Known issues

IDERA strives to ensure our products provide quality solutions for your SQL Server needs. The following known issues are described in this section. ***If you need further assistance with any issue***, please contact support.

> ⚠ SQL Safe is **ONLY** compatible with IDERA Dashboard version 4.6 and with limited support.

Known Issues for 9.2.1

Backup

- Backup operations are skipped for databases set on an always-on setting in a secondary server.

Virtual Database

- SQL Virtual Databases cannot be renamed or changed from their default location.
- You cannot unmount Virtual Databases through the CLI commands.

Known Issues for 9.2

SQL Safe Agent

- A communications delay when working with SQL Server instances in a clustered configuration has been identified. A patch is available for this issue, please contact support.
- After upgrading the management components to 9.2 and using older SQL Safe agent components, backups may be failing. A patch is available for this issue, please contact support.

Known Issues for 9.1

SQL Safe Repository

- The installation of the SQL Safe repository fails when it is installed on a SQL Server version lower than SQL Server 2019.

Known Issues for 9.0

Installation

- The remote installation of the SQL Safe Backup agent fails in scenarios where the Microsoft Visual C++ 2015 redistributable or greater is previously installed in the machine. To install the SQL Safe Backup agent properly, log onto a machine directly and install the Agent\Management components.
- During the installation of SQL Safe, the installer may identify that the VC++2015 redistributable or greater is not installed and suggests that you install it. The installer uses a registry key to detect whether the correct version of the VC++ redistributable is installed. There is a Microsoft bug with some versions of VC++ that causes that registry key to be

deleted which triggers this problem. However, during your SQL Safe installation, you are prompted with dialog boxes to complete the installation of the required VC++ version.

Known Issues for 8.7.2

Installation

- The remote installation of the SQL Safe Backup agent fails in scenarios where the Microsoft Visual C++ 2015 redistributable or greater is previously installed in the machine. To install the SQL Safe Backup agent properly, log onto a machine directly and install the Agent\Management components.
- During the installation of SQL Safe, the installer may identify that the VC++2015 redistributable or greater is not installed and suggests that you install it. The installer uses a registry key to detect whether the correct version of the VC++ redistributable is installed. There is a Microsoft bug with some versions of VC++ that causes that registry key to be deleted which triggers this problem. However, during your SQL Safe installation, you are prompted with dialog boxes to complete the installation of the required VC++ version.

Known Issues for 8.7.1

Installation

- The remote installation of the SQL Safe Backup agent fails in scenarios where the Microsoft Visual C++ 2015 redistributable or greater is previously installed in the machine. To install the SQL Safe Backup agent properly, log onto a machine directly and install the Agent\Management components.

Known Issues for 8.7

Installation

- The remote installation of the SQL Safe Backup agent fails in scenarios where the Microsoft Visual C++ 2015 redistributable or greater is previously installed in the machine. To install the SQL Safe Backup agent properly, log onto a machine directly and install the Agent\Management components.

Object Level Recovery

- When performing an Object Level Recovery, the operation may fail if the object for restore is selected without its associated schema.

Known Issues for 8.6.1

Management Service

- The Management Service may leave open SQL Server connections in a 'sleeping' state until the SQL Server or SQL Safe Management is restarted. In extreme cases, the number of open connections may cause the number of concurrent connections to reach the maximum allowed by SQL Server. Please contact support for further assistance.

Policies

- Email notifications are not sent for Restore policy failures. Please contact support for further assistance.
- When creating a restore policy from a cloud backup, specifying the Temporary Download Location path may produce an error if the SQL Server is a named instance. Please contact support for further assistance.

Restore

- After a successful restore using the 'Change Path' option to change the data and log file paths, the 'Restore Again' feature does not show the altered paths.
- When performing restore operations from Microsoft Azure Cloud with T-SQL and CLI commands, the WITHMOVE option is broken.
  The error presented is:
  Value cannot be null.
  Parameter name: sqlUsername

Known Issues for 8.6

Backup

- When saving native format SQL Server backups and storing to Azure cloud storage, customers need to confirm that their Azure accounts are of the type "General Purpose". This is not a SQL Safe Backup limitation but a Microsoft mandate, please refer to the Microsoft Support document.
- On SQL 2012 instances, databases may be skipped from jobs without displaying their skipped status or an error in the Policy Status view. Please contact support for further assistance.

Cluster Environment

- When a Virtual Database is mounted to a cluster and a failover occurs, the Virtual Database entry will disappear from the Virtual Database list in the Web Console. The Virtual Database will still be present and functional on the instance but will no longer be seen in the SQL Safe Virtual Database list.

Policies

- Statuses for deleted databases are not removed from the Last Operation Status section of the Policy Status view. Please contact support for further assistance.
- When performing a restore policy from the Amazon S3 location for a large database with the "Download File from Cloud" option unchecked, the SQL Safe Backup product will download the file from the cloud and choose the SQL Server data folder default destination.

Restore

- Restore operations to TSM Striped Files may result in an error message reporting that the second striped file could not be found.

Upgrades

- When upgrading from Microsoft Visual C++ 2015 to Microsoft Visual C++ 2017 version 14.14 there is a bug in the Microsoft upgrade that incorrectly removes the registry key that

the SQL Safe installation is checking. This bug is detailed in the following Developer Community. The bug was fixed in later versions of Microsoft Visual C++, so the workaround is to manually install the latest Microsoft Visual C++ version from the latest supported Visual C++ downloads.

Known Issues for 8.5.2

IDERA Dashboard

- Setting email notification configurations via the web UI may show an error "Failed to decrypt password" when attempting an ad-hoc backup from the web UI.

> ⓘ Email notification configurations set through the desktop client are not affected by this bug.

Installation

- SQL Safe Backup can be installed without the IDERA Dashboard on an Operating System 2003.
  Running the combined installer will display the following message: *"The current Operating System is not supported by this product"*.
- The remote installation of SQL Safe Backup agent fails in scenarios where the Microsoft Visual C++ 2017 Redistributable or greater is previously installed in the machine.
  To install SQL Safe Backup agent properly, log onto a machine directly, and install the Agent\Management components.

Policies

- Statuses for deleted databases are not removed from the Last Operation Status section of the Policy Status view. Please contact support for further assistance.

Upgrades

- After upgrading from SQL Safe Backup 8.5.1 to 8.5.2, the Web Console may need to be re-registered. Go to the product registration in the Web Console, delete the SQL Safe Backup 8.5.1 product, and register the SQL Safe Backup 8.5.2 product.
- Email notifications for SQL Safe Backup operations are not generated after upgrading to SQL Safe Backup 8.5.2. Please contact support for further assistance.
- The upgrade to SQL Safe Backup 8.5.2 may fail if your SQL Safe Backup installation uses a repository with a non-default name. Please contact support for assistance in completing the upgrade.
- The upgrade to SQL Safe Backup 8.5.2 may fail for customers who have previously backed up the system database TempDB using SQL Safe Backup. Please contact support for assistance in completing the upgrade.

Known Issues for 8.5.1

Installation

- The installation of SQL Safe Backup fails in scenarios where the Microsoft Visual C++ Redistributable requires Operating System updates.
  The following patches are required depending on your Operating System:
    ○ For Windows 8.1, install KB2999226 which has a pre-requisite of KB2919355.
    ○ For Windows Server 2012 R2, install KB2919355 which has a pre-requisite of KB2919442.

Policies

- Statuses for deleted databases are not removed from the Last Operation Status section of the Policy Status view. Please contact support for further assistance.

Upgrades

- After upgrading from SQL Safe Backup 8.5 to 8.5.1, the Web Console needs to be re-registered. Go to the product registration in the Web Console, delete the SQL Safe Backup 8.5 product, and register the SQL Safe Backup 8.5.1 product.

Known Issues for 8.5

Backup

- SQL Safe Backup Policies only support availability groups where the Backup preferences are configured for the Primary Replica. If configured with any other option, Full Backup operations will result in an error when running against any Secondary Replica.

Installation

- The installation of SQL Safe Backup fails in scenarios where an existing SQL Safe Backup database already exists.

  To avoid a failure, make sure that the specified name of the SQL Safe repository database matches the existing database.

Policies

- The SQL Safe Management Console can become unresponsive when editing a policy that contains a server where the SQL Safe Backup Agent is unreachable.

- Statuses for deleted databases are not removed from the Last Operation Status section of the Policy Status view. Please contact support for further assistance.

SQL Safe Backup Agent

- When deploying the SQL Safe Backup Agent components from the SQL Safe Management Console, an error message appears indicating an installation failure. Refreshing the SQL Server instance will detect if the SQL Safe Backup version or the deployment was successful. Deployments of the SQL Safe Backup Agent components from the SQL Safe Web Console do not present this issue.

Known Issues for 8.4.2

Installation

- The SQL Safe Filter Service and SQL Safe OLR Service can be installed on Windows version 10 and later once you disable the Secure boot (in the VM properties for a VM or the BIOS settings for a physical machine).

Object Level Recovery

- The Object Level Recovery feature is dependent on an existing installation of SQL Server 2008 R2 Management Objects from the Microsoft SQL Server 2008 Feature Pack.

Policies

- Statuses for deleted databases are not removed from the Last Operation Status section of the Policy Status view. Please contact support for further assistance.

Known Issues for 8.4.1

Native Backup

- When submitting an ad-hoc native backup operation against SQL Safe Agents prior to the 8.4 version, the operation will not perform any work. Native backup operations are only supported for SQL Safe Backup Agents 8.4 version and later.

Known Issues for 8.4

Cloud Support

- When backups fail while using Windows Azure, partial files will remain unless the user deletes them manually.

IDERA Dashboard

- SQL Safe Backup does not currently support IDERA Dashboard's tag management.
- Instances removed from the web and desktop console are still displaying under Dashboard Managed Instances.
- IDERA Dashboard does not support Microsoft Windows 2003.

Installation

- When installing or upgrading SQL Safe Backup, the installer is not able to parse SQL Server instance names with space within the entered name. For example, use "SERVER, 1433" instead of "SERVER, 1433".

Licensing

- The licenses users add should be valid for the Centralized Licensing model. When Centralized Licensing is enabled, all licensing information is managed using the SQL Safe Management Service, and each of the individual SQL Safe Backup Agent licenses is removed.

Object Level Recovery

- The SQL Safe Management Service and SQL Safe Backup Agent must be upgraded to the 8.4 version in order to run Object Level Recovery successfully.
- Object Level Recovery operations can fail when the SQLsafe repository database is hosted on a SQL Server 2014 or SQL Server 2016 instance with the following error: "Could not load file or assembly 'Microsoft.SqlServer.Smo, Version=10.0.0.0, Culture=neutral, PublicKeyToken=89845dcd8080cc91' or one of its dependencies. The located assembly's manifest definition does not match the assembly reference. (Exception from HRESULT: 0x80131040)". The recommended workaround is to use the InstantRestore or Virtual Database feature to recover the database in an expedited fashion.

Policies

- Users should take into account that time fields for the Policies, Operation History, and Databases tabs in the SQL Safe Web Console are currently expressed in the GMT time zone.
- In the web console Policies tab, options to start jobs and disable policy are not available.
- SQL Server Agent service account authentication for the Network path provided as the Primary location in the Log Shipping Policy wizard fails with an error even though the Service account has full permissions to the shared path.

TSM

- Low-level file selection is not working properly with TSM backup/restore.

Virtual Database

- SQL Virtual Database does not support compressed native backup from SQL Server 2014 and SQL Server 2016 instances. Attempting to mount these kinds of backups results in the following error: "The header for the backup archive cannot be read. The file may not be a valid backup archive".
- When using an appended SQL Safe Backup file, mounting a virtual database automatically selects the first backup set within the backup file.

Other Issues

- After registration, SQL Safe Web Console will list all available instances in the repository. Users have to use the options to Bulk Edit credentials to change credentials for those instances they are not able to monitor.
- The SQL Safe Web Console is not currently sending e-mail notifications for Restore Operations.
- "Agent deployment service account" changes made in the desktop console are not replicating in the web console.

Known Issues for 8.3

Cloud Support

- When backups fail while using Windows Azure, partial files will remain unless the user deletes it manually.

IDERA Dashboard

- Safe does not currently support IDERA Dashboard's tag management.
- Product registration at the IDERA Dashboard is currently not supported in this release.
- Instances removed from the web and desktop console are still displaying under Dashboard Managed Instances.

Installation

- When installing or upgrading SQL Safe, the installer is not able to parse SQL Server instance names with space within the entered name. For example, use "SERVER,1433" instead of "SERVER, 1433".

Licensing

- The licenses users add should be valid for the Centralized Licensing model. When Centralized Licensing is enabled, all licensing information is managed using the SQL Safe Management Service and each of the individual SQL Safe Backup Agent licenses are removed.

Policies

- Users should take into account that time fields for the Policies, Operation History, and Databases tabs in the SQL Safe Web Console are currently expressed in the GMT time zone.
- In the web console Policies tab, options to start jobs and disable policy are not available.
- SQL Server Agent service account authentication for the Network path provided as the Primary location in the Log Shipping Policy wizard fails with an error even though the Service account has full permissions to the shared path.

TSM

- Low-level file selection is not working properly with TSM backup/restore.

VDB

- Users who plan to install Safe 8.0 on the same system as VDB should obtain the VDB 2.1 buddy drop which addresses compatibility issues between the two products. Please contact IDERA Support for more information.
- After installing SQL Safe, existing virtual databases may not be accessible. IDERA recommends to first upgrade with the VDB 2.1 buddy drop, unmount virtual databases, install SQL Safe, and then recreate the respective VDBs. Contact IDERA Support for more information.
- When uninstalling SQL Safe, users may need to reboot their computers to remove the SQLvdb Filter Service.

Other Issues

- After registration, SQL Safe Web Console will list all available instances in your repository. Users have to use the options to Bulk Edit credentials to change credentials for those instances they are not able to monitor.
- The SQL Safe Web Console is not currently sending e-mail notifications for Restore Operations.

- Agent deployment service account changes made in the desktop console are not replicating in the web console.

Known Issues for 8.2

IDERA Dashboard

- Instances removed from the web and desktop console are still displaying under Dashboard Managed Instances.

Policies

- SQL Server Agent service account authentication for the Network path provided as the Primary location in the Log Shipping Policy wizard fails with an error even though the Service account has full permissions to the shared path.
- Users may find the option for wildcards is not available when defining databases to backup in the respective policy wizard.

- In the web console Policies tab, options to start jobs and disable policy are not available.

TSM

- Low-level file selection is not working properly with TSM backup/restore.

VDB

- Users who plan to install Safe 8.0 on the same system as VDB should obtain the VDB 2.1 buddy drop which addresses compatibility issues between the two products. Please contact support for more information.
- After installing SQL Safe, existing virtual databases may not be accessible. IDERA recommends to first upgrade with the VDB 2.1 buddy drop, unmount virtual databases, install SQL Safe, and then recreate the respective VDBs. Contact IDERA Support for more information.

Other Issues

- After registration, SQL Safe Web Console will list all available instances in your repository. Users have to use the options to Bulk Edit credentials to change credentials for those instances they are not able to monitor.
- Users should take into account that time fields for the Policies, Operation History, and Databases tabs in the SQL Safe Web Console are currently expressed in the GMT time zone.
- When uninstalling SQL Safe, users may need to reboot their computers to remove the SQLvdb Filter Service.
- The SQL Safe Web Console is not currently sending e-mail notifications for Restore Operations.
- Agent deployment service account changes made in the desktop console are not replicating in the web console.

Known issues for 8.0

- To upgrade from build 8.0.0.423 to Hotfix build (8.0.0.503) users need to follow these steps:

    ○ Open the installer to prompt the upgrade.
    ○ Type the credentials for the newly created SQLsafe REST service.
    ○ When upgrading the instance of SQL Safe, the installer displays the value to be added to the location property.
    ○ Access the web application. When an "exception" message is displayed, select the option "Redirect me to Dashboard."
    ○ Go to the Administration tab of the IDERA Dashboard, select Manage Products, and edit the respective SQL Safe instance. In the Location field, add the value specified during installation.
    ○ Restart the IDERADashboardCoreService (Automatically the IDERADashboardWebAppService service is restarted.)

- After registration, SQL Safe Web Console will list all available instances in your repository. Users have to use the options to Bulk Edit credentials to change credentials for those instances they are not able to monitor.
- Users should take into account that time fields for the Policies, Operation History, and Databases tabs in the SQL Safe Web Console are currently expressed in the GMT time zone.
- The Progress bar of the Operation History tab in the SQL Safe Web Console does not update its progress during the operation execution.
- When uninstalling SQL Safe, users may need to reboot their computers to remove the SQLvdb Filter Service.
- The SQL Safe Web Console is not currently sending e-mail notifications for Restore Operations.
- When uninstalling SQL Safe, users should manually remove the product from their IDERA Dashboard before rebooting their system.
- Users who plan to install Safe 8.0 on the same system as VDB should obtain the VDB 2.1 buddy drop which addresses compatibility issues between the two products. Please contact IDERA Support for more information.
- After installing SQL Safe, existing virtual databases may not be accessible. IDERA recommends to first upgrade with the VDB 2.1 buddy drop, unmount virtual databases, install SQL Safe, and then recreate the respective VDBs. Contact IDERA support for more information.

Known issues for 7.4

- When a backup operation in SQL Safe is performed at the same time as the native SQL Server, the successful backup job on SQL Safe may not always show the correct timestamp in the file name of the repository
- When upgrading from an older version, the user may experience Log Shipping policies with an "out of date" message in the console. Clicking the "out of date" link will fix this issue.
- Instead of being assigned the default location set in Preferences, users may find that the location paths of stripped files are the same as those of the mirror paths when changing from single to stripped location type.
- Users may find that pressing the "Enter" key in the Backup, Restore, and Log Shipping wizards may lead them to consecutive pages instead of inserting new lines in fields as is done in the Backup Policy Wizard.

- When setting up a log shipping wizard with a cluster instance, users may find that the secondary database file location does not display the same path as the one configured in the respective wizard but it displays the location from the primary database.
- Users may get a Last operation status of "Backups did not start as scheduled" in policies that are configured to run full and differential backups at specific times and where backups are done with no compression and no encryption.
- When running Instant Restore, users may experience problems if they have the same drive mounted as a drive letter and as a folder and they are using both paths for the Instant Restore procedure: the backup file accessed via the drive letter and the data files accessed via the folder path.
- Users may experience timeouts with the Instant Restore processes over a SQL Server 2012 SP1 with cumulative updates.
- Users may find that when the InstantRestore process is running in a clustered SQL Server and a failover occurs during the Hydration process, the Management Console displays the InstantRestore and Hydration processes as halted. The operation will not complete until the cluster fails back to the original node where the operation was started.
- Users who select the SQL Safe Backup Agent to create policies on servers where the timezone has been changed may need to restart the SQL Safe Backup Agent service to update the timezone and ensure policies run on the correct schedules.

Previous known issues

SQL Safe Repository no longer supports SQL Server 2000

SQL Safe Repository no longer supports SQL Server 2000. Supported versions include:

- SQL Server 2008 R2
- SQL Server 2008 Standard and Enterprise Editions
- SQL Server 2005 Standard and Enterprise Editions SP1 or later

SQL Safe no longer supports Itanium

SQL Safe 7.0 and later does not support the Itanium processor architecture. For more information, see the software requirements.

Pentium II processors are not supported

You should not install SQL Safe on a computer running a Pentium II processor. For more information, see the hardware requirements.

User must select the SQL Server hosting the Repository when using the Maintenance wizard

Users of the SQL Safe Maintenance wizard to modify, repair, or remove this version of SQL Safe must click **Browse** to select the current SQL Server hosting the Repository in the SQL Safe Repository window of the wizard. The wizard does not let you continue until an entry appears in the **SQL Server hosting the Repository** field.

Backup file names that use the %timestamp% macro may change when upgrading to SQL Safe 6.5 or later

When some users upgrade to SQL Safe 6.5 or later, the backup file names using the `%timestamp%` macro may change. This issue affects users who have SQL Safe to groom their backup files at backup time, using either the `-delete` command line option or the **Remove files older than** an option in the Backup Policy wizard. Previous versions expand `%timestamp%` to the UTC time of the backup.

Beginning with SQL Safe 6.5, `%timestamp%` expands to the local time of the backup. As a result, SQL Safe may write new backups to files already created by an earlier version of SQL Safe immediately after upgrading. By default, SQL Safe appends to backup files and this issue does not occur as the new backup appends to the existing file. This situation resolves itself after the time difference between UTC and local time passes. For example, this issue is resolved after five hours in the Central Standard Time zone (US).

Note that if you specify to overwrite, SQL Safe overwrites the existing files instead of appending the new information. If you upgrade from a release earlier than SQL Safe 6.4, appends fail and display an error message.

The setup program removes the previous version when the upgrade fails

If the upgrade fails while you are upgrading from a previous version of SQL Safe, the setup program removes the previous version from the SQL Server computer on which you attempted the upgrade.

XSP installation fails on clustered SQL Server instances

When you use the Agent Only install to manually deploy the SQL Safe Backup Agent to a clustered SQL Server instance, the corresponding SQL Safe XSP installation will fail. After the Backup Agent install completes, you can manually install the SQL Safe XSP.

For more information, see the Using the SQL Safe XSP Technical Solution located in the Documentation folder (by default, `C:\Program Files\IDERA\SQL Safe\Documentation`).

Remote Backup Agent install fails when SQL Server is not installed

In order to install the SQL Safe Backup Agent remotely, the computer from which you install SQL Safe must have a version of SQL Server already installed. For more information, see the software requirements.

Table Restore wizard is no longer available in SQL Safe version 6.0 or later

To restore objects and data from your backup files, use the new IDERA SQL virtual database tool. For more information, see Recover objects using Virtual Database.

FIPS-compliant encryption no longer requires additional software when installing SQL Safe version 6.0 or later

In a FIPS-compliant environment, SQL Safe uses only FIPS-compliant algorithms to encrypt your backup files. These encryption methods do not require any additional software. For more information, see Ensure FIPS compliance.

Upgrade any Backup Agents that perform TSM backups

Due to the extensive TSM enhancements included in SQL Safe 6.4 and later, older Backup Agents are not compatible with 6.4. To ensure you can continue backing up your SQL Server data to TSM, upgrade any Backup Agent that is used to perform TSM backups in your environment.

64-bit users need additional steps to install reports

Users with 64-bit installations must follow different steps to install reports. For more information, see IDERA solution 3891, "Where do I find the SQL Safe reports," in the knowledge base on Support (www.IDERA.com/support).

SQL Safe 4.0 users who upgrade to SQL Safe 7.1 or newer cannot use existing backup policies as part of new restore policies

SQL Safe 4.0 users who upgrade to SQL Safe 7.1 or newer receive error messages if they attempt to create and then run a restore policy that includes a backup policy created on the earlier version of SQL Safe.

SQL Safe Management Service logging multiple grooming events per day

Some users may notice the SQL Safe Management Service logging multiple grooming events in the Windows Application log each day. SQL Safe should be logging only one such event per day.

Attempting to restore a database from the list of backups on the SQL Server details page fails

A failure results when you attempt to restore a database file by right-clicking a file backup in the Backup/Restore Operation Status list and selecting **Restore Database**. To avoid this issue when restoring a file backup, click **Restore > Database Files** from the menu and complete the available restore wizard. You can also access the wizard from the Servers tree by right-clicking the appropriate SQL Server instance and selecting **Restore Database(s) Files**.

InstantRestore performance is affected by whether the SE_MANAGE_VOLUME_NAME privilege is on your SQL Server

Enabling the SE_MANAGE_VOLUME_NAME privilege for your SQL Server account improves general SQL Server file I/O performance as well as SQL Safe InstantRestore. If this privilege is not enabled for the SQL Server Service, InstantRestore performance could be negatively impacted, just as with the SQL Server itself. The degree of impact varies depending on environmental conditions. For more information about SQL Server Instant File Initialization, see the Microsoft Knowledge Base article located at Database Instant File Initialization.

InstantRestore appears to stall when restoring databases that contain read-only file groups

SQL Safe 7.0 Beta hydration appears to stall at 99% complete when restoring databases that contain read-only file groups. SQL Server triggers InstantRestore hydration when it performs

read/write I/O on the database files. Because SQL Server does not perform read/write I/O on the read-only files, hydration does not begin. Eventually, hydration begins when the SQL Server performs read I/O on the files. You can delete the database if you experience this issue.

Adding a new drive requires you to restart the InstantRestore Service

When you add a new drive to a server, you must restart the SQL Safe Filter Service to make sure that the SQL Safe Filter driver is attached to the new drive. When the SQL Safe Filter Service starts, it attaches the SQL Safe Filter driver to all the fixed drives on the server. If you add a new drive after the service starts, the driver is not attached and any files created on this drive during InstantRestore do not function correctly. To avoid this issue, simply restart the SQL Safe Filter Service after adding any new drive.

Not all files are removed when you delete a database restored using InstantRestore

Some files may remain after you attempt to delete a database previously restored using the InstantRestore feature. In most cases, you can manually delete these mdf, ndf, ldf, and vbm files. If the files are locked, restart either the SQL Safe Filter Service or the SQL Server Instance and then delete the files manually.

Offline SQL Safe Web Help may display a blank page

Some users experience a blank page when pressing F1 and using the offline SQL Safe Help. If this issue occurs, access the online version of SQL Safe 7.1 Help at http://www.IDERA.com/help /SQL Safe/7-1/web/default.htm.

SQL Safe Backup Agent may stop unexpectedly

The SQL Safe Backup Agent may stop unexpectedly and SQL Safe displays an error similar to, ".NET Runtime version 2.0…-Fatal Execution Engine Error." Microsoft recommends that users make sure that their environments include the following patches:

- Windows 2003: MS11-044: Description of the security update for the .NET Framework 3.5 Service Pack 1 and .NET Framework 2.0 Service Pack 2 on Windows XP Service Pack 3 and on Windows Server 2003 Service Pack 2: June 14, 2011
- Windows 2008 R2/Windows 7: MS11-044: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and on Windows Server 2008 R2 Service Pack 1: June 14, 2011

Importing backup archive sets may result in an error

SQL Safe may experience an issue when you attempt to import backup archive sets into your Repository.

Logins data archived only on Full backups

SQL Safe archives Logins data only when you perform a Full backup. SQL Safe does not archive this data when you perform a Differential or Log backup. You can restore Logins data only when you use a single backup set. When you specify multiple backup sets such as Full, Differential, and Log, you cannot restore Logins data.

Policy views may be blank after upgrading to version 6.6

The new granular alert notifications available in version 6.6 provide more detailed feedback about policy compliance and status. Because policy jobs created with SQL Safe 6.4 or earlier do not support this feature, the Management Console policy views will not display compliance status related to previous backup or restore operations. Instead, the policy views will track the policy status from the time you upgraded. To see the status of previous backup and restore operations, use the backup/restore operation status pane on the instance and database status views.

No Restore Policy support for backup files stored on TSM Servers

The SQL Safe 6.6 Restore Policy does not support restoring a database from a backup file stored on a TSM Server.

Metadata for SQL virtual database is not generated

SQL Safe is unable to generate SQL virtual database metadata for backups that use the following options:

- SQL Server 2008 databases that use FILESTREAM to manage unstructured data
- Read-write file groups
- File backups

Errors occurring when saving changes may delete policies

If an error occurs while saving changes to an existing policy, the policy may be deleted.

InstantRestore appears to stall when restoring databases that contain read-only file groups

SQL Safe 7.0 Beta hydration appears to stall at 99% complete when restoring databases that contain read-only file groups. SQL Server triggers InstantRestore hydration when it performs read/write I/O on the database files. Because SQL Server does not perform read/write I/O on the read-only files, hydration does not begin. Eventually, hydration begins when the SQL Server performs read I/O on the files. You can delete the database if you experience this issue.

Adding a new drive requires you to restart the InstantRestore Service

When you add a new drive to a server, you must restart the SQL Safe Filter Service to make sure that the SQL Safe Filter driver is attached to the new drive. When the SQL Safe Filter Service starts, it attaches the SQL Safe Filter driver to all the fixed drives on the server. If you

add a new drive after the service starts, the driver is not attached and any files created on this drive during InstantRestore do not function correctly. To avoid this issue, simply restart the SQL Safe Filter Service after adding any new drive.

Not all files are removed when you delete a database restored using InstantRestore

Some files may remain after you attempt to delete a database previously restored using the InstantRestore feature. In most cases, you can manually delete these mdf, ndf, ldf, and vbm files. If the files are locked, restart either the SQL Safe Filter Service or the SQL Server Instance and then delete the files manually.

InstantRestore Hydration statistics are incorrect if the IR Server restarts during Hydration

During the Hydration phase of the InstantRestore feature, if the IR filter service is restarted, the statistics incorrectly show the hydration process reset to zero. This is not accurate as hydration correctly picks up where it left off in the process.

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