

Login Vulnerability

The **Login Vulnerability** report shows all SQL Server and Azure SQL Database instances whose SQL logins have weak passwords.



Recommendation

Weak passwords can be easily guessed or hacked, creating a high-security risk on your SQL Server instances. Remember to use strong passwords that meet your corporate password policy guidelines.

Getting Started

Follow these steps to create a report:


1. Select Date, Policy, and Baseline options from the Report Settings box.
2. Select a target instance.
3. Click the "View Report" button to generate your report.


SQL Secure™
Assess and audit security risks and access rights

Login Vulnerability

Most current audit data as of Tuesday, September 13, 2022

Server: All servers in policy



There are no SQL logins with weak passwords.

About: This report shows any SQL login that has a weak password.

Recommendation: SQL logins whose passwords are weak (can be easily guessed or hacked) create a high security risk on the target SQL Server, Azure SQL Database and Amazon RDS for SQL Server instances. It is recommended that any weak passwords be replaced with strong passwords that meet your corporate password policy guidelines.

APPENDIX: Audit Data

The following snapshots were used to generate this report. For complete information on what audit data was captured, check the filter settings and status of each snapshot.

SQL Server	Version	Audited On
	SQL Server 2016 v13.0.1601.5	6/15/2022 6:13:57 PM


Generated by on 9/13/2022 8:00:07 AM

Execution Time: 0 hours, 0 minutes, 0 seconds

Page 1 of 1

Copyright © 2005-2022 Idera, Inc.