Oracle Database Password

Change Instructions

06/28/2017

Contents

[Types of Accounts 2](#_Toc486409121)

[Oracle Individual Users 2](#_Toc486409122)

[Oracle “Application” or “Department ID” Users 2](#_Toc486409123)

[Password Requirements Individual Users 2](#_Toc486409124)

[Password Complexity Requirements 2](#_Toc486409125)

[Password Life Time and Grace Time 2](#_Toc486409126)

[Password Reuse Max and Time 2](#_Toc486409127)

[Failed Login Attempts and Lock Time 2](#_Toc486409128)

[Password Requirements for “Application” or “Department ID” Users 3](#_Toc486409129)

[Password Complexity Requirements 3](#_Toc486409130)

[Password Life Time and Grace Time 3](#_Toc486409131)

[Password Reuse Max and Time 3](#_Toc486409132)

[Failed Login Attempts and Lock Time 3](#_Toc486409133)

[Oracle Password Restrictions 3](#_Toc486409134)

[Password Change Process 4](#_Toc486409135)

[Reset your password using SQL\*Plus or SQL Developer command line: 4](#_Toc486409136)

[Reset your password in SQL Developer GUI: 4](#_Toc486409137)

[Password Troubleshooting 5](#_Toc486409138)

[Protect Your Password 6](#_Toc486409139)

# Types of Accounts

This document addresses changing passwords for Oracle accounts only.

When changing Oracle User account passwords in PeopleSoft databases, some users choose to keep their passwords synched between their Oracle database accounts and their PeopleSoft application accounts. Changing your PeopleSoft account will not be addressed in this document. This does not apply when changing your Oracle account password in non-PeopleSoft databases.

## Oracle Individual Users

Business Analysts, Change Management, Developers, and Database Administrators

The individual accounts are used by individuals and usually consist of initials which may have an extension such as \_DV or \_SA appended. These are personal accounts and must not be shared.

## Oracle “Application” or “Department ID” Users

These are Oracle accounts which are used within an application to access the database.

# Password Requirements Individual Users

## Password Complexity Requirements

* The password contains 7-30 characters
* The password must include at least 1 upper case, 1 lower case, and 1 numeric character.
* The password cannot be the same as the user name or the user name reversed.
* The password cannot be the same as the server name.
* The password cannot contain the word oracle (such as oracle123).
* The password cannot be too simple (for example, welcome1, database1, account1, user1234, password1, oracle123, computer1, abcdefg1, or change\_on\_install).
* The password differs from the previous password by at least 3 characters.

## Password Life Time and Grace Time

* Password life time is set to 90 days. This means that the next time the user logs in with the current, correct password, they will be prompted to change the password.
* Password grace time is set to 7 days. The grace time is the period during which each attempt to log in to the database account receives a warning message to change the password. If the user does not change it by the end of that period, then Oracle Database expires the account.

## Password Reuse Max and Time

* Password Reuse Max is set to 5. (The number of password changes required before the current password can be reused.)
* Password Reuse Time is set to 365. (The number of days before a password can be reused.)

## Failed Login Attempts and Lock Time

* Failed login attempts is set to 5. (The maximum times a user may try to log in and fail before locking the account.)
* Password lock time is set to 1/48 day (30 minutes). (The number of days an account will be locked after the specified number of consecutive failed login attempts.)

# Password Requirements for “Application” or “Department ID” Users

Due to the concerns about breaking production applications, Department ID users will not expire. The trade-off for not expiring passwords will be longer more complex passwords.

## Password Complexity Requirements

* The password must contain exactly 30 characters
* The password must include at least 2 upper case, 2 lower case, and 2 numeric characters.
* The password is not the same as the user name or the user name reversed.
* The password is not the same as the server name.
* The password does not contain the word oracle (such as oracle123).
* The password is not too simple (for example, welcome1, database1, account1, user1234, password1, oracle123, computer1, abcdefg1, or change\_on\_install).
* The password differs from the previous password by at least 4 characters.

## Password Life Time and Grace Time

* Password life time is set to UNLIMITED. The password will not expire.

## Password Reuse Max and Time

* Password Reuse Max is set to UNLIMITED. The previous password can never be reused.

## Failed Login Attempts and Lock Time

* Failed login attempts is set to 5. (The maximum times a user may try to log in and to fail before locking the account.)
* Password lock time is set to 1/48 day (30 minutes). (The number of days an account will be locked after the specified number of consecutive failed login attempts.)

# Oracle Password Restrictions

Oracle has password restrictions that can make logging in challenging if not adhered to. The Database Administration team recommends the guidelines below. Failure to follow these guidelines may require the password to be enclosed in double-quotation marks and can have unpredictable results. The Database Administration team strongly recommends that you do not use any password that requires it to be enclosed in double quotes.

* Start the password with an alphabet character (a–z, A–Z). Passwords starting with numbers or special characters and containing alphabetical characters must be enclosed in double-quotation marks.
* Use special characters including the underscore (\_), dollar ($), and number sign (#) characters. The use of all other special characters must be enclosed in double-quotation marks.
* Do not use passwords containing multibyte characters. Passwords containing multibyte characters must be enclosed in double-quotation marks.
* Do not include double-quotation marks within the password.

# Password Change Process

Many databases get refreshed from the Production database. A refreshed database will inherit the username/password from the source database. When you get a reminder to change your password in any database, change your password in that database, the **production database**, and any other databases you use.

## Reset your password using SQL\*Plus or SQL Developer command line:

The Database Team supports Oracle clients such as SQL\*Plus and SQL Developer. We will try to assist with other products, but can’t guarantee successful results.

Changing passwords command line:

SQL> alter user [username] identified by [new\_password] replace <oldpassword>;

Or

SQL> password
Changing password for [username]
Old password:
New password:

## Reset your password in SQL Developer GUI:

In SQL Developer, after you are connected, you can right click on the connection and select “Reset Password”. If you are not connected “Reset Password” will be grayed out.



This is really easy to use if you change your password before it expires. After your password expires you can no longer connect and the “Reset Password” is grayed out and not available. The workaround is to download and install the Oracle Client. Once the client is installed, you can use SQL\*Plus to reset the password or configure SQL Developer to enable the “Use OCI/Thick driver” option. The best option is to change your password in SQL Developer before it expires.

## Password Troubleshooting

If you are locked out please either wait 30 minutes and try again or submit a Service Now ticket to the Database Administration team to unlock your user account.

If a database has been recently refreshed try the username/password of the source database. This confusion can be alleviated by changing your password in all the databases you use and **production**.

Occasionally a database is refreshed from an older version of the database. If you think this may be the case, please try your old password and immediately reset it.

If you still can’t login please submit a Service Now ticket for the database team to reset your password. If you need any assistance contact the Database Administration Team:

* Service Ticket: [Service Now](https://nau.service-now.com)
* Email: ccs-dba@xdl.nau.edu
* Team Phone: 928-523-9985

## Protect Your Password

Remember that it is against the NAU Acceptable Use policy to share your password. If you follow the above guidelines and you protect your password, you will be taking a big step toward protecting the University’s and your own information.