Known issues

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

Previous known issues

Installation and configuration issues

Phase out SQL Secure Itanium support

IDERA is beginning to phase out all Itanium support in SQL Secure 2.6 and all subsequent 2.x versions. While 2.x will continue to operate with Itanium and support is available through November 2012, 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 2.6 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.

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.

Assessment Comparison server list reflects policy membership only

When you generate an Assessment Comparison, the SQL Server report parameter lists the instances that are currently audited by the original policy. This behavior can create unexpected report results when the assessments you are comparing audit different instances from those included in the original policy. To view all available audit data, select All servers in policy for the SQL Server report parameter.

SQL Secure tells you who has access to what on your SQL Server databases. Learn more > >

IDERA Website	Products	Purchase	Support	Community	About Us	Resources	Legal