```
SELECT CREATED, EXPIRY_DATE FROM DBA_USERS WHERE USERNAME = 'user_name';
```

If the user who is assigned this profile is currently logged in when you set the `PASSWORD_LIFE_TIME` parameter and remains logged in, then Oracle Database does not change the user's account status from `OPEN` to `EXPIRED(GRACE)` when the currently listed expiration date passes. The timing begins only when the user logs into the database. You can check the user's last login time as follows:

```
SELECT LAST_LOGIN FROM DBA_USERS WHERE USERNAME = 'user_name';
```

When making changes to a password profile, a database administrator must be aware that if some of the users who are subject to this profile are currently logged in to the Oracle database while their password profile is being updated by the administrator, then those users could potentially remain logged in to the system even beyond the expiration date of their password. You can find the currently logged in users by querying the `USERNAME` column of the `V$SESSION` view.

This is because the expiration date of a user's password is based on the timestamp of the last password change on their account plus the value of the `PASSWORD_LIFE_TIME` password profile parameter set by the administrator. It is *not* based on the timestamp of the last change to the password profile itself.

Note the following:

- If the user is not logged in when you set `PASSWORD_LIFE_TIME` to a low value, then the user's account status does not change until the user logs in.
- You can set the `PASSWORD_LIFE_TIME` parameter to `UNLIMITED`, but this only affects accounts that have not entered their grace period. After the grace period expires, the user must change the password.

3.2.5 Managing Gradual Database Password Rollover for Applications

22

A gradual database password rollover enables the database password of an application to be updated while avoiding application downtime while the new password is propagated to application clients, by allowing the older password to remain valid for a specified period.

- About Managing Gradual Database Password Rollover for Applications
  You can configure a gradual database password rollover process to begin for database application clients when the database administrator changes the database password for the application.
- Password Change Life Cycle During a Gradual Database Password Rollover
  After a password is created or changed, it follows a life cycle and grace period in four phases.
- Enabling the Gradual Database Password Rollover
  To enable the gradual database password rollover, you must configure the `PASSWORD_ROLLOVER_TIME` user profile parameter.
- Changing a Password to Begin the Gradual Database Password Rollover Period
  After you have set a non-zero `PASSWORD_ROLLOVER_TIME` value, change the user's password and update the password with all the applications.
- Changing a Password During the Gradual Database Password Rollover Period
  After the rollover period has begun, you can still change the password.

  - As an administrator, expire the password by executing the `ALTER USER username PASSWORD EXPIRE` statement. The next time the user logs in, he or she will be required to change their password.

Beginning with the first connection attempt after the password rollover period expires, Oracle Database drops the earlier password `p1`. Any attempt to login using the old password `p1` returns an `ORA-1017 Invalid Username/Password` error, and is recorded as a failed login attempt. In effect, connections after the rollover period are authenticated with only the new password, and connections that are attempted with the old password are recorded as failed login attempts. The failed login attempts could lock an account after a sufficient number of consecutive logon attempts with the old password.

Connection attempts to read-only database servers after `PASSWORD_ROLLOVER_TIME` expires will require new password (`p2`). The password change to `p2` will be made effective for all database clients.

3.2.5.7 Database Behavior During the Gradual Password Rollover Period

Users can perform their standard password changes and logins during the password rollover period.

The following database behavior is implemented during the rollover period:

- The user can log in to the database using either the new or the old password. This effectively increases the lifetime of the old password by the time set with `PASSWORD_ROLLOVER_TIME`.
- Passwords can be changed by using the following methods:
  - An administrator or the user changes his or her own password by using the `ALTER USER` statement.
  - The user changes his or her own password by using the SQL*Plus `password` command.
  - The user's password is programmatically changed when the Oracle Call Interface (Oracle OCI) `OCIPasswordChange` function is executed.
- Oracle Database does not send any special messages to the database clients that indicate that the user account is in the password rollover period. This design avoids any errors from applications that may not be equipped to handle error and warning messages when a user logs in.
- Too many failed login attempts move the user account into a timed lock state, depending on the value of profile limit `PASSWORD_LOCK_TIME`. After the timed lock period expires, the state of the password rollover period determines what happens when the user attempts to log in.
- User administrators can perform other password lifecyle related actions as usual, such as `ACCOUNT LOCK`, `ACCOUNT UNLOCK`, `EXPIRE PASSWORD` operations.
- The password limits that have been set by the `PASSWORD_REUSE_TIME` and `PASSWORD_REUSE_MAX` in the user profile continue to be honored during the rollover period. Any password changes during the rollover period are validated against password change history and added into the password change history.
- Expiring a user account does not affect the password rollover status. As with locked accounts, Oracle Database maintains the password verifiers in their current state. The user can log in using either old or new password (`p1` or `p2`). However, after the user