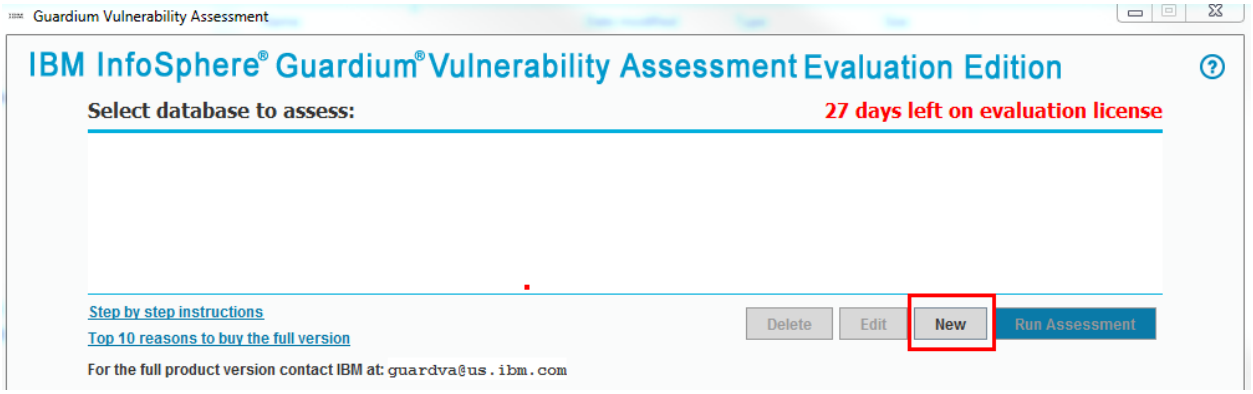
Guardium Vulnerability Assessment Evaluation, Step-by-Step

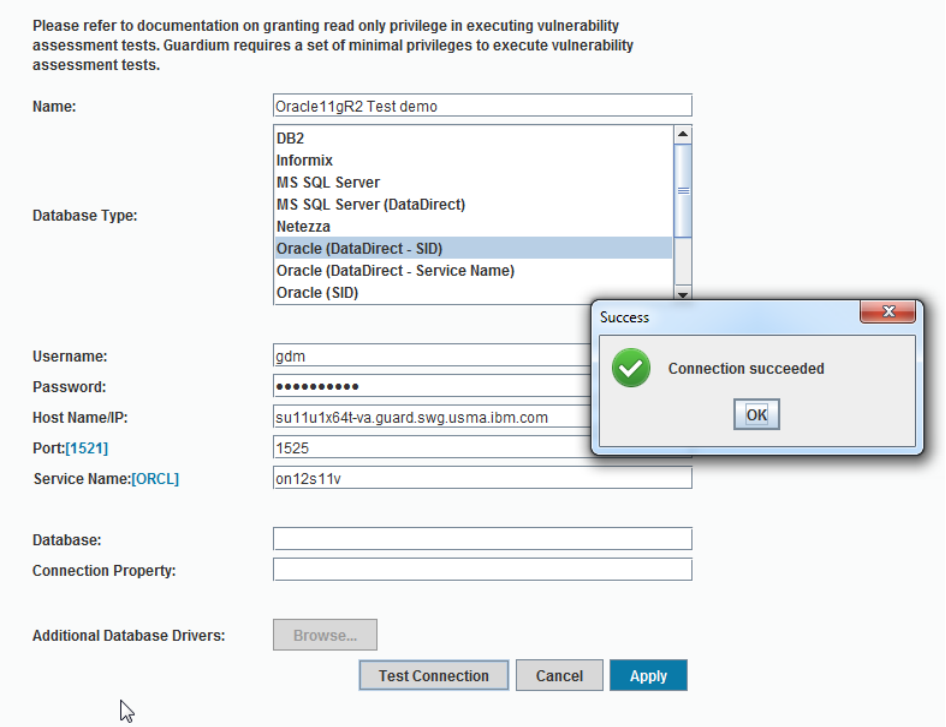
1. Click on ‘New’ to create a datasource for a database that you want to execute vulnerability assessment against.



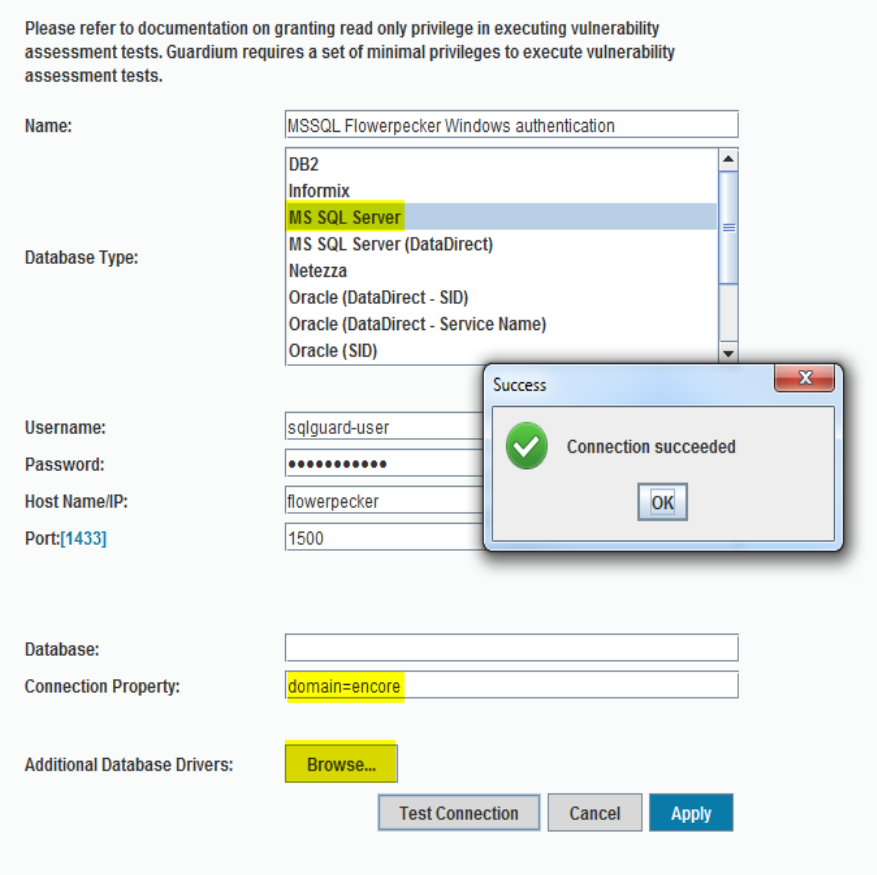
2. All the database drivers are shipped with the product. For Oracle and SQL Server, the default driver that is shipped is from DataDirect. The evaluation allows you to upload alternative drivers for these two database types. For MS SQL Server, you can optionally use the open source JDBC drivers if you need to connect to your database using Windows authentication. For Oracle, if you prefer to use Oracle driver instead of DataDirect, you can upload the ojdbc6.jar that you download from the Oracle site. For both cases, you would need to download these drivers. Put them somewhere on your workstation and click on the 'Browse' button to select it.

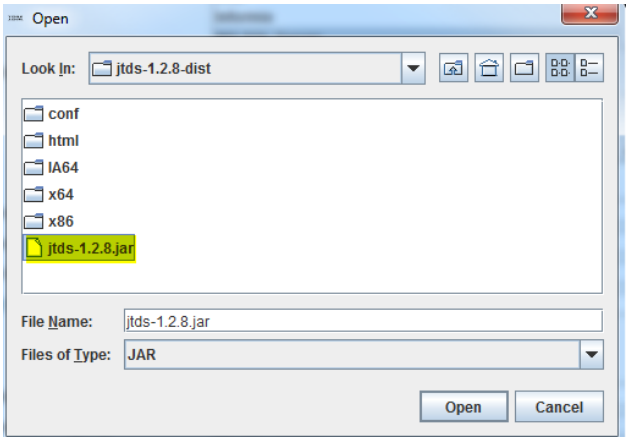
   Select the database type and setup a connection for it. In this example, we are creating a connection for Oracle11gR2 database. The screen below shows all the required fields for this connection. For Oracle, you can choose to connect to Oracle by using SID or service name. Depending on your database type choice, you can enter either SID or Service Name in the 'Service Name' column. Once all the required fields are entered, click on 'Test Connection' and the 'Apply' to save. For more details about the required fields for each database type, please refer to our help documentation.

   For username and password, you can refer to our documentation for creating a role/group with limited read only privileges. If you just want a quick test, you can also use a DBA account privileges to run the assessment. The choice is yours.

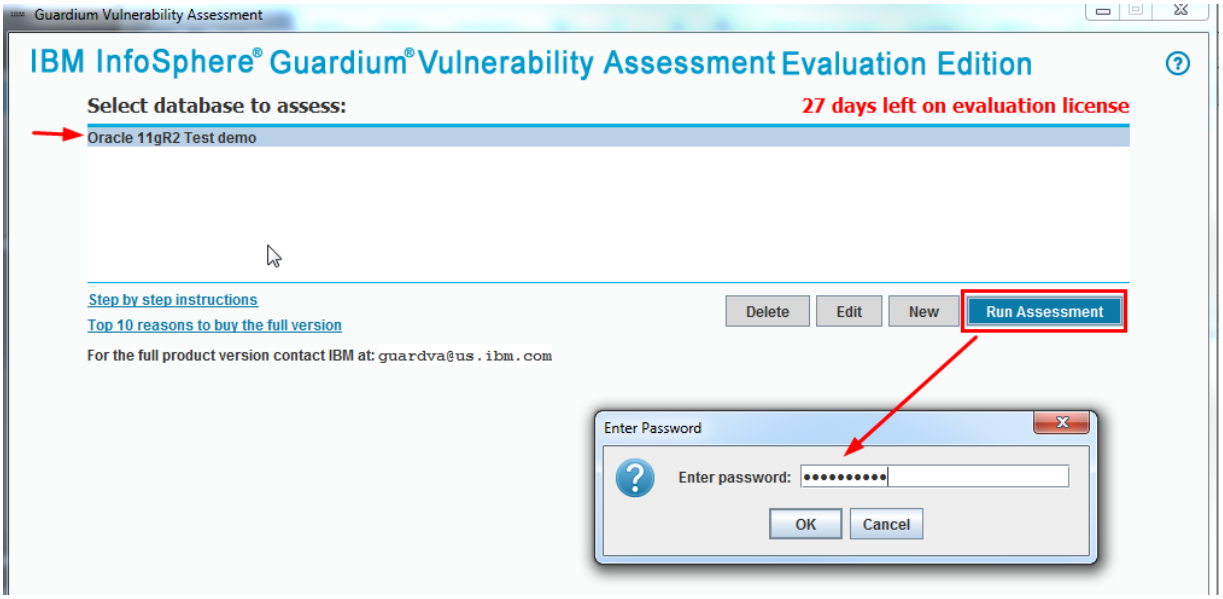


The screen shot below shows an example of using Windows authentication for SQL Server. In this case, you would need to download the open source JDBC driver and save that somewhere on your desktop. Then click on 'Browse..' to select the driver 'jtds-1.2.8.jar' and fill out the rest of the require fields. You need to specify your Windows domain name in the 'Connection Property' field. In the example, our domain name is encore. The syntax would be 'domain=encore'.

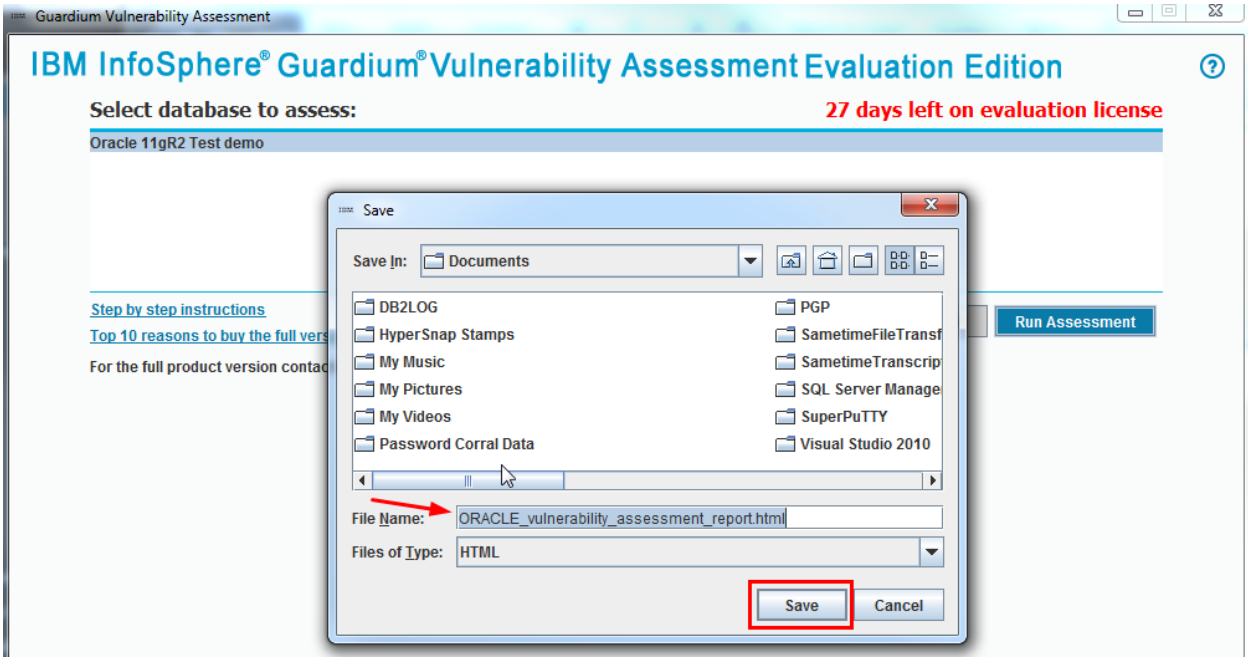




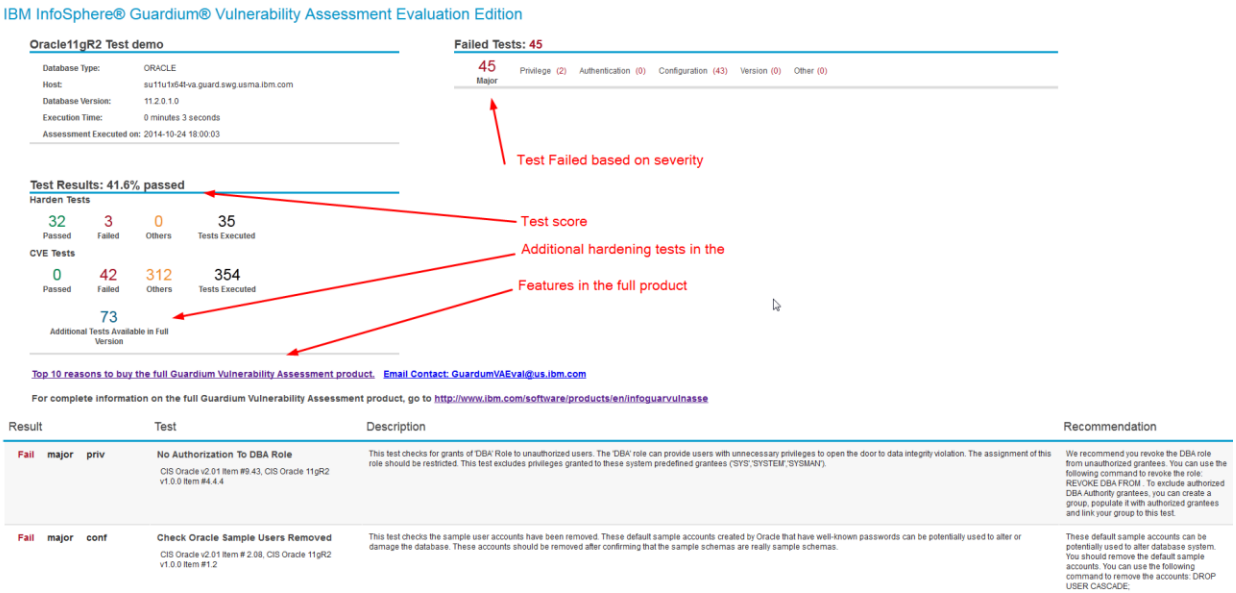
3. Once a datasource connection is created, select the datasource you want to run a vulnerability assessment on and click 'Run Assessment'. For security reasons, we choose not to save your password on the evaluation edition. You will need to enter your password at the prompt. Password does get saved in the full version. For the evaluation edition, the password is cached and once you enter the correct password per datasource configuration, the evaluation version will not prompt you to enter the password again. As long as the password is in memory or until you exit. This means if you ran the same datasource assessment multiple times, it only prompts you for the password on your first execution.



4. Before running the assessment, it will prompt you to save the HTML result in a default location. Pick an alternate name and/or location if you like and click on 'Save' to continue.



5. Review the results. We are showing the description and recommendation for only 10 tests for all database types except Netezza. The full product has many more tests available with detailed recommendations, violations and test-tuning features. The full product also has the latest CVE vulnerability detection tests.



2014 October 31