Use Reporting Services to generate reports

IDERA SQL Secure includes the ability to take the existing built-in SQL Secure reports and seamlessly integrate them into Microsoft Reporting Services. For each built-in SQL Secure report, the Deploy Reports wizard installs a Report Definition Language (RDL) file. These RDL files define the report layout and parameters, using the data source (SQL Secure Repository) you specified during install. Reporting Services automatically acknowledges these files, allowing you to immediately generate and view reports on audit data using the Reports Manager Web interface.

You can view, customize, and develop new reports based on any of the built-in SQL Secure reports to fit your unique auditing needs. Reports can be viewed in an existing SQL Server environment that uses a dedicated Report Server. If you decide to use Microsoft Reporting Services, consider the following best practices:

- Save your new and modified reports to a separate folder
- Use a different file name for modified reports

For more information about the Reporting Services architecture, see the Reporting Services Books Online. For more information about developing custom reports using Microsoft Reporting Tools, see the Reporting Services Books Online.

Microsoft Reporting Services and SQL Secure

You can implement Reports on any computer running Reporting Services. The following installation scenario illustrates how you can implement Microsoft Reporting Services reports in an existing SQL Server environment that uses a dedicated Report Server.

Required permissions for Microsoft Reporting Services

Microsoft Reporting Services Reports leverage the existing role-based security model provided with Reporting Services. These reports support Windows authentication (mixed mode on SQL Server) and require the following permissions and rights to successfully generate reports on your audit data.

Assessing the appropriate role on the SQL Secure folder in Report Manager, the individual report files inherit the permissions you set. By default, the Deploy Reports Wizard writes the report files to the `C:\Program Files\IderaSQLsecure\Reports` folder on the Report Server computer.

Account	Action	Requirement
Logon account used for install	Write RDL files to the Report server computer and configure reports	Write access to the Report Server file system and Content Manager role
Proxy user	Connect to the Repository and read data per report parameters	Read access to the Repository databases
Administrator	Configure reports and set security	Content Manager role
End user (auditor or manager)	Generate and view audit reports	Browse role

Install reports

The Deploy Reports wizard allows you to specify the proxy user account credentials and deploy the reports. Perform this deployment for each Repository that contains data you want to audit using Reports. Once installed, click the **View Deployed Reports** link at the bottom of the SQL Secure Reports window to find your reports.

Set up permissions for auditors to generate reports

To grant auditors the ability to view and generate reports, create a SQL Server login and grant the **Can view** and **Report on audit data** permissions. Ensure that this account has the **Browse** role on the root folder.