Previous features and fixed issues

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

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 **L evel** 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.

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.