application (for example, <i>BannerIdentityProxy</i> )
<b>Advanced:Use a custom model that you have configured on the realm's configuration page</b>	Select the radio button.
<b>Copy this application onto every target for me</b>	Select the radio button.

13. Click **Next**.
14. Select **No, I will review the configuration later**.
15. Click **Finish** to start the deployment. When deployment is completed, the Summary of Deployments page is redisplayed with the newly deployed application.
16. In the Change Center pane, click **Activate Changes**.
17. Start the newly deployed application as follows:
  - 17.1. Make sure the Summary of Deployments page is displayed.
  - 17.2. Select the newly deployed application.
  - 17.3. Click **Start > Servicing all requests**.
  - 17.4. Click **Yes** to start the application.

## Step 8 - Evaluate the environment

After you upgrade the Banner Identity Gateway and the Banner Identity Proxy, you should run `post_install_beis_checksript.sql` to evaluate your environment and identify potential problems. This script reports on several criteria that are essential for a

fully functioning BEIS environment. You can use the script to evaluate both new installations and upgrades. Depending on the current state of your Banner/Oracle RDBMS environment, you might need to make changes based on the output of the script.

Use the following steps to run the check script and evaluate the results.

1. Extract `IdGtwyPrxy_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/util`.
3. Ensure that `post_install_beis_checksript.sql` has read permission.
4. Connect to SQL\*Plus as the `BANINST1` user.
5. Execute `post_install_beis_checksript.sql`:  

```
sqlplus> @post_install_beis_checksript
```
6. When prompted, enter the following information:
  - Username for the `BNIXMGR` schema (for example, `BNIXMGR`)
  - Username for the `IDENTMGR` schema (for example, `IDENTMGR`)
7. Exit SQL\*Plus.
8. Evaluate the results as follows:

Result	Evaluation
BNIXMGR schema	The BNIXMGR schema must exist.
Roles assigned to BNIXMGR	The following roles must be assigned to BNIXMGR: <ul style="list-style-type: none"> <li>• RESOURCE</li> <li>• CONNECT</li> </ul>
Privileges granted to BNIXMGR	The following privileges must be granted to BNIXMGR: <ul style="list-style-type: none"> <li>• DROP PUBLIC SYNONYM</li> <li>• CREATE PUBLIC SYNONYM</li> <li>• UNLIMITED TABLESPACE</li> <li>• CREATE SESSION</li> <li>• CREATE SYNONYM</li> <li>• CREATE VIEW</li> </ul>
Database objects in BNIXMGR database schema	The BNIXMGR schema should have the following tables: <ul style="list-style-type: none"> <li>• BNIXVAL</li> <li>• GTWMETA</li> <li>• PSPALOG</li> <li>• T_UDC_ERROR_LOG</li> <li>• T_UDC_ERROR_LOG_H</li> </ul>

<b>Result</b>	<b>Evaluation</b>
Sequences that belong to BNIXMGR	The BNIXMGR schema should have the following sequences: <ul style="list-style-type: none"> <li>• T_UDC_ERROR_LOG_SEQ</li> <li>• T_UDC_ERROR_LOG_H_SEQ</li> <li>• PSPALOG_SEQ</li> </ul>
Views that belong to BNIXMGR	The BNIXMGR schema should have the VW_UDC_ERROR_LOG view.
Triggers that belong to BNIXMGR	The BNIXMGR schema should have the following triggers: <ul style="list-style-type: none"> <li>• TRG_UDC_ERROR_LOG_BUS</li> <li>• TRG_UDC_ERROR_LOG_BUR</li> <li>• TRG_UDC_ERROR_LOG_AUS</li> </ul>
Packages that belong to BNIXMGR	The BNIXMGR schema should have the following packages: <ul style="list-style-type: none"> <li>• IOKP_GTW_METADATA</li> <li>• IOKP_UDC_ERROR_LOG</li> <li>• IOKP_PSPALOG</li> <li>• IOKP_UDC_ERROR_LOG_H</li> </ul>
IDENTMGR schema	The IDENTMGR schema must exist.
Roles assigned to IDENTMGR	The following roles must be assigned to IDENTMGR: <ul style="list-style-type: none"> <li>• RESOURCE</li> <li>• CONNECT</li> </ul>
Privileges granted to IDENTMGR	The following privileges must be granted to IDENTMGR: <ul style="list-style-type: none"> <li>• CREATE VIEW</li> <li>• UNLIMITED TABLESPACE</li> <li>• DROP PUBLIC SYNONYM</li> <li>• CREATE PUBLIC SYNONYM</li> <li>• CREATE SYNONYM</li> <li>• CREATE SESSION</li> </ul>
Database objects in IDENTMGR database schema	The IDENTMGR schema should have the following tables: <ul style="list-style-type: none"> <li>• T_UDC_PST_LIST</li> <li>• T_UDC_SPML_MSG_BALANCER</li> <li>• T_UDC_SPML_MSG_LOG</li> <li>• T_UDC_SPML_RES_ERROR_LOG</li> </ul>

Result	Evaluation
Sequences that belong to IDENTMGR	The IDENTMGR schema should have the following sequences: <ul style="list-style-type: none"> <li>• T_UDC_PST_LIST_SEQ</li> <li>• T_UDC_SPML_MSG_LOG_SEQ</li> <li>• T_UDC_SPML_RES_ERROR_LOG_SEQ</li> </ul>
Packages that belong to IDENTMGR	The IDENTMGR schema should have the following packages: <ul style="list-style-type: none"> <li>• IOKP_UDC_SPML_MSG_LOG</li> <li>• IOKP_UDC_PST</li> </ul>

### Step 9 - Verify that messaging is working

During the BEIS 8.2 installation, seed data for BEISIdentityEvent was loaded into the Banner Event Publisher (BEP). BEP uses this event to capture identity data changes in Banner, evaluate the changes, and publish XML messages for BEIS processing.

Use the following steps to verify that the seed data was loaded and that BEP is publishing XML messages properly.

1. Log in to Internet-Native Banner (INB).
2. Access the Identification (SPAIDEN) form.
3. Change the first name of a person.
4. Save the change.
5. Connect to the Oracle WebLogic Server administration console:

`http://<host>:<port>/console`

6. In the Domain Structure pane, expand and click **Services > Messaging > JMS Servers**.



- Click the name of the JMS server that was created for BEP.

**Summary of JMS Servers**

JMS servers act as management containers for the queues and topics in JMS modules that are targeted to them.

This page summarizes the JMS servers that have been created in the current WebLogic Server domain.

[Customize this table](#)

**JMS Servers (Filtered - More Columns Exist)**

New Delete Previous | Next

<input type="checkbox"/>	Name	Persistent Store	Target	Current Server	Health
<input type="checkbox"/>	bepJMServer	BEPFileStore	BEPmanagedServer	BEPmanagedServer	

New Delete Previous | Next

- Select the **Monitoring > Monitoring** tab on the Settings page.

**Settings for bepJMServer**

Configuration Logging Targets **Monitoring** Control Notes

**Monitoring** Paging Store Active Destinations Active Transactions Active Connections Active Session Pools Active Pooled Connections

Use this page to view runtime statistics for all of the active JMS servers, active destinations, active transactions, active connections, and session pools in the current domain.

[Customize this table](#)

**Statistics (Filtered - More Columns Exist)**

Showing 1 to 1 of 1 Previous | Next

Name	Destinations Current	Messages Current	Messages Pending	Messages Received	Messages Pageable Current	Messages Paged Out Total	Bytes Current
bepJMServer	1	0	0	1	0	0	0

Showing 1 to 1 of 1 Previous | Next

- Verify that the **Messages Received** count increased by 1.
- Return to SPAIDEN and update the person's first name to the original value. This should trigger another event.
- Refresh the Settings page for the JMS server.
- Verify that the **Messages Received** increased by 1. If the message count increased, BEP consumed the message from the queue and posted it to the JMS topic.

## Step 10 - Confirm access to the Banner Identity Gateway and the Banner Identity Proxy

Use the following steps to confirm that you can successfully access the Banner Identity Gateway administrative interface and the Banner Identity Proxy administrative interface.

- Connect to the Banner Identity Gateway:

```
http://<host>:<port>/bnigweb
```

2. Log in with the user name and password for the Banner Identity Gateway.  
If the login fails, verify that the credentials are correct and that the Oracle WebLogic Server is configured correctly to assign the appropriate users and roles to the application. Repeat these steps until login is successful.
3. Connect to the Banner Identity Proxy:  
`http://<host>:<port>/idproxyweb`
4. Log in with the user name and password for the Banner Identity Proxy.  
If the login fails, verify that the credentials are correct and that the Oracle WebLogic Server is configured correctly to assign the appropriate users and roles to the application. Repeat these steps until login is successful.

## Step 11 - Configure the Banner Identity Gateway and the Banner Identity Proxy

Refer to the *Banner Enterprise Identity Services 8.2. User Guide* for instructions on configuring the Banner Identity Gateway and the Banner Identity Proxy as follows.

If...	Then...
You are implementing outbound account provisioning	<p>Refer to chapter 2 of the user guide to configure Banner:</p> <ul style="list-style-type: none"> <li>• Declare the PIDM as a bind variable.</li> <li>• Configure email, address, and telephone number content.</li> <li>• Configure the display of tax IDs.</li> <li>• Customize the UDCIdentity XML structure.</li> <li>• Define attributes for the LDAP user name and password (if you are integrating with an LDAP directory).</li> <li>• Define capture data for monitoring the LDAP user name and password (if you are integrating with an LDAP directory).</li> </ul> <p>Refer to chapter 4 of the user guide to configure BEIS:</p> <ul style="list-style-type: none"> <li>• Identify the Banner instance that provides identity data.</li> <li>• Configure the location of each Provisioning Service Provider (PSP).</li> </ul>
You are implementing inbound account provisioning	<p>Refer to chapter 2 of the user guide to configure Banner:</p> <ul style="list-style-type: none"> <li>• Configure email, address, and telephone number content.</li> <li>• Configure a GTVSDAX rule for Common Matching.</li> </ul> <p>Refer to chapter 5 of the user guide to update the default user profile for new INB users.</p>

# Upgrade SSO Manager to 8.2.1

---

You can choose an automated process or a manual process.

## Automated upgrade for SSO Manager

Use the following steps if you choose an automated process to upgrade the SSO Manager:

- [Step 1 - Delete deprecated objects](#)
- [Step 2 - Upgrade the database schema](#)
- [Step 3 - Run the automated installer](#)
- [Step 4 - Evaluate the environment](#)
- [Step 5 - Confirm access to the SSO Manager](#)
- [Step 6 - Configure supporting components](#)

The following sections provide details for each step.

### Step 1 - Delete deprecated objects

Use the Oracle WebLogic Server administration console to delete the SSO Manager 8.2 application.

### Step 2 - Upgrade the database schema

Use the following steps to upgrade the database tables that the SSO Manager requires.

1. Extract `SSOManager_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/tables`.
3. Connect to the database instance where the SSO Manager is installed as the `SSOMGR` user.
4. Execute `db_821_upgrade.sql` to upgrade the SSO Manager:  

```
sqlplus> @db_821_upgrade
```
5. Exit SQL\*Plus.

### Step 3 - Run the automated installer

The automated installer must be run on the Oracle WebLogic Server to configure the following files:

```
sso-manager.ear    SSO Manager
ssoclient.jar     SSO Client
```

Use the following steps to run the automated installer.

1. Extract `SSOManager_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/ant-installer`.
3. Execute the following command:

```
java -jar sso-manager-weblogic-installer.jar
```

The automated installer is launched. The user interface depends on whether you are running in a windowing (GUI) or non-windowing (command-line) environment. The remaining instructions are based on using the GUI for configuration. Configuration options are identical for a command-line interface.



**Note:** In command-line mode, each configuration option is displayed with the default value in brackets. To accept the default value, press Enter on your keyboard. To enter a different value, enter the correct value and press Enter on your keyboard. Valid values for the configuration options are `true` and `false`. All values must be entered without leading and trailing spaces.



4. Click **Next**.

5. Select the following check boxes:

**Configure and Save EAR**

**Configure and Save SSO Client**

**Deploy EAR**

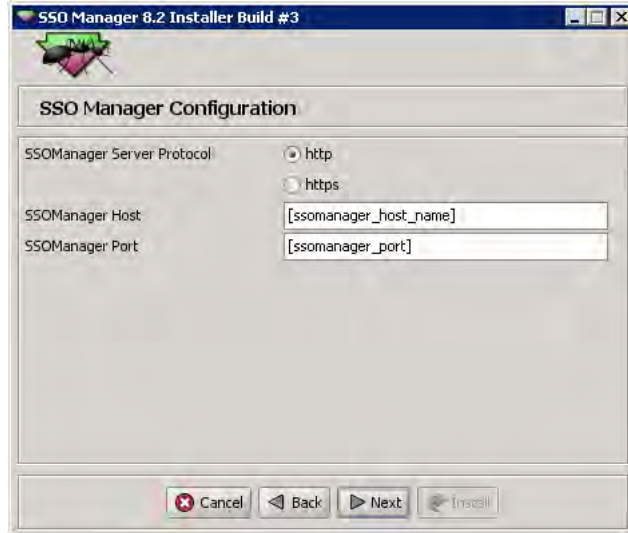


6. Click **Next**.
7. Enter the following SSO Manager information:

**SSO Manager Server Protocol** Protocol used by the SSO Manager (`https` or `http`)

**SSO Manager Host** SSO Manager server host name

**SSO Manager Port** Managed Server port number where the SSO Manager is deployed



8. Click **Next**.
9. Enter the SSO Manager user configuration:

**Username**                      User name for the SSO Manager web application

**Password**                      Password for the SSO Manager web application



10. Click **Next**.

11. Choose one of the following:

11.1. If you are using the SSO Manager with a third-party access manager, skip to step 12.

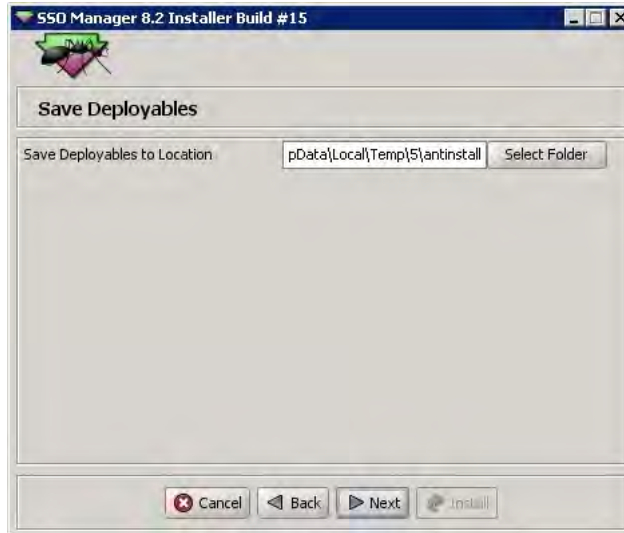
11.2. If you are using the SSO Manager with CAS, enter the following information:

- |                            |   |
|----------------------------|---|
| <b>CAS Server Protocol</b> | Protocol used by the CAS server (https or http)   |
| <b>CAS Server Host</b>     | CAS server host name  |
| <b>CAS Server Port</b>     | Port number where the CAS server is running   |
| <b>CAS Server Context</b>  | Context under which CAS is deployed and accessible via a browser (for example, <code>http(s)://&lt;host&gt;:&lt;port&gt;/&lt;context&gt;</code> ) |



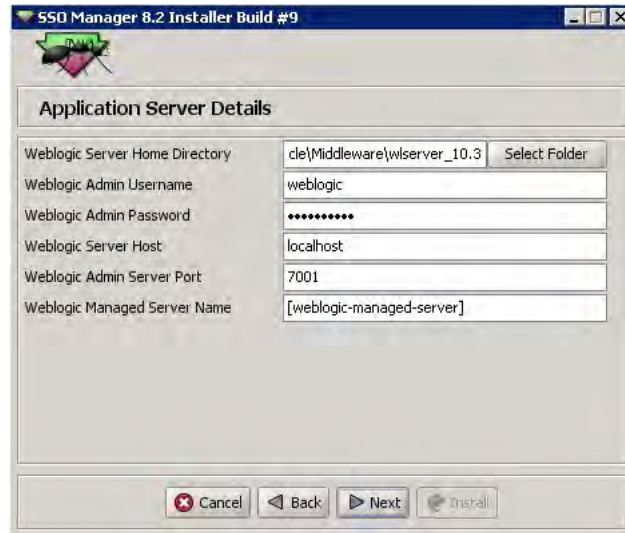
12. Click **Next**.

13. Click **Select Folder** and browse to the location where you want to save `sso-manager.ear` and `ssoclient.jar`.

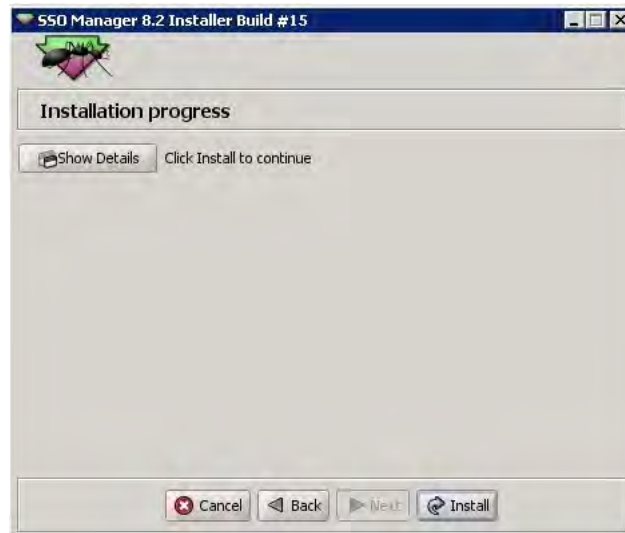


14. Click **Next**.
15. Enter the following application server information:

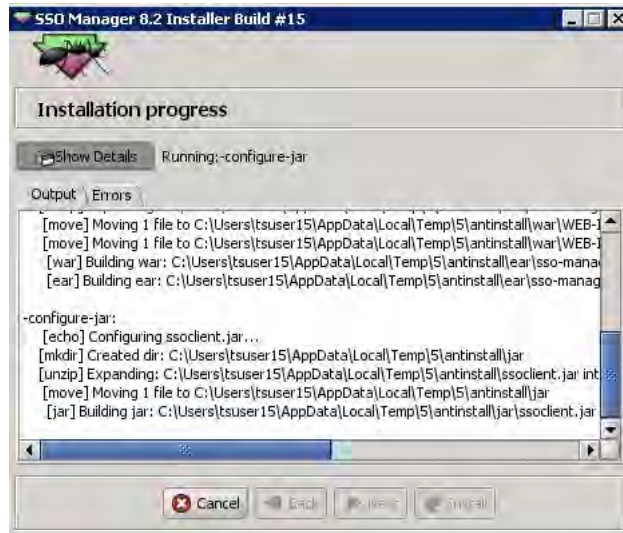
<b>Weblogic Server Home Directory</b>	Path of the Oracle WebLogic Server home directory (for example, <code>C:\Oracle\Middleware\wlserver_10.3</code> )
<b>Weblogic Admin Username</b>	User name for the application server administrator
<b>Weblogic Admin Password</b>	Password for the application server administrator
<b>Weblogic Server Host</b>	IP address or host name of the machine where the Oracle WebLogic Server is installed
<b>Weblogic Admin Sever Port</b>	Port where the Oracle WebLogic Server is running
<b>Weblogic Managed Server Name</b>	Name of the Oracle WebLogic Managed Server where the data sources are created and the application is deployed



- 16. Click **Next**.
- 17. Click **Show Details**.
- 18. Click **Install**.



Installation details are displayed as the installation progresses.



The message *Install Finished* is displayed when the installation is complete. The `sso-manager.ear` and `ssoclient.jar` files are saved in the selected folder.

#### Step 4 - Evaluate the environment

After you upgrade the SSO Manager, you should run `post_install_ssomgr_checksript.sql` to evaluate your environment and identify potential problems. This script reports on several criteria that are essential for a fully functioning SSO Manager environment. You can use the script to evaluate both new installations and upgrades. Depending on the current state of your Banner/Oracle RDBMS environment, you might need to make changes based on the output of the script.

Use the following steps to run the check script and evaluate the results.

1. Extract `SSOManager_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/util`.
3. Ensure that `post_install_ssomgr_checksript.sql` has read permission.
4. Connect to SQL\*Plus as the `BANINST1` user.
5. Execute `post_install_ssomgr_checksript.sql`:  

```
sqlplus> @post_install_ssomgr_checksript
```
6. When prompted, enter the username for the SSOMGR schema (for example, `SSOMGR`).
7. Exit SQL\*Plus.

8. Evaluate the results as follows:

Result	Evaluation
SSOMGR schema	The SSOMGR schema must exist.
Roles assigned to SSOMGR	The following roles must be assigned to SSOMGR: <ul style="list-style-type: none"> <li>• RESOURCE</li> <li>• CONNECT</li> </ul>
Privileges granted to SSOMGR	The following privileges must be granted to SSOMGR: <ul style="list-style-type: none"> <li>• UNLIMITED TABLESPACE</li> <li>• ALTER USER</li> </ul>
Database objects in SSOMGR database schema	The SSOMGR schema should have the following tables: <ul style="list-style-type: none"> <li>• APP_CONFIG</li> <li>• UDC_CREDENTIAL_INFO</li> <li>• UDC_CREDENTIAL_SERVICES</li> <li>• UDC_TICKET_SERVICES</li> </ul>
Sequences that belong to SSOMGR	The SSOMGR schema should have the following sequences: <ul style="list-style-type: none"> <li>• APP_CONFIG_SEQ</li> <li>• UDC_CREDENTIAL_SERVICES_SEQ</li> <li>• UDC_CREDENTIAL_INFO_SEQ</li> </ul>
Packages that belong to SSOMGR	The SSOMGR schema should have the IP_SSO_MANAGER package.

### Step 5 - Confirm access to the SSO Manager

Use the following steps to confirm that you can successfully access the SSO Manager administrative interface.

1. Connect to the SSO Manager:

```
http://<host>:<port>/ssomanager
```

2. Log in with the user name and password for the SSO Manager.

If the login fails, verify that the credentials are correct and that the Oracle WebLogic Server is configured correctly to assign the appropriate users and roles to the application. Repeat these steps until login is successful.

## Step 6 - Configure supporting components

Refer to Chapter 6, "Single Sign On," in the *Banner Enterprise Identity Services 8.2. User Guide* for instructions on configuring the components that support SSO:

- SSO Manager settings
- Banner Web Tailor settings for Self-Service Banner (SSB)
- Oracle Forms server settings for Internet-Native Banner (INB)

## Manual upgrade for SSO Manager

Use the following steps if you choose a manual process to upgrade the SSO Manager:

- [Step 1 - Delete deprecated objects](#)
- [Step 2 - Upgrade the database schema](#)
- [Step 3 - Configure the SSO Manager .ear file and the SSO client .jar file](#)
- [Step 4 - Deploy the SSO Manager](#)
- [Step 5 - Evaluate the environment](#)
- [Step 6 - Confirm access to the SSO Manager](#)
- [Step 7 - Configure supporting components](#)

The following sections provide details for each step.

### Step 1 - Delete deprecated objects

Use the Oracle WebLogic Server administration console to delete the SSO Manager 8.2 application.

### Step 2 - Upgrade the database schema

Use the following steps to upgrade the database tables that the SSO Manager requires.

1. Extract `SSOManager_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/tables`.
3. Connect to the database instance where the SSO Manager is installed as the SSOMGR user.
4. Execute `db_821_upgrade.sql` to upgrade the SSO Manager:  

```
sqlplus> @db_821_upgrade
```
5. Exit SQL\*Plus.

### Step 3 - Configure the SSO Manager .ear file and the SSO client .jar file

The automated installer *must* be run on the Oracle WebLogic Server to configure the following files:

<code>sso-manager.ear</code>	SSO Manager
<code>ssoclient.jar</code>	SSO Client

Use the following steps to run the automated installer.

1. Extract `SSOManager_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/ant-installer`.
3. Execute the following command:

```
java -jar sso-manager-weblogic-installer.jar
```

The automated installer is launched. The user interface depends on whether you are running in a windowing (GUI) or non-windowing (command-line) environment. The remaining instructions are based on using the GUI for configuration. Configuration options are identical for a command-line interface.



**Note:** In command-line mode, each configuration option is displayed with the default value in brackets. To accept the default value, press Enter on your keyboard. To enter a different value, enter the correct value and press Enter on your keyboard. Valid values for the configuration options are *true* and *false*. All values must be entered without leading and trailing spaces.



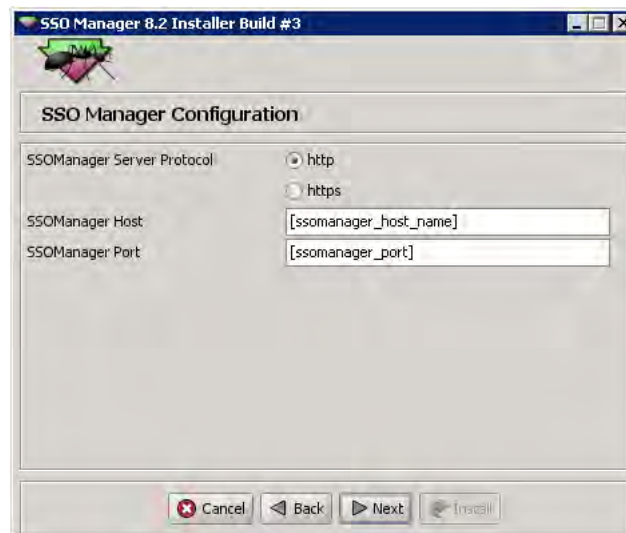
4. Click **Next**.

5. Select the **Configure and Save EAR** and the **Configure and Save SSO Client** check boxes.



6. Click **Next**.
7. Enter the following SSO Manager information:

<b>SSO Manager Server Protocol</b>	Protocol used by the SSO Manager ( <code>https</code> or <code>http</code> )
<b>SSO Manager Host</b>	SSO Manager server host name
<b>SSO Manager Port</b>	Managed Server port number where the SSO Manager is deployed

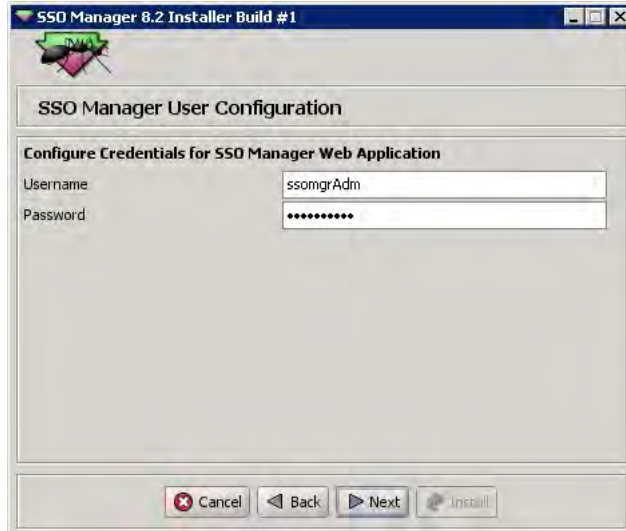


8. Click **Next**.

9. Enter the SSO Manager user configuration:

**Username**                      User name for the SSO Manager web application

**Password**                      Password for the SSO Manager web application



10. Click **Next**.

11. Choose one of the following:

11.1. If you are using the SSO Manager with a third-party access manager, skip to step 12.

11.2. If you are using the SSO Manager with CAS, enter the following information:

**CAS Server Protocol**                      Protocol used by the CAS server (`https` or `http`)

**CAS Server Host**                      CAS server host name

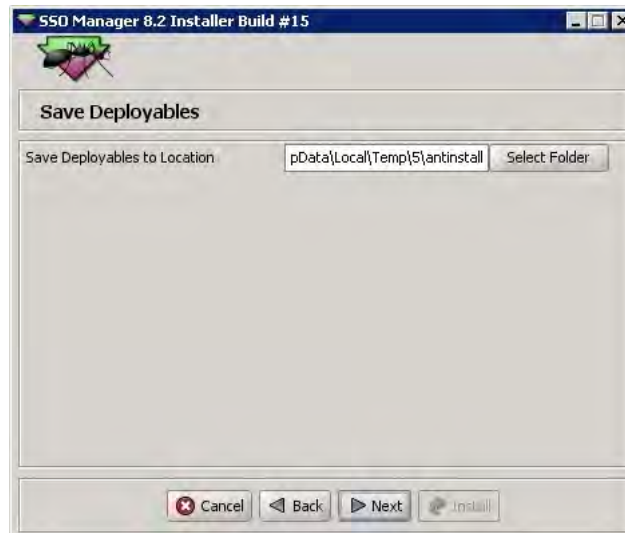
**CAS Server Port**                      Port number where the CAS server is running

**CAS Server Context**                      Context under which CAS is deployed and accessible via a browser (for example, `http(s)://<host>:<port>/<context>`)



12. Click **Next**.

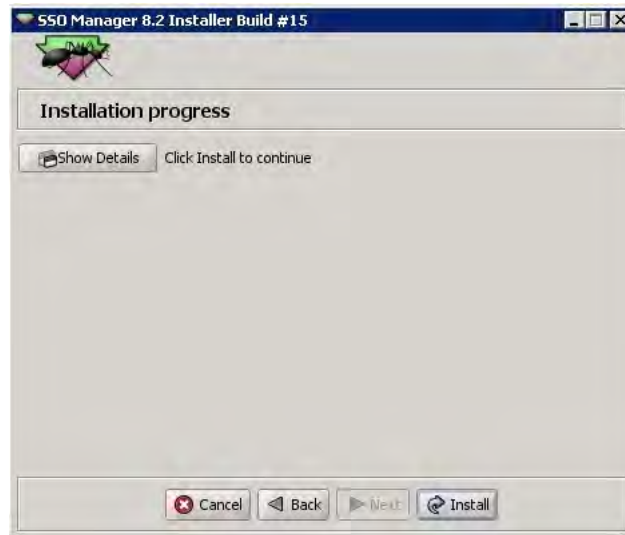
13. Click **Select Folder** and browse to the location where you want to save `sso-manager.ear` and `ssoclient.jar` for manual deployment.



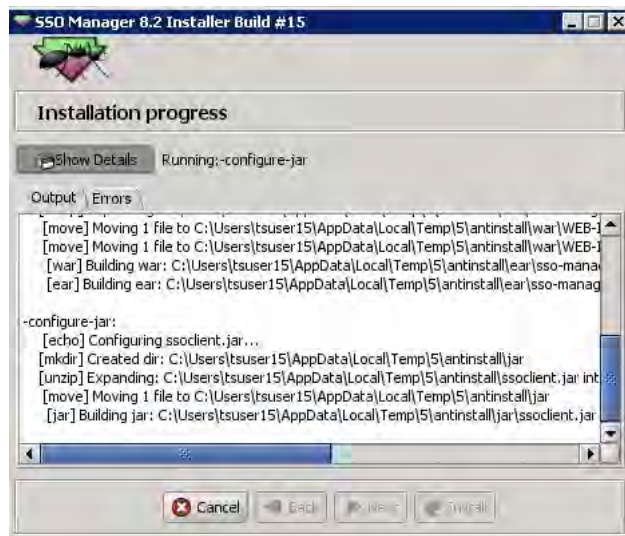
14. Click **Next**.

15. Click **Show Details**.

16. Click **Install**.



Installation details are displayed as the installation progresses.



The message *Install Finished* is displayed when the installation is complete. The `sso-manager.ear` and `ssoclient.jar` files are saved in the selected folder.

## Step 4 - Deploy the SSO Manager

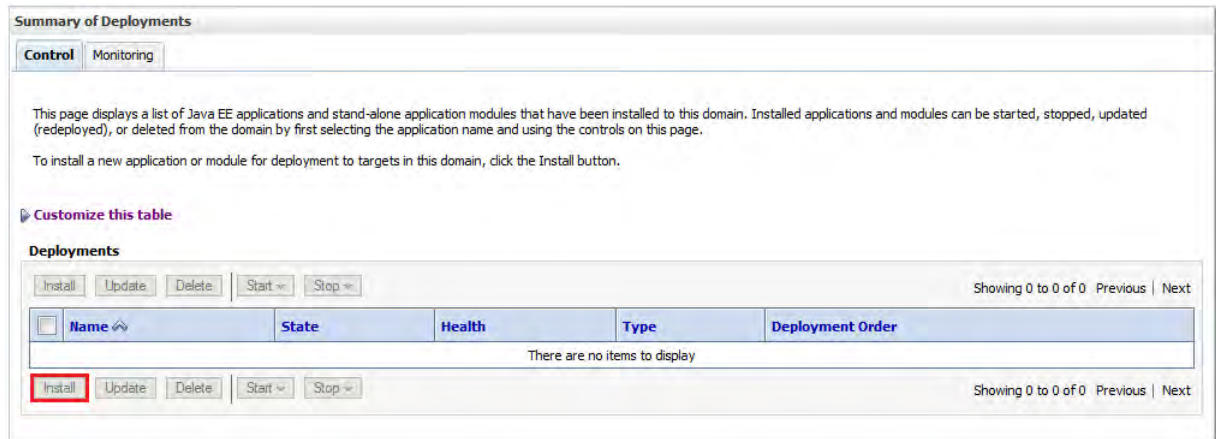
Use the following steps to deploy the SSO Manager.

1. In the Change Center pane, click **Lock & Edit**.

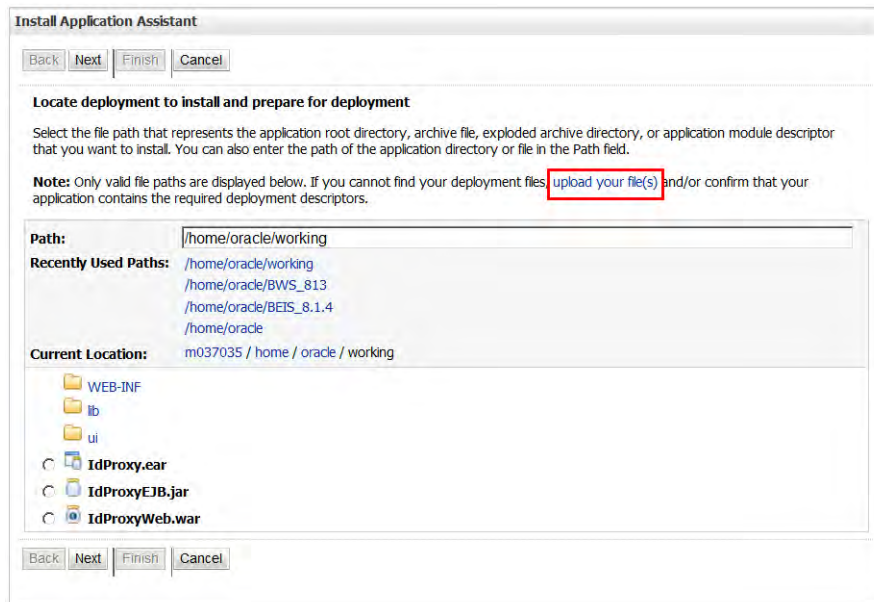
- In the Domain Structure pane, click **Deployments**.



- Click **Install**.

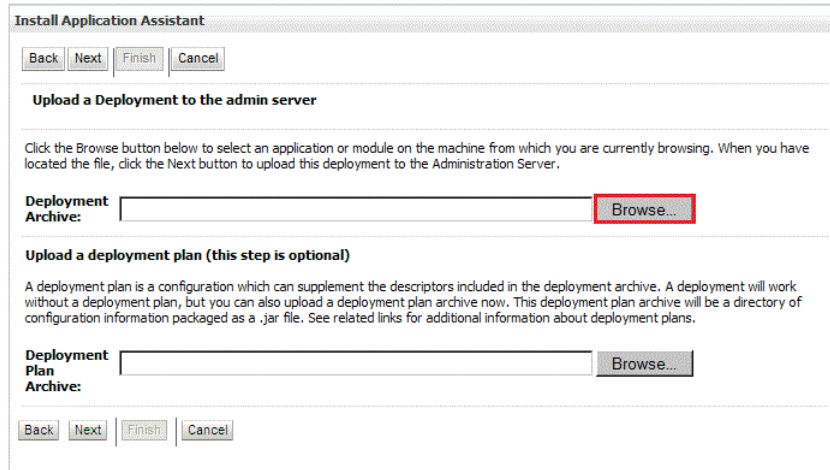


- Click **upload your file(s)**.



5. Select the file to be uploaded as follows:

5.1. In the **Deployment Archive** field, click **Browse**.



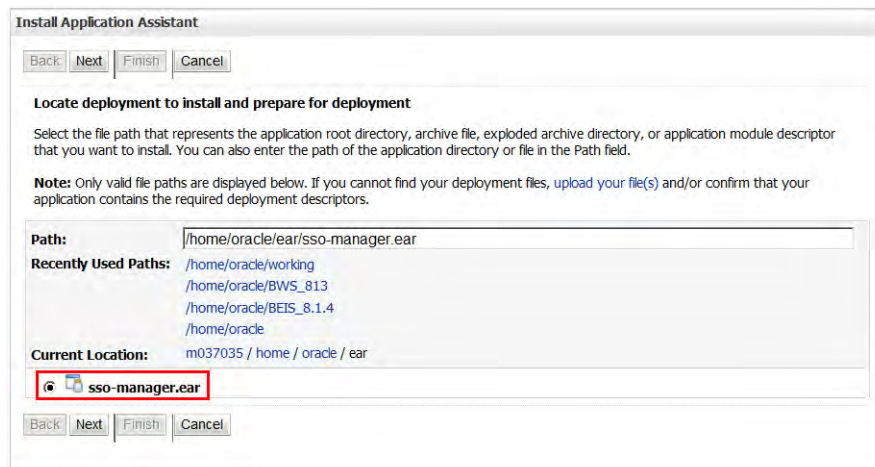
5.2. Navigate to `sso-manager.ear`.

This file was copied to a specified location when the automated installer was run in [Step 3 - Configure the SSO Manager .ear file and the SSO client .jar file](#).

5.3. Select the file and click **Open**.

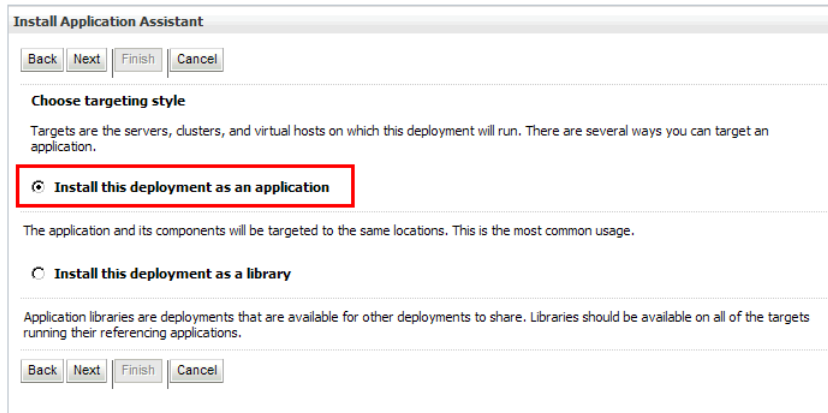
6. Click **Next**.

7. Select `sso-manager.ear` from the list at the bottom of the page.



8. Click **Next**.

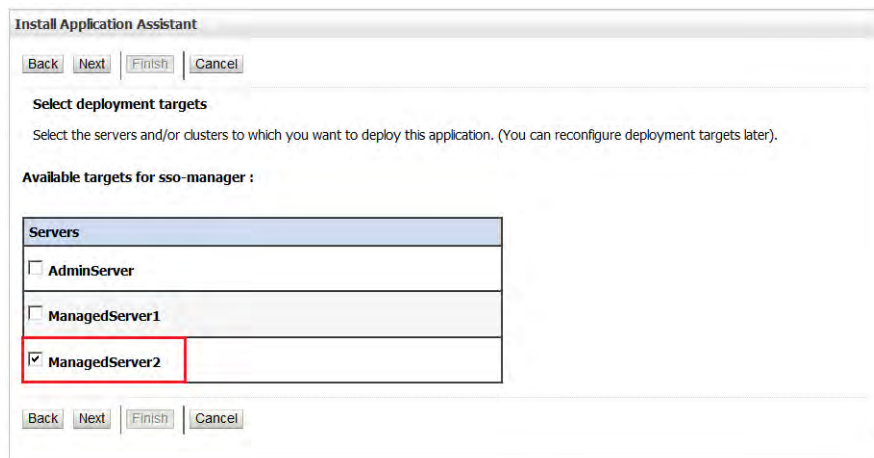
9. Select **Install this deployment as an application.**



10. Click **Next.**

11. The next page is either an optional settings page or a deployment targets page, depending on the domain.

- If an optional settings page is displayed, check your Oracle WebLogic Server configuration before you continue. Make sure that a Managed Server is available for deployment of applications. If a Managed Server is not available, the application will be deployed to the Admin Server, which is not a recommended configuration. For more information, consult the Oracle WebLogic Server Documentation Library. Then go to step 12.
- If a select deployment targets page is displayed, select the server where the application should be deployed. The application can be deployed to an existing server. The application should be installed to a Managed Server, not to the Admin Server. Then click **Next** and go to step 12.



12. Enter the following settings:

**Name** Name for the application (for example, SSOManager )

**Advanced: Use a custom model that you have configured on the realm's configuration page** Select the radio button.

**Copy this application onto every target for me** Select the radio button.

The screenshot shows the 'Install Application Assistant' dialog box with the following settings:

- Optional Settings:** You can modify these settings or accept the defaults.
- General:** What do you want to name this deployment? Name:
- Security:** What security model do you want to use with this application?
  - DD Only: Use only roles and policies that are defined in the deployment descriptors.
  - Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.
  - Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.
  - Advanced: Use a custom model that you have configured on the realm's configuration page.**
- Source accessibility:** How should the source files be made accessible?
  - Use the defaults defined by the deployment's targets
  - Copy this application onto every target for me**
  - I will make the deployment accessible from the following location
- Location:**

Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.

13. Click **Next**.

14. Select **No, I will review the configuration later.**

**Install Application Assistant**

Back Next Finish Cancel

**Review your choices and click Finish**

Click Finish to complete the deployment. This may take a few moments to complete.

**Additional configuration**

In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?

Yes, take me to the deployment's configuration screen.

**No, I will review the configuration later.**

**Summary**

**Deployment:** /home/oracle/ear/sso-manager.ear

**Name:** SSOManager

**Staging mode:** Copy this application to every target for me

**Security Model:** Advanced: Use a custom model that you have configured on the realm's configuration page.

**Target Summary**

Components	Targets
sso-manager.ear	ManagedServer2

Back Next Finish Cancel

15. Click **Finish** to start the deployment. When deployment is completed, the Summary of Deployments page is redisplayed with the newly deployed application.

**Summary of Deployments**

Control Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

[Customize this table](#)

**Deployments**

Install Update Delete Start Stop Showing 1 to 5 of 5 Previous Next

Name	State	Health	Type	Deployment Order
bnig	Active	OK	Enterprise Application	100
IdProxy	Active	OK	Enterprise Application	100
jst(1.2,1.2.0.1)	Active		Library	100
ldap-spmi-ppsp	Active	OK	Enterprise Application	100
<b>SSOManager</b>	<b>distribute Initializing</b>		Enterprise Application	100

Install Update Delete Start Stop Showing 1 to 5 of 5 Previous Next

16. In the Change Center pane, click **Activate Changes.**

17. Start the newly deployed application as follows:

17.1. Make sure the Summary of Deployments page is displayed.

17.2. Select the newly deployed application.

17.3. Click **Start > Servicing all requests**.

Summary of Deployments

Control Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Customize this table

Deployments

Install Update Delete Start Stop Showing 1 to 5 of 5 Previous Next

Name	State	Health	Type	Deployment Order
bmg	Active	OK	Enterprise Application	100
IdProxy	Active	OK	Enterprise Application	100
jst(1.2,1.2.0.1)	Active		Library	100
ldap-spmi-ppp	Active	OK	Enterprise Application	100
SSOManager	Prepared	OK	Enterprise Application	100

Install Update Delete Start Stop Showing 1 to 5 of 5 Previous Next

17.4. Click **Yes** to start the application.

Start Application Assistant

Yes No

Start Deployments

You have selected the following deployments to be started. Click 'Yes' to continue, or 'No' to cancel.

- SSOManager

Yes No

## Step 5 - Evaluate the environment

After you upgrade the SSO Manager, you should run `post_install_ssomgr_checksript.sql` to evaluate your environment and identify potential problems. This script reports on several criteria that are essential for a fully functioning SSO Manager environment. You can use the script to evaluate both new installations and upgrades. Depending on the current state of your Banner/Oracle RDBMS environment, you might need to make changes based on the output of the script.

Use the following steps to run the check script and evaluate the results.

1. Extract `SSOManager_8.2.zip`. The extract directory is referred to as `<ZIP_HOME>`.
2. Open a command prompt and navigate to `<ZIP_HOME>/db-scripts/util`.

3. Ensure that `post_install_ssomgr_checksript.sql` has read permission.
4. Connect to SQL\*Plus as the BANINST1 user.
5. Execute `post_install_ssomgr_checksript.sql`:  

```
sqlplus> @post_install_ssomgr_checksript
```
6. When prompted, enter the username for the SSOMGR schema (for example, SSOMGR).
7. Exit SQL\*Plus.
8. Evaluate the results as follows:

Result	Evaluation
SSOMGR schema	The SSOMGR schema must exist.
Roles assigned to SSOMGR	The following roles must be assigned to SSOMGR: <ul style="list-style-type: none"> <li>• RESOURCE</li> <li>• CONNECT</li> </ul>
Privileges granted to SSOMGR	The following privileges must be granted to SSOMGR: <ul style="list-style-type: none"> <li>• UNLIMITED TABLESPACE</li> <li>• ALTER USER</li> </ul>
Database objects in SSOMGR database schema	The SSOMGR schema should have the following tables: <ul style="list-style-type: none"> <li>• APP_CONFIG</li> <li>• UDC_CREDENTIAL_INFO</li> <li>• UDC_CREDENTIAL_SERVICES</li> <li>• UDC_TICKET_SERVICES</li> </ul>
Sequences that belong to SSOMGR	The SSOMGR schema should have the following sequences: <ul style="list-style-type: none"> <li>• APP_CONFIG_SEQ</li> <li>• UDC_CREDENTIAL_SERVICES_SEQ</li> <li>• UDC_CREDENTIAL_INFO_SEQ</li> </ul>
Packages that belong to SSOMGR	The SSOMGR schema should have the IP_SSO_MANAGER package.

## Step 6 - Confirm access to the SSO Manager

Use the following steps to confirm that you can successfully access the SSO Manager administrative interface.

1. Connect to the SSO Manager:

```
http://<host>:<port>/ssomanager
```

2. Log in with the user name and password for the SSO Manager.

If the login fails, verify that the credentials are correct and that the Oracle WebLogic Server is configured correctly to assign the appropriate users and roles to the application. Repeat these steps until login is successful.

## Step 7 - Configure supporting components

Refer to Chapter 6, “Single Sign On” in the *Banner Enterprise Identity Services 8.2 User Guide* for instructions on configuring the components that support SSO:

- SSO Manager settings
- Banner Web Tailor settings for Self-Service Banner (SSB)
- Oracle Forms server settings for Internet-Native Banner (INB)