Previous features and fixed issues

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

4.3 New features

- SQL Secure allows you to schedule snapshots at the policy level, which lets you apply them to multiple instances.
- SQL Secure allows you to add system-supplied or user-specified certificates to the whitelist for the **Certificate private key were never exported** security check

> ⚠ The whitelist is already populated with the Microsoft certificates marked with **NO-PRIVATE-KEY** .

- The Suspect SQL Logins report now includes 'Enforce Password Policy" and 'Enforce Password Expiration' information.
- The **Database Roles** report now has an **Only active employees** filter that allows selecting Active, Disabled, or All AD accounts.

4.3 Fixed issues

- The **Suspect SQL Logins** report correctly lists SQL accounts avoiding Windows NT accounts.
- SQL Secure improved Snapshots performance for large databases.
- Fixed an issue when performing a snapshot comparison containing certificate changes.
- SQL Secure now shows the correct values for **CLR SAFE_ACCESS** and **CLR Enabled** security checks.
- SQL Secure now contains the CIS for SQL Server 2022 benchmark. All other CIS benchmarks have been updated to their most recent available benchmark version.

4.2 New features

- SQL Secure now allows you to take a snapshot of all registered servers in a policy. Snapshots can also be scheduled at the policy level
- The Server Roles report now shows members from Windows groups.
- The Database Roles report now displays the creation date of the database.

4.2 Fixed issues

- SQL Secure successfully monitors a set of databases after taking a snapshot, avoiding the "Some databases were unavailable for auditing" warning.
- SQL Secure now correctly labels log-shipped databases in standby/read-only recovery as "Databases Files" when running a snapshot.
- Collation settings no longer cause a conflict between the audited server and what it is expecting to match.
- "Backups compliance with RTO and RPO requirements" security check includes non-system databases that never had a backup, excluding system databases.
- Latest SQL Secure version no longer supports SQL Server 2000 and SQL Server 2005, a workaround is to install Secure on a SQL instance with a different collation.
- Database Roles report now shows results in Alphabetical order.
- The Database Roles report now allows a filter on active and inactive AD accounts.
- SQL Secure correctly reports "SQL Server Database Level Encryption" security check for Azure SQL Databases.

4.1 New features

- The Configuration Security Checks now allows you to configure your Backups compliance more freely with the **Backups compliance with RTO and RPO requirements check** . Now, you can set up the backup frequency and select the databases to backup.

4.1 Fixed issues

- When exporting a Policy, SQL Secure no longer checks all the checkboxes by default. It only keeps the enabled ones of the exported policy.
- The results of the snapshot show the 'Weak Passwords' security check identifying the new SQL Login a user created with the password set to one of the passwords from the list of Default Weak Passwords, and flags that as a finding.
- When the **sa** login is renamed and disabled, SQL Secure reports a Warning level risk finding.

- SQL Secure no longer displays Orphaned Users check findings when database users are mapped to certificates.
- Now the **Risk Assessment Report** correctly reports the **sa** account status when it is disabled.
- The **Risk Assessment Report** correctly reports when the sa account does not exist on the server.
- Now SQL Secure Grooming Job runs correctly and as expected.

4.0 New features

- The SQL Secure Data Collector Job Keys allow you to manage snapshot collection jobs. Use this option to throttle the collector jobs so that they do not overload the SQL Server instance.
- SQL Secure supports TLS 1.2 to send email requests to SMTP.

4.0 Fixed issues

- SQL Secure enhanced the assessment's loading time; they no longer take several minutes to display information.
- Snapshot collection on Availability Group Nodes no longer generates a file permissions warning message.
- Snapshot collection completes successfully for a log-shipped database.
- The number of Stored Procedures in the Stored Procedures Encrypted details of the security check no longer differs from the number of Stored Procedures in SSMS.
- SQL Secure no longer displays timeout errors while generating the Database Roles Reports.
- Renaming and disabling sa login account no longer shows a "sa Account Not Disabled" security check.
- "Public Server Role only granted default Microsoft permissions" security check shows the correct information related to Server Roles
- The Snapshot Comparison Report no longer displays server changes when no changes have been made.
- The User Permission Report works correctly with different collations sets.
- SQL Secure imports hidden instances using CSV files.
- The Snapshot collection process completes successfully for imported instances using CSV files.
- The Risk Assessment Report no longer reports the sa login account incorrectly.
- SQL Secure no longer has issues with bulk email notification settings.
- Renaming the sa login in a SQL Server instance no longer generates a false warning risk level in the 'sa account is not disabled' check.
- SQL Secure enhanced the SQL Job Permission security check.

3.4.1 Fixed issues

- The time to keep snapshots before letting them be groomed is no longer set by default to one day when importing files in CSV format.
- The User Permission report is no longer showing errors in the db_role information.
- The User Permissions report shows all schema-level permissions data. The Object Type filter is no longer generating blank spaces after any object type name.
- You can access registry key information and the SQL Server install folder with Local Administrador and Sysadmin permissions. The Snapshot collection is no longer displaying warning messages caused by permissions on the SQL Server instance.
- "Orphaned Users" security check is no longer identifying users without matching logins as orphan users.

- The All User Permissions report now allows you to expand or collapse results upon report execution. When the report has many permission results, displaying the results collapsed will allow the report to complete execution faster while permissions can be expanded and explored for each audited database.
- Generating the Database Roles report is no longer causing a "maximum recursion" error message.

- SQL Secure fixed the "Is the SQL Server sa account enabled" security check to have a passed status when the finding is "The sa account is not enabled".

3.4 New features

- SQL Secure adds a DISA-NIST STIG policy and security check templates for SQL Server 2016, with 11 security checks enabled by default.
- An additional policy field filtering option was implemented in the Assessment Comparison report.

3.4 Fixed issues

- The error message where "SQL Secure was unable to acquire a valid key" is no longer displayed while trying to take snapshots after decommissioning some servers.
- The SQL Mail or Database Mail Enabled security check now is working as expected.
- Addressed several areas causing poor performance and usability in the user permissions report with significant success.
- Streamlined workflow for the snapshot data collection operation.

3.3.2 New features

- SQL Secure now supports Windows Server 2019 and SQL Server 2019.
  - Install, upgrade, uninstall SQL Secure using SQL Server 2019 based repository.
  - Monitor SQL Server 2019 based instances where SQL Secure repository uses SQL Server 2019 or previous versions.
  - Monitor SQL Server 2019 and previous versions from environments where SQL Secure repository uses SQL Server 2019.
  - Register SQL Server 2019 on Azure VM and Azure SQL Database, generates all available reports.
  - Register SQL Server 2019 on Amazon EC2 and Amazon RDS for SQL Server, generates all available reports.
- SQL Secure adds policy templates: CIS for SQL Server 2017 and SQL Server 2019.

3.3.2 Fixed issues

- The CIS for SQL Server 2016 policy lists all the corresponding security checks.
- Snapshot comparison report doesn't show server role change.
- Exporting the User Permission Report is working as expected.

3.3.1 Fixed issues

- The Operating System Security Check no longer generates risks when the Operating system matches the details.
- Unauthorized Account Security Check is no longer displaying inconsistent results and details.
- SQL Secure improved its performance significantly decreasing report generation times.
- Snapshot Comparison Report displays the correct Server Role when a difference is generated between snapshots.

3.3 New features

- Adds audit support for Amazon RDS and Amazon EC2.
- Supports installing SQL Secure on Azure VM and Amazon EC2.
- Adds new security checks to support GDPR and provide a GDPR policy template.
- Updates Idera Level 1 - 3 policy templates.
- Enhances the Import/Export Policy.
- Provides an option to make bulk changes to email notification settings.
- Allows users to archive snapshots for decommissioned servers.

3.3 Fixed issues

- SQL Secure is no longer having issues with expired Licenses.
- SQL Secure Grooming Job is no longer failing while classifying errors from warnings.
- The Unauthorized Account Check security check is not returning findings on SQL Server 2008 R2, it works with SQL Server 2016 and above.
- The explanation notes functionality is working for all security checks.
- The uninstallation process completes removing all SQL Secure files.
- SQL Secure reports show Snapshot missing data when all Sequence Objects are included in the filter.
- The Snapshot Data Collection process for Windows Server 2016 is no longer showing incorrect warnings.
- TracerX-Viewer.application no longer requires to upgrade the .NET version.
- SQL Secure includes the option to add new servers to Server Group Tags.
- The Risk Assessment Report includes the Show Risk Only option.
- HIPAA policy now includes msdb database as default in the criteria.
- SQL Secure installer includes the Visual C++ 2015 Redistributable.

3.2 New features

New Security Templates

IDERA SQL Secure 3.2 includes the following New Security Templates:

- Center for Internet Security (CIS) for SQL Server 2008 R2, 2014, and 2016.
- Defense Information Systems Agency (DISA) & National Institute of Standards and Technology (NIST) for SQL Server 2012 and 2014.
- Sarbanes-Oxley Act, Section 404 (SOX 404).
- North American Electric Reliability Corporation (NERC).

Security Templates Updates

On this release IDERA SQL Secure updates the following Security templates:

- Center for Internet Security (CIS) in 2008 and 2012.
- Payment Card Industry Data Security Standard (PCI-DSS).

New Configuration Checks

IDERA SQL Secure 3.2 adds the following configuration checks:

- Hidden Instance Option is Set
- Auto Close Set for Contained Databases
- Max Number of Concurrent Sessions
- Backups Must Be in Compliance with RTO and RPO Requirements
- Shutdown SQL Server on Trace Failure
- Ad Hoc Distributed Queries Enabled

New Access Checks

IDERA SQL Secure 3.2 adds the following access checks:

- Asymmetric Key Size
- Database Master Key Encrypted by Service Master Key
- SQL Server Database Level Encryption
- Appropriate Cryptographic Modules Have Been Used to Encrypt Data
- Database Master Keys Encrypted by Password
- Symmetric Keys Not Encrypted with a Certificate
- Implement Cell Level Encryption

New Auditing Checks

IDERA SQL Secure 3.2 adds the following auditing checks:

- SQL Server Audit is Configured for Logins
- DISA Audit Configuration
- Implement Change Data Capture

New Login Checks

IDERA SQL Secure 3.2 adds the following login checks:

- SQL Logins Not Using Must Change

New Permissions Checks

IDERA SQL Secure 3.2 adds the following permissions checks:

- Limit propagation of access rights
- Direct access permissions

Supports SQL Server 2017

IDERA SQL Secure 3.2 now supports the repository and a monitored server of SQL Server 2017 on Windows.

3.2 Fixed issues

- This version of SQL Secure improves the execution time of the Snapshot Comparison Report, making it able to display large datasets.
- Time out error is no longer displayed on the User Permissions Report when the report was running for 80+ databases. In addition, users can export the report to CSV format.

- Users now are able to filter for specific databases in the Database Roles Report.
- Increased Excel Report Export capability to support reports with more than 65,000 rows of data.
- This release improves Risk Assessment performance, which now is able to process policy information.
- This release updates the console installation to use the existing repository.
- Users can configure STMP for SQL Secure mail server.
- Users can choose to monitor Always On Availability Group by registering the listener or individual nodes. Take into account there may be some gaps if you register using the listener.
- Under Security Report Card users are able to see Logins Information with Windows Accounts Details for the Suspect Logins Security Check.
- The Integration Services Running security check now is updated depending on the integration service status.
- The Details Reports for SQL Server 2000 show database roles and members, it was previously not available for this version.
- Updated SQL Secure version for the deployed report target folder for SSRS reports.
- Users need to restart the application to update the SQL Secure Repository Connection Status after adding a new license in the SQL Secure Manage License section.
- SQL Secure now supports international date time format.
- The Integration Services Login Account Not Acceptable Security Check is no longer showing incorrect data for azure databases.