Password Checker

The Password Checker tool helps you evaluate and strengthen your SQL Server password policy, such as finding weak passwords that can make your SQL Servers vulnerable to outside attack. You can see exactly which logins are at risk so you can replace the weak passwords with strong passwords.

The Password Checker tool allows you to:

- Use proven approaches to test password strength, including use of built-in password lists.
- Use a custom password list that enforces your specific corporate password policy.
- Choose which logins you want to check.
- Drill down to identify logins associated with weak passwords.
- Save your test results.

By default, Password Checker connects to the specified SQL Server instances using the credentials of your currently logged on Windows account.

Password Checker then finds bad passwords by performing a dictionary scan against one of the built-in password lists provided with the Password Checker tool or against your own custom list.

Considerations before using the Password Checker tool

The Password Checker tool uses a list of common words to test for bad passwords. As a best practice, users should not use blank passwords, common words, or passwords that match a login name. The Password Checker tool uses lists of common passwords compiled by industry experts.

There are a number of factors you should consider before using the Password Checker. It is important that you:

- Decide whether you need to check specific SQL Server instances or a server group.
- Ensure the authentication account has CONTROL SERVER or sysadmin privileges on each instance you intend to check.
- Choose which password list you want to use for the check. You can check against your own password, a custom password file, or one of the built-in password lists. You can also check for blank passwords.

You can use Manage Server Groups and SQL Discovery with the Password Checker tool to further enhance your validation. These other tools work with the Password Checker tool in the following ways:

Manage Server Groups

Use Manage Server Groups to create logical groups of SQL Server instances. By creating a server group, you can easily check passwords on instances that are mission-critical or host sensitive data.

SQL Discovery

Use SQL Discovery to find SQL Server instances on your network, and then use the Password Checker tool to test the security of those instances.

Use the Password Checker tool

To check a password using the Password Checker tool:

1. Open the IDERA SQL Admin Toolset Launchpad, and then click **Password Checker**.
2. Specify whether you want to check passwords on a SQL Server instance or a server group.
3. Search for and then select the SQL Server instance or server group whose backup status you want to check. To specify multiple SQL Servers, separate each instance name with a semicolon.
4. Check the options of passwords you want to check against. You can use:
   - **Top 10 List**. Contains the most popular passwords as defined by *PC Magazine* and actually contains 11 passwords as a blank password is in the list.
   - **Blank password and passwords matching login**. Contains a blank password plus any passwords that match the user account used to log in to the system.
   - **Nifty Fifty**. Contains 50 of the most commonly used passwords including a blank password and the user name as a password.
   - **Other**. Allows you to specify specific passwords to look for.
   - **800 Common Passwords**. Contains 800 of the most commonly used passwords including a blank password and the user name as a password.
   - **Custom List**. Allows you to attach a file to check passwords against.
   - **The Big List (2400+ Passwords)**. Contains over 2400 of the most commonly used passwords including a blank password and the user name as a password.
   - **Test Common Variations of Selected Passwords**. Checks different variations of passwords already selected using one of the previous check boxes.
5. Specify which logins you want to check on the selected SQL Servers, separating each login name with a semicolon. Always check logins containing elevated privileges, such as members of the built-in server roles.
6. **Check Passwords**.
7. View the results.
8. ***If you want to view login details for a specific SQL Server instance*** , click the appropriate login listed in the **Test Results** right pane.
9. ***If you want to save the results*** , right-click to save the results as a TXT, XML, or CSV file.

Create a custom password list

The Password Checker tool allows you to attach a document containing a custom list of passwords to check against. You can attach this list using the **Custom List** check box, and then searching for and selecting the appropriate file.

To create a custom password list using the Password Checker list:

1. Open a text editor program, such as Notepad.
2. Type each word or phrase on individual lines. This list should represent strings that should not be used in SQL Server login passwords.
3. Save the file in a secured folder.