

Suspect SQL Logins

The **Suspect SQL Logins** report complements Suspect Windows Accounts and shows all SQL Server, Azure SQL Database, and Amazon RDS for SQL Server logins with no permissions.



Recommendation

The report will only show the SQL Logins that do not have permissions assigned.

Getting Started

Follow these steps to create a report:

1. Select the 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

Suspect SQL Logins

Most current audit data as of Monday, September 26, 2022

Server: All servers in policy

About: This report shows all the SQL Server, Azure SQL Database and Amazon RDS for SQL Server logins that do not have any permissions.

Recommendation: Show all the SQL Logins that do not have any permissions assigned.

Server	Login	Type	Probable Status
Server 1		User	

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
Server 1	SQL Server 2019 v15.0.2095.3	9/15/2022 4:56:21 PM
Server 2	SQL Server 2017 v14.0.3356.20	9/15/2022 4:52:03 PM
Server 3	SQL Server 2017 v14.0.3356.20	9/15/2022 4:56:23 PM