Previous features and fixed issues

This build of IDERA SQL Secure includes many fixed issues, including the following previous updates.

2.7 New features

New policy templates for PCI and HIPAA

The SQL Secure policy templates now address security standards for the Payment Card Industry (PCI) and the Health Insurance Portability and Accountability Act (HIPAA), allowing you to immediately begin accessing your SQL Server environment against these regulations.

New weak password detection

SQL Secure now detects and analyses the password health of SQL logins on your audited SQL Server instances, reporting when passwords are blank or weak.

New security checks

SQL Secure now provides these additional security checks to help you further harden the security of your SQL Server instances:

- Weak Passwords
- Public Role Has Permissions on Database User Objects
- Integration Services Roles Have Dangerous Security Principals
- Integration Services Permissions Not Acceptable
  These security checks are enabled in the IDERA Level 3 policy template.

New FIPS support

SQL Secure now supports auditing and assessing the security of SQL Server instances located in environments that require FIPS compliance.

New SQL Server 2012 support

SQL Secure now offers full support of SQL Server 2012 RTM.

2.7 Fixed issues

- When changing server connection credentials, SQL Secure now identifies other audited SQL Server instances that use the same account and then lets you change their connection credentials as well.
- SQL Secure now correctly processes local account information for SQL Server instances operating in clustered environments.
- Snapshots that have been marked as baselines are no longer deleted from the SQL Secure Repository database during grooming.
- The SQL Secure Collector now correctly gets file permissions for service executable files when the file name is specified in upper case.
- The SQL Secure Collector now correctly gets permissions data for system databases that are not located on the local drive of the target SQL Server instance.
- SQL Secure now successfully displays the Server Security Report Card and generates the Risk Assessment report when the audited SQL Server instance and the instance hosting the SQL Secure Repository have been assigned different collations.
- When scheduling monthly snapshots, SQL Secure now correctly applies the "3rd," "4th," and "Last" options for specific days of the month.

2.6 New features

SQL Secure 2.6 includes the following fixed issues.

- SQL Secure is now correctly collects database file permissions when the SQL Server files are located in the root directory of a drive.
- The SQL Secure Common TCP Port security check will now generate a finding if a SQL Server instance is using dynamic ports only when "dynamic" is entered in the configuration list. Previously, dynamic ports would always generate a finding.
- The Full-Text Search Login Account Not Acceptable security check now correctly checks on and reports findings for all Full Text Search service logins on your audited SQL Server instances.
- SQL Secure now correctly collects file permissions from audited SQL Server instances hosted by a clustered Windows 2008 Server computer.

1.5 New features

SQL Secure 2.5 includes the following fixed issues.

- SQL Secure now correctly detects whether the SQL Server Agent is running on SQL Server instance hosting the Repository. This issue occurred when the SQL Server instance was configured to use a double-byte character set, such as the Turkish language.
- SQL Secure correctly excludes stored procedures listed in the Startup Stored Procedures security check criteria.
- SQL Secure now correctly collects audit data when you configure your snapshot filters to retrieve security information about System Only or User Only object types.

- SQL Secure now includes improved file data collection. Previously, when attempting to run a snapshot, SQL Secure had returned snapshot warnings and logged the following error: "Method failed with unexpected error code 53."
- SQL Secure now correctly handles data collection from instances located in an Active-Active cluster running Windows Server 2008.
- The Database File Permissions Not Acceptable security check now includes the system resource database files for SQL Server 2005 or later. On SQL Server 2005 instances, if these database files are not located in the same folder as the Master database, then SQL Secure may not be able to find the files and thus the security check may not return a correct finding.
- The Audited SQL Server Properties window now correctly applies your policy membership changes.
- SQL Secure now stores the Collector logs in the IDERA installation directory by default.