

**Description:** The use of strong passwords is critical to proper authentication of users. Strong passwords are characterized by the fact that they can not be easily guessed. Easily guessed passwords include common proper names, common dictionary words, blank passwords, login IDs appended with numbers, passwords same as login IDs, passwords reverse of login IDs, dates, common keystrokes, and sequential letters and numbers. SQL Server does not provide a mechanism to enforce password strength. To ensure users are choosing strong passwords, you should run periodic password strength tests.

Of special note is the account probe. The probe account is used for coordinating distributed transactions and collecting performance statistics. Problems arises because using the probe account for these purposes requires that no password be set. This leaves the server vulnerable to attack.

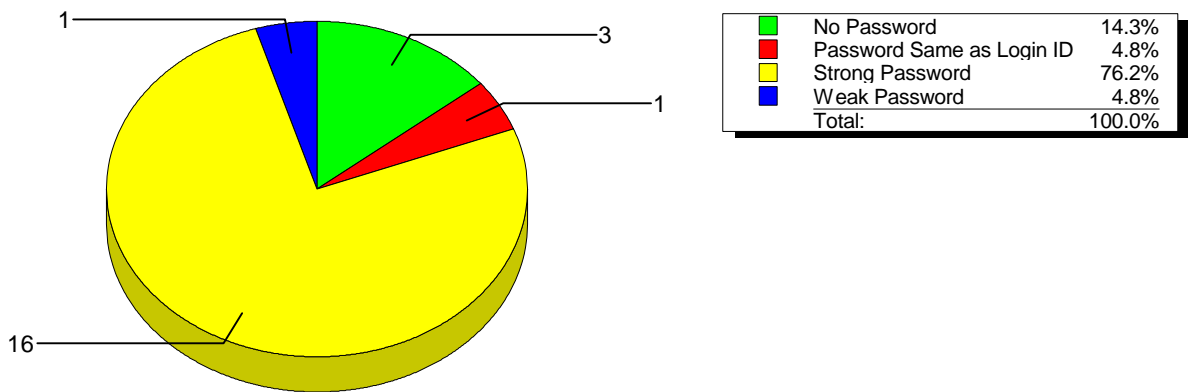
The probe account is used when the security is set to standard mode. If you must operate in standard mode, and require the use of the probe account, you should tighten your servers security by revoking all permissions from the public group in the master database (including the system tables) and removing guest user IDs from other databases. If you do not need the probe login, reset the probe login with a strong password.

In mixed or integrated mode, distributed transactions and collecting performance statistic can be accomplished using NT accounts mapped to the sa login. In this case, reset the probe with a strong password.

**Compliance Status:** Assessment was performed using option <Use faster password dictionary>. There is a small number of passwords that failed.

**Fix:** Notify the login ID owners that they should change their passwords. Educate users on how to choose appropriate passwords. Provide guidelines for choosing hard-to-guess passwords. This may include the use of numbers or special characters in passwords.

### Password Strength By Category



#### Password strength: No Password

Login ID	
abishop	jlesser
probe	

Logins for password strength: 3

**Password strength: Password Same as Login ID**

**Login ID**

jdoe

**Logins for password strength:** 1

**Password strength: Weak Password**

**Login ID**

jmaas

**Logins for password strength:** 1

**Total Failed Passwords:** 5