

How does Weak Password detection help you?

The **Weak Password Detection** option lets you set up how IDERA SQL Secure enforces password health. When setting up this option, take the following points into account:

- Users should not use blank passwords, passwords with common words, or passwords that match a login name.
- The SQL Logins of your audited SQL Server instances will be checked against a list of known words used in weak passwords.
- SQL Secure allows you to specify a custom list that includes words and phrases you have restricted in order to ensure passwords meet corporate security policies.
- Password detection is enabled by default for all SQL Server instances registered with SQL Secure.



SQL Secure determines the password health for all SQL logins but not for Windows user accounts or groups who have privileges on the audited SQL Server instance.

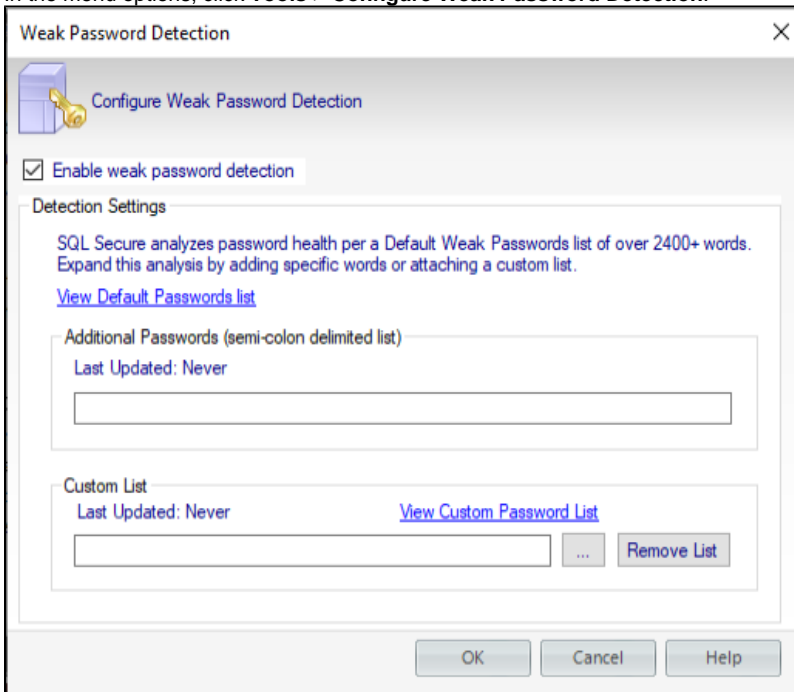
Weak password detection


The password analysis is performed during snapshot collection. When a snapshot is taken, the passwords of all SQL logins on the target SQL Server instances are collected and then compared against the default weak password list as well as any custom lists you defined. Each password is also compared against the name of its login.

The result (a security check finding) is stored in the Repository database but the passwords themselves are not stored.

To configure your Weak Password Detection settings:

1. In the menu options, click **Tools > Configure Weak Password Detection**.



2. Select **Enable weak password detection**. SQL Secure uses a default list with over 2400+ words. In the **Detection Settings** you can:
 - Add new words to the default list by typing the additional words or phrases separated by a semicolon in the Additional Passwords textbox. If you want to access the Default Passwords list, click **View Default Password List**.
 - Customize the password analysis by importing a custom list. For this purpose, type the name of the list file (text file *.txt) or click the ellipsis button  to browse a file in your computer. Format the text file such that each word or phrase is located on a separate line. If you want to view the imported list, click **View Custom Password List**. To specify a different text file, click **Remove List**, and then add the new file.
3. Click **OK**.

- ✓ Determine which policy assessments should analyze password health. For each assessment, review its settings to ensure the **Weak Passwords** security check is enabled.

Test your configuration by [taking a snapshot](#) and then [reviewing the security check findings](#) for your target servers.

About the Default Weak Passwords list

The Default Weak Passwords list was compiled by industry experts. This list includes over 2,400 common words and phrases used in passwords that are considered weak (easy to guess or hack), including blank passwords. By default, SQL Secure uses this list to analyze your enterprise's password health, comparing each SQL login password to the list, then reporting the result as a security check finding.

- ⚠ The weak password check is currently **case sensitive**. For example, "password" can trigger weak password alerts but "Password" don't.

You can add specific words and phrases to the default list, such as popular Internet memes like "kitteh" and "double rainbow." You can also add a custom list, such as words restricted by your corporate password policy or words that are common in your own environment.

- ✓ To create stronger passwords and help to ensure password security in your environment, enable the 'Enforce password policy' test. The security check name for this test is '*SQL Logins Not Using Password Policy*', find it enabled by default for the 'All Servers' audit policy, you can enable it manually in other custom policies."

Security Checks that enforce password health

To audit and enforce password health, enable the **Weak Passwords** security check in your assessment policies. This security check is enabled by default in the IDERA Level 2 and Level 3 [policy templates](#).

Detected types of password health

As SQL Secure analyzes the password health of your SQL logins, it records one of the following results. These findings are displayed in the corresponding [Login Properties](#) window and the [Login Vulnerability](#) report.

Password health results	What it means
Blank	The password for this login is either blank or null, which means no password is required for authentication or successful connection to databases hosted by your audited SQL Server instances.
Matches login name	The password for this login matches the name of the login.
N/A	The password for this login was not checked, most likely because either the login is a Windows user account or weak password detection is disabled.
OK	This login most likely has a strong password because the password does not match any of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.
Weak	The password for this login matches one or more of the words and phrases in the Default Weak Passwords list or the additional and custom passwords you specified.

About password detection

When weak password detection is disabled, SQL Secure stops collecting password health data. All previously collected data remains stored in the SQL Secure Repository database and can be evaluated using your policy assessments. For future assessments, SQL Secure will no longer report on whether any SQL login passwords are considered weak but it will continue to report on whether a password is blank.

If the **Weak Passwords** security check is enabled for a policy assessment and the snapshot you selected does not include password health data, the **Snapshot May Be Missing Data** security check will warn you that weak password detection has been disabled and password health data is not available to analyze.



To stop reporting on password health, disable the **Weak Passwords** security check in your policy assessments.

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)