Password profiles can enforce policies on password management. Which of the following statements, if any, are correct? (Choose all that apply.)

A. Profiles can prevent a user from changing his password.

 B. A profile can be used to configure an account that you can connect to without a password.

 C. Profiles can be used to track password changes.

D. Profiles can control how long an account is locked for following repeated failed logins.

E. The FAILED\_LOGIN\_ATTEMPTS profile limit will lock an account only if the failed login attempts are consecutive.

 F. The PASSWORD\_GRACE\_TIME profile limit controls the number of days before password expiration during which you will be prompted to change your password.

Step 1:

A password management policy can be used to define and enforce a set of constraints that will help users keep their passwords safer. Passwords must be kept secret at all times in database security systems that rely on them.

Oracle Database has a password management policy because passwords are sensitive to theft and misuse. This policy is controlled by database administrators and security officers through user profiles, giving them more control over database security. Oracle recommends password management, which includes account locking, password ageing and expiration, password history, and password complexity verification, to improve security while utilising database authentication.

Step 2: Answer with Explanation

Answer

D and E are correct answer

D. Profiles can control how long an account is locked for following repeated failed logins.

E. The FAILED\_LOGIN\_ATTEMPTS profile limit will lock an account only if the failed login attempts are consecutive.

The profile directive PASSWORD LOCK TIME controls how long an account is locked after several failed login attempts; however, the failed login attempts must be consecutive in order for the account to be lost.

failed login attempts - The number of failed login attempts that must be made before the Oracle user account is locked. In 11g, the default is ten failed attempts. The grace period after the password life time limit has been reached is called password grace time.