# Previous features and fixed issues

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

## 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 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.

## 3.1.200 New features

### Allows reference to decommissioned server instance snapshots

IDERA SQL Secure 3.1.200 now allows you to reference snapshots of decommissioned instances. Previously, IDERA SQL Secure removed permissions data for a server when it is removed from auditing. The only way to save the permissions and snapshot information for that instance was to back up the repository before decommissioning.

### Supports TLS 1.2

IDERA SQL Secure 3.1.200 includes support for Transport Layer Security (TLS) version 1.2. The TLS protocol provides encryption, authentication, and data privacy and integrity when transferring information over a network, including VPN, VOIP, and instant messaging.

### Includes new product versioning (x.x.x.x)

For internal tracking reasons, this release of IDERA SQL Secure includes an updated product versioning format from three to four parts. For example, the previous version of SQL Secure was version 3.1.0 (x.x.x) and this release is 3.1.200.x (x.x.x.x).

## 3.1.200 Fixed issues

- This release fixes an issue causing the SQL Secure Risk Assessment Comparison Report to show changes between snapshots when no changes actually occurred.
- Users now can remove a server instance without first removing it from an assessment or draft. If any assessment data exists, the user is asked whether they want to remove the server from all active assessments as well. If **Yes**, the assessment is kept intact while the instance is deleted. If **No**, the server is removed from the assessment as well.
- The **SQL Server SYSADMIN Accounts** security check now reports an accurate status instead of always reporting **OK** and not displaying any accounts. This metric did and continues to report correctly in a snapshot.

- Resolved an issue that caused the following error while processing a security check when **Database roles and members** is enabled: "Error 515 encountered on line xxxx: Cannot insert the value NULL into column 'usertype', table '@DatabaseRoleUsers'; column does not allow nulls. INSERT fails."
- This release fixes an error regarding SQL Server 2014 and SQL Server 2016 accounts in the **Unauthorized Account** security check. Previously, the Unauthorized Account security check for SQL Server 2014 initially reported, "No issues found." Then, when a SQL Server 2016 server was added, it listed the unauthorized accounts in the result. However, when going back to the SQL Server 2014 server, it displayed the same unauthorized accounts results that the SQL Server 2016 server revealed.
- Resolved an issue causing the error message,"Cannot insert duplicate key in object 'dbo.<servername>'. The duplicate key value is (1281, 327). The statement has been terminated." when attempting to create a snapshot.
- Changed the Unauthorized Account Check wording from, "Specify the unauthorized accounts," to "Specify the authorized accounts," in the description for the **Criteria** entry on the Policy Properties page and on the edit Values for Security Check window.
- When a user registers a virtual server that is part of a failover cluster, the name now correctly resolves to the cluster name.
- Resolved an issue with the **Database roles and members** and the **Server roles and members** security checks that caused metrics to provide details from other instances/databases.
- The GUI on the final screen of the SQL Secure Setup Wizard was updated to resolve the cut-off content of the descriptive text.
- The **Launch SQL Secure Console** is now enabled after a new installation or upgrade.
- The uninstallation wizard is updated to no longer show an incorrect final window.
- The copyright year is now correct throughout the product.
- The descriptive text within the **Row-Level Security** check is changed from, "... is configured for specific *databases* ..." to, "... is configured for specific *tables* ...".
- The descriptive text within the **Dynamic Data Masking** security check is changed from, "... is configured for specific *databases* ..." to, "... is configured for specific *columns* ...".

# 3.1 New features

## Supports auditing of Azure SQL Database and SQL Server running in Azure virtual machines

IDERA SQL Secure 3.1 offers Cloud-specific capabilities for Azure-hosted SQL Server databases, including:

- Azure SQL Database and SQL Server running on Azure Virtual Machines (VMs).
- Security audits on Azure SQL Database instances and Azure Active Directory.
- Connecting to fully-qualified domain names for Azure VMs and Azure SQL Database instances as registered servers.

## Expands installation options

IDERA SQL Secure 3.1 includes expanded installation options to support hybrid cloud environments.

## Expands Security Check coverage

This release expands Security Check coverage for data protection, encryption, and firewall rules for the SQL Server platform, including Always Encrypted and Transparent Data Encryption.

## Moved to the Windows .NET 4.6 framework

IDERA SQL Secure 3.1 supports Microsoft Windows operating systems using .NET 4.6. For more information about requirements, see Product requirements.

# 3.1 Fixed issues

There are no fixed issues in this release.

# 3.0 New features

## Added SQL Server file import

Users now can import a .csv file containing the SQL Servers they want to import for registration in IDERA SQL Secure. This is an important feature for environments having more than a few SQL Servers as it allows you to bulk import data into IDERA SQL Secure. For more information about this feature, see Import SQL Server instances.

## Added tags for easier server management

IDERA SQL Secure now features server group tags to allow you to more easily manage your SQL Server instance snapshots. You can select tags when registering a SQL Server or simply add a tag to your existing instances. Tags allow you to select a specific group of SQL Servers rather than selecting servers one by one. For more information about server group tags, see Manage server group tags.

## Added suspect SQL Server logins report

The new Suspect SQL Logins report displays all of the suspect SQL Server Accounts that do not have any assigned permissions, i.e. databases, objects, or server files. For more information about reporting, see Report on SQL Server Security.

## Expanded Risk Assessment reporting

IDERA SQL Secure 3.0 includes multiple additions and modifications to the existing Security Checks in the Risk Assessment report. These new checks include:

- **Access**
  - **Files on Drive Using Not Using NTFS**. Updated to support ReFS for SQL Server 2016.
  - **Supported Operating Systems**. Removed support for Microsoft Windows 2003 and added support for Windows 2012, Windows 2012 R2, and Windows 2016.
  - **SQL Jobs and Agent**. Updated to flag any case where a proxy account is not in use.
  - **Encryption Methods**. Updated to flag any case where unsupported encryption methods are in use. Note that beginning with SQL Server 2016, all algorithms other than AES_128, AES_192, and AES_256 are deprecated.
  - **Certificate private keys were never exported**. Verifies that Certificate private keys are exported.
- **Configuration**
  - **Linked Server**. Checks to see if there are linked servers, and then checks to see if the linked server is running as a member of the sysadmin group. Linked servers can lead to performance issues and running them using sysadmin privileges can leave a database vulnerable to corruption.
  - **SQL Server Version**. Checks to make sure a supported version of SQL Server is in use. Flags any case where an unsupported SQL Server version is in use.
  - **Full Text Search Service Running**. Checks to make sure that this service is running on the selected instance.
  - **Unauthorized Accounts Check**. Updated to include checks for roles beyond sysadmin, including the Separation of Duties roles in SQL Server 2014 and the roles surrounding encryption for SQL Server 2016.
  - **Other General Domain Accounts Check**. Update to include checks for general domain accounts such as domain Users, Everyone, and Authenticated Users added to the selected instance.
- **Surface**
  - **SQL Server Available for Browsing**. Updated the name of this check to **SQL Server Browser Running**.

For more information about using reports within IDERA SQL Secure, see Report on SQL Server Security.

# 3.0 Fixed issues

The following issues are fixed in IDERA SQL Secure:

- Resolved an issue that occurred when trying to register a SQL Server instance, which is clustered and using AlwaysOn Availability Groups. The system tried to register the Cluster Server Name instead of the SQL Server Instance Name.
- Resolved an issue that caused SQL Server administrator accounts to show sysadmin accounts for other servers in the Server Security Report Card.
- IDERA SQL Secure no longer incorrectly pulls database role information from SQL Server 2000 databases.
- Users no longer receive false warning messages when running a snapshot.
- Resolved an issue that caused the system to display authorized accounts as unauthorized when a wildcard was included in the list of authorized accounts in Unauthorized Accounts Are Sysadmins.

# 2.9 New features

## Improved Name Matches selection of rule filter properties

IDERA SQL Secure 2.9 simplifies the process for selecting a named variable when setting filter properties. Click **Any** in the **Name Matches** column of the Filter Properties dialog box, and IDERA SQL Secure displays a dialog box that allows you to see a list of available elements and a list of selected elements, and easily move the databases, tables, views, or functions between the two lists.

The list is populated based on the row where you click **Any**, i.e. if you click to select items from the **Tables where** row, the list displays only tables. To select more than one element at a time, press and hold the Shift key to click the first and last element in a series or press Ctrl and then click each element not in a series. Click **Add** to move elements form the **Available** list to the **Selected** list. Click **Remove** to move elements from the Selected list to the Available list. Search functionality also is available in this dialog box. Note that you can use wildcards when entering a search string. For more information about using Filter Properties, see Edit filter settings.

## Enhanced reporting

### Expanded some reports to show users within groups

The User Permissions, All User Permissions, and Database Roles reports now provide an option to view access at the user level within a group. The new **Level** field in the report filter allows you to select **Member** to display access results at the group (member) level or select **User** to display access results that show individual user account names within the group as well as whether the account is enabled. For more information about using reports within IDERA SQL Secure, see Report on SQL Server Security .

### Additional enhancements to the All User Permissions report

While the All User Permissions report now includes user-level information, it also includes updates that allow you to run the report for one or more specific databases. The All User Permissions report displays user permissions at the object level. IDERA SQL Secure 2.9 includes a new **Database** field and corresponding **All Databases** check box that allows you to enter specific databases to include in the report, or check the box to include all databases within the selected SQL Server.

Clear the **All Databases** check box to enable selection of one or more databases in the displayed list. To select more than one database at a time, press and hold the Shift key to click the first and last databases in a series or press Ctrl and then click each database not in a series. For more information about using reports within IDERA SQL Secure, see Report on SQL Server Security .

## Supports SQL Server 2016

IDERA SQL Secure 2.9 and later support SQL Server 2016 for the repository and audited instances. For more information about supported platforms, see Product requirements.

## Enumerates group members in a one-way trust

IDERA SQL Secure 2.9 now can enumerate users within a group when the target server is in an environment when IDERA SQL Secure is across domains configured as a one-way trust.

## Updates Guest User Enabled Access functionality

The Guest User Enabled Access check now includes msdb, master, and tempdb in the **Approved** user access list for all default templates.

# 2.9 Fixed issues

The following issues are fixed in IDERA SQL Secure:

- IDERA SQL Secure 2.9 fixes an issue causing IDERA SQL Secure to incorrectly report some servers as failing the Login Audit Level security check.
- An issue that triggered an email notification after data collection that stated that suspect windows were encountered no longer occurs.

# 2.8 New features

- IDERA SQL Secure now supports SQL Server 2014
- IDERA SQL Secure now supports Always On Availability Groups
- IDERA SQL Secure now allows you to install the SQL Secure Repository on a failover cluster. The installer provides an option to select Cluster installation and specify a cluster node.
- Policy Templates have been updated to use the latest versions of SQL Server and OS:

    - Updated to policy templates:
        - CIS v 2.0 for SQL Server 2005 (from version 1.2)
        - PCI-DSS v 3.0 Guidelines for SQL Server (from version 2.0)
        - HIPAA Guidelines for SQL Server - update security checks as needed e.g. Operating System Version
    - Added templates for:
        - CIS v1.1.0 for SQL Server 2008
        - CIS v1.0.0 for SQL Server 2012
        - MS Best Practices Analyzer for 2008
        - MS Best Practices Analyzer for 2012
- This version had updated to a granular process for Exporting and Importing policies, so that authorized SQL Logins can be excluded from exporting, and when imported the active settings for those checks remain unmodified.
- The process for registering new SQL Server instances with IDERA SQL Secure now allows to define folders for file system permissions checks.
- IDERA SQL Secure now supports Sequence Objects for SQL Server 2012.
- IDERA SQL Secure supports users in contained databases for SQL Server 2012 and 2014.
- IDERA SQL Secure now provides the following new Security Checks:
    - Security Check for SQL Server Integration Services (SSIS) to verify if any public or other unauthorized principals have been granted permissions to use SSIS stored procedures.
    - Security Check added to level 1 and level 2 policy templates that shows risk on systems where permissions have been granted to the public role on objects outside the sys schema in user databases.
    - Security Check: *Unacceptable Database Ownership* detects if a database is found with an unacceptable owner
    - The Risk Assessment Report has been updated with new nine security checks.

# 2.8 Fixed issues

## Phase out IDERA SQL Secure Itanium support

IDERA is beginning to phase out all Itanium support in IDERA SQL Secure 2.6 and all subsequent 2.x versions. While 2.8 will continue to operate with Itanium and support is available, IDERA SQL Secure 3.0 will not support the Itanium processor architecture. For more information, see the product requirements.

## SQL Secure Repository requires SQL Server 2005 or later

When upgrading, migrating, or deploying the SQL Secure Repository for the first time, ensure you select an instance running SQL Server 2005 or later for your target location. SQL Secure no longer supports SQL Server 2000 platform for the SQL Secure Repository.

***If you are upgrading from SQL Secure version 2.0 or earlier*** , you will need to migrate the Repository to a SQL Server 2005 or later instance. For more information, see IDERA Solution 00002617 ("How do I migrate SQL Secure from one server to another?").

## Microsoft Reporting Services 2000 is no longer supported

***If you are upgrading reports from Microsoft Reporting Services 2000*** , then upgrade to Microsoft Reporting Services 2005 before installing the new reports in SQL Secure 2.8 to ensure the upgrade is successful.

## New credentials may be necessary when upgrading

SQL Secure no longer uses the default credentials of your SQL Server Agent to collect Operating System and SQL Server security information. If, in a previously installed version, SQL Secure was configured to use the default SQL Agent credentials to collect security information, a window will open when you first open SQL Secure 2.8, prompting you for new credentials.

## Blank password not accepted when registering a SQL Server instance

When registering a new SQL Server instance, blank passwords are not accepted for SQL logins due to the extreme security risk this poses.

## SQL Secure can now audit the same cluster node on which it is installed

The SQL Secure now allows you to audit security data from SQL Server instances hosted on the same cluster node that hosts the SQL Secure Collector.

## Support for contained database authentication security

SQL Secure now displays information and report on the security settings of database principals used for contained database authentication and connections. Contained databases are a new security feature available in SQL Server 2012.

## SQL Secure now collects security data for AlwaysOn Availability Groups

When you take snapshots of the SQL Server 2012 instances you audit, SQL Secure now collects properties or security data for the AlwaysOn Availability Groups feature. AlwaysOn can be enabled only on instances running SQL Server 2012 & 2014 Enterprise Edition.

**IDERA** | **Products** | **Purchase** | **Support** | **Community** | **Resources** | **About Us** | **Legal**