

dataLink

User Manual

Version 3.2



Washington State Board for Community and
Technical Colleges



Revisions

Date	Version	Change Reference
1/19/2016	1.0	Original version
6/16/2016	1.1	Added GoldenGate Replication Data Flow Changed Access form to Control form with spaces to remove access to users Added Change Reference table Updated to reflect Version 1.1
4/7/2017	1.2	Added the password change information
6/20/2017	1.3	Updated password change language to remove special characters from passwords
1/25/2018	1.4	Updated password section and added screenshot of the SQL connection properties
2/14/2019	1.5	Updated documentation to reflect name change to dataLink Added types of filtering
9/16/2019	2.0	Revised and prepared for implementation system-wide
4/16/2019	2.1	Changed SQL Developer connection string instructions to reflect Phase Two host
5/28/2020	3.0	Added additional information about views
12/15/2020	3.1	Added more information about views
2024/02/28	3.2	Updated Contact info

Table of Contents

Revisions	1
Table of Contents	2
Overview of dataLink	3
dataLink Replication Data Flow.....	4
Suggested Local College Data Flow Schema	4
Guiding Principles	5
Gaining Access	6
dataLink Access Request Form	7
dataLink Notice of Nondisclosure Form.....	8
dataLink Replication Filtering Methods	8
Overview	8
Types of Filtering.....	8
Criteria Information and Examples	8
Table Replication Requests	9
Overview	9
Locating a record/table.....	9
Requesting Replication on a table	9
Installing SQL Developer and Connecting to Oracle	9
SBCTC dataLink Password Policy.....	11
Changing a User Password.....	12
Unsuccessful Password Change Attempts	15

Overview of dataLink

dataLink is an Oracle database used to replicate the production PeopleSoft databases to individual district Pluggable Databases (PDBs). dataLink allows for near real-time access to data from the ctcLink production databases without actually connecting to the production databases.

Only tables used for reporting or feeding supporting systems are included in dataLink. The ctcLink production system consists of over 140,000 tables, of which only about 1,000 tables are needed for reporting or supporting systems.

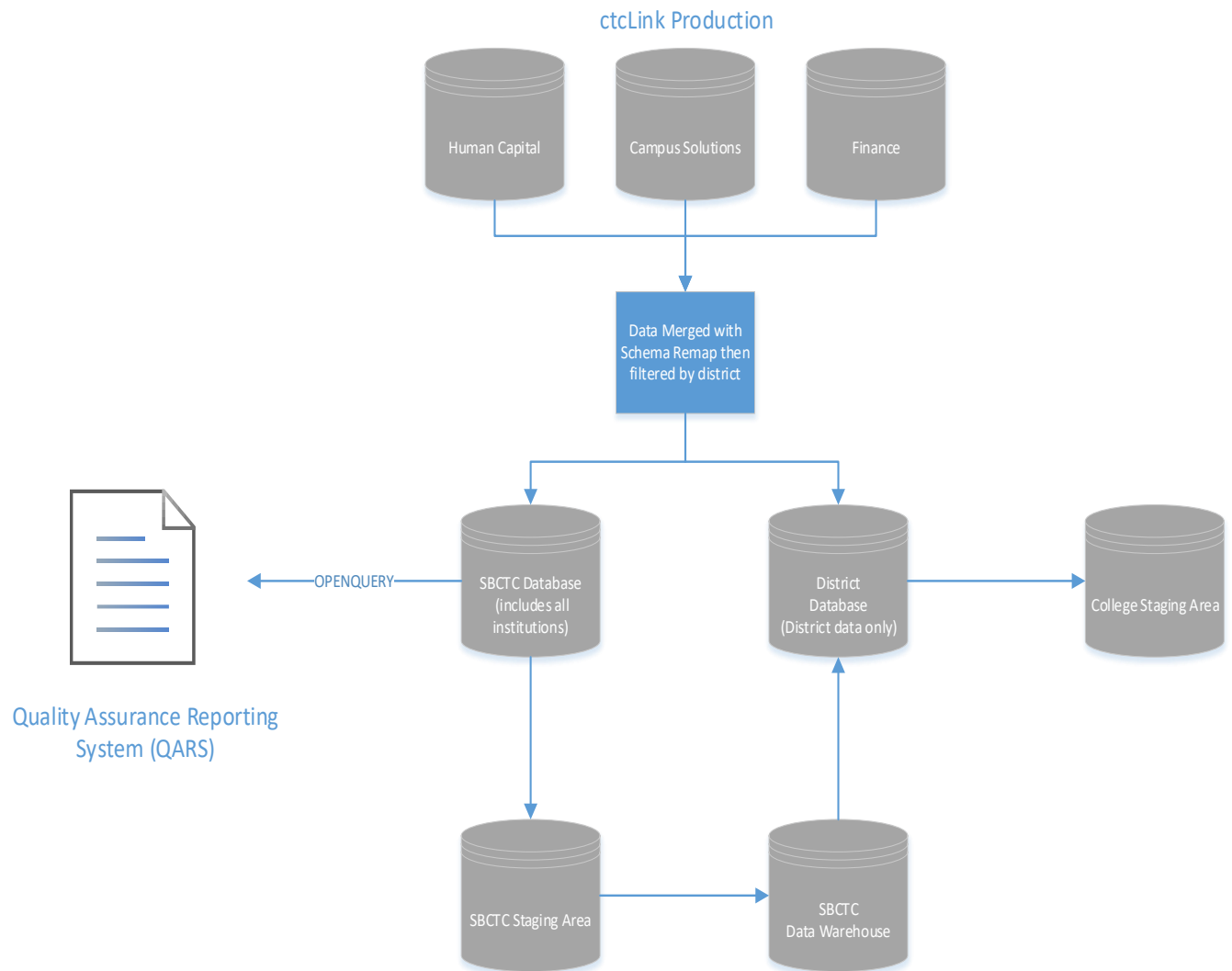
Each district has its own dedicated Pluggable Database that contains only data pertaining to that district. Filtering of the data is handled by the Golden Gate replication software during the replication process. For tables that contain no district or college identifier but do contain an EMPLID, the filtering of data is handled utilizing views in each PDB. Tables that do not contain a district or college identifier and do not contain an EMPLID are considered global tables and are not filtered.

Each of the district PDBs contain all three pillars of ctcLink data divided into three separate schema/owner names. Each PDB also contains individual schemas for each SBCTC Data Warehouse data mart. The State Board Master Data (SBMD) views, which are used for the Data Warehouse and system-wide reporting, use a separate schema name. An inventory of the Data Warehouse tables can be found here: <https://www.sbctc.edu/colleges-staff/data-services/datalink.aspx>

Schema/Owner	Description
SYSADM_HCM	Human Capital
SYSADM_CS	Campus Solutions
SYSADM_FIN	Finance
WAREHOUSE_XXXX	SBCTC Data Warehouse data marts (eg WAREHOUSE_SMIS)
SBMD	State Board Master Data views

This configuration allows for ease of use as all datasets will be contained within a single database which then simplifies the process of querying across pillars.

dataLink Replication Data Flow



Suggested Local College Data Flow Schema

The Information Technology Commission (ITC) has developed two suggested college data flows.

- [Ideal College Level Data Flow Schema](#)
- [Reduced College Level Data Flow Schema](#)

Guiding Principles

ITC Data & Integrations Committee

Guiding Principles for college use of PeopleSoft data through Golden Gate

Final Draft 2017.04.25

Assumptions:

- This document is intended to guide and govern college connections to Golden Gate data; while it requires certain agreements and accommodations from SBCTC Data Services, it does not govern internal SBCTC operations.
- Information Technology (IT) professionals have a responsibility to guarantee availability of data while also maintaining a reasonable level of cybersecurity for all college interests.
- Institutional Research (IR) professionals have a requirement to access data pertaining to all functional areas of the college (admissions, registration, financial aid, finance and budget, facilities, human resources, etc.).
- Each group, represented through ITC and RPC respectively, is invested in the other Group's professional success. Both ITC and RPC understand and acknowledge that it is the role of IR professionals to determine the legitimacy of a problem or data request, and that it is the role of IT professionals to safeguard institutional data.
- These guiding principles and the accompanying technical standards are intended to provide structure, tools and processes for college IT operations, working with SBCTC Data Services, to provide secure, stable, and uniform access to data across all colleges.

Guiding Principles

- Maximize accessibility, availability, and quality of data for local use
 - Each college is responsible for internal data governance, and maintains a local data governance structure representative of all stakeholder groups (including IR, IT, and data owners) in accordance with best practices
- Minimize use of remote server resources to the extent possible.
 - Each campus will utilize a single connection to the Golden Gate data to perform full and near-real-time replication to a campus staging area with the Golden Gate schema
 - Each campus will have at least one exact replica of the data, and any data transformations will be processed locally at the college (such as in a staging area or in the application and reporting layers).
 - Connections for third-party application integrations, such as Tableau or Civitas, will be made to the local campus staging area or a local replication and not directly to the SBCTC.
- Maximize data security using best practices, including
 - SQL Views and Stored Procedures will be used at each campus to provide secure and limited access to campus end users and application integrations.
 - Approvals for individual direct access to Golden Gate for IR purposes should be governed by local college Data Governance policies and procedures.
 - Individual users will receive minimum permissions required to perform their job duties; temporary elevation of privileges will be granted when necessary

Gaining Access

Access to dataLink is requested via the attached dataLink Access Form. A signed Notice of Nondisclosure form is also required. These forms require approval of an IT Director at your college or your supervisor. The forms must be signed, scanned, and submitted to our DBA team via email at DBARequests@sbctc.edu.

Once access to the system is granted, you will be notified and can then install SQL Developer and/or establish ODBC connections.

Detailed instructions on the technical aspects of how to connect are included in this document.

Please note that Service Accounts do not need to sign and attach the Notice of Nondisclosure, only the Access Control Form.



dataLink Access Request Form

College District				
Account Type (eg Service Account or Named User)	Contact Name	Contact Phone Number	Contact Email Address	Connecting IP Address
Authorization	Approver Name			Contact Phone Number / Email
	Approver Signature			
	Additional Comments			

To remove access for a user listed above, please resubmit this form with the information below.

Remove access for this user:	As of this date:	Signature:

dataLink Notice of Nondisclosure Form

All users of dataLink will be required to complete and submit the following NonDisclosure form found here: <https://www.sbctc.edu/resources/documents/colleges-staff/data-services/goldengate/ctclink-nondisclosure-form.pdf>

dataLink Replication Filtering Methods

Overview

Filtering of transactions so that only transactions relevant to a particular college district are applied to that district database.

Types of Filtering

- **Filtering via Replication**
 - Most data filtering happens during replication. Tables that contain key “identifier” fields are configured to only receive data that pertains to that district database. Records filtered out by this method will never show up in the target database
- **Filtering via View**
 - Tables that do not contain an institution or district level identifier but do contain an EMPLID value (student or employee identifier) instead have all data replicated to the destination database and tables, however access to those tables is restricted and instead a view is created with the same name as the table, but with a suffix of “_GGVW”. Filtering of the data is then handled by the view.
 - **A full list of GGVW views can be found by querying SBMD.GGVW_LIST in your Oracle PDB.**

Criteria Information and Examples

- **Filtering via Replication**
 - Filtering happens if any of the following fields is present and populated in the table: INSTITUTION, BUSINESS_UNIT, SETID or COMPANY
- **Filtering via View**
 - For Campus Solutions, a “Master List” of all EMPLID’s valid for a given district is created by aggregating the EMPLID’s from the following tables in the Campus Solutions Pillar:
 - PS_ADM_APPL_PROG
 - PS_STDNT_CAR_TERM
 - PS_ADM_PRSPCT_CAR
 - PS_ADM_APPL_DATA
 - PS_ISIR_STUDENT
 - For Human Capital Management, a “Master List” of all Employee EMPLID’s valid for a given district is created by aggregating the EMPLID’s from the following tables in the Human Capital Management Pillar:
 - PS_JOB

Table Replication Requests

Overview

When a college needs a table replicated from production that's not already on the replication list, a request can be sent to elusby@sbctc.edu and DBARequests@sbctc.edu to have the table added. Note that the rules in the datalink Replication Filtering Methods section will all apply.

Locating a record/table

1. Query table PSRECDEFN (A copy of this table exists in each pillar).
2. PSRECDEFN contains a list of all PeopleSoft tables and Views along with a RECTYPE value indicating what type of object it is.
3. Only table objects (RECTYPE = 0) can be replicated.

Requesting Replication on a table

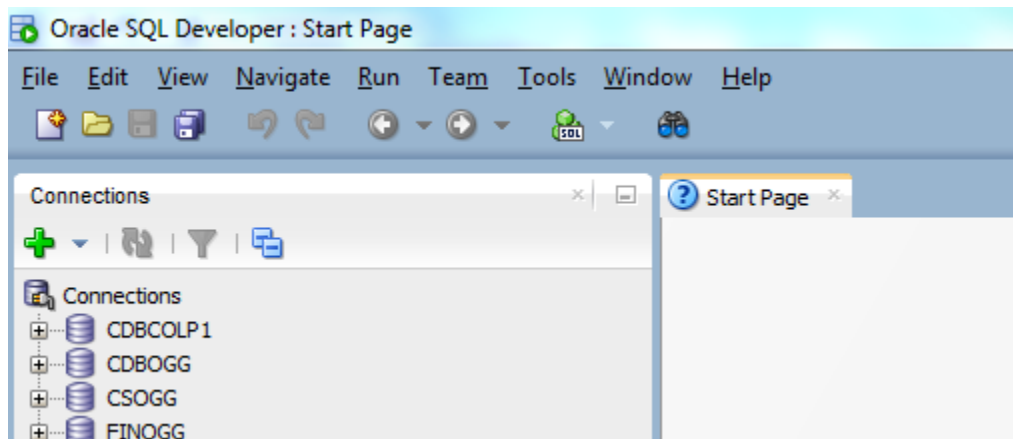
1. Once the table has been located and verified, email elusby@sbctc.edu CC DBARequests@sbctc.edu with the table name being requested as well as the pillar it belongs to.

Installing SQL Developer and Connecting to Oracle

4. Open your browser and connect to the following URL:
<https://www.oracle.com/database/technologies/appdev/sqldeveloper-landing.html>
5. Click "SQL Developer" and pick the appropriate version for your machine.
6. Extract the downloaded file to a folder on your computer
7. Browse to the extraction destination using Windows Explorer and double-click the "sqldeveloper.exe" file
8. Click "Run" if prompted to Run or Cancel
9. SQL Developer should then launch

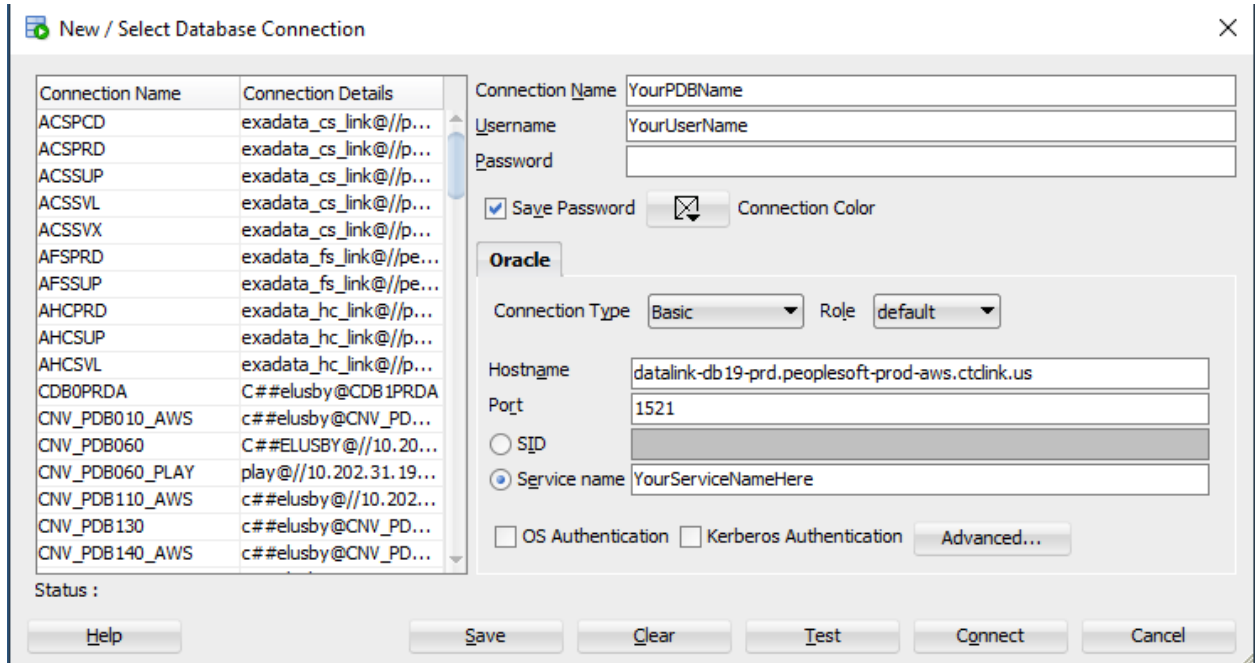


10. Once open, click the green “+” sign in the upper left hand corner of SQL Developer to create a new database connection



Populate the New / Select Database Connection dialog box with the following values:

- a. Connection Name: <Your PDB Name here>
- b. Username: <provided>
- c. Password: <provided>
- d. Check “Save Password” if you would like
- e. Under the Oracle Tab, select “Basic” in the Connection Type drop-down menu.
- f. Paste in the dataLink hostname and Port info. (Available from your IT department)
- g. Click Test (Status in lower left should show “Success”)



11. Click Save
12. Click Connect

SBCTC dataLink Password Policy

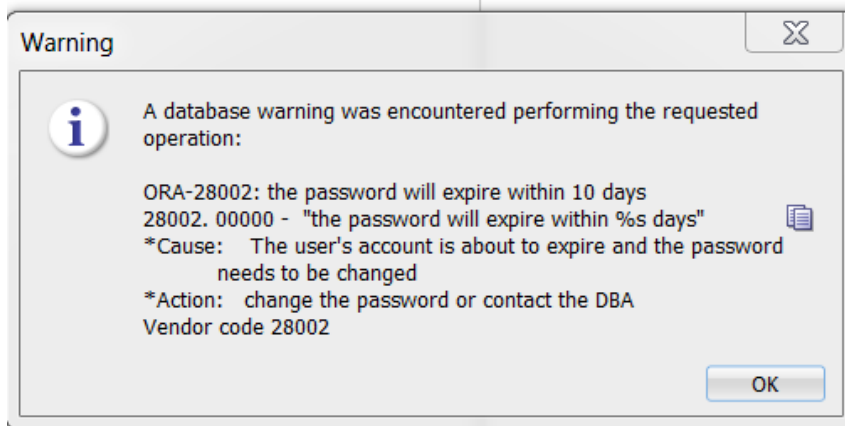
Named User Accounts

Password handling for dataLink logins is based on OCIO Security Policy 141.10 Section 6. User passwords will adhere to the following requirements:

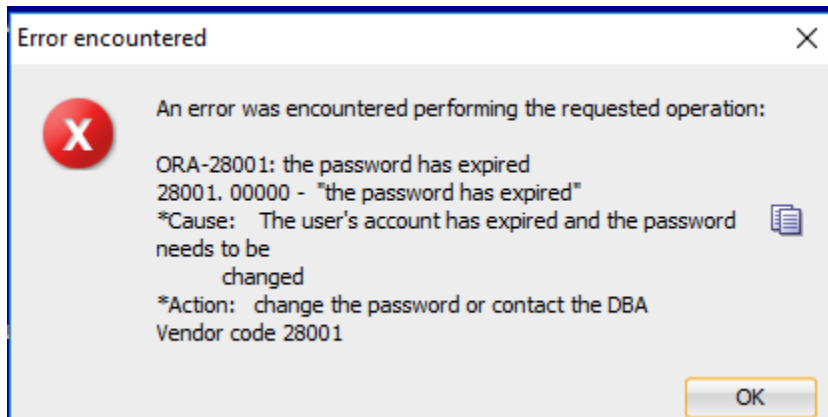
- Be a minimum of 10 characters long and contain at least three of the following character classes: Uppercase letters, lowercase letters and numerals. The password must contain both an uppercase or lowercase letter.
- Cannot contain the user's name or UserID

- Not consist of a single complete dictionary word, but can include a passphrase.
- Be significantly different from the previous password. Passwords with an incrementing suffix (password1,password2, Password3...) are not considered significantly different.
- Cannot contain your school name, three digit college code or city.

User passwords will expire after 120 days. The system will provide a notice when the password is about to expire. A password cannot be reused for 365 days and 10 different intervening passwords. The account will be locked for 15 minutes after three unsuccessful login attempts.



If the password does expire, the user can still create a new password using SQL Developer as described in the next section.



Service Accounts

Each college may have one service account for linked servers for the purpose of replication. No individual users should utilize this connection for any ad hoc or Open Query connection.

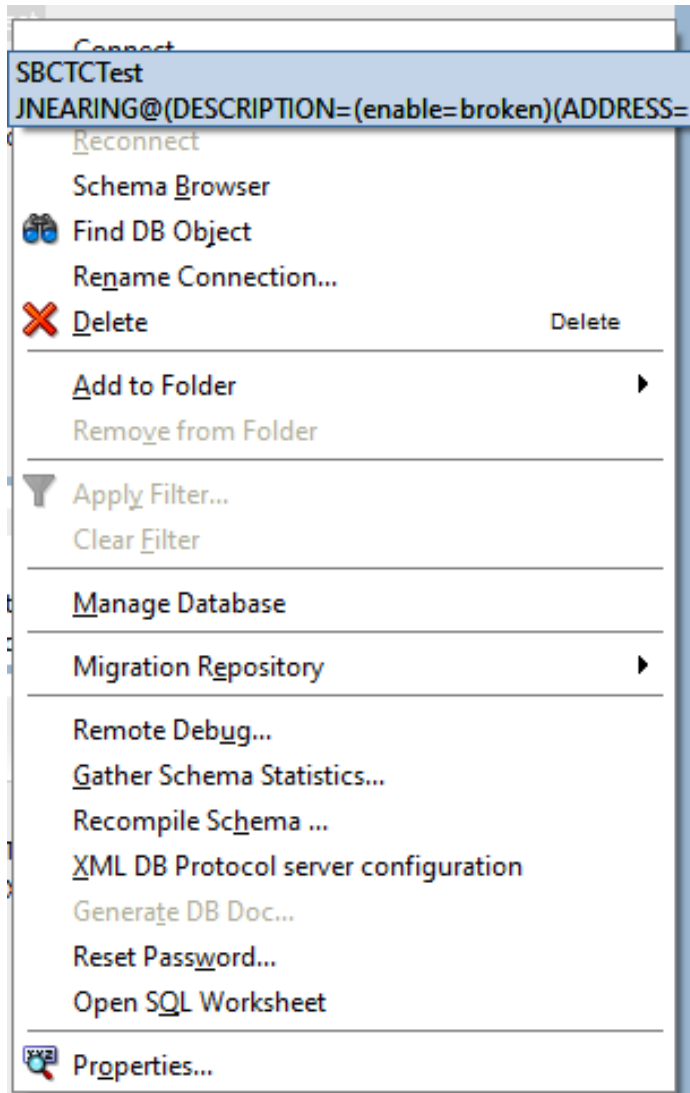
Service Account passwords will be issued and maintained by SBCTC.

Changing a User Password

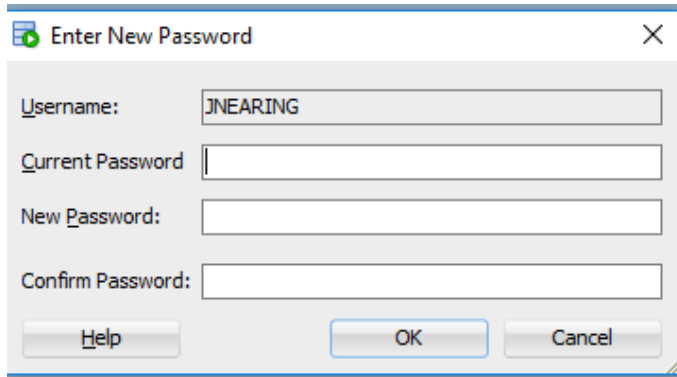
The user can change the password without the assistance of a database administrator. The password can be changed using the Oracle SQL Developer Tool or SQL Plus as below.

Changing password using Oracle SQL Developer

There is a menu selection for the connection that allows the password to be changed. Right click on the connection name and select Reset Password. This procedure allows an expired password to be changed.



A password change dialog box will be displayed.



Enter New Password

Username: JNEARING

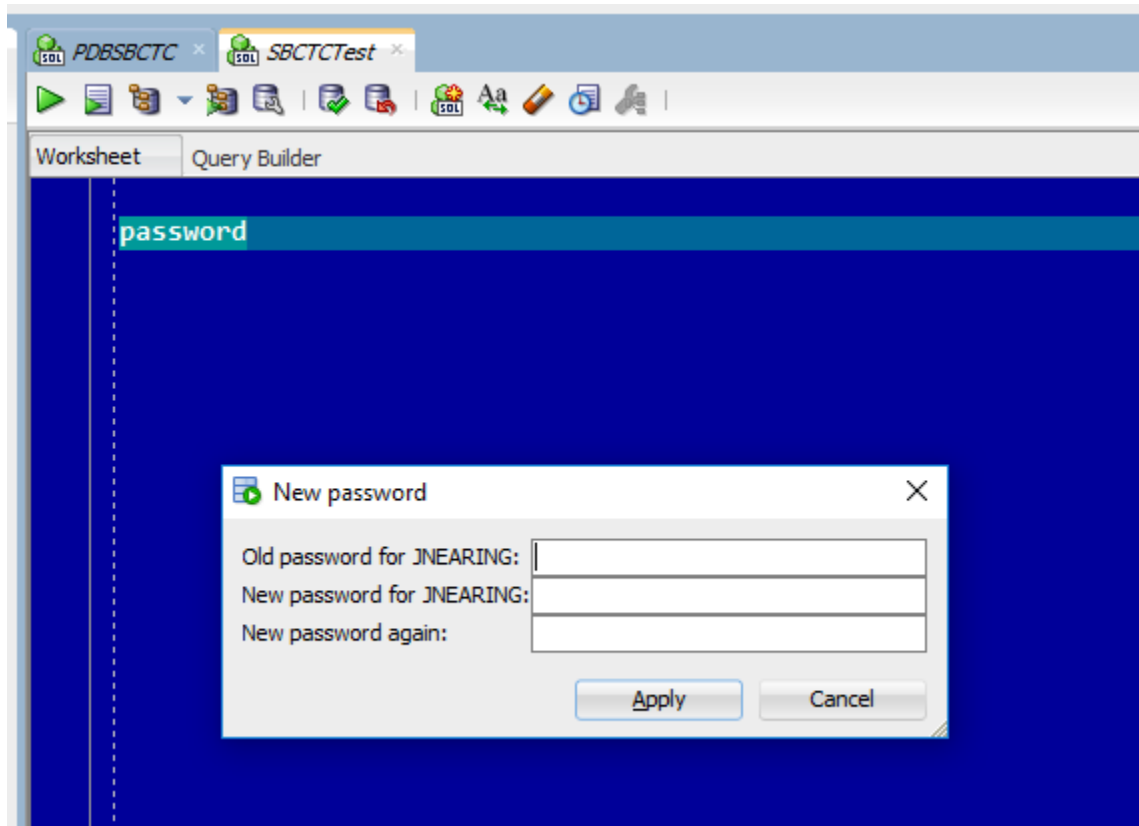
Current Password:

New Password:

Confirm Password:

Help OK Cancel

A password change can also be performed in an open SQL Developer session by typing “password” in the Query Builder window.



Worksheet Query Builder

password

New password

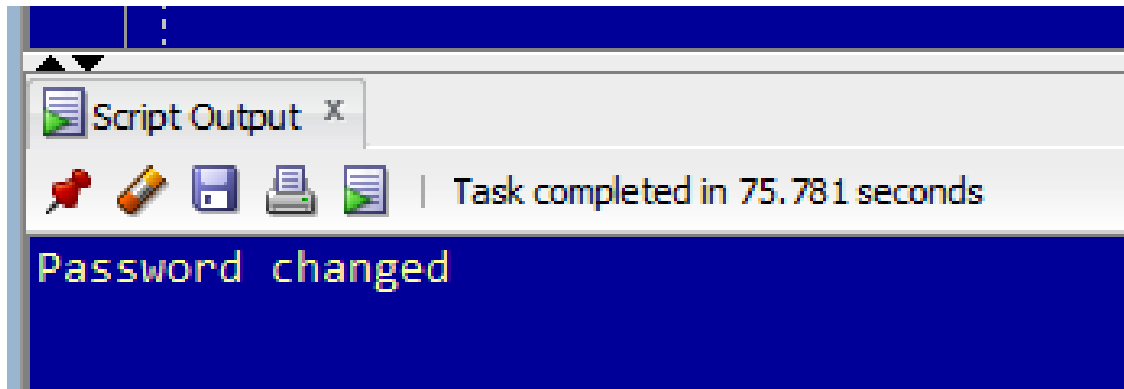
Old password for JNEARING:

New password for JNEARING:

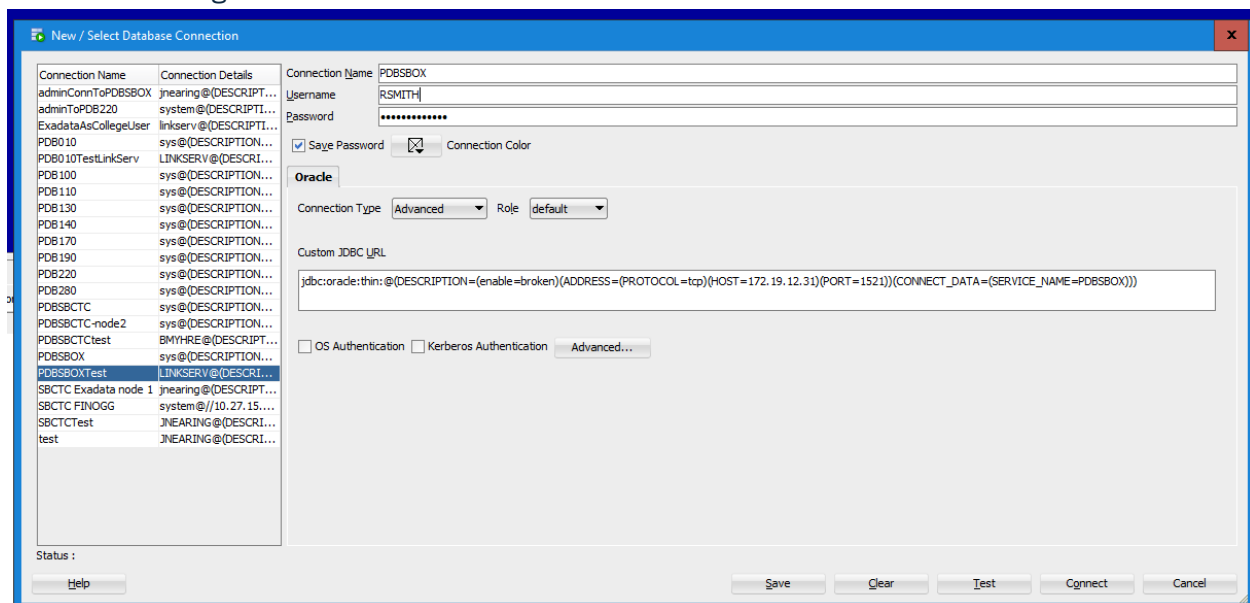
New password again:

Apply Cancel

A successful password change will be acknowledged in the script output window.



After changing your Oracle password you will want to change your password in the SQL Developer connection configuration.



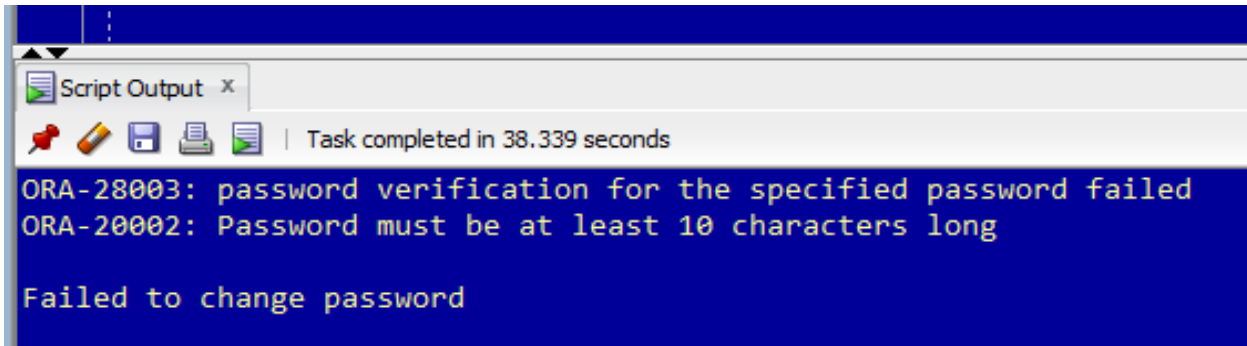
Put your new password in the Password text box. Click on the Test button to make sure the password is correct.

Changing password using Oracle SQL Plus

Changing the password using SQL Plus is the same process as that shown above using the SQL Developer query window.

Unsuccessful Password Change Attempts

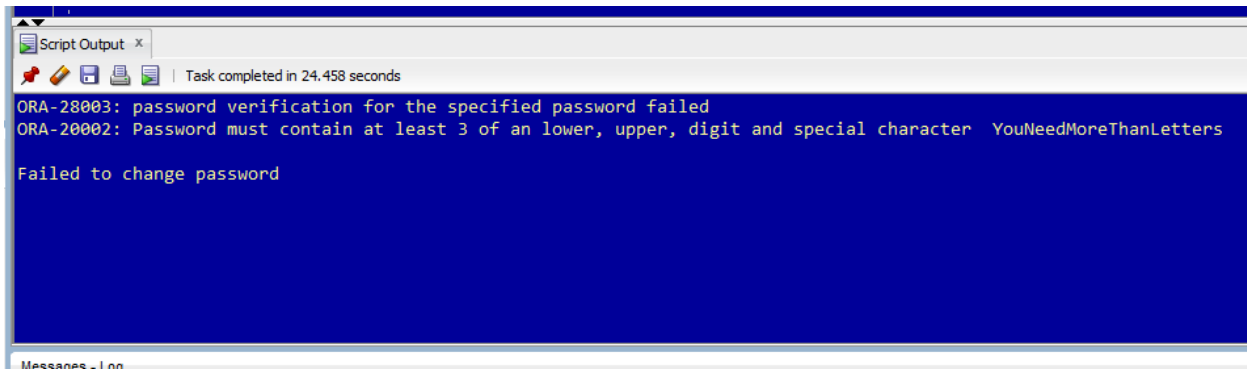
Passwords that do not meet the specifications provided will result in an error, with an explanation.



```
Script Output x
Task completed in 38.339 seconds
ORA-28003: password verification for the specified password failed
ORA-20002: Password must be at least 10 characters long

Failed to change password
```

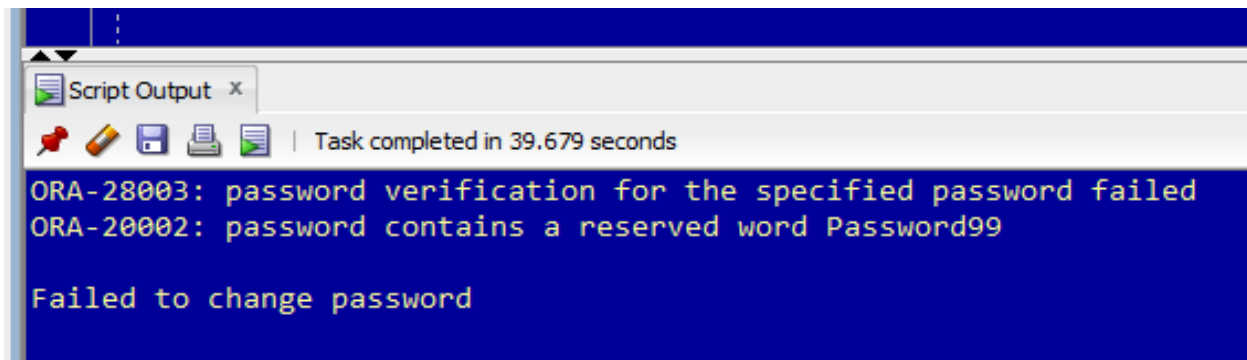
Password is shorter than 10 characters.



```
Script Output x
Task completed in 24.458 seconds
ORA-28003: password verification for the specified password failed
ORA-20002: Password must contain at least 3 of an lower, upper, digit and special character YouNeedMoreThanLetters

Failed to change password
```

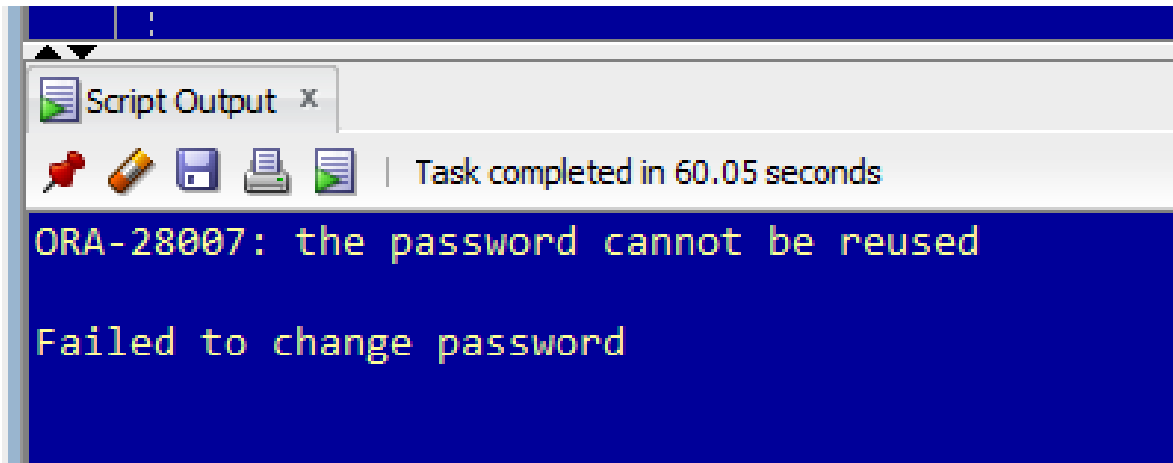
Password does not contain at least three different types of characters. The entered password is shown.



```
Script Output x
Task completed in 39.679 seconds
ORA-28003: password verification for the specified password failed
ORA-20002: password contains a reserved word Password99

Failed to change password
```

The password cannot contain a reserved word or dictionary word. See the section below for reserved words.



The password cannot be reused until the password has changed 10 times, and cannot be reused for 365 days.

Reserved Words that cannot be used in a password

The following words are not allowed in a user password, in addition to common dictionary words.

SECRET	DISTRICT	SPOKANE
PASSWORD	EDMONDS	STEILACOOM
P@SSWORD	EVERETT	TACOMA
DATABASE	FALLS	VALLEY
ORACLE	GRAY	WALLA
ABC%123	GREEN	WASH
USER	HARBOR	WENATCHEE
EXADATA	HIGHLINE	WHATCOM
ACCOUNT	LAKE	YAKIMA
GOLDEN	LOWER	The three digit college code
GATE	NORTH	
PDB	OLYMPIC	
BASIN	PARK	
BATES	PENINSULA	
BELLEVUE	PIERCE	
BELLINGHAM	PUGET	
BEND	PUYALLUP	
BIG	RENTON	
CASCADIA	RIVER	
CENTRAL	SBCTC	
CENTRALIA	SEATTLE	
CIS	SHORELINE	
CLARK	SKAGIT	
CLOVER	SOUND	
COLUMBIA	SOUTH	

Dictionary Words

In addition to the reserved words in the previous section, a file containing common dictionary words is installed on the ExaData server. The password change process compares the suggested replacement password to the words found in the dictionary file. A password containing a dictionary word will be rejected. The reason for this is hackers will use a dictionary-based attack to attempt to guess your password. Passphrases however are allowed. See the section below on passphrases.

Character substitution in dictionary words

The password verification process will check for common character substitution in dictionary words. The following character substitutions are checked:

- 0 (zero) for the letter O
- 1 (one) for the letters l and L
- \$ and 5 (five) for the letter S
- @ for the letter A

For example the dictionary check would catch the word dollars AND would also catch the following permutations:

- d0llars substituting a zero for the letter O
- do11ars substituting the number 1 for the letter L
- doll@rs substituting the @ for the letter a
- dollar\$ substituting \$ for the letter S
- D011@R\$ all of the letter substitutions

Passphrases

A passphrase is a string that contains two or more words along with numbers and special characters. Passphrases are usually longer than regular passwords and are considered to be secure.

Examples of passphrases:

- Z9Ocean%cHair
- cAlendar%toNight
- hTrouBle#8blrd