Known issues

IDERA strives to ensure our products provide quality solutions for your SQL Server needs. ***If you need further assistance with any issue,*** pleas e contact Support (www.idera.com/support).

Known issues

General

- Database roles and members are not included in the Report Card Details list on registered SQL Server 2000 instances.
- The repository grooming job does not delete snapshots which are in an Error state. Snapshots in an OK or Warning state are appropriately deleted.
- Clicking Technical Support Site on the IDERA SQL Secure Quick Start window redirects to an error page.
- SMTP email configuration may not work for a secure mail server.
- The Register SQL Server error message regarding supported versions needs updating to include SQL Server 2016.
- SSRS reports do not extract to a .csv file.
- The file type of an exported policy is not selected as .xml by default. In addition, when importing a policy, the file must be manually selected by selecting **All Files**.
- IDERA SQL Secure displays an incomplete error message if a specific user/role is given GRANT and/or WITHGRANT permissions by one grantor, and DENY permission by another grantor. The error message does not include identifying detail about the conflicting user or role.

Installation

- Console only installations may display an incorrect message stating that the repository specified is not compatible with this version of the Console. Click **OK** to continue installation.
- During a new installation, the Ready to Install the Program window refers to an upgrade instead of an installation.
- Uninstalling IDERA SQL Secure does not remove the Secure folder from the registry.
- The License Agreement does not display the correct year.

Security Checks

- **General Domain Accounts** security check does not display results.
- The **Integration Services Running** security check displays as green even when the service is not running.
- The **Integration Services Login Account Not Acceptable** security check displays incorrect data.
- The **Row-Level Security** security check causes the Risk Assessment Report to display, "The following tables do not have row-level security configured: '[R7].[DB1].[Table_1]' " for registered SQL Server 2016 instances.
- The **Transparent Data Encryption** security check causes the Risk Assessment Report to display, "The following databases do not have transparent data encryption configured: '[R7].[ReportServer]', '[R7.[ReportServerTempDB]' " for registered SQL Server 2016 instances.
- The following security checks for Integration Services are not returning accurate information: Integration Services Login Account Not Acceptable and Integration Services Running. It is recommended that users seeking to harden Integration Services review the login account and service run status of Integration Services using the server's SQL Server Configuration Manager.
- If the **Weak Password Detection** security check is disabled, the **Description** displays a list of all the usernames that have a blank password associated with the account.

Snapshots

- When changes occur between snapshots, IDERA SQL Secure displays the change information only in the **Difference** column of the Snapshot Comparison window and all other columns are blank.
- Clicking the **Hide and Notify when Complete** button while a snapshot is in progress will hide the snapshot progress screen, but no notification is sent when the snapshot does complete.
- Taking a snapshot of an Azure SQL Database from an on-premises installation of SQL Secure may take an extended length of time. This time is decreased when the snapshot is taken from an Azure VM installation of SQL Secure.
- In the Snapshot Comparison, the difference is mentioned in reverse order. For example, "Changed from [DescriptionOld] to [DescriptionNew]" is incorrectly displayed as, "Changed from [DescriptionNew] to [DescriptionOld]."

- If a user deletes a snapshot while it is running, and then tries to take another snapshot soon after, SQL Secure may show an error message.

Previous known issues

- The repository grooming job does not delete snapshots which are in an Error state. Snapshots in an OK or Warning state are appropriately deleted.
- Clicking the "Hide and Notify when Complete" button while a snapshot is in progress will hide the snapshot progress screen, but no notification is sent when the snapshot does complete.
- Taking a snapshot of an Azure SQL Database from an on-premises installation of SQL Secure may take an extended length of time. This time is decreased when the snapshot is taken from an Azure VM installation of SQL Secure.
- The following security checks for Integration Services are not returning accurate information: Integration Services Login Account Not Acceptable and Integration Services Running. It is recommended that users seeking to harden Integration Services review the login account and service run status of Integration Services using the server's SQL Server Configuration Manager.
- SQL Secure does not support SMTP servers which require SSL connections.
- IDERA SQL Secure 3.1 supports only the Active Directory Password Authentication and Active Directory Integrated Authentication modes to connect to Azure SQL database. ***If you are using this feature,*** you are responsible for setting up the VPN tunnel and any further infrastructure setup necessary for Active Directory to work those authentication modes. The VPN tunnel and infrastructure setup is *not the responsibility of IDERA, Inc.*
- Clicking Technical Support Site on the IDERA SQL Secure Quick Start window redirects to an error page.
- Console only installations may display an incorrect message stating that the repository specified is not compatible with this version of the Console. Click **OK** to continue installation.
- During a new installation, the Ready to Install the Program window refers to an upgrade instead of an installation.
- Uninstalling IDERA SQL Secure does not remove the Secure folder from the registry.
- The License Agreement does not display the correct year of 2016.
- SMTP email configuration may not work for a secure mail server.

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 2.6 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 2.6, 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 cannot audit the same cluster node on which it is installed

The SQL Secure cannot audit security data from SQL Server instances hosted on the same cluster node that hosts the SQL Secure Collector. To successfully audit your virtual instances, deploy the SQL Secure Collector on an instance that does not belong to the clusters you want to audit.

Incomplete support for contained database authentication security

SQL Secure does not fully display information about nor report on the security settings of database principals used for contained database authentication and connections. To see how many database principals have been created on the audited instance, as well as which permissions have been assigned to these users, navigate to the Object Permissions Explorer and then view the user properties.

Contained databases are a new security feature available in SQL Server 2012.

SQL Secure does not collect security data for AlwaysOn Availability Groups

When you take snapshots of the SQL Server 2012 instances you audit, SQL Secure does not collect properties or security data for the AlwaysOn Availability Groups feature. AlwaysOn can be enabled only on instances running SQL Server 2012 Enterprise Edition.

With Grant and Grant permissions

When SQL Secure displays the With Grant permission as checked, it does not also check the Grant permission as is the case in SQL Server Enterprise Manager or SQL Server Management Studio.

Incorrect timeout error message

SQL Secure may display an incorrect timeout error message when processing policy information.

Incorrect security check message

SQL Secure displays an incorrect message that some servers are failing the Login Audit Level security check even with proper settings.

Possible freeze when creating reports

SQL Secure may freeze when creating User Permissions reports for over 80 databases.

Policy findings for snapshots taken in previous versions do not contain all necessary data

When you create a policy in SQL Secure 2.5 or later and view a snapshot taken in a previous version, the snapshot may not contain required data. If this issue occurs, the security check “Snapshot May Be Missing Data” will return a finding.

Assessment Comparison window may not refresh display

When comparing assessments using the SQL Secure Console, the Assessment Comparison window may not refresh its display when you choose a different set of assessments to compare. To avoid this issue, close the window, and then click Compare Assessments on the actions ribbon to perform the next comparison.

Collector job fails when the port used to access the Repository changes

The port number is included in the Collector Job when it is first configured. If the port number changes, the Collector Jobs will fail. To fix this issue, delete the Collector Jobs that are failing and recreate them.

Collector job fails to get registry information from 64-bit Server

The Collector Job will fail to retrieve registry settings from an audited server running a 64-bit version of the Windows operating system, such as Itanium or x64, when the SQL Secure Repository is located on a server running a 32-bit version of the Windows operating system. To collect registry settings from the target server, install the Repository on a server running Itanium or x64.

SQL Agent job issue

The SQL Agent jobs used by SQL Secure can fail when the owner is from a one-way trusted domain. SQL Secure requires that the sysadmin account used in SQL Secure must be the owner of all SQL Agent jobs created. This setting has no effect on what the job does beyond execution of the job. This setting is required to ensure that only system administrators can run SQL Secure jobs, and prevents any problems with the snapshot collection process.

SQL Secure Collector logging issue

If a SQL Secure job has an error and the Collector is not started, a SQL Secure log entry is not created. Although a SQL Secure log entry is not created, you can see the error in the Windows Application log.

Snapshot Comparison may not report correct permissions status

When you generate a Snapshot Comparison, the report may indicate that differences exist in the file, folder, or registry key permissions when, in fact, there are no differences. This issue is most likely to occur when Windows user accounts have been granted multiple permissions on those files, folders, or registry keys.