

# New features and fixed issues

IDERA SQL Secure provides the following new features and fixed issues.

## 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) 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 dataset.
- 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 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 policies information.
- This release updates console installation to use existing repository.
- Users can configure SMTP 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.

[IDERA Website](#) | [Products](#) | [Buy](#) | [Support](#) | [Community](#) | [About Us](#) | [Resources](#) | [Legal](#)