Use the Console to generate reports

IDERA SQL Secure includes built-in reports specially designed to generate commonly requested audit reports using the SQL Server permission data collected in your snapshots.

SQL Secure built-in reports allow you to quickly and easily meet the demands of on-the-spot audits, routine audits, and long-term event trending. Each report provides detailed information about events in your SQL Server environment.

> ⚠ Using the Console to generate reports against large audit data sets can result in degraded performance. For example, when the selected snapshot is large (contains thousands of objects and permissions), the report performance may be impacted. ***If you experience degraded performance*** , try increasing the Console timeout value and, if the performance issues continue, run the report with Microsoft Reporting Services instead.

Generate a report

To report on audit data:

1. In the console tree pane, click **Reports**.
2. In the view pane, select the report you want to generate.
3. Specify the appropriate parameters for the selected report, and then click **View Report**.

Available general reports

Report Name	Report Description
Audited SQL Servers	Displays all the SQL Server instances that are being audited by SQL Secure
Cross Server Login Check	Displays all SQL Server instances where a selected user has access
Data Collection Filters	Displays the data collection filters for all SQL Server instances
Risk Assessment	Displays all policy and risk assessment results. You can customize this text using the Policy Properties window. For more information, see Internal Review Notes.
Activity History	Displays all SQL Secure activity history
SQL Secure Users	Displays all SQL Secure users

Available entitlement reports

Report Name	Report Description
Suspect Windows Accounts	Displays all the suspect Windows Accounts that have Server Logins or Server Files Permissions. For more information, see Suspect Windows accounts.
Suspect SQL Logins	Displays all the suspect SQL Server Accounts that do not have any assigned permissions, i.e. databases, objects, or server files.
Server Logins and User Mappings	Displays all Server Logins and associated Database User Mappings for each SQL Server instance being audited
User Permissions	Displays permissions for a user across all SQL Server instances
All User Permissions	Displays all objects with permissions in the database for all SQL Server instances
Server Roles	Displays all direct members of Server Roles on all SQL Server instances
Database Roles	Displays all direct members of Database Roles on all SQL Server instances

Available vulnerability reports

Report Name	Report Description
Mixed Mode Authentication	Displays all SQL Server instances where Windows Authentication is not the only login method

Guest Enabled Databases	Displays all databases on a SQL Server instance where the Guest user has access
OS Vulnerability via XSPs	Displays all extended stored procedures that allow access to operating system features that could compromise system security
Vulnerable Fixed Roles	Displays all SQL Server instances that contain fixed roles assigned to public or guest
System Administrator Vulnerability	Displays all SQL Server instances that include built-in Administrators as members of the sysadmin role
Dangerous Windows Groups	Displays all SQL Server instances that grant access to any OS controlled Windows Group
Database Chaining Enabled	Display all SQL Server instances that have cross-database ownership chaining enabled
Mail Vulnerability	Displays all SQL Server instances with SQL Mail stored procedures
Login Vulnerability	Displays any SQL logins that have weak (easily guessed or hacked) passwords and lists their security properties, including the state of their password health.

Available comparison reports

Report Name	Report Description
Assessment Comparison	Displays any differences identified in the security settings and findings of two assessments.
Snapshot Comparison	Displays any differences identified in the configuration settings and audit data of two snapshots.