Exor / IMS Integration

Configuration Guide

0.4

February 2020

Document Version History

Version	Owner	Update Source	Date	Description
0.1	Chris Baugh		March 2017	Initial Draft
0.2	Upendra Hukeri		May 2018	
0.3	Chris Baugh		August 2019	Midtier User password changes
0.4	Chris Baugh		February 2020	Midtier user creation amendment
0.5	Chris Baugh		February 2020	Added Note on Username length restrictions when defining Midtier User

For review:			For approval:

Table of Contents

1 Introduction

1.1 Summary

This document details the steps required to configure integration between Exor Core and the Bentley IMS product, allowing for Single Sign-On access to the Exor Forms Application. The Exor user will no longer be required to provide a username and password for access, but will be authenticated with their network credentials, providing access to the Exor Forms Application for their associated Exor username.

Introducing IMS Authentication will result in the current login Form being replaced by the Identity Provider Login Screen, as detailed in 5.2.2

CONFIDENTIALITY STATEMENT

The contents of this document, including system ideas and concepts, are confidential and proprietary in nature and are not to be distributed in any form without the prior written consent of Bentley Systems Inc.

2 Configure Identity Provider

2.1 Overview

This document is written with the assumption that the installation will make use of a WS-Federation compatible authentication provider. Bentley offer this with the IMS product. The following instructions describe the information needed to configure Bentley IMS support and the steps to collect that information. For brevity, the authentication provider will be referred to as the identity provider or IdP.

2.2 Configuration

2.2.1 Application URL – RP Identifier

The first piece of information required is the URL under which you will locate the Exor forms application. This will be the URL that users will use in their browser to access the forms implementation. This information is critical as you must register the application URL with the IdP for the purposes of validation.

Let's assume that the forms URL will be:

https://app-server.sample.com

and will run on port 9001 then we can see that the first part of the URL will be:

https://app-server.sample.com:9001

The installation you will perform will create a path on that URL named exor-ims. So, the full URL for this example will be:

https://app-server.sample.com:9001/exor-ims/

The site specific URL will be similar to the one above, however the server details and port number will differ. If exor-ims has been installed to a sub folder of the site, then that will also impact the URL. For the purposes of configuring the IdP we will refer to the URL identified as the URI of the **Relying Party** (RP) or RP Identifier. This is WS-Federation terminology but is useful to know when communicating with the IdP administrators. Make a note of the real RP Identifier:

RP Identifier:	

2.2.2 Registering Relying Party

Contact the IdP administrators to register the RP Identifier and request information needed for the local configuration to be carried out.

The process to register an RP will be dictated by the IdP involved. They will need to know the RP Identifier, and may need other information to reinforce the validity of the application for registration.
For the purposes of registering this implementation, the RP identifier (see above) is the value to be used for **audienceuris**, **realm** and **reply** parameters specified in the federation.properties file (see section 3 Step 5), if specifically requested by the IdP request process.

The information needed from the IdP will be the following:

i. **The URI of the IdP security token service (STS)**
   This is the web address that will accept WS-Federation requests

ii. **A friendly name for the IdP/STS**
    Provide a short name to identify the IdP, it is not significant, but should be helpful in explain the service that has been configured (e.g. Bentley IMS)

iii. **The X509 thumbprint of the STS signing certificate**
     This will be in the form of a hexadecimal string, e.g.:
     74dcf3da6dc654bceae79403d7848db29e350f10
     This must be supplied to ensure security tokens are validated by the thumbprint.
     (Multiple thumbprint values can be handles if separated by the 'pipe' symbol |)

iv. **The federation metadata URI**
    This must be provided to enable polling of metadata and automatic certificate rotation (recommended)

v. **The entity ID to be used from the above metadata document**
   Not mandatory, the STS issuer URL will be used if not overridden here.

3 Application Server Configuration

1. Go to the relevant `<ORACLE_INSTANCE>` directory on the Application Server e.g. E:\Oracle\Product\Middleware\instance and create the following sub-directory – `exorsso`
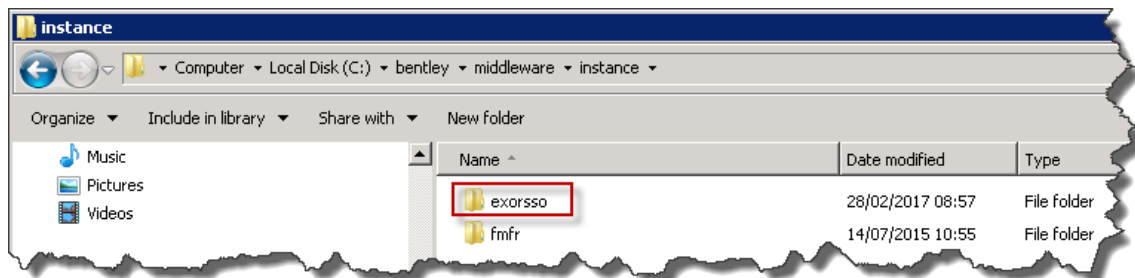
2. Change directory to the newly created exorsso sub-directory, copy in **exor-ims.war** and rename it to **exor-ims1.war**

3. Create a subdirectory named **exor-ims.war**.
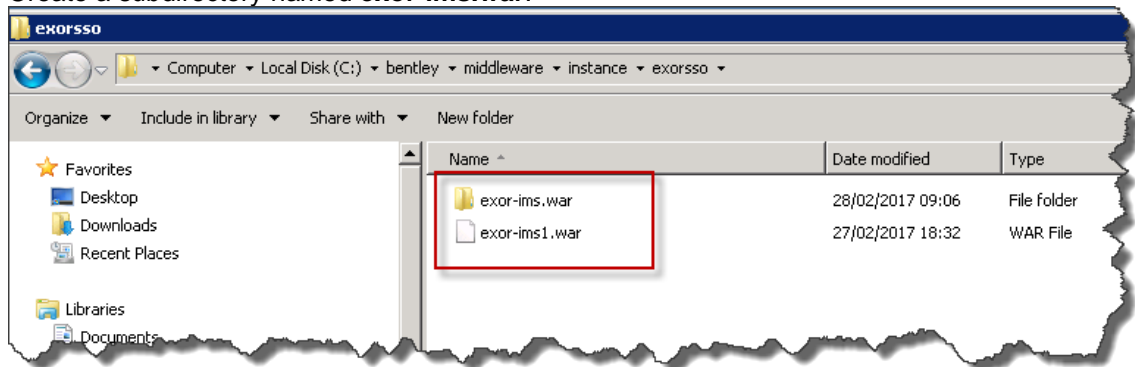
4. Unpack **exor-ims1.war** into the **exor-ims.war** directory

Custom logo can be used for the application by replacing `\exor-ims.war\images\bentley-logo.jpg` with another JPG image.

Note: The new image must be of **JPG format** only and must have name – **bentley-logo.jpg** only.

5. Change directory to exor-ims.war\WEB-INF\classes\ and modify the entries in the **federation.properties** file as follows:

| Property	Value
federation.trustedissuers.issuer	Value Identified in 2.2.2 Step i
federation.trustedissuers.thumbprint	Value Identified in 2.2.2 Step iii
federation.trustedissuers.friendlyname	Value Identified in 2.2.2 Step ii
federation.audienceuris	Value of the RP Identifier, noted in 2.2.1
federation.realm	Value of the RP Identifier, noted in 2.2.1
federation.reply	Value of the RP Identifier, noted in 2.2.1
federation.metadata.uri	Value Identified in 2.2.2 Step iv
federation.metadata.entityid	Value Identified in 2.2.2 Step v If no value is provided, then this property should be removed from the file

6. Launch **Oracle WebLogic Server Administration Console** in an internet browser and Navigate to **Domain Structure** > **Deployments**
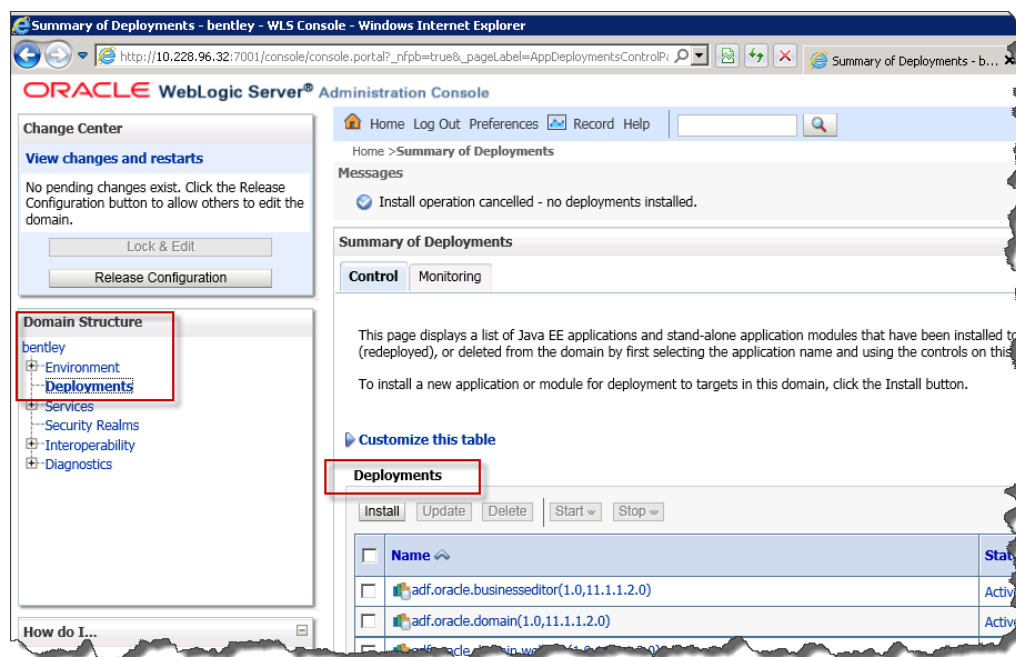
Click the **Install** button. Note: you may have to click the **Lock and Edit** button if in P**roduction** mode for the **Install** button to become available.
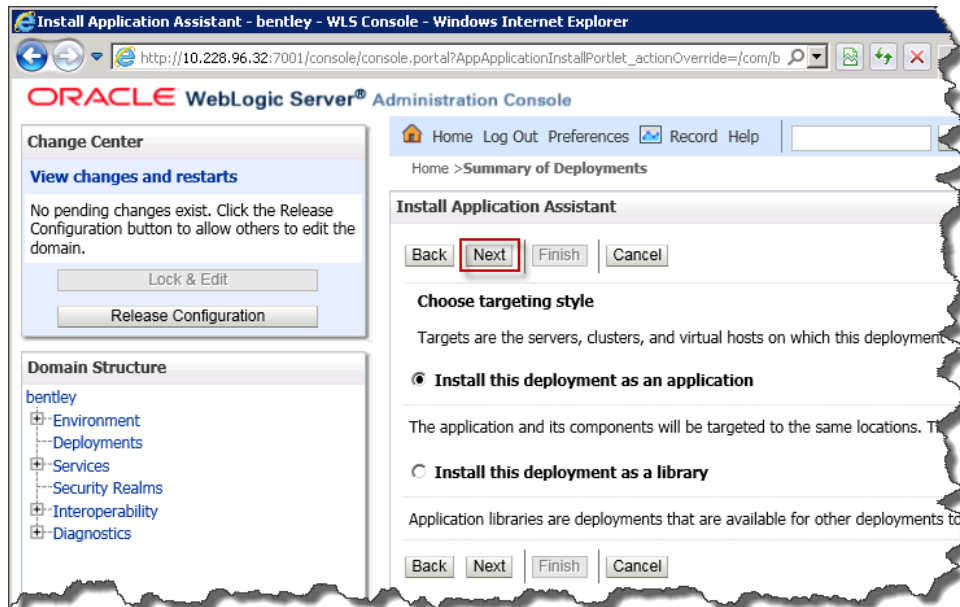
7. Select **exor-ims.war** in the **Install Application Assistant** screen, and click **Next**.
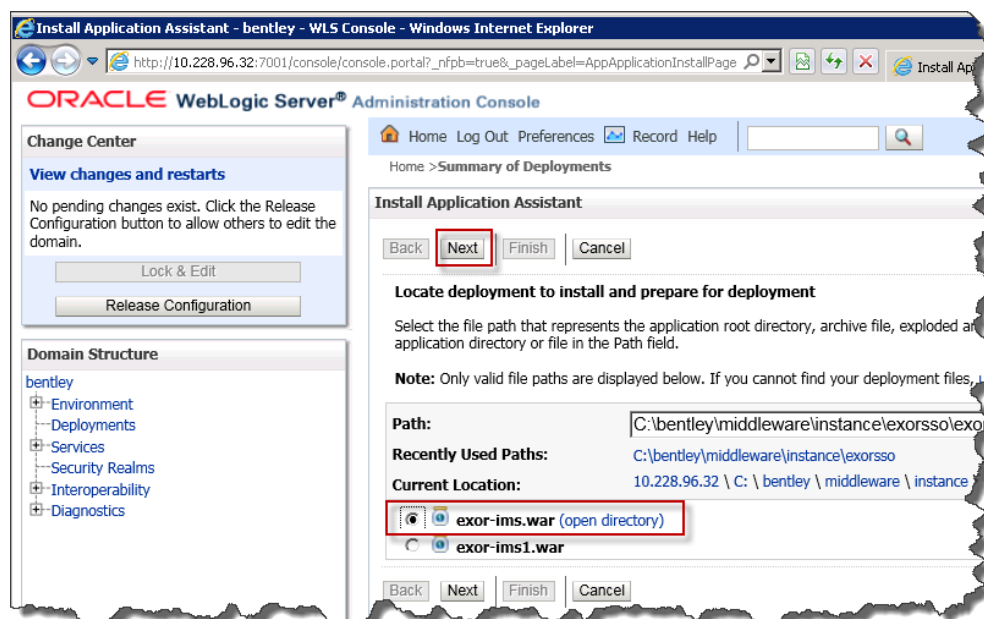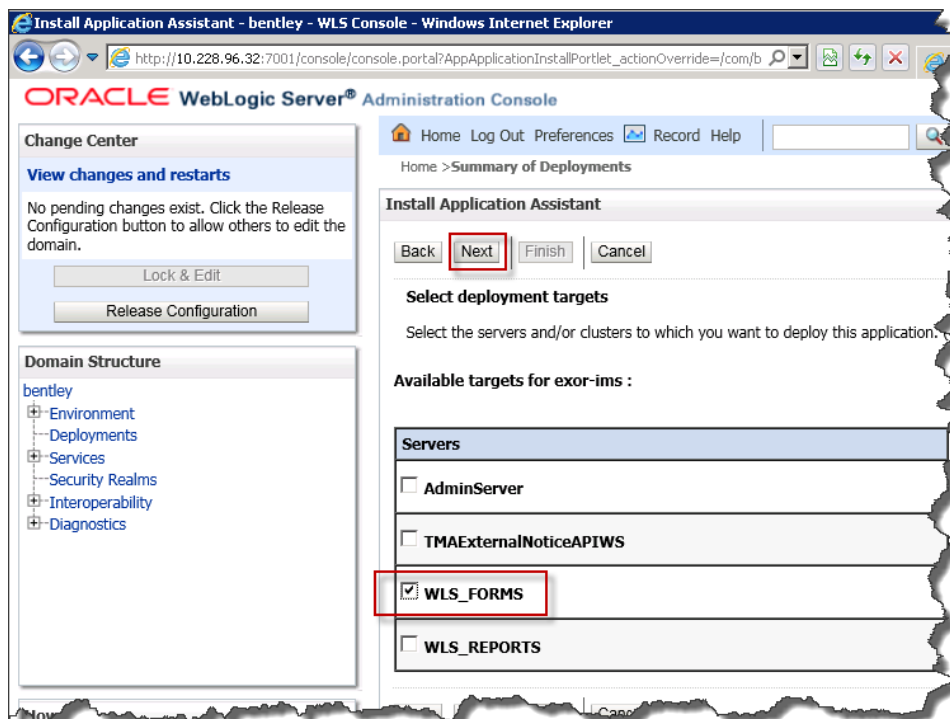

---

8. Under **Choose targeting style**, accept the default (**Install this deployment as an application**), and click **Next**.
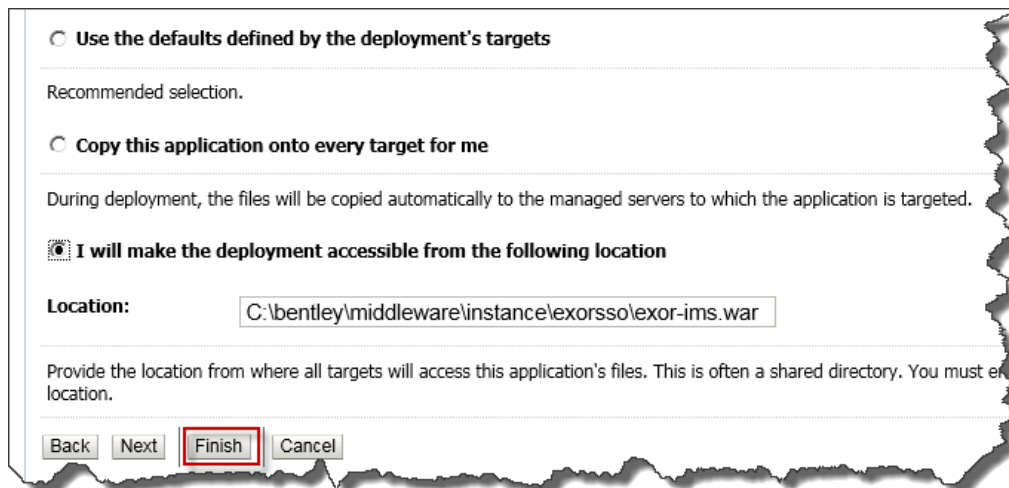

9. In the **Select deployment targets**, under **Servers** select the WebLogic Forms Server (i.e. **WLS_FORMS**), and click **Next.**

10. In **Install Application Assistant** screen, under **Source Accessibility**, select **I will make this deployment accessible from the following location** and click **Finish**

11. If the WebLogic Server was configured in **Production** mode, click **Activate Changes** to activate the deployment.

CONFIDENTIALITY STATEMENT

The contents of this document, including system ideas and concepts, are confidential and proprietary in nature and are not to be distributed in any form without the prior written consent of Bentley Systems Inc.

4 Start and Test exor-ims Application

4.1 Starting Application

1. On the **Summary of deployment**s page select the just installed **exor-ims** application from the list.
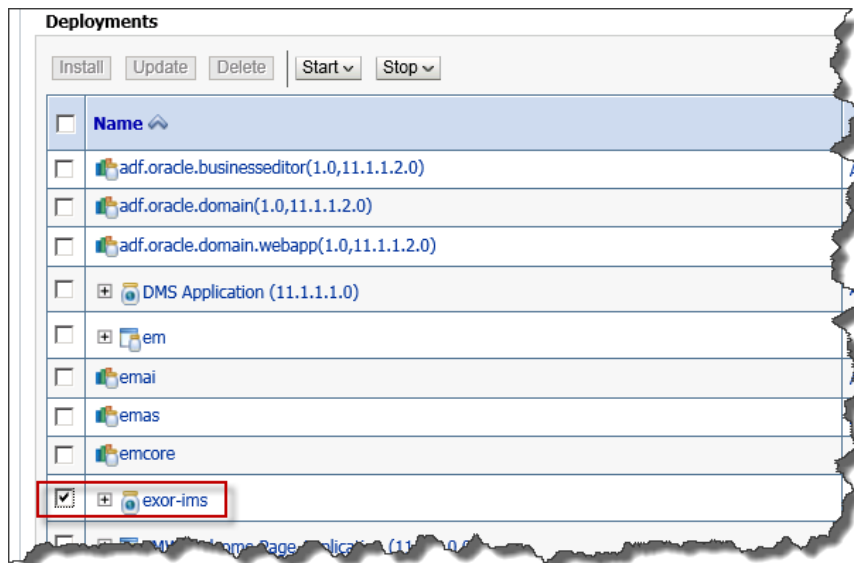
2. Click **Start > Servicing all requests** and click **Yes** on the confirmation screen produced.

The exor-ims deployment should have a **State** of **Active**, and **Health** of **OK**

4.2 Testing Application

The exor-ims application can be tested as follows:

1. Launch **exor-ims** application URL

    e.g. http://app-server.sample.com:9001/exor-ims/
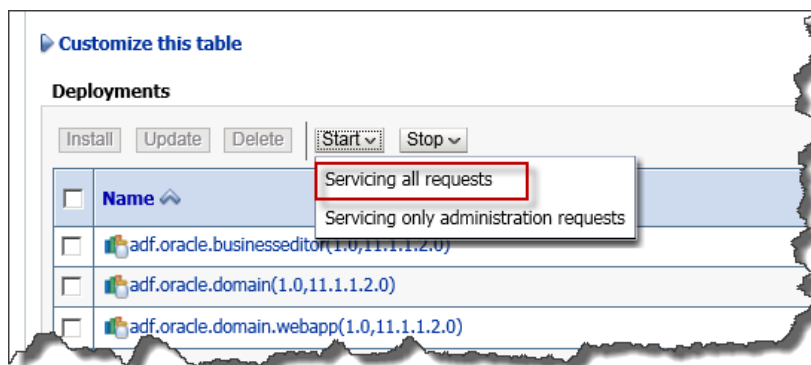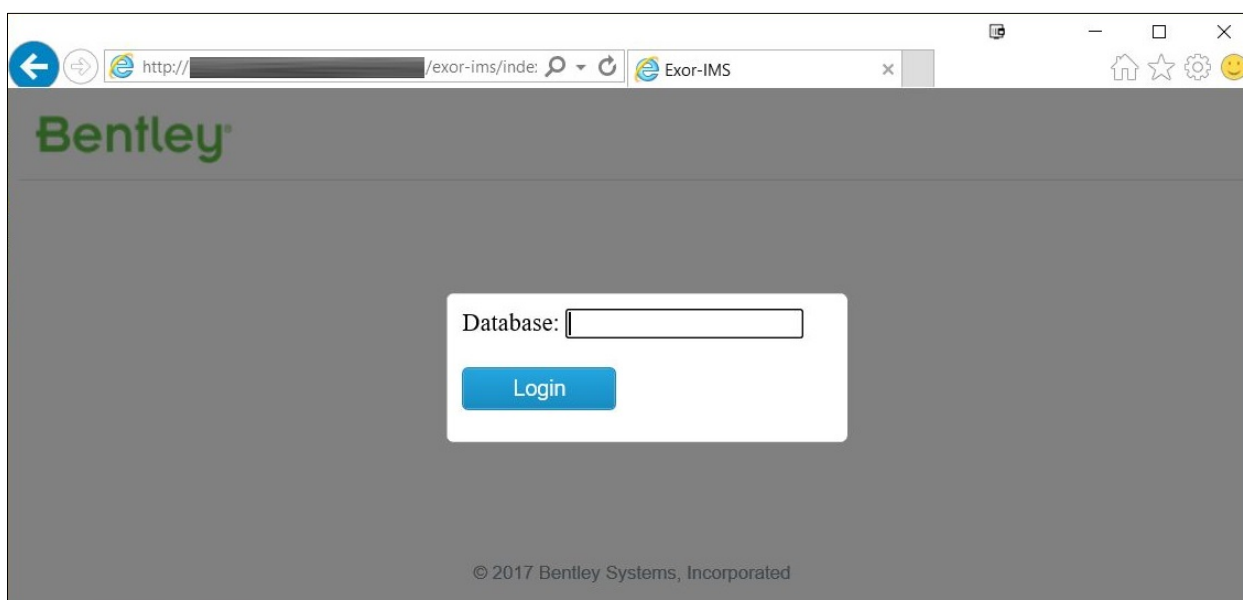
2. After successful authentication by Identity Provider, you should be presented with the application's main page, as below

3. If this page does not display, ensure that the configuration specified in section 3 step 5 is correct, and that the RP Identifier, specified in 2.2.1 is valid.

4.3 MidTier User

User Authentication via IMS makes use of Oracle's Proxy Authentication, where a Proxy User is defined that will connect and authenticate against the database on behalf of another database user.

The Proxy User username and password would be known, and would allow connection to the Exor Forms Application where users have granted permission to connect on their behalf.

To allow for this, the PROXY_OWNER Role has been created, where any user granted this role can be used as a Proxy User.

As an example:

- *MidTier* is defined as an Oracle user and is assigned PROXY_OWNER role (i.e. *MidTier* is a Proxy User).
- *SSOUser* is defined as an Exor user and is registered as a Single Sign-On user.
- *SSOUser* assigns *MidTier* as a Proxy User

The result of the above is that *MidTier* can connect to the Exor Forms Application as *SSOUser.* The connection would be as if *SSOUser* had logged on, where the roles, privileges etc. would be those assigned to *SSOUser.*

Within this document the Proxy User will be identified as the MidTier User.

4.3.1 Creating the MidTier User

The MidTier user is created by logging on to SQL*Plus as the Highways Owner and executing the following:

start midtier_user_definition.sql

You will be prompted for the Userid and Password for the midtier user.

Note 1: The MidTier user must not be Highways Owner user. The Midtier user must not be created using the Exor Users Form (HIG1832).

Note 2. When defining the Midtier user, the length of the Userid + Length of longest Exor Username must not exceed 28 characters.

4.3.2 Midtier User Password settings

As the MidTier User is used as a Proxy User the password must be changed periodically to ensure the User account does not expire. Alternatively, the MidTier user could be configured with a profile that contains an unlimited expiry period. (ie password does not expire);

Important Note: Whenever the MidTier user password is changed, the Mapviewer Datasource details MUST be updated (see 4.5.2) and the credentials will need updating using HIGENC form, as specified in 5.1 Any application that stores the MidTier user password in configuration files MUST also be updated.
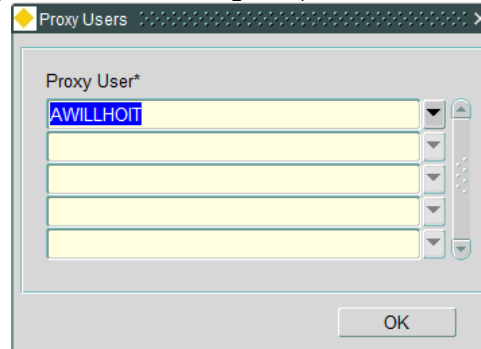
4.4 Enabling User Authentication via IMS

To allow access to the Exor Forms Application using IMS Integration, the user must be an existing Exor User and must be registered for Single Sign-On, using Users form (HIG1832), as follows:
SSO User checkbox must be checked
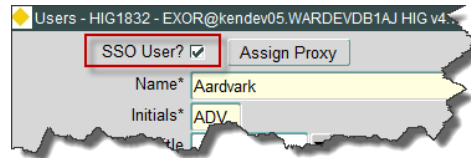
- A Proxy User must be assigned (Note this will be the MidTier User defined in 4.3.1, above)

- An email address must be specified for the user in the E-Mail tab

4.4.1 Credential Storage to Support Single Sign-On

4.4.1.1 HIG_RELATIONSHIP table

HIG1832 will save any credentials to a new table, HIG_RELATIONSHIP, for those users that are registered as Single Sign-On users. For security reasons the column names are non-descriptive, making it more difficult to identify the data being held.

HIG_RELATIONSHIP		
Column	Datatype	Notes
HIR_ATTRIBUTE1	VARCHAR2(50)	Email address of user
HIR_ATTRIBUTE2	RAW(2000)	Encrypted Username
HIR_ATTRIBUTE3	VARCHAR2(1)	Override Automatic Password Management (Y/N)
HIR_ATTRIBUTE4	RAW(2000)	Encryption Key

4.4.1.2 HIG_RELATIONSHIP Policies

To ensure the HIG_RELATIONSHIP table is secure, ORACLE policies have been defined restricting Select, Insert, Update & Delete privileges, as follows:

- Insert, Update & Delete privileges will only be available to users with HIG_ADMIN Role assigned
- Select privilege will only be available to users with HIG_ADMIN Role, or to users defined as MidTier Users, as defined in 4.3

4.4.1.3 HIG_RELATIONSHIP population

Details are created in the HIG_RELATIONSHIP table as follows:

- The email address is used as the key to identify the credentials, and is saved in HIR_ATTRIBUTE1.

- A random 32-character RAW value is generated, and is used to populate HIR_ATTRIBUTE4.

- The RAW value held in HIR_ATTRIBUTE4 is used as a key for Oracle's DBMS_CRYPT package routines to encrypt the user's Username, which is then stored in HIR_ATTRIBUTE2.

- HIR_ATTRIBUTE3 will define whether Automatic Password Management is overridden for a user (i.e. If set to 'Y' the password is not automatically generated).

4.5 Update or Create MapViewer Datasource with MidTier User

Note: This section is only applicable if the Highways Owner has been defined as an SSO User and the password is system generated, otherwise this section can be ignored.

4.5.1 Midtier User Proxy Configuration

The Mapviewer configuration needs to be amended, to allow for the MidTier user to Proxy as the current Map User. This is achieved as follows:

- Log on to SQL*Plus as **SYS** user

- Enter the following command:

 alter user <MapUser> grant connect through <MidtierUser>;

  Where <MapUser> =   User currently defined for jdbc_user in **mapViewerConfig.xml** –see 4.5.2

  <MidtierUser> =   MidTier User defined in 4.3.1

4.5.2 Mapviewer Datasource changes

The MapViewer Datasource needs to be updated to replace the current user details to allow for access via the MidTier User. On the Mapviewer Application Server, modify the datasource as follows:

1. Launch **Oracle MapViewer Administration Console** in an internet browser select the **Admin** URL, ie
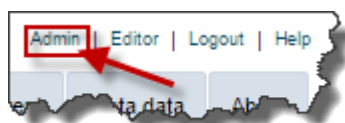
2. Select **Configuration**, and edit the appropriate Mapviewer Data Source details as follows:

```
<map_data_source name="mvdemo"
jdbc_host="db1.sample.com"
jdbc_sid="orcl"
jdbc_port="1521"
jdbc_user="<MidTierUser>[<MapUser>]"
jdbc_password="!MidTierPassword"
jdbc_mode="thin"
number_of_mappers="21"
max_connections="100"
allow_jdbc_theme_based_foi="false"
editable="false"
```

```
plsql_package="web_user_info"
web_user_type="SUBUSERNAME"
/>
```

Where **<MapUser>** =   User currently defined for jdbc_user in **mapViewerConfig.xml** –see 4.5.2

<MidtierUser> =   MidTier User defined in 4.3.1

MidTierPassword =   Password defined for MidTier User

3. After modification, apply the changes using the **Save & Restart** button.

5 New Exor Forms

5.1 HIGENC – Exor Encryption Form

5.1.1 Overview

To enable Single Sign-On via IMS, the database connection string using the MidTier user credentials, i.e:

<MidTierUser>/<MidTierPassword>@<Database name>

needs to be encrypted and stored securely, along with the encryption key, on the application server.

This form allows for this, performing the following:

- Create, encrypt and store **User Encryption Key**
- Encrypt and store database connection string

5.1.2 Functionality

1. The form is accessed using a URL of the following format:

   http://<server-name>:<port>/forms/frmservlet?config=<config-name>&form=higenc.fmx

2. The form can only be accessed from the Application Server. Attempting access from any other machine will show an error message similar to the following:
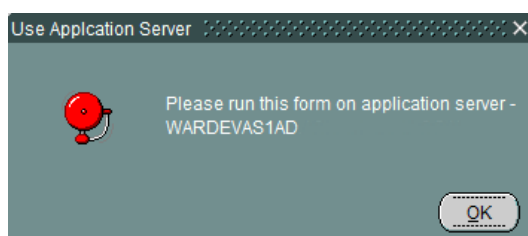
3. The form will initially check if a **User Encryption Key** already exists on the server, if not the following dialog will be produced:
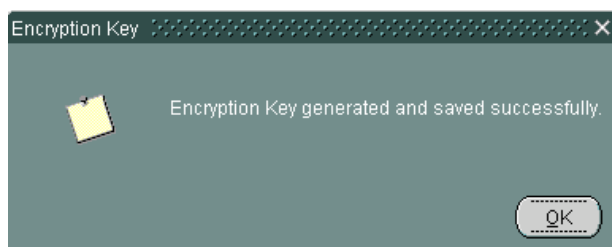

   Clicking on **Ok** button will create, encrypt and save a **User Encryption Key** on the server. Clicking on **Cancel** or *closing the message window* will exit the form.
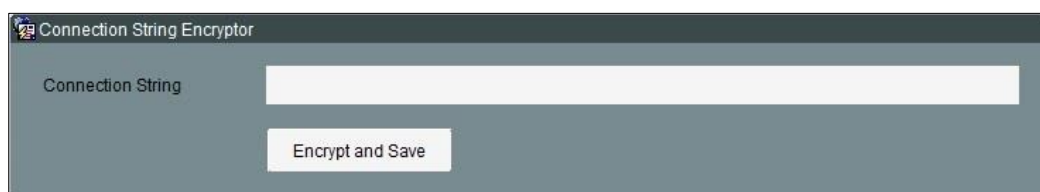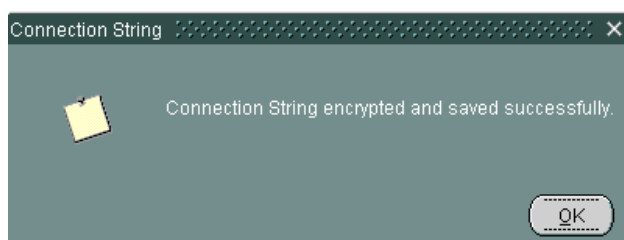
4. After successful **User Encryption Key** generation, the following dialog is displayed:

5. Once the **User Encryption Key** has been generated, the Connection String (as specified in 5.1.1) can be encrypted using the **Connection String Encryptor** screen:

6. After successful encryption, the following dialog is displayed:

5.2 HIGSSO – Exor SSO Form

5.2.1 Exor Application access
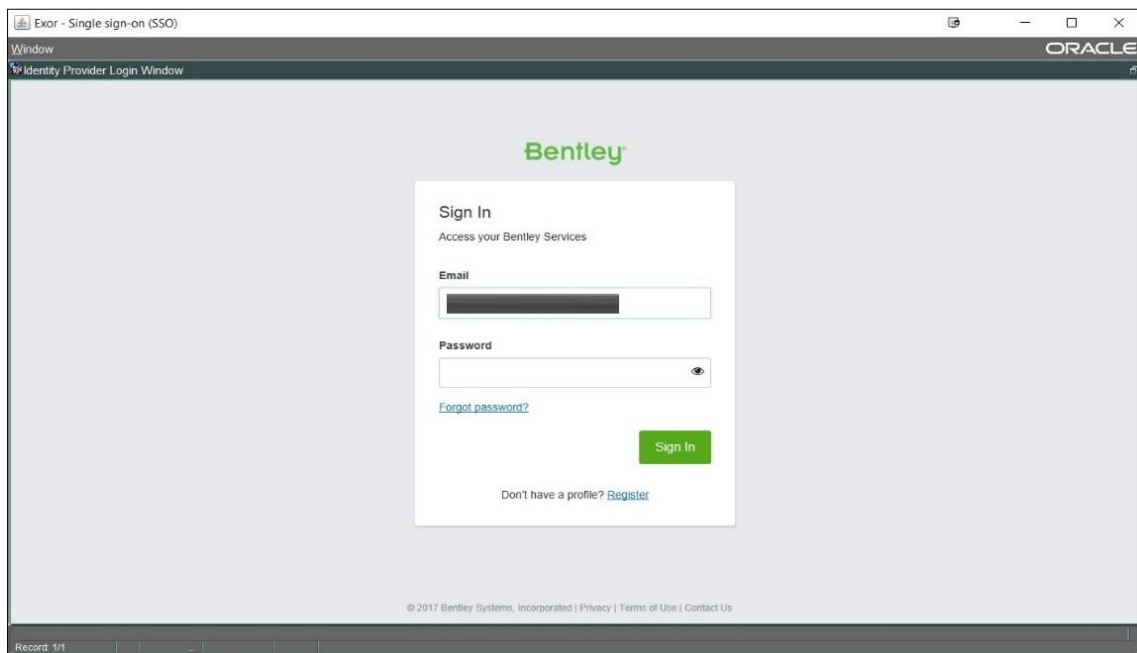
Access to the Exor Forms Application is via a URL of the following format:

http://<server-name>:<port>/forms/frmservlet?config=<config-name>&userid=@<database>

Note: This is similar to existing URLs, but where the username/password may have been used previously, this is no longer required. If the username and password are provided, as they are currently, this will have no effect.

5.2.2 Identity Provider's Login Screen

The Identity Provider's login screen will be displayed. The following is the login form from Bentley IMS, as an example
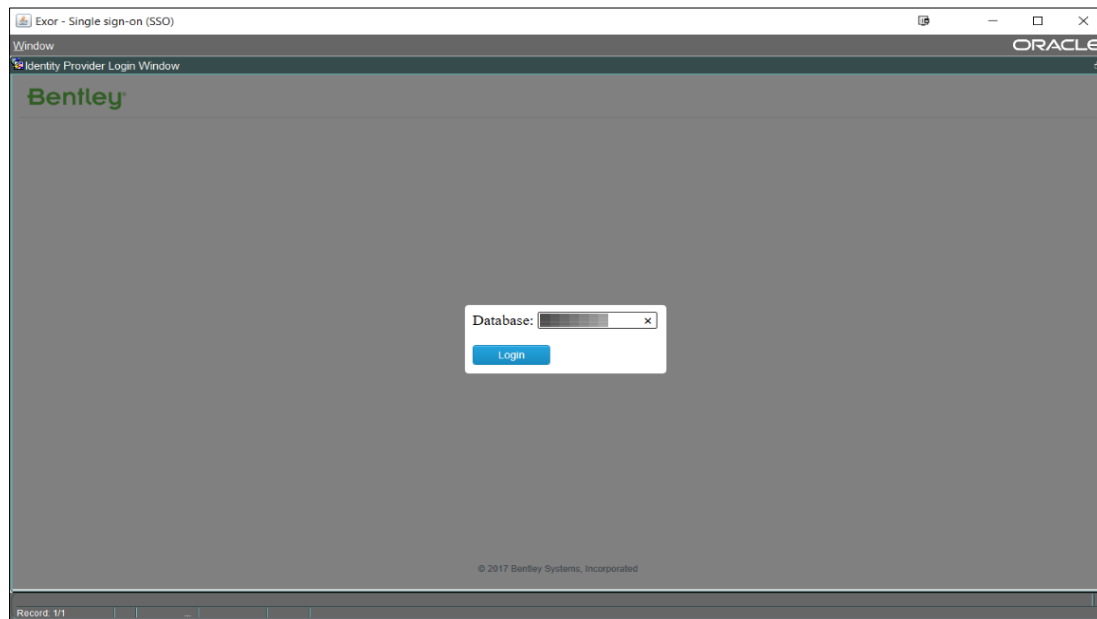
5.2.3 **Database Screen**

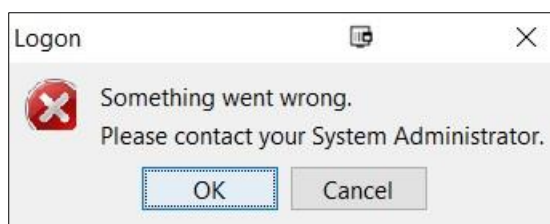If the <ins><database></ins> value is not supplied in the URL, the user will be presented with the following screen, requiring it to be provided, the Identity Provider's screen, as above, will then be displayed.

5.2.4 **Error Handling**

If a problem is encountered, the following error dialog will be displayed to the user:

Closing the above dialog will exit the Exor application. The cause of the problem will be logged on the Application Server, which will only be accessible to the System Administrator. The user must contact the System Administrator to resolve the issue.

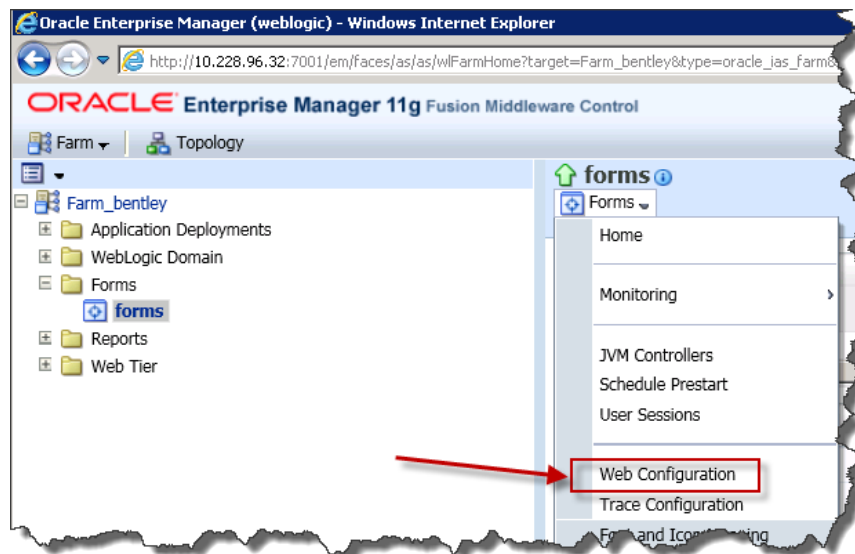Details on Error Logging can be found in section 6.
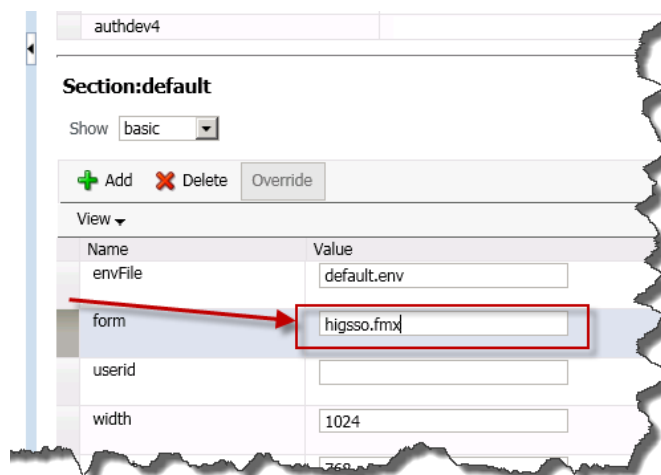
5.3 Oracle Forms Configuration

5.3.1 Update fomsweb.cfg

1. Launch **Enterprise Manager Fusion Middleware Control** in an internet browser using the URL *http://<server_name>:<port>/em* and navigate to the **forms** page. From the **forms** dropdown menu choose **Web Configuration** i.e.

2. For the appropriate **Web Configuration** change the **form** value to higsso.fmx
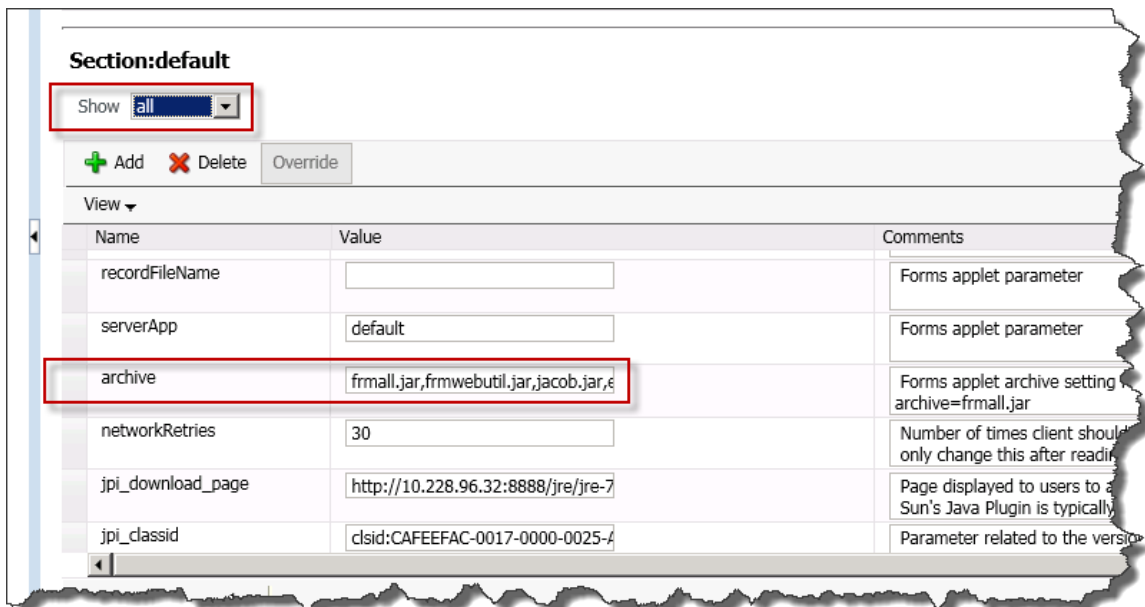
3. Change the section view to **All** and modify the archive value to include

```
exor_login_util.jar
DJNativeSwing-SWT.jar
DJNativeSwing.jar
swt.jar
bouncy-castle-provider.jar
commons-codec.jar
```

separating each value by a **comma** only

4. Press **Apply** to save the settings.

5. Restart the **WLS_FORMS** server to apply all the configuration changes mentioned above.

6 Logging

6.1 Configuring logging

1. Copy the **log4j.properties** file from staging folder to a suitable location on **WebLogic Forms Server** –

    e.g. `E:\log\`

2. Edit the log4j.properties file in a text editor to configure the logging, as follows:

Property	Description	Sample Value
log4j.rootLogger	Log Level. Allowed parameters are DEBUG, INFO, TRACE, WARN, FATAL and ERROR. Do not remove the 'file' from value.	TRACE ERROR, file
log4j.appender.file.File	Path to the target file.	E:\\exor\\log\\exception.log
log4j.appender.file.MaxFileSize	Maximum allowed file size (in bytes) before rolling over. Suffixes "KB", "MB" and "GB" are allowed. 10KB = 10240 bytes, etc.	5MB
log4j.appender.file.MaxBackupIndex	Maximum number of backup files to keep.	10

Note: In the above example only exception messages will be logged. To also include debug messages log4j.rootlogger property should be defined as follows:

   DEBUG TRACE ERROR, file

i.e. all parameters added prior to ', file' must be separated by a ' ' (SPACE character)

3. **Updating Forms Environment Configuration**

Launch **Enterprise Manager Fusion Middleware Control** in an internet browser using the URL *http://<server_name>:<port>/em* and navigate to the **forms** page. From the **forms** dropdown menu choose **Environment Configuration**, i.e.
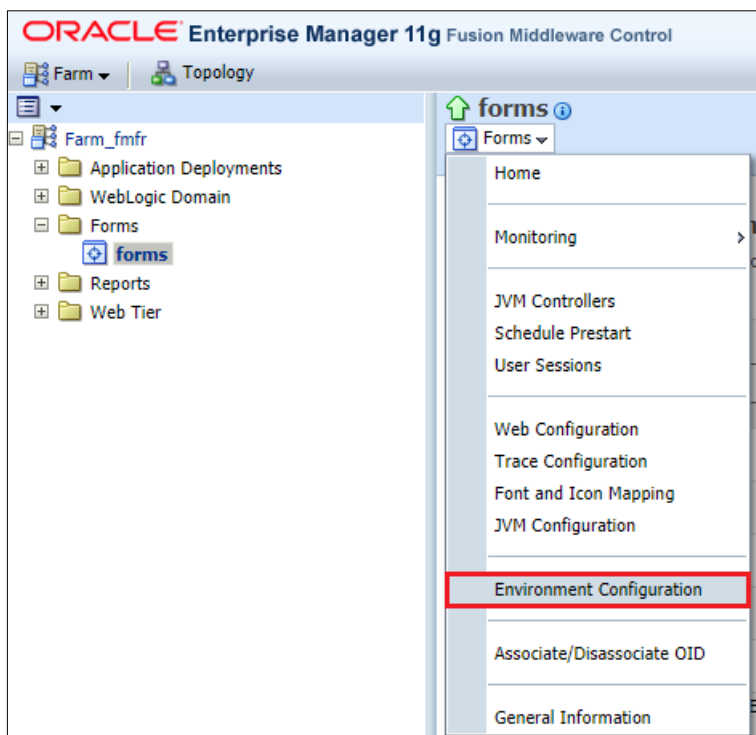
Select appropriate `.env` file from the dropdown for respective **Web Configuration**, i.e.

Update the `CLASSPATH` value to include the path to `log4j.properties` file's directory (as set in step 1 in this section)

e.g. `E:\log\` (separated by semicolon - ';')

CLASSPATH	E:\log\;	

Press **Apply** to save the settings.

6.2 Exception Logging

There are two parts to the authentication with Single Sign-On (SSO):

- Authentication at **Identity Provider** level

- Authentication at **Exor Database** level

If an exception is encountered at Identity Provider level, the corresponding error will be displayed in the **higsso** form.

If an exception is encountered at Exor Database level, (e.g. The user has not been registered for Single Sign-On), the dialog in 5.2.4 will be displayed to the user and all exception and error details will be logged on the Application Server, as shown in the following example log file:

```
2017-09-07 20:39:39 DEBUG IMSLogger:41 - getOracleConnection(): Getting Oracle DB Connection...
2017-09-07 20:39:47 TRACE IMSLogger:53 - user BENTLEY\John.Smith, at HUKEU4809PUNL : Successfully authenticated user at Exor level
2017-09-07 20:40:28 TRACE IMSLogger:53 - user BENTLEY\John.Smith, at HUKEU4809PUNL : Authenticating user at Bentley-IMS level...
2017-09-07 20:41:17 TRACE IMSLogger:53 - user BENTLEY\John.Smith, at HUKEU4809PUNL : Successfully authenticated user with configured Identity Provider
2017-09-07 20:41:17 TRACE IMSLogger:53 - user BENTLEY\John.Smith, at HUKEU4809PUNL : Authenticating user at Exor level...
2017-09-07 20:41:17 DEBUG IMSLogger:41 - getRelationship()_    Forms URL - 99.999.99.99:9001_  Datasource - ENFDEV47_  Email-ID - john.smith@bentley.com
```

7 Auto-generated Password Reset Process

Where users have been registered for Automatic Password management, a new process has been introduced which will allow for regular password updates. A random password will then be generated for each of these users.
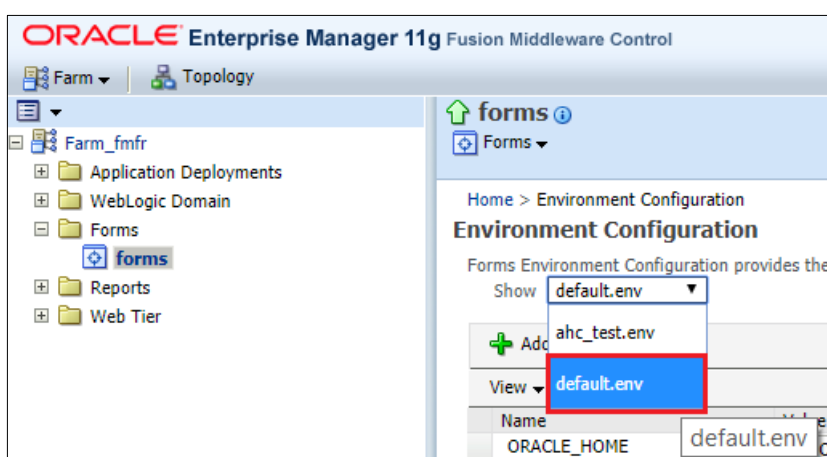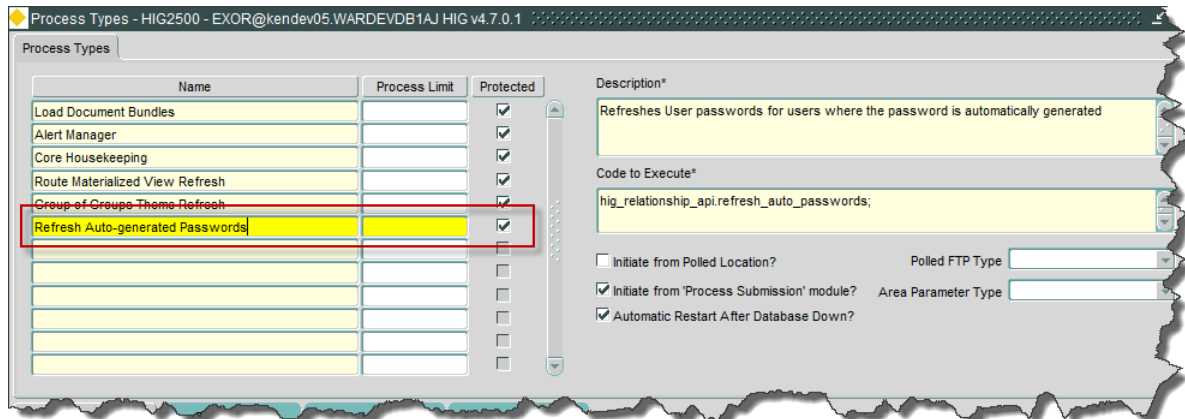
CONFIDENTIALITY STATEMENT

The contents of this document, including system ideas and concepts, are confidential and proprietary in nature and are not to be distributed in any form without the prior written consent of Bentley Systems Inc.

8 User Migration

8.1 Enabling User Authentication via IMS

Exor users can be registered for authentication via IMS using the Users form (HIG1832), as specified in 4.4

8.1.1 Example Migration Script

As it would be laborious to register all existing users via the Users form, the **migrate_users.sql** script has been provided as an example, to automate this process.

This script should be run in SQL*Plus as the Highways owner and assumes the following:

- All users to be migrated will have an account status of 'OPEN'
- There will only be one MidTier User (ie Only one user defined with PROXY_OWNER Role)
- All Users to be migrated will have an email address defined

As this may not be suitable for all implementations this script may require modification.

8.1.2 IMS Authentication Exclusion

The **migrate_users.sql** script allows for any users that require access via the existing method to be excluded from authentication via IMS by adding the username to an exclusion list. The following line should be modified to include usernames that should be excluded:

lv_exclude_list VARCHAR2(32767) := 'USERNAME1,USERNAME2,USERNAME3';

Where USERNAME1, USERNAME2 etc are existing Exor usernames