

****HOSTED LEARNING GATEWAY** SQL 2012 Migration - Additional Migration Tasks for ADPS2/SLG2 Users**

KBA-10309-J9Y1J5

Notes

Additional Migration Tasks for ADPS2/SLG2 Users

The following sections describe the additional tasks necessary for ADPS2 and SLG2 customers when migrating the SIMS database to SQL Server 2012.

Workaround

Decrypting the ADPS2 Client Configuration Files

If you have encrypted the ADPS2 Client configuration files, you must decrypt the SIMS Web Service web.config file and ADPS2 Client Scheduled Process ConnectionSettings.xml file before making the configuration file updates on each ADPS2 Client.

If you have not encrypted these files, you can skip directly to *Updating the ADPS2 Client Configuration Files* section.

NOTE: When using a 64-bit machine, you must substitute Program Files with Program Files (x86) in the file path.

Login to the machine hosting the ADPS2 Client as an Administrator.

In Windows Explorer, navigate to C:\Program Files\SIMS\ADPClient\Encryption Utilities\

Run ConfigEncryptor.exe to display the **ASP.Net Password Encryptor** dialog.

Click the **Browse** button to display the **Open** dialog. *Browse button*

Navigate to the location of the web.config file for your SIMS Web Service www_root folder (usually C:\Program Files\SIMS\ADPClient\www_root), then highlight the web.config file and click the **Open** button.

Select the **Decrypt** radio button then click the **Go** button to decrypt the file. Once the file has been decrypted, the **Success** dialog is displayed.

Click the **Browse** button to display the **Open** dialog. *Browse button*

Navigate to the location of the ConnectionSettings.xml file (usually C:\Program Files\SIMS\ADPClient\ChangeTracking\), then highlight the ConnectionSettings.xml and click the **Open** button.

Select the **Decrypt** radio button then click the **Go** button to decrypt the file. Once the file has been decrypted, the **Success** dialog is displayed.

If necessary, repeat this procedure on all of the ADPS2 Clients affected by the SIMS database being migrated to SQL Server 2012.

Updating the ADPS2 Client Configuration Files

You must perform this procedure for each school that has migrated its SIMS database to SQL Server 2012.

Login to the machine hosting the ADPS2 Client as an Administrator.

In Windows Explorer, navigate to the location of the web.config file for your SIMS Web Service www_root folder (usually C:\Program Files\SIMS\ADPClient\www_root), then right-click the web.config file and select **Edit** from the pop-up menu to open the file in Notepad.

Change the Catalogue and SERVER entries to those of the migrated SIMS database.

IMPORTANT NOTE: As of ADPS2 August Update Release (SIMS 7.122) the web.config file can contain connection information for multiple SIMS databases. In this situation you must ensure that you update the settings for all SIMS databases that have been migrated to SQL Server 2012.

Select **File | Save** and close Notepad.

In Windows Explorer, navigate to the location of the ConnectionSettings.xml file (usually C:\Program Files\SIMS\ADPClient\ChangeTracking\), then right-click the ConnectionSettings.xml file and select **Open With | Notepad** from

the pop-up menu to open the file in Notepad.

Change the ServerName and DatabaseName entries to those of the migrated SIMS database.

Select **File | Save** and close Notepad.

Encrypting ADPS2 Client Configuration Files

Even if you did not originally encrypt the ADPS2 Client configuration files, it is highly recommended that you encrypt them after making the configuration file updates.

NOTE: When using a 64-bit machine, you must substitute Program Files with Program Files (x86) in the file path.

Login to the machine hosting the ADPS2 Client as an Administrator.

In Windows Explorer, navigate to C:\Program Files\SIMS\ADPClient\Encryption Utilities\.

Run ConfigEncryptor.exe to display the **ASP.Net Password Encryptor** dialog.

Click the **Browse** button to display the **Open** dialog. *Browse button*

Navigate to the location of the web.config file for your SIMS Web Service www_root folder (usually C:\Program Files\SIMS\ADPClient\www_root), then highlight the web.config file and click the **Open** button.

Select the **Encrypt** radio button then click the **Go** button to encrypt the file. Once the file has been encrypted, the **Success** dialog is displayed.

Click the **Browse** button to display the **Open** dialog. *Browse button*

Navigate to the location of the ConnectionSettings.xml file (usually C:\Program Files\SIMS\ADPClient\ChangeTracking), then highlight the ConnectionSettings.xml and click the **Open** button.

Select the **Encrypt** radio button then click the **Go** button to encrypt the file. Once the file has been encrypted, the **Success** dialog is displayed.

If necessary, repeat this procedure on all of the ADPS2 Clients affected by the SIMS database being migrated to SQL Server 2012.

If you also run SLG2, please continue to the next section.

Add Encryption by Service to new SQL instance

Browse to C:\Program Files\SIMS\ADPClient\Encryption Utilities and double click the SLGDBEncryptionSetup.exe

Once this opens select the server\instance, the authentication and then click on load databases and select the SIMS database. Click OK

Click on Options | Advanced and then click on Add Decryption By New Service

Enter the password that was used when the SQL tables were encrypted and click on Add decryption By New Service.

Close the SIMS Database Encryption Setup tool

Once the above has been completed please log a case with the SIMS Service Desk for the Hosted SLG platform to be updated with the new SQL instance name.

Please log this as a new case and when logging this issue please advise the new instance name along with the external access username and password. This can be found in the ConnectionSettings.xml

Release Notes
