Idera SQLsafe®

Version 7.4

SQLsafe Release notes

Idera SQLsafe provides a high-performance backup and recovery solution for Microsoft SQL Server. SQLsafe saves money by reducing database backup time by up to 50% over native backups and reducing backup disk space requirements by up to 95%. SQLsafe also enables complete 'hands-free' automated backup of your entire SQL Server infrastructure and ensures compliance with your organization's backup and recovery policies. From implementations with tens of SQL servers to enterprises with hundreds of servers spread around the globe, SQL safe is the only SQL Server backup and recovery solution that scales to meet the challenge.

To get a quick glimpse into the newest features, fixed issues, and known issues in this release of SQLsafe, review the following sections of the Release Notes:

New features and fixed issues

SQLsafe provides the following new features and fixed issues.

7.4 New features

Support for SQL Server 2014

Idera SQLsafe 7.4 now supports SQL Server 2014

Support for SQL Server Express

Idera SQLsafe now supports SQL Server Express in all its editions and versions.

Availability to use the SQL Safe Backup Agent to schedule policies

Users can now choose between using the SQLsafe Backup Agent for scheduling backup, restore, and log shipping policies or the SQL Server Agent as another option for scheduling these policies. Previous versions only allowed to use the SQL Server Agent to schedule policy jobs but now the user can choose the SQLsafe Backup Agent as a scheduler for these jobs too.

Centralized license management in the Management Service

License Management has now been centralized in the SQLsafe the Management Service which is in charge of keeping track of those SQL Server instances that are licensed for backup operations. The user specifies which instances they want to license through the License Management view in the Management Console and the Management Service will contact the respective Backup Agents for licensing.

The new License Management view allows users to add multi-instance license keys with no expiration date. On this view users can see which instances are licensed and which ones are only registered but not licensed yet. Users can manage licenses on this view and select those instances that they need to be licensed.

New Upgrade Installer

Users can now access upgrade production installers from our Customer Support Portal. These installers are different from the trial installer, which now generates a trial license for unlimited instances with a 14-day expiration key on a fresh install.

Support on Always On Availability Groups

SQLsafe now supports SQL Server Availability Groups and allows you to perform backup and recovery strategies on your primary and secondary replicas.

7.4 Fixed issues

You no longer need to restart the InstantRestore service when adding a new drive to a server.

Previous features and fixed issues

This build includes many fixed issues, including the following updates.

7.2.1 New features

Improved backup performance

SQLsafe now offers faster backup times when backing up SQL Server instances in the following types of environments:

- When the instance is hosted on server computer that is experiencing heavy resource loads.
- When the instance is running on a virtual machine (VM)

7.2.1 Fixed issues

- SQLsafe now ensures backup jobs do not fail when the SQLsafe Backup Agent cannot read the registry on the target SQL Server instance.
- SQLsafe now provides more stability and better performance when using the Management Console.
- SQLsafe now displays the correct file locations for mirrored and striped backup sets in the following windows:
  - View Policy Settings
  - Summary tab of Backup Policy wizard
- SQLsafe now handles NULL values that may be returned from the operating system when an InstantRestore is in progress, allowing the operation to continue.

7.2 New features

New ability to specify mirror backup locations for Log Shipping policies

You can now store mirrored copies of transaction log backup files in multiple locations, and then select which location should be used as the backup source when the log is shipped. This setting can be configured for each secondary server in the Log Shipping policy.

7.2 Fixed issues

- The SQLsafe Management Console now displays the correct database name when you attempt to cancel an operation and the operation status grid has been sorted by a column other than Start Date.
- When a server is reinitialized for a Log Shipping Policy, the Management Console now correctly refreshes, and no longer returns the error “System.InvalidOperationException: Collection was modified; enumeration operation may not execute."
- SQLsafe now retries failed restore operations associated with Log Shipping policies.
- The SQLsafe Backup Agent now incurs minimal performance impacts when running backup operations on servers that have heavy loads.

7.1 New features

Enhanced Log Shipping Policy features

Log shipping policy enhancements provide a way to specify an alternate network path from where you want the secondary database to pull the file to restore. For additional information about the new log shipping policy features, see Configure Secondary Options window of the Log Shipping Policy wizard.

Enhanced Restore wizard features

Restore wizard enhancements provide an easier way to restore from a mirrored database when the primary database location is unavailable. For more information about the Restore wizard enhancements, see Backup Sets tab of the Restore Wizard.

Enhanced Cluster support

SQL safe now supports failovers for Instant Restore during hydration. For additional information about the using SQLsafe in a clustered environment, see Using SQLsafe on a Microsoft Windows cluster environment.

SQL Server 2012 experimental support

SQLsafe 7.1 is SQL Server 2012 RC0 compatible. This version of SQLsafe is not certified against newer builds of SQL Server and should not be used with these builds in a production environment. Idera provides experimental support while you use your installation in a testing environment to ensure the features you rely on most are working as or better than expected.

7.1 Fixed issues

- Users who have a case-sensitive SQL Server user name no longer finds SQLsafe failing to create a job. This issue was the result of SQLsafe adding the characters in an all lowercase format.
- SQLsafe now prompts for a user name and password if a user runs the SQLsafeCmd DELETE command when they do not have access to the remote file system.
- This release fixes an issue that caused some users attempting to upgrade to SQLsafe 7.0 to receive a message stating that a previous version already exists.
- An issue preventing the backup service from starting after some users upgraded to SQLsafe 7.0 is resolved.
- Restore policies no longer become out of sync with the database for users who have multiple data files.
- An issue occurring during an upgrade that prevented backups from starting is resolved. In the job history, this issue logged an error stating, "The process could not be created for step 1 of job *X* (reason: The system cannot find the file specified). The step failed."

- A data format issue that caused some users to see a number of their policies as "Not Loaded" is fixed. All policies should successfully appear after any SQLsafe version upgrade.
- SQLsafe now prompts the user to sync policies after changing SQL authentication details for a SQL Server.

7.0.2 Fixed issues

- SQLsafe applications and services no longer experience a long delay when starting if Windows cannot verify the Authenticode signature on the associated applications and services.
- SQLsafe Agent deployment no longer fails due to an issue that occurs when accessing the registry on the remote machine during installation.
- The SQLsafe Management Console now properly handles creating and re-initializing log shipping databases that include several data files.
- The SQLsafe Management Console now properly handles creating restore policies for databases that include several data files.

7.0.1 Fixed issues

- The SQLsafe Today page now accurately displays the status for each item on the policy list and includes the status for operations that occasionally did not appear because the UTC offset was set to hours instead of minutes.

7.0 New features

Access your database quickly during a restore

SQLsafe gives you the option to bring your database back online quickly when performing a restore. The InstantRestore feature lets you work on restoring a database while allowing users to perform read and write operations to the database during this process. InstantRestore is available only for restoring full databases and does not support a restore of individual files or file groups.

Automatically run a Full backup prior to a Diff/Log backup

SQLsafe simplifies the initial setup process by automatically detecting and performing a Full backup prior to a Differential or Transaction Log backup.

7.0 Fixed issues

- The **Retry reading backup files after network errors** check box on the Backup Sets tab of the SQLsafe Database Restore wizard is renamed **Enable network resiliency**. The functionality remains the same while the name of the field was changed to improve usability.
- The **Verify (checks integrity, no data restored)** option moved from the Recovery State tab to the Target tab in the SQLsafe Database Restore wizard.
- SQLsafe now properly displays the selection in the **Select backup sets manually** box when the user switches from one database to another using the Restore wizard. This issue affected users attempting to restore multiple databases.
- New rolling logs improve troubleshooting by avoiding issues that result when a single log file continues to store information and grows without a limit. This file can cause performance issues and be hard to search for clues to find the issue you are trying to resolve. This feature is recommended for use only when instructed by Idera support.
- SQLsafe Reporting no longer displays an error message when a user attempts to run the Last Backup report.
- Dependent SQLsafe operations in a series are now associated so that when one of the operations fails, all of the following operations are canceled.
- The Restore wizard now properly handles the LSN chain when there is an intermediate Full backup.
- Performance updates improve the speed of the SQLsafe installation.
- Enhancements to SQLsafe memory usage decrease the chance of memory leaks or fragmentation.
- Users can now backup a database using only one thread as specified in the Thread Count field on the SQLsafe Backup Policy wizard Options tab.
- SQLsafe alerting now properly handles log shipping restore schedule start times when set to a non-default value.
- SQLsafe network retry updates fixed an issue that resulted when the SQLAgent job hung during a backup and the network retry function is disabled.
- SQLsafe no longer causes an extreme load on the tempdb while backing up a database.
- SQLsafe now properly handles FQDN names when connecting to the Backup Service.
- SQLsafe no longer truncates text within the **Result Text** field.
- Users can now sort the list of databases in the SQLsafe Backup wizard by clicking the appropriate column name.
- SafeToSQL users who submit an encryption password that fails verification now receive the correct error message.
- The Backup Policy wizard no longer re-runs the file access check after a user edits the policy unless the change was made to the Location tab.
- SQLsafe now allows encryption passwords of more than 24 characters. This update allows users to implement pass phrases as a more effective method of security.
- Users no longer experience an issue causing the default SQL Server instance file path to change when re-running a failed or skipped backup.
- SQLsafe now features **Cancel** buttons in a number of areas available when the user runs a task. You can cancel a task when performing log shipping re-initialization, deleting a policy, enabling or disabling a policy, running a job, re-synching a policy, or updating a license.
- SQLsafe now prompts the user immediately after a user account credential check fails.
- Improved Command-line Interface (CLI) documentation regarding SQLsafe and TSM server is located in the SQLsafe Help topic, Back up to the TSM Server.
- Accessing sample Command-line Interface (CLI) and Extended Stored Procedure (XSP) script sample access is now documented in the Product components and architecture
- Users who submit a script that contains unnecessary backslash characters in the file path no longer receive an error message stating, "Value cannot be null." SQLsafe now omits the unnecessary backslash characters and continues the operation.

- Users can now create and run log shipping or restore policies on a database that contains multiple files on different drives.
- The SQLsafe Management Console now contains the proper certificate so the user no longer receives a request for credentials each time they launch the Console. This issue affected Windows 2008 users replying on user account control functionality.
- The default **Connection Settings** detail on the SQLsafe Backup wizard Locations tab no longer retains any changes made during previous use.
- Users can now quickly find an instance in the SQLsafe Database Restore wizard Databases tab by typing the name directly into the instance field and selecting the appropriate instance when it appears.
- Users can now successfully change the IP address on the server hosting the SQLsafe Management Service without causing IP address resolution issues with the Backup Agent.
- Users attempting to restore an older, inactive backup file stored to a TSM server no longer receive an error message.
- SQLsafe XSP now correctly handles wide-character Unicode file names.
- Updated file access permissions fixed a performance issue caused when SQLsafe ran the Backup Policy File Access Check on every database within a SQL Server instance.
- SQLsafe performance is improved when a user attempts to create or run a policy, or load the policy status pages.
- Users with large SQLsafe repositories no longer encounter a timeout when accessing the Backup Sets page in the Management Console during a restore.
- If a backup policy specifies both a FULL as well as DIFF or LOG backups to be performed, the FULL backup is automatically run for new databases that have no previously-performed FULL backup existing at the time the FULL, DILL, or LOG backup is scheduled, whichever occurs first.
- The SQLsafe Management Console no longer prevents users from deleting some policies. These policies failed when loading from the Repository before the user attempted to delete the policy.
- PDF files of the SQLsafe Help and SQLsafe Release Notes now include hot links to access related information within the document.

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 (www.idera.com/support).

Known issues for 7.4

- When a backup operation in SQLsafe is performed at the same time as the native SQL Server, the successful backup job on SQLsafe 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 location paths of stripped files are the same as that 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 the consecutive pages instead of inserting new lines in fields as it is done in the Backup Policy Wizard.
- When setting up a log shipping wizard with a cluster instance, users may find that 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 is failed back to the original node where the operation was started.
- Users that select the SQLsafe Backup Agent to create policies on servers where the timezone has been changed may need to restart the SQLsafe Backup Agent service to update the timezone and ensure policies run on the correct schedules.

Previous known issues

SQLsafe Repository no longer supports SQL Server 2000

SQLsafe 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

SQLsafe no longer supports Itanium

SQLsafe 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 SQLsafe 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 SQLsafe Maintenance wizard to modify, repair, or remove this version of SQLsafe must click **Browse** to select the current SQL Server hosting the Repository in the SQLsafe 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 SQLsafe 6.5 or later

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

Beginning with SQLsafe 6.5, `%timestamp%` expands to the local time of the backup. As a result, SQLsafe may write new backups to files already created by an earlier version of SQLsafe immediately after upgrading. By default, SQLsafe 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, SQLsafe overwrites the existing files instead of appending the new information. If you upgrade from a release earlier than SQLsafe 6.4, appends fail and display an error message.

Setup program removes previous version when upgrade fails

If the upgrade fails while you are upgrading from a previous version of SQLsafe, 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 SQLsafe Backup Agent to a clustered SQL Server instance, the corresponding

SQLsafe XSP installation will fail. After the Backup Agent install completes, you can manually install the SQLsafe XSP.

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

Remote Backup Agent install fails when SQL Server is not installed

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

Table Restore wizard is no longer available in SQLsafe 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 SQL virtual database.

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

In a FIPS-compliant environment, SQLsafe 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 SQLsafe 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 SQLsafe reports," in the knowledge base on Support (www.idera.com/support).

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

SQLsafe 4.0 users who upgrade to SQLsafe 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 SQLsafe.

SQLsafe Management Service logging multiple grooming events per day

Some users may notice the SQLsafe Management Service logging multiple grooming events in the Windows Application log each day. SQLsafe 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 select **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 SQLsafe InstantRestore. If this privilege is not enabled for the SQL Server Service, InstantRestore performance could be negatively impacted, just as with 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

SQLsafe 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 SQL Server performs read I/O on the files. You can deleted 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 SQLsafe Filter Service to make sure that the SQLsafe Filter driver is attached to the new drive. When the SQLsafe Filter Service starts, it attaches the SQLsafe 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 SQLsafe 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 SQLsafe Filter Service or the SQL Server Instance and then delete the files manually.

Offline SQLsafe Web Help may display a blank page

Some users experience a blank page when pressing F1 and using the offline SQLsafe Help. If this issue occurs, access the online version

of SQLsafe 7.1 Help at http://www.idera.com/help/sqlsafe/7-1/web/default.htm.

SQLsafe Backup Agent may stop unexpectedly

The SQLsafe Backup Agent may stop unexpectedly and SQLsafe displays an error similar to, ".NET Runttime 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

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

Logins data archived only on Full backups

SQLsafe archives Logins data only when you perform a Full backup. SQLsafe 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 SQLsafe 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 SQLsafe 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

SQLsafe 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

SQLsafe 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 SQL Server performs read I/O on the files. You can deleted 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 SQLsafe Filter Service to make sure that the SQLsafe Filter driver is attached to the new drive. When the SQLsafe Filter Service starts, it attaches the SQLsafe 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 SQLsafe 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 SQLsafe 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.

Recommended Idera Solutions

Idera strives to ensure our products provide quality solutions for your database needs. The following Idera Solutions have been recently added to the knowledge base at our Support portal.

Number	Title
203	SQLsafe backup fails with the error message "Could not initialize Virtual Device Set" if the Backup Agent's service account is not a member of the `sys_admin` server role.
727	The SQLsafe console doesn't show status for backup and restore operations.
1109	SQLsafe back/restore operation or agent deployment returns error "The CPU type and CPU family of <server> could not be determined."
1384	How to manually install the SQLsafe extended stored procedures.
1394	How to install the SQLsafe Backup Agent on a clustered SQL Server.

Welcome to SQLsafe

SQLsafe saves money by reducing database backup time by up to 50% over native backups, reducing backup disk space requirements by up to 95%, and providing automated, 'hands-free,' multi-server backup management and monitoring.

Need help using SQLsafe? See the following sections:

- Create a backup policy
- Create a log shipping policy
- Restore databases

SQLsafe is a high-performance backup and recovery solution for your SQL Servers. Learn more > >

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal

What is SQLsafe?

Idera SQLsafe (SQLsafe) provides a high-performance backup and recovery solution for Microsoft SQL Server. SQLsafe saves money by reducing database backup times by up to 50% over native backups and reducing backup disk space requirements by up to 95%. SQLsafe also enables complete "hands-free" automated backups of your entire SQL Server infrastructure and ensures compliance with your organization's backup and recovery policies. From implementations with tens of SQL Servers to enterprises with hundreds of instances spread around the globe, SQLsafe is the only SQL Server backup and recovery solution that scales to meet the challenge.

SQLsafe is a high-performance backup and recovery solution for your SQL Servers. Learn more > >

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal

How does SQLsafe help me?

In many organizations today, SQL Server databases are the repositories for large volumes of business-critical data. As database size grows, the time required to back up your data using native tools can easily exceed your maintenance windows, plus a huge amount of storage space is needed for the files. Restore operations also become time-consuming. DBAs need a powerful backup and recovery solution that greatly reduces backup and recovery time, minimizes storage requirements, and provides enterprise management capabilities to conduct backups across a large numbers of servers simultaneously. SQLsafe has been specifically designed to meet these requirements, resulting in increased application and business availability for your critical SQL Server infrastructure.

As a state-of-the-art backup and recovery solution, SQLsafe provides:

- Maximum backup file compression
- Minimum backup times
- Reduced failures due to network glitches
- Accelerated mean time to restore
- Ensured compliance with corporate backup policies

SQLsafe is a high-performance backup and recovery solution for your SQL Servers. Learn more > >

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal

Find Answers

This documentation set includes a comprehensive online Help system as well as additional resources that support you as you install and use the product. You can also search Idera Solutions, available at the Idera Customer Service Portal (www.idera.com/support/faq).

Document conventions

Idera documentation uses consistent conventions to help you identify items throughout the printed online library.

Convention	Specifying
Bold	Window items
Italics	Book and CD titles Variable names New terms
Fixed Font	File and directory names Commands and code examples Text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value 1 | value 2	Exclusively command parameters where only one of the options can be specified

How to use the Help

The Idera wiki includes a comprehensive online Help system as well as additional resources that support you as you install and use Idera products. You can also search multiple Idera support solutions, available at www.idera.com/support/faq.

Additionally, Idera helps you by providing:

- 24/7 technical support for critical issues.
- Availability to report cases and access a web-based customer portal for update status.
- Access to our Knowledge Center where you can find FAQs, How To's, Best Practices, and Webcasts.

This wiki includes the following Web browser minimum requirements:

- Internet Explorer 8.0
- Mozilla Firefox 4
- Google Chrome 6

You can access the Idera SQLsafe Help system through the **Help** icon on the top right section of your window or by pressing F1 on the section where you need more information.

You can print a help topic from the wiki using the Print function in your browser.

Definition of terms

The following terms are used in the product and throughout the documentation.

Application Feature

SQLsafe performs tasks and displays information depending on the Application Feature you have selected. You can change the application feature by clicking a button in the navigation pane on the Management Console. SQLsafe Today, an additional feature, can be reached by clicking the globe icon on the menu bar, or through the View menu.

Backup Agent

The Backup Agent is a service that runs on each of the SQL Server instances hosting databases you want to backup and restore. Before you can deploy a Backup Agent to a SQL Server instance, you must register the SQL Server instance with SQLsafe.

Operation

An Operation is a work item that can be scheduled to be performed by the Backup Agent. Backups and restores are executed as operations.

Policy

A policy consists of a list of databases, a set of operations to be performed on those databases, and a set of schedules according to which the operations will be performed. Policies allow you to define a maintenance plan across multiple SQL Server instances, which can reside on one or more physical servers. You can then use the Management Console to monitor the status of policies and their associated database backup operations.

Server Groups

Server Groups are collections of similarly tasked SQL Server instances, whose performance and policy status is more easily monitored together. You are not required to place SQL Server instances into groups but, in an enterprise with hundreds of servers, compliance review can be greatly simplified.

About Idera

Idera is a leading provider of application and server management solutions. We have a wide variety of performance management products for Microsoft SQL Server, and award-winning server backup solutions for both managed service providers and enterprise customers. Idera products install in minutes and start solving server problems immediately, giving administrators more time, reduced overhead and expenses, and increased server performance and reliability. We are a Microsoft Gold Certified partner, headquartered in Houston, Texas, with offices in Asia Pacific, Australia, New Zealand, Europe, Africa, and Latin America. So we're everywhere your IT needs are.

SQLsafe is a high-performance backup and recovery solution for your SQL Servers. Learn more > >

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal

Contact Idera

Please contact Idera with your questions and comments. We look forward to hearing from you. For support around the world, please contact us or your local partner.

For a complete list of our partners, please visit our Idera website.

Sales	713.523.4433 1.877.GO.IDERA (464.3372) (only in the United States and Canada)
Sales Email	sales@idera.com
Support	713.533.5144 1.877.GO.IDERA (464.3372) (only in the United States and Canada) www.idera.com/support
Website	www.idera.com/

Idera products

Our tools are engineered to scale - from managing a single server to enterprise deployments with thousands of servers. Idera products combine ease of use with a design that installs in minutes, configure in hours, and deploy worldwide in days. To learn more about Idera products, visit our products page.

SQLsafe is a high-performance backup and recovery solution for your SQL Servers. Learn more > >

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal

Legal notice

Idera, Inc. (“Idera”) makes information and products available on this web site, subject to the following terms and conditions. By accessing this web site, you agree to these terms and conditions. Idera reserves the right to change these terms and conditions, and the products, services, prices, and programs mentioned in this web site at any time, at its sole discretion, without notice. Idera reserves the right to seek all remedies available by law and in equity for any violation of these terms and conditions. THIS WEB SITE COULD INCLUDE TECHNICAL OR OTHER INACCURACIES. CHANGES ARE PERIODICALLY MADE TO THE INFORMATION HEREIN. HOWEVER, IDERA MAKES NO COMMITMENT TO UPDATE MATERIALS ON THIS WEB SITE.

Trademark

IntelliCompress, PowerShellPlus, SharePoint enterprise manager, SharePoint security manager, SharePoint diagnostic manager, SharePoint backup, SharePoint performance monitor, SQL Elements, SQL check, SQL change manager, SQL comparison toolset, SQL compliance manager, SQLcompliance, SQLcm, SQL defrag manager, SQL diagnostic manager, SQLdm, SQL mobile manager, SQLpermissions, SQLsafe, SQLsafe Freeware Edition, SQLsafe Lite, SQL schema manager, SQLsecure, SQLsmarts, SQLstats, SQLtool, SQL toolbox, SQL virtual database, SQLvdb, virtual database, Idera, BBS Technologies and the Idera logo are trademarks or registered trademarks of Idera, Inc., or its subsidiaries in the United States and other jurisdictions. All other company and product names may be trademarks or registered trademarks of their respective companies. Elements of this web site are protected by trade dress or other laws and may not be imitated or reproduced in whole or in part.

Copyright

The information on this web site is protected by copyright. Except as specifically permitted, no portion of this web site may be distributed or reproduced by any means, or in any form, without Idera’s prior written consent.

Use of the Software

The software and accompanying documentation available to download from this web site are the copyrighted work of Idera. Use of the software is governed by the terms of the License Agreement, which accompanies such software. If no license accompanies the download, the terms of the license, which accompanied the original product being updated, will govern. You will not be able to use, download, or install any software unless you agree to the terms of such License Agreement.

Use of web site information

Except as otherwise indicated on this web site, you may view, print, copy, and distribute documents on this web site subject to the following terms and conditions:

1. The document may be used solely for informational, personal, non-commercial purposes;
2. Any copy of the document or portion thereof must include all copyright and proprietary notices in the same form and manner as on the original;
3. The document may not be modified in any way; and
4. Idera reserves the right to revoke such authorization at any time, and any such use shall be discontinued immediately upon notice from Idera.

Documents specified above do not include logos, graphics, sounds or images on this web site or layout or design of this web site, which may be reproduced or distributed only when expressly permitted by Idera.

Warranties and Disclaimers; Liability Limitations

EXCEPT AS EXPRESSLY PROVIDED OTHERWISE IN AN AGREEMENT BETWEEN YOU AND IDERA, ALL INFORMATION AND SOFTWARE ON THIS WEB SITE ARE PROVIDED "AS IS" WITHOUT WARRANTY OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

IDERA ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THE INFORMATION OR SOFTWARE OR OTHER DOCUMENTS WHICH ARE REFERENCED BY OR LINKED TO THIS WEB SITE.

IN NO EVENT SHALL IDERA BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION) WHETHER OR NOT IDERA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Submissions

With the exception of credit card numbers for the purchase of products and services, Idera does not want to receive confidential or proprietary information through its web site.

Any information sent to Idera, with the exception of credit card numbers, will be deemed NOT CONFIDENTIAL. You grant Idera an unrestricted, irrevocable license to display, use, modify, perform, reproduce, transmit, and distribute any information you send Idera, for any and all commercial and non-commercial purposes.

You also agree that Idera is free to use any ideas, concepts, or techniques that you send Idera for any purpose, including, but not limited to,

developing, manufacturing, and marketing products that incorporate such ideas, concepts, or techniques.

Idera may, but is not obligated to, review or monitor areas on its web site where users may transmit or post communications, including bulletin boards, chat rooms, and user forums. Idera is not responsible for the accuracy of any information, data, opinions, advice, or statements transmitted or posted on bulletin boards, chat rooms, and user forums.

You are prohibited from posting or transmitting to or from this web site any libelous, obscene, defamatory, pornographic, or other materials that would violate any laws. However, if such communications do occur, Idera will have no liability related to the content of any such communications.

Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

Governing Law and Jurisdiction

You agree that all matters relating to your access to, or use of, this web site shall be governed by the laws of the state of Texas. You agree and hereby submit to the exclusive personal jurisdiction and venue of the state courts of Texas located in Harris County, Texas, and the United States District Court for the Southern District of Texas, with respect to such matters.

Idera makes no representation that information on this web site are appropriate or available for use in all countries, and prohibits accessing materials from territories where contents are illegal. Those who access this site do so on their own initiative and are responsible for compliance with all applicable laws.

Export Control Laws

Certain Idera products, including software, documentation, services, and related technical data, available on the Idera and other web sites are subject to export controls administered by the United States (including, but not limited to, the U.S. Department of Commerce Export Administration Regulations (“EAR”)) and other countries including, controls for re-export under European Union, the Singapore Strategic Goods Control Act, and the import regulations of other countries. Diversion contrary to U.S. or other applicable law of any Idera product or service is prohibited. Export, re-export or import of products and services may require action on your behalf prior to purchase and it is your responsibility to comply with all applicable international, national, state, regional and local laws, and regulations, including any import and use restrictions. Idera products and services are currently prohibited for export or re-export to Cuba, Iran, North Korea, Sudan, Syria, or to any country then subject to U.S. trade sanctions. Idera products and services are prohibited for export or re-export to any person or entity named on the U.S. Department of Commerce Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Idera products and services are prohibited from use with chemical or biological weapons, sensitive nuclear end-users, or missiles, drones or space launch vehicles capable of delivering such weapons. By downloading or using any product from this web site, or purchasing any service, you are acknowledging that you have read and understood this notice and agree to comply with all applicable export control laws. You are also representing that you are not under the control of, located in, or a resident or national of any prohibited country, and are not a prohibited person or entity. This notice is not intended to be a comprehensive summary of the export laws that govern the products and services. It is your responsibility to consult with a legal adviser to ensure compliance with applicable laws.

United States Government Rights

All Idera products and publications are commercial in nature. The software, publications, and software documentation available on this web site are "Commercial Items", as that term is defined in 48 C.F.R.§2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R.?12.212 and 48 C.F.R. 227.7202, as applicable. Pursuant to 48 C.F.R. §12.212, 48 C.F.R.§252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-19, and other relevant sections of the Code of Federal Regulations, as applicable, Idera's publications, commercial computer software, and commercial computer software documentation are distributed and licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in the license agreements that accompany the products and software documentation, and the terms and conditions herein.

Get Started

Use the following checklist to get started using SQLsafe.

☑	**Follow these steps ...**
☐	Register the SQL Server instances you want to back up and restore.
☐	Deploy Backup Agents to your registered instances.
☐	***If you want to receive alert notifications through e-mail***, configure the e-mail settings.
☐	***If you want the option to use the InstantRestore feature to restore a database***, enable the InstantRestore service.
☐	Determine what your backup and recovery strategy will be.
☐	Determine whether you will perform manual backups of create policies to automate your backups.
☐	Determine which types of compression and encryption are best for your environment.
☐	Determine whether you will use log shipping policies as part of your recovery strategy.
☐	Ensure that you are able to restore the database. You can perform a full backup or you can test your configuration by running a verify-only backup. To perform a verify-only backup, run the Restore Wizard and select the **Verify only** option on the Recovery tab.

SQLsafe is a high-performance backup and recovery solution for your SQL Servers. Learn more > >

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal

Upgrade to this release

Upgrading SQLsafe allows you to take advantage of the new features available in this version.

The backup file names using the `%timestamp%` macro may change and cause issues with your backup files. This issue only affects some users. For more information, see the known issues section of the Release Notes.

SQLsafe includes a file system filter driver to support the InstantRestore feature. The driver, named SQLsafeFilterDriver, allows SQL Server to access database data while SQLsafe is executing InstantRestore. The driver is only used during this action and is no longer in use once the database is completely hydrated.

Upgrade checklist

To successfully upgrade your Microsoft SQL Server environment to this build, complete the procedures outlined in the following table. These procedures support upgrades from SQLsafe versions 5.0 or later.

☑	Follow these steps
☐	Ensure the computers on which you want to upgrade SQLsafe meet or exceed the product requirements for this version of SQLsafe. For example, ensure .NET Framework 2.0 SP1 or later is running on the target computer.
☐	Ensure your Windows logon account has local administrator permissions on the computers you intend to upgrade.
☐	Review the Product components and architecture.
☐	Review the Supported installation scenarios.
☐	Close all open applications on the computers you intend to upgrade.
☐	Upgrade your SQLsafe installation.

Available upgrade paths

Because each component can be installed separately on different computers, the type of upgrade you will need to perform will depend on your environment. The following table describes the conditions under which you would follow a typical or staged upgrade path.

Environment Description	Recommended Path	Why
Simple environment, where the Management Console, the Repository, and the Management Service all reside on the same computer	Typical	A simple environment can be upgraded through the setup program.
Distributed environment, where each SQLsafe component resides on a different computer.	Staged	A distributed environment requires a staged upgrade to maintain backup continuity while each component is upgraded.
Multiple Management Consoles deployed to different computers.	Staged	A SQLsafe installation with multiple Management Consoles requires a staged upgrade in order to maintain connection with all Backup Agents while each component is upgraded.
Backup Agents from different SQLsafe versions.	Staged	An environment that manages Backup Agents from different SQLsafe versions requires a staged upgrade in order to maintain connection with all Backup Agents while each component is upgraded.
Change control policies that require multi-phased upgrades.	Staged	An environment with stringent change control policies requires a multi-phased upgrade in order to test each updated component thoroughly before moving on to the next step.

New encryption options in 6.0 and later

SQLsafe 6.0 and later provides new, more secure encryption algorithms. To use these new algorithms, upgrade your Backup Agents to the latest version.

Previous Encryption Options	SQLsafe 6.x Encryption Options
AES	AES-128
DES	AES-256
Triple-DES	
RC2	

These new encryption options replace the options previously available in SQLsafe 5.0 or earlier. You can select the new encryption options when you manually perform a backup, or create and edit existing Backup Policies.

If you had set encryption options when creating your Backup Policies , the encryption method specified in the corresponding SQL Server job will be automatically updated to AES-128 when you upgrade the associated Backup Agent. You can later change this setting by editing the policy.

SQLsafe 6.0 and later does support previously encrypted archives; you can continue to restore any encrypted backup file created with a previous version of SQLsafe.

Perform a staged upgrade

Use a staged process to upgrade your SQLsafe installation if you have a distributed environment, have deployed multiple Backup Agents that cannot be upgraded during the same time period, or you need to adhere to change control policies.

What is a distributed environment?

A distributed environment consists of the SQLsafe management components running on different physical computers. The management components are:

- Repository database
- Management Service
- Management Console

The time scale over which you choose to perform a staged upgrade will depend on the size of your SQL Server environment and your corporate change control policies. For example, you may choose to perform one of the following steps per day or per week; however, the order in which you perform them should remain the same.

How to perform a staged upgrade

Use this process if your environment meets the following conditions:

- The SQLsafe components are installed on different computers
- All Backup Agents are version 5.0 or earlier

To perform a staged upgrade:

1. Upgrade the Management Service and Repository database to the newest version of SQLsafe by using the setup program to perform a Custom install.
2. Upgrade your Management Console installations to the newest version of SQLsafe. Although you can upgrade the Management Console installations over time, keep in mind that 5.0 and earlier Management Consoles should not be used with 7.x Backup Agents.
3. ***If you use policies to automate your backup and restore operations***, start the SQLsafe Management Console to synchronize the jobs associated with each policy. This synchronization should happen automatically.
4. Upgrade deployed Backup Agents according to your change control policies. As you upgrade your Backup Agents, ensure you use a 7.x Management Console to manage the corresponding instances and Backup Policies.

Perform a typical upgrade

Use the Typical install to upgrade your SQLsafe installation if you have centralized SQLsafe deployment or are upgrading from a trial installation. This process assumes you can upgrade all deployed Backup Agents during the same time period.

What is a typical environment?

In a typical environment, the SQLsafe management components will be installed on the same physical computer. These components include:

- Repository database
- Management Service
- Management Console

Existing backups executed through maintenance plans, SQL Server jobs, or the CLI will continue to run successfully using older Backup Agents. Once you have completed the installation of the management components, you can upgrade your Backup Agents.

How to perform a typical upgrade

A typical upgrade can be easily completed during off-hours.

To perform a typical upgrade:

1. Perform a Typical install to upgrade the management components to the newest version of SQLsafe. When prompted, verify the name of SQLsafe Repository database.
2. ***If you use policies to automate your backup and restore operations***, start the SQLsafe Management Console to synchronize the jobs associated with each policy. This synchronization should happen automatically.
3. Upgrade all previously deployed Backup Agents.

Upgrade deployed Backup Agents

Consider upgrading previously deployed Backup Agents off-hours during a single time period or in stages according to your corporate change policies. You can remotely upgrade previously deployed agents through the SQLsafe Agents view in the Management Console.

The Backup Agent is automatically installed on the local computer when you install or upgrade any of the other SQLsafe components.

Backup Agent compatibility with Tivoli Storage Manager (TSM)

SQLsafe 6.4 and later includes extensive enhancements to how SQLsafe handles backing up to and restoring from TSM Server. ***If you store backup files on a TSM Client node***, ensure you upgrade the Backup Agents that perform backups and restores using those files.

Backup Agent compatibility with Backup Policies

SQLsafe 7.x requires version 7.x Backup Agents to successfully run new Backup Policies and edit existing Backup Policies (created with SQLsafe 5.0 or earlier).

If you want to continue using 5.0 or earlier Backup Agents for existing Backup Policies, install SQLsafe 7.x along side your current SQLsafe deployment. Use SQLsafe 7.x to create and manage new Backup Policies, and use SQLsafe 5.0 to maintain existing policies.

Backup Agent compatibility with Log Shipping Policies

Because SQLsafe 5.0 Backup Agents cannot restore backups written by 7.x Backup Agents, environments that include Log Shipping policies require a specific upgrade path. First upgrade the Backup Agents running on the SQL Server computers hosting the secondary databases, and then upgrade the Backup Agents running on the SQL Server computers hosting the primary databases. Otherwise, when SQLsafe attempts to ship a new transaction log backup, the restore operation will fail and the Log Shipping policy status will show that the associated jobs are out of date until all the Backup Agents have been upgraded.

How to upgrade a Backup Agent using the Management Console

This procedure guides you through the process of upgrading previously deployed Backup Agents using the Management Console. You can also manually upgrade a Backup Agent using the setup program.

To upgrade deployed Backup Agents:

1. Verify that your environment includes the newest version of the SQLsafe Management Console.
2. Start the new SQLsafe Management Console, and navigate to the **SQLsafe Agents** view. To access the SQLsafe Agents view, click the **SQLsafe Agents** tab at the bottom of the **Servers** tree.
3. For each Backup Agent you want to upgrade, select the SQL Server computer that is hosting the agent, and then click **Upgrade SQLsafe Backup Agent** on the right-click context menu. Upgrading the Backup Agent automatically upgrades the SQLsafe XSP deployed to each registered SQL Server instance running on the selected computer.

Upgrade the Lite or Freeware Edition

The Management Console detects when a registered SQL Server instance is running SQLsafe Lite or SQLsafe Freeware Edition. You can upgrade the Backup Agent to the current version of SQLsafe enterprise edition using one of the following methods:

- Deploy the current version of the agent. For more information, see Install SQLsafe Backup Agent.
- Select the instance in the Servers tree, and then click **Enable trial license** on the Instance View. This upgrades the license to an enterprise edition trial license.
- Click **Upgrade** on the SQLsafe Agent Properties window. For more information, see Modify Backup Agent properties.

When you upgrade the Backup Agent, SQLsafe deploys the current version of the Backup Agent with a trial license enabled. The trial license allows you full access to the SQLsafe enterprise features for all SQL Server instances hosted on that computer. The trial license is a limited-time, limited-instance license that you will need to upgrade with a production license key.

Upgrade the SQLsafe Freeware Edition

SQLsafe Freeware Edition is no longer available. However, you can easily upgrade your SQLsafe Freeware Edition deployment to either SQLsafe or SQLsafe Lite.

Upgrade SQLsafe Freeware Edition to SQLsafe Lite

You can upgrade SQLsafe Freeware Edition to SQLsafe Lite 6.x by running the SQLsafe setup program on the target SQL Server computer and selecting **Agent Only Install**.

The first time you perform a backup using SQLsafe Lite, the tool will generate a trial license. To install and activate your production license, click **Idera > SQLsafe Lite > Activate License** on the **Start** menu.

Upgrade SQLsafe Freeware Edition to SQLsafe

To upgrade from SQLsafe Freeware Edition to SQLsafe 6.x, first perform a full installation of SQLsafe, and then Upgrade the Lite or Freeware Edition through the Management Console.

If you install SQLsafe on the same computer as your existing SQLsafe Freeware Edition , the corresponding Backup Agent will be automatically upgraded as part of this installation.

After installation, apply your new SQLsafe 6.x production license by clicking **Manage License** on the **Tools** menu in the Management Console.

Deploy the SQLsafe XSP

There are two ways to deploy the SQLsafe XSP: remotely through the Management Console or locally through the command-line interface (CLI).

If you are upgrading a Backup Agent, you will be prompted to perform an upgrade of the XSP for all instances on the target SQL Server.

If you do not want to deploy the XSP to all instances on a given SQL Server, you can deploy the XSP to a single instance through the Management Console or the CLI.

XSP deployment through the Management Console

You can upgrade the XSP when you deploy or upgrade the Backup Agent from the Management Console. At that time, you will be prompted for permission to install or perform an upgrade of the XSP for all instances on the target SQL Server. To install or upgrade the XSP, click **Yes**, and complete the authentication information as necessary. This action will install the new XSP on all instances on the SQL Server.

You can also deploy the XSP to a single instance.

To deploy the SQLsafe XSP to a single instance:

1. In the **Servers** tree, select the instance to which you want to deploy the XSP.
2. On the right-click context menu, click **Install SQLsafe Extended Stored Procedures**.
3. Click **OK**.

XSP deployment using the SQLsafe CLI

If you did not install the XSP during the Backup Agent upgrade, or you want to deploy the XSP to select instances on a given SQL Server, you can install the XSP manually.

To deploy the SQLsafe XSP with the standalone installer:

1. Log on with an administrator account to the SQL Server computer on which you want to install the SQLsafe XSP. Ensure your logon account also belongs to the System Administrators role on each SQL Server instance.
2. Ensure you have the most current version of SQLsafe.
3. Open the Command Prompt, and navigate to the directory where the SQLsafe CLI is installed. By default, the CLI is installed in `C:\Program Files\Idera\SQLsafe`.
4. Type `SQLsafeCmd InstallXsp –InstanceName` *`MyInstance`* `–Server` *`MyServerComputer`* , specifying the name of the instance and the SQL Server computer. For more information about available InstallXSP options, such as specifying authentication credentials, see the CLI Help. To view the CLI Help, type `SQLsafeCmd Help InstallXSP`.

Upgrade SQLsafe in non-trusted domains

SQLsafe 6.4 and later supports seamless integration and communications between trusted and non-trusted domains. ***If you want to take advantage of this feature***, use the following instructions to upgrade your SQLsafe 6.3 or earlier environment.

To upgrade SQLsafe 6.4 or later to the current release version, follow the standard Typical or Staged upgrade instructions.

How to upgrade a single Repository deployment

This deployment consists of:

- One SQLsafe Repository hosted in the trusted domain
- A Management Service in each non-trusted domain
- A single Management Service that manages SQL Server instances in your trusted domain
- Management Consoles in trusted and non-trusted domains
- Backup Agents in trusted and non-trusted domains

To upgrade this deployment:

1. Uninstall the Management Service from each non-trusted domain.
2. Ensure your Backup Service and Management Service accounts have the appropriate permissions.
3. Ensure the required ports are open in all trusted and non-trusted domains.
4. Decide how many SQLsafe Management Consoles you need to keep in each domain, and uninstall those consoles you no longer need. Maintaining a Management Console in a non-trusted domain is no longer required.
5. Run the setup program to upgrade:
    - The SQLsafe Repository and Management Service in the trusted domain
    - The Management Consoles in the trusted domain
    - The Management Consoles in the non-trusted domains. Note that this step is optional, depending on whether you decided to maintain these consoles.
6. ***If you use policies to automate your backup and restore operations***, start the SQLsafe Management Console to synchronize the jobs associated with each policy. This synchronization should happen automatically.
7. Upgrade all deployed Backup Agents in your trusted and non-trusted domains.

How to upgrade an island deployment

This deployment consists of:

- A complete SQLsafe installation in each non-trusted domain
- A single centralized installation that manages SQL Server instances in your trusted domain

To upgrade this deployment:

1. Decide how many SQLsafe Management Consoles you need to keep in each domain. Maintaining a Management Console in a non-trusted domain is no longer required.
2. Identify which domain you want to host your new centralized SQLsafe deployment.
3. Ensure your Backup Service and Management Service accounts have the appropriate permissions.
4. Ensure the required ports are open in all trusted and non-trusted domains.
5. Uninstall the SQLsafe management components from the domains you do not intend to use to host SQLsafe. Remember to preserve the Management Consoles you identified in Step 1.
6. Upgrade the SQLsafe management components that were previously deployed to the selected domain.
7. Run the setup program to upgrade all remaining Management Consoles.
8. ***If you use policies to automate your backup and restore operations***, start the SQLsafe Management Console to synchronize the jobs associated with each policy. This synchronization should happen automatically.
9. In each Management Console, verify that:
    - It can connect to the upgraded SQLsafe Repository
    - It is using the correct Management Service
10. Upgrade all deployed Backup Agents in your trusted and non-trusted domains.

Installation and deployment

You can install and deploy SQLsafe in any sized environment.

- Learn about the product components and architecture
- Review the hardware, software, permission, and port requirements
- Check the supported installation scenarios
- View trial installation instructions

Product components and architecture

SQLsafe provides a robust, easy-to-use SQL Server database backup and restore solution. Behind a simple user interface, SQLsafe offers an architecture that is both flexible and extremely powerful. SQLsafe fits your environment, no matter how simple or complex.

The SQLsafe architecture easily runs in your SQL Server environment with minimal configuration. All SQLsafe components run outside and separate from SQL Server processes. SQLsafe does not add to or modify any of your native SQL Server files or services. After you install these components, you can implement features such as Reports.

> ⚠ You must use the same Windows account for the Backup Agent and InstantRestore Service. During installation, you are asked to enter credentials for only one account and the other is created with the same information. If you manually change your account information, make sure you change it in the other service as well to avoid any issues.

Product components

Management Console

The Management Console is a centralized, intuitive user interface that allows you to easily and quickly back up and restore data on specific SQL Server instances.

The Management Console also provides a T-SQL generator, allowing you to create backup and restore T-SQL scripts. You can execute these scripts through scheduled SQL Server jobs or combine several scripts into a single SQL Server scheduled batch job.

Repository Database

The SQLsafe Repository (Repository) is a central database that tracks all SQLsafe backup and restore operations and the corresponding backup archive file paths for your enterprise.

Management Service

The Management Service receives events from the Backup Agent, and then relays the status of all current and completed operations to the SQLsafe Repository.

Backup Agent

The Backup Agent performs backup and restore operations. The agent is a service that runs on the target SQL Server computer.

InstantRestore Service

The InstantRestore Service is used by the Backup Agent to query and change any InstantRestore properties not managed by the Agent. For more information about InstantRestore properties, see InstantRestore.

Command-line Interface and Extended Stored Procedures

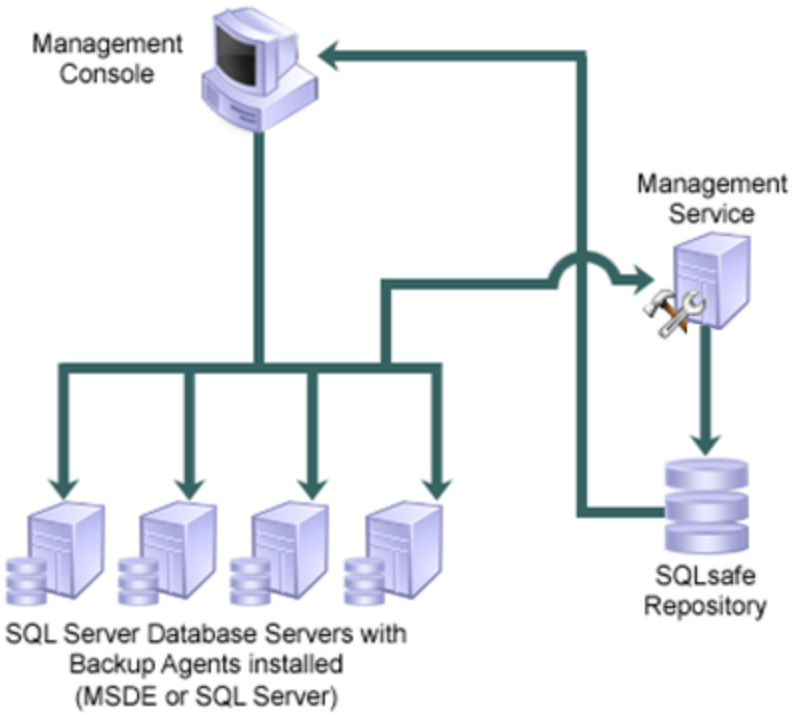
The SQLsafe command line interface (CLI) and extended stored procedures (XSPs) allow you to execute SQLsafe backup and restore procedures with batch files or through your preferred scripting language. You can also use the CLI or XSPs as an alternative to the Management Console.

For sample XSP scripts, see the Sample Scripts programs menu shortcut (**Start > All Programs > Idera > SQLsafe > XSP > Sample Scripts**). The following scripts are available:

- `xp_ss_backup`
- `xp_ss_browse`
- `xp_ss_expire`
- `xp_ss_extract`
- `xp_ss_restore`
- `xp_ss_restorefilelistonly`
- `xp_ss_restoreheaderonly`
- `xp_ss_restorelast`
- `xp_ss_verify`

Product architecture

The following diagram illustrates the components of the SQLsafe architecture.



SQLsafe is a high-performance backup and recovery solution for your SQL Servers. Learn more > >

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal

Hardware requirements

SQLsafe requires the following hardware.

Hardware Type	Requirement	Recommendation
CPU	1 GHz	2 GHz
Memory	512 MB	1 GB
Hard Drive Space	80 MB (installation files only)	1 GB (temporary disk space for backup and restore operations as they write data to and from files)
Monitor Resolution	1024 by 768 pixels	1024 by 768 pixels

Permission requirements

SQLsafe requires specific permissions and rights to successfully execute backup and restore operations. Generally, the rights of the Management Console user dictate the rights available to SQLsafe.

If you are deploying SQLsafe to a non-trusted domain, specify an account with sysadmin fixed role rights for the Management Service and Backup Agent Service accounts, and ensure that SQL Authentication is enabled on each SQL Server instance where a SQLsafe component has been installed.

Recommended permissions for trial installations

Type	Requirement
Windows Permissions	Your Windows logon account has local Administrator permissions.
SQL Server Privileges	Your Windows logon account is a member of the sysadmin fixed server role on the SQL Server instance.

Required permissions for production installations

Account	Action	Permissions Required
Windows user account	• Allows you to install the Backup Agent on local or remote SQL Server instances. • Allows you to install SQLsafe components. • Allows you to perform SQLsafe tasks, such as executing a backup or restore operation, using standard Windows authentication. • Allows you to create the SQLsafe Repository database. • Allows you to read and write backup files. • Allows you to access the SQLsafe Repository.	• Windows administrator permission on the Management Console computer and target database server. • Windows administrator permission on the target computer. • `db_owner` or `db_backupoperator` role on each user or system database on the registered SQL Server instance. • Create Database rights on the target SQL Server instance. • Windows account credentials with read and write permission on the volume of share you want to write or read backup files. • Read and write privileges on the SQLsafe Repository database, execute privileges for stored procedures.
SQL Server login	• Allows you to perform SQLsafe tasks, such as executing a backup or restore operation, using standard SQL authentication. • Allows you to create the SQLsafe Repository database.	• `db_owner` or `db_backupoperator` role in each user or system database on the registered SQL Server instance. • Create Database Rights on the target SQL Server instance.
Management Service account	Allows the SQLsafe Management Service to access the SQLsafe Repository database.	`db_owner` role or the following SQL permissions on the SQLsafe Repository database: • EXECUTE • INSERT • SELECT • UPDATE • DELETE
Backup Service account	Allows the Backup Agent to access the SQL Server instances in your environment.	`sysadmin` privileges on each SQL Server instance.
MSSQLSERVER service	Allows SQLsafe XSP to read and write backup files.	Read and write permission on the volume or share you want to write or read backup files.
TSM Server	Allows you to configure TSM Server and client nodes for communication.	Administrator privileges within TSM Server.

Port requirements

The SQLsafe services use specific ports to communicate to each other as well as other SQLsafe components. Before installing SQLsafe, ensure the following ports are available.

Service	Port for trusted domains	Port for non-trusted domains
Backup Service	5164	5165
Management Service	5162	5163

SQLsafe automatically detects whether its components have been installed in trusted or non-trusted domains.

If your environment requires SQLsafe to use a different port, you can specify a custom port by changing the associated registry key. For more information about how to assign different port numbers, see Idera Solution 204. To confirm which ports to use, or to verify whether a domain is trusted or not, contact your network administrator.

When you specify a custom port setting for communications in your trusted domain, SQLsafe automatically assigns the non-trusted port (CustomPort + 1). For example, if the custom port is 6000, the port used for communications in non-trusted domains will be 6001.

Software requirements

The SQLsafe components have the following general software requirements, as well as specific requirements outlined in the following sections. ***If a service pack is not specified*** , a service pack is not required for that version of the software.

SQLsafe supports the built-in clustering technology included with the following versions of Microsoft Windows operating systems:

- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2

General Software Requirements

- Microsoft Data Access Components (MDAC) 2.8 or later
- Microsoft .NET Framework version 2.0 or 3.5. ***If this software is not already installed on your computer*** , you must install it prior to the installation of SQLsafe. This software can be installed from the installation kit by clicking **Prerequisites** on the Install window of the setup program. For more information about the .NET Framework, see the .NET Framework Versions and Dependencies article on MSDN.
- The following Web browser minimum requirements for this Wiki:
  - Internet Explorer 8.0
  - Mozilla Firefox 4
  - Google Chrome 6

Management Console and Management Service

The Management Console and Management Service can run on both 32- and 64-bit computers. Each component requires one of the following operating systems.

- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows 2000 SP4 (Excludes InstantRestore feature support)
- Microsoft Windows XP Professional SP3 or later
- Microsoft Windows Vista SP2 or later
- Microsoft Windows 7
- Microsoft Windows 8

Backup Agent

The Backup Agent is supported to run on both 32- and 64-bit computers. The Backup Agent requires one of the following operating systems and one of the following Microsoft SQL Server versions.

- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows 2000 SP4 (Excludes InstantRestore feature support)
- Microsoft Windows XP Professional SP3 or later
- Microsoft Windows Vista SP2 or later
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft SQL Server 2000 SP4
- Microsoft SQL Server 2005 SP1 or later - All Editions (Express, Standard, Enterprise, etc.)
- Microsoft SQL Server 2008 - All Editions (Express, Standard, Enterprise, etc.)
- Microsoft SQL Server 2008 R2 - All Editions (Express, Standard, Enterprise, etc.)
- Microsoft SQL Server 2012 - All Editions (Express, Standard, Enterprise, etc.)
- Microsoft SQL Server 2014 - All Editions (Express, Standard, Enterprise, etc.)

SQLsafe Repository

The computer hosting the SQLsafe Repository requires one of the following operating systems and one of the following Microsoft SQL Server versions.

- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

- Microsoft Windows 2000 SP4 (Excludes InstantRestore feature support)
- Microsoft Windows XP Professional SP3 or later
- Microsoft Windows Vista SP2 or later
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft SQL Server 2005 SP1 or later - All Editions (Express, Standard, Enterprise, etc.)
- Microsoft SQL Server 2008 - All Editions (Express, Standard, Enterprise, etc.)
- Microsoft SQL Server 2008 R2 - All Editions (Express, Standard, Enterprise, etc.)
- Microsoft SQL Server 2012 All Editions (Express, Standard, Enterprise, etc.)
- Microsoft SQL Server 2014 All Editions (Express, Standard, Enterprise, etc.)

InstantRestore

For the InstantRestore feature take into account the following operating systems:

- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows XP Professional SP3 or later
- Microsoft Windows Vista SP2 or later
- Microsoft Windows 7

You cannot use the InstantRestore feature on any version of the Microsoft Windows 2000 operating system.

TSM requirements

SQLsafe supports the following versions of the TSM Client application:

- TSM Client 7.1.x.x
- TSM Client 6.4.x.x
- TSM Client 6.3.x.x
- TSM Client 6.2.x.x
- TSM Client 6.1.x.x
- TSM Client 5.6.x.x
- TSM Client 5.5.x.x
- TSM Client 5.4.x.x

By default, SQLsafe supports any version of the TSM Server to which the supported TSM Client versions can connect. For more information about TSM Server requirements, see your IBM TSM documentation.

Supported installation scenarios

You can install and deploy SQLsafe to meet your unique backup, recovery, and SQL Server environment needs.

Typical environment

The following figure illustrates a typical SQLsafe implementation scenario. This configuration includes the following installations:

- Management Console on your workstation
- Repository and Management Service on a SQL Server instance
- Backup Agents on each computer hosting databases you want to back up and recover

Clustered environment

You can install and configure SQLsafe to back up and recover virtual SQL Servers. A virtual SQL Server is a SQL Server running on a Microsoft failover cluster managed by Microsoft Cluster Services.

This configuration can be limited to deploying the Backup Agent to your virtual instances, or can include a full SQLsafe deployment.

A Backup Agent deployment to a virtual instance includes the following installations:

- Management Console on your workstation
- Repository and Management Service on a SQL Server instance (not located in the cluster)
- Backup Agents on each cluster node hosting the virtual SQL Server you want to manage

For more information, see Installing backup/restore components in a clustered environment.

A full SQLsafe deployment on a cluster includes the following installations:

- Management Service and Backup Agent on each node of the Windows cluster
- Repository on any virtual SQL Server instance
- Management Console on your workstation (can also be installed on the cluster nodes)

For more information, see Installing management components in a clustered environment andInstalling backup/restore components in a clustered environment.

Non-trusted environment

You can install and configure SQLsafe to backup and recover SQL Server databases running in non-trusted domains or workgroups.

This configuration includes the following installations:

- Management Console on your workstation in a trusted or non-trusted domain
- Repository and Management Service on a SQL Server instance in a trusted or non-trusted domain
- Backup Agents on each SQL Server instance you want to manage (server can belong to a trusted or non-trusted domain or workgroup).

When deploying SQLsafe to a non-trusted domain, specify an account with sysadmin fixed role rights for the Management Service and Backup Agent Service accounts, and ensure that SQL Authentication is enabled on each SQL Server instance where a SQLsafe component has been installed.

How to install SQLsafe

This procedure guides you through a typical install of SQLsafe. A typical install sets up all SQLsafe components on the same computer. Use this procedure for first-time installs and evaluation installs.

Before you begin the installation process, ensure you review:

- Product components and architecture
- Hardware, software, permission, and port requirements
- Supported installation scenarios

You can install each SQLsafe component in domains with or without trust relationships. For example, you can install the Management Service and Repository in a trusted domain and then install the Management Console and Backup Agents in a non-trusted domain.

Start the setup program

You can install SQLsafe on any computer that meets or exceeds the product requirements.

To start installing SQLsafe:

1. Log on with an administrator account to the computer on which you want to install SQLsafe.
2. Close all open applications.
3. Run `Setup.exe` in the root of the installation kit.
4. Click **All components** on the **Install** section of the Welcome window.
5. Click **Run** to proceed with the installation file.
6. On the Welcome wizard window of the setup program, click **Next**.
7. Review and accept the license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.

Choose where you want to install SQLsafe and who should use the product on this computer

You can use the default install location or specify a different location. For your first install, we recommend using the default location.

To choose a different location:

Click **Change** to navigate to the location you want to use, and then click **Next**.

To restrict access:

Choose whether you want any user or only the current user to access this application, and then click **Next**.

Choose which components you want to install

For your first install, we recommend using the **Typical** setup type. This type ensures you install and configure all required SQLsafe components, so you can immediately begin using SQLsafe in your environment.

Click **Typical**, and then click **Next**.

Choose which SQL Server instance you want to host the Repository database

You can use a SQL Server instance installed locally on this computer or on another computer. For your first install, we recommend using a local instance.

SQLsafe can connect to the selected SQL Server instance using the credentials of your current Windows logon account or a SQL Server login. For your first install, we recommend using your current logon account credentials.

To choose a different instance:

1. Click **Browse** to select the SQL Server instance you want to use. The Select SQL Server window lists all available instances in your current domain and other trusted domains.
2. Click **OK**.
3. Click **Next**.

To specify a SQL Server login:

1. Click **Use Microsoft SQL Server authentication**, and then click **Change**.
2. Specify the credentials of a login with `sysadmin` privileges on that instance, and then click **OK**.
3. Click **Next**.

Choose which Windows user account you want the Management Service to use

For your first install, we recommend using your Local System Account for the Management Service account. SQLsafe uses this service account to communicate between the Backup Agent, the Management Console, and the SQLsafe Repository.

To choose a different account:

1. Determine whether your environment uses Windows or SQL authentication, and then pick a secure account that has the appropriate per missions.
2. ***If you use Windows authentication***, click **User Account**, and then provide the appropriate credentials.
3. ***If you use SQL authentication***, click **Use Microsoft SQL Server authentication**, provide the appropriate credentials, and then click **OK** .
4. Click **Next**.

Choose the account that SQLsafe uses for the Backup Agent service

Specify the account under which the SQLsafe Backup Agent Service will run. This account runs as a Windows service on the computer hosting the managed SQL Server instances. This service account must have System Administrator access to the SQL Server instance.

Specify if you will use a **User Account** or a **Local System Account.** For your first install, we recommend you use your Local System Account. If you choose to use a User Account, then you must provide the appropriate credentials.

Choose whether you want to install the SQLsafe XSP

You can install the SQLsafe extended stored procedures (SQLsafe XSP) to all local instances when you install SQLsafe. The SQLsafe XSP extends the Backup Agent so you can integrate SQLsafe backup operations with existing T-SQL backup scripts. You can always deploy the SQLsafe XSP at a later time.

To skip this install, click **No**, and then click **Next**.

By default, the setup program uses the credentials of your Windows logon account to create the SQLsafe extended stored procedures. You can enable the option **Using Microsoft SQL Server authentication** and specify the respective credentials of a login with sysadmin privileges on that instance. Click **Next**.

Choose where you want SQLsafe to store backup files

You can use the default backup location or specify a different location. For your first install, we recommend using the default location (`C:\Backup`).

If you want to save backup files to a different local folder, type the directory path in the **Local Path** field or click **Browse** to search for a specific location, then click **Next**.

If you want to save backup files to a network share, type a valid path (`\\server\share`) in the **UNC Path** field, and then click **Next**.

> ⚠ Ensure the Backup Agent Service account has read and write access to the specified location.

Complete the install

Indicate that you are ready to complete your install and apply the configurations you specified. After install is complete, you can start the Management Console to immediately begin experiencing the benefits SQLsafe provides.

To complete your install:

1. Click **Install**.
2. Click **Finish**.

Install SQLsafe Backup Agent

You can remotely deploy the SQLsafe Backup Agent from the Management Console to SQL Server instances across your enterprise.

To install a SQLsafe Backup Agent:

1. In the navigation pane, click **SQLsafe Agents**.
2. Right-click on the computer in question in the tree pane.
3. Click **Install SQLsafe Backup Agent** from the context menu.
4. Choose whether you want to install the SQLsafe XSP. You can also enable or disable the option for installing SQLsafe Agent Extended Stored Procedures.
5. Click **OK**.

Deploy the Backup Agent

When deployment is complete, you can back up and recover databases hosted on your virtual instances. You do not need to install any other SQLsafe components on your clustered servers to implement a disaster recovery strategy for those virtual instances. If you have a clustered environment hosting multiple instances, you must manually deploy the SQLsafe Backup Agent on each node.

Using SQLsafe on a Microsoft Windows Cluster environment

SQLsafe is comprised of multiple application components, each providing specific functionality in different areas of the product. These different areas of functionality have specific concerns when deploying in a clustered environment, as redundancy and high availability are an issue. The following table includes the applications and services that SQLsafe is comprised of, with a summary of the requirements of each to be fully fault tolerant using the Microsoft Windows Clustering technology. SQLsafe components can work in either *active-passive* or *active-active* cluster configurations.

Component	Clustering Configuration Considerations
SQLsafe Management Console	None.
SQLsafe Command Line	None.
SQLsafe Management Service	This component is responsible for managing operational and policy status and alerting for your entire SQLsafe deployment. If you require these SQLsafe functions to be fault tolerant, configure this component as a *Generic Service Resource* on a clustered server. You need to deploy this component only once onto a single cluster, not on each server you are backing up. For more information about installing the SQLsafe Management Service on a Windows cluster, see Installing management components in a clustered environment.
SQLsafe Repository Database	This component is a SQL Server database used to stored operational history and policy configuration information. The SQLsafe Repository Database is used by the Management Console to display operational history and by the Management Service to process and send alerts. For this component to be fault-tolerant, simply host the database on a clustered SQL Server.
SQLsafe Backup Service	This component is responsible for executing backup and restore operations on nodes hosting any clustered SQL Servers. You need to install this service only on each node of the cluster. No failover or cluster resource configuration is necessary. You can deploy the agent from the Management Console or the product installer.
SQLsafe Filter Service	This component is responsible for performing instant restore operations on nodes hosting any clustered SQL Servers. If you require that SQLsafe Instant Restore functionality be fault tolerant, configure this component via the SQLsafe Command Line. You should not configure this service as a clustered resource. Instead, a failover mechanism is activated via a *Generic Script Resource*, and is automatically configured for you using a SQLsafe command. For more information about installing the SQLsafe Filter Service on a Windows cluster, see Installing backup/restore components in a clustered environment.

Installing backup/restore components in a clustered environment

For a fault-tolerant backup and restore infrastructure, you must install the SQLsafe Backup Service and SQLsafe Filter Service on the computers hosting your SQL Servers. Although you are using a clustered environment, **you should not configure these services as clustered resources**. Doing so would compromise their functionality in *active-active* clustering configurations. In the case of InstantRestore, you can perform the optional step of executing a one-time command to enable failover support for SQLsafe hydration operations. See the following topic to enable fault tolerance for IR hydration per SQL Server instance.

Install or upgrade the SQLsafe backup and restore components via the SQLsafe Management Console

1. Install the SQLsafe Management Console onto a computer using the FULL Installer. You can install on any computer, as long as it can access the servers to which you want to deploy the SQLsafe Management Console.
2. Launch the SQLsafe Management Console.
3. Register the clustered SQL Server instances on which you want to install or upgrade SQLsafe by right-clicking **SQL Server Instances**, and then selecting **Register SQL Server**.
4. Right-click the SQL Server instance in the Servers tree, and then select **Install SQLsafe Backup Agent**.
5. Follow the on-screen instructions and finish deploying the Backup Service components.
6. Once this process is complete, click the **SQLsafe Agents** tab. SQLsafe displays the active and inactive node names of the clustered SQL Server onto which you installed the SQLsafe Backup Agent.
7. Right-click the first of the remaining nodes, and then select **Install Backup Agent**. Repeat this step for each of the remaining nodes to install or upgrade the Backup Service components on the remaining nodes.
8. Verify that the **Management Server** column matches the correct management service. This setting is automatically set during your installation or upgrade.
9. ***If want to use InstantRestore functionality***, right-click the first node, and then choose **Enable SQLsafe Instant Restore**. Repeat this step for each of the remaining nodes. Your SQLsafe Backup Services are now installed.

Enable fault tolerance for InstantRestore Hydration per SQL Server instance (Optional)

This process is necessary only if you want fault tolerance for databases still going through the hydration process of InstantRestore. Before you begin, make sure that your SQLsafe Backup service components are already installed.

1. Remotely log on to a node of the cluster.
2. Open a new Command Window.
3. For each clustered SQL Server instance hosted on that cluster server, run the following command:
   SQLsafeCmd Cluster FilterService `sqlserver_name`
   Where `sqlserver_name` is the full SQL Server name of the clustered SQL Server.

This command creates a Generic Script Resource that controls failover for Hydration operations for that specific SQL Server. Note that this command is run only once per clustered SQL Server, not per node.

Installing management components in a clustered environment

For a fault-tolerant SQLsafe management infrastructure, follow the standard procedure for installing SQLsafe by running the FULL installer on all the cluster nodes you want to host your SQLsafe Management Service, whether active or inactive. For new installations, choose at least the Management Service and Repository Database components. Upgrades automatically choose the correct components for you. To make the repository database clustered, simply specify a clustered SQL Server to host the Repository database.

Before you begin, open the Windows Services application (services.msc) and find the SQLsafe Management Service. Make sure that the **Startup Type** is set to **Manual** and that the service status is **Stopped** in all but the active node. ***If you are upgrading your installation***, there are no more requirements. ***If you are installing a new deployment***, you must also configure the Management Service as a Generic Service Resource. Select the appropriate task below to perform this action.

Configuring the SQLsafe Management Service as a Generic Service Resource using Windows Server 2003

1. Open the Windows Cluster Administrator application named `cluadmin.exe`.
2. Create or choose a resource group containing defined **IP Address** and **Network Name** resources. Note that the **IP Address** and **Network Name** resources in this group are used to access your SQLsafe Management Service. If you choose to use an existing group, note that fail over for each component in this group occurs together. If you choose to create a new group and resources , make the owners of the new resources the same nodes on which you installed the Management Service. Once you configure or choose a group for the SQLsafe Management Service, you can add the Generic Service Resource using the following steps.
3. Right-click the group, and then select **New** > **Resource .**
4. On the New Resource window,type a name for the Management Service resource, such as SQLsafe Management Service.
5. Select the **Generic Service** resource type, and then click **Next.**
6. On the Possible Owners window, click **Next** .
7. On the Dependencies window, add the IP address and network name resources by selecting the appropriate address and name, and then clicking **Add >** to move them to the dependencies area.
8. Click **Next.**
9. On the Generic Service Parameters window, type **SQLsafe Management Service** as the service name.
10. Check the **Use Network Name for Computer Name** check box, and then click **Next** .
11. On the Registry Replication window, click **Add** .
12. In the root registry field, type the following text:
    Software\Idera\SQLsafe\Management Service
13. Click **OK.**
14. Click **Finish** .
15. Right-click your new Generic Service resource, and then select Bring Online . Your SQLsafe Management Service is now configured for cluster failover.
16. Right-click your new Generic Service resource, and then select Bring Online . Your SQLsafe Management Service is now configured for cluster failover.

Configuring the SQLsafe Management Service as a Generic Service Resource using Windows Server 2008/ Windows Server 2008 R2

Use the following steps if you **do not** have an existing application or service that you want to use for the SQLsafe Management Service.

1. Open the Windows Failover Cluster Management application named **cluadmin.msc.**
2. Right-click Services and Applications, and then select **Configure a Service** or **Application .**
3. On the Select Service or Application window, click **Generic Service** , and then click **Next** .
4. On the Select Service window, click **SQLsafe Management Service** , and then click **Next.**
5. On the Client Access Point window, type or select the IP address and network name that you want to use to access the SQLsafe Management Service, and then click Next.
6. On the Select Storage window, click **Next.**
7. On the Replicate Registry Settings window, click **Add** .
8. In the root registry field, type the following text:
    Software\Idera\SQLsafe\Management Service
9. Click **OK.**
10. Click **Next** .
11. On the Confirmation window, click **Next** . The wizard configures the service as displayed on the Configure High Availability window, and then displays the Summary window.
12. On the Summary window, click **Finish.** Your SQLsafe Management Service is now configured for cluster failover.

Use the following steps if you **do** have an existing application or service, already configured with the IP address and network name that you want to also use for the SQLsafe Management Service.

1. Open the Windows Failover Cluster Management application named **cluadmin.msc**.
2. Right-click the application, and then select **Add a resource > 4 - Generic Service .**
3. On the Select Service window, wait while the services populate the fields with a list of services installed on this computer.
4. Click **SQLsafe Management Service** , and then click **Next.**
5. On the Confirmation window, click **Next** . The wizard configures the service as displayed on the Configure Generic Service window, and then displays the Summary window.
6. On the Summary window, click **Finish** .
7. Right-click your new Generic Service resource, and then select Properties. SQLsafe now displays the SQLsafe Management Service Properties window which contains many tabs.
8. On the General tab, check the **Use Network Name for Computer Name** check box.
9. On the Dependencies tab, add the **Network Name** and **IP Address** resources belonging to this application.

10. On the Registry Replication tab, click **Add.**
11. In the root registry field, type the following text:
    Software\Idera\SQLsafe\Management Service
12. Click **OK.**
13. On the SQLsafe Management Service Properties window, click **OK.**
14. Right-click your new Generic Service resource, and then select **Bring this resource online.** Your SQLsafe Management Service is now configured for cluster failover.

Configure your deployment

After initially installing and setting up SQLsafe, there are several tasks you might want to do in order to further customize and streamline your install. Review the following sections to get a good understanding and make the best of your SQLsafe installation.

Configure e-mail settings

You can enable SQLsafe to send email notifications about the current status of your backup and restore operations.

Access these settings by clicking **Configure E-mail Notifications** on the **Repository and Management Service Settings** window, accessible from the bar menu (gear icon), or by selecting **E-mail Notification Settings** in the **Tools** menu.

What email settings can I change?

If you enable **E-mail Notifications**, you can configure how the email will appear in your Inbox.

Sender Name

Enter the name that will appear as the sender of the email.

Reply-to Address

Enter the email address that will appear as the sender, and where replies to the message will be sent.

Priority

Select low, normal, or high priority for the email alerts.

What mail server information is required?

You must specify the mail server information so that SQLsafe can send email notifications.

Server Address

Enter the address of your mail server.

Server Port

If you want to specify a port different from 25 (set by default), you can do that in this section. You can also enable SSL encrypted connection.

SMTP Authentication

If your SMTP server requires authentication , you must type a valid **User Name** and **Password** that SQLsafe should use to access to the mail server.

Test your settings

To be sure that your settings are correct, click **Test Settings** on the bottom section of the window, then check the test email sent to your email server.

Configure Console preferences

SQLsafe allows you to modify many of the default settings of the application, and you can change your **Management Console Preferences** at any time. To access this option go to the **Tools** Menu and select the respective option. The window for **Management Console Preferences** allow s you to modify settings in the following categories:

- Backup
- Agent Deployment
- User Experience
- Policy Data

What Backup settings can I change?

On the **Backup** tab, you can set the default parameters that appear on the **Backup Wizard**. Set the default parameters to the values you typically use. If you want to use different settings on any given backup, you can still make changes on the wizard itself.

The parameters you can set include the following:

- Backup archives location
- Tivoli Storage Manager backup archives location
- Default compression and encryption algorithms
- Generating maps containing metadata for use with InstantRestore and SQL virtual database
- Auto-generated backup file names
- Number of threads employed in a backup

What Agent Deployment settings can I change?

On the **Agent Deployment** tab, you can identify service account used to run the agents. You can also choose whether or not you want to automatically upgrade the Backup Agents and the XSP if you upgrade to a new SQLsafe version.

What User Experience settings can I change?

On the **User Experience** tab, you can:

- Enable automatic refresh on screen and set the number of seconds between each refresh.
- Change display status for server status.t
- Set the Total Cost of Ownership parameter necessary to calculate your return on investment.
- Configure troubleshooting settings.

What Policy Data settings can I change?

On the **Policy Data** tab you can define the location of your policy data files.

By default policy data files are stored in the *C:*\<InstallPath>*SQLsafe**PolicyData* folder, but you can use this option to specify a different location. Click **Local Path** and browse the folder where you want to store your policy data files or select the respective option for creating a new folder.

By default each agent uses its own installation directory to store policy data. If a custom location cannot be created on a specific server, the Backup Agent will use <InstallPath>\PolicyData.

Configure the Management Service

You can specify the location and authentication credentials necessary to access the SQLsafe Repository. You can connect to the Repository database using Window Authentication or SQL Server Authentication.

You can also change the port assignment for the Management Service.

What are the available fields?

Computer

Allows you to select the computer where the Management Service is located.

SQL Server

Specify the SQL Server instance that currently hosts the SQLsafe Repository.

Database

Allows you to specify the name of the SQLsafe Repository.

Windows Authentication

Allows you to specify Windows Authentication for accessing the selected SQL Server instance. Selecting this option uses the credentials of the Management Service to log on to the SQLsafe Repository.

SQL Server Authentication

Allows you to specify SQL Server Authentication for accessing the selected SQL Server instance. Selecting this option allows you to specify the SQL Server login ID and password you want to use to access the target SQL Server instance.

Test Connection

Allows you to verify that the Management Service can use the specified account to connect to the Repository database.

Configure E-mail Notifications

Allows you to configure the settings for sending email alerts. In this section you can also enable or disable the option for sending these notifications to the Windows Application Event Log on the Management Service Computer.

Repository Grooming

Allows you to specify how long (in days) you want to keep operational history, such as status messages for backup and restore operations. By default, the Repository is groomed every 30 days. Operational history older than 30 days is permanently deleted.

How do I configure the Management Service?

To configure the Management Settings you can use any of the following paths:

- Go to the **Tools** Menu and click **Repository and Management Service Settings.**
- Select the gear icon on the bar menu.

Import archived backup sets

SQLsafe allows you to import archived backup sets into the SQLsafe Repository to manage all your backups from one place.

SQLsafe cannot import copies of backup files that have been previously deleted or groomed. You can still access the backup files from the alternate location through the Restore wizard.

How do I import archived backup sets?

You can find and add archive files created outside your current SQLsafe environment to the Repository. You can also use this feature to help you recreate the SQLsafe Repository in the event of a critical failure.

You can reach the **Locate Backup Sets** dialog from the **File** menu and then selecting **Import Backup Archive(s).**

To import backup archives from a local folder:

1. In the **Locate Backup Sets** window, click **Browse Locally** .
2. Select the archive file to import.
3. Review the displayed backup set information and click **OK** .

To import backup archives from a remote share:

1. In the **Locate Backup Sets** window, click **Browse Remotely** .
2. Select the SQL Server instance from the drop-down menu.
3. Select the archive file to import.
4. Review the displayed backup set information and click **OK.**

To import backup archives from TSM tape backup:

1. In the **Locate Backup Sets** window, click **Browse TSM** .
2. Select the appropriate TSM options file.
3. Enter a High Level and Low Level search parameters and choose whether to include or not inactive files.
4. From the Results text box, select the found files to be imported.
5. Review the displayed backup set information and click **OK** .

Manage licenses

The License Key Manager provides an intuitive, simple-to-use interface for SQLsafe license key management. You can:

- View the instances licensed with your current license
- Select which instances you want SQLsafe to take into account for your license key instance count
- See how many available instances you can still license for backup operations.
- Edit your license key
- Save your license information to a file

The Management Service manages your SQLsafe license and receives requests from the respective Backup Agents to license your instances.

How do I manage my licenses?

You may need to edit your current license if you exhaust your trial license, or if you need to replace it with one that allows you to license more instances.

To access these options, on the **Tools** menu, click **License Key Manager.** Y ou can also click the key icon located on the task bar to access the same option.

What information can you see on the License Key Manager window?

On the License Key Manager window you can find:

- Your license keys
- Instances licensed for backup operations

On the License Keys tab you can find:

- Your current licences keys, type, the number of instances allowed for each key, and the expiration date.
- Options for Removing and adding license keys.
- The number of Used licenses.
- An option for Automatically licensing instances for scripted agent deployments.
- An option to save this information to a file

On the Instances tab you can find:

- A list of the instances licensed for backup operations and all available registered instances.
- An option to license All or None of them
- An option for Automatically licensing instances for scripted agent deployments.

To upgrade a trial license to a permanent license:

1. On the **License Key Manager** window, on the License Keys tab, click **Add.**
2. Enter the respective license key.
3. Click **OK** . The license key will be displayed in the License Key Manager window.
4. If you want to save the list to a file, click **Save to a File** and save the file to your desired location.

What is a multi-instance license key?

A multi-instance license key allows you to centralize the license management with the SQL Safe Management Service. SQL Safe Backup Agents configured to this Management Service will use this licensing management method and enable you to enter a license key through the Management Console and support the licensing of a certain number of instances.

Please take into account that a multi-instance key will replace any single instance keys previously installed and the user will be prompted to switch to centralized license management.

Standalone SQL Safe Backup Agents not configured to a SQL Safe Management Service will be treated as standalone installations and therefore use the old licensing model.

How can you license your instances for backup operations?

On the **License Key Manager** window, you can see the list of all your registered instances. Check or uncheck those instances that you want SQLsafe to license to perform backup operations. The number of available licenses will be updated according to your choices.Then click **OK.**

What are the terms of the trial license?

By default, SQLsafe installs with a limited 14-day time, unlimited instances trial license key. After you install the SQLsafe components using the Typical or Custom setups, the Management Console lists your trial license in the **License Key Manager.** This license key is stored in the SQLsafe Management Server.

What are the terms of the production license?

SQLsafe licenses are issued per SQL Server instance and for a specific time period. You can manage this license with the License Key Manager. The SQLsafe production license gives you full access to the Backup Agent through the Management Console, including operation status information.

What is the SQLsafe Lite license?

When you have different versions of SQLsafe deployed in your environment, one or more registered SQL Server instances may be running SQLsafe Lite.

SQLsafe Lite does not support backup and restore operations through the Management Console. For example, you cannot create a backup policy for a SQL Server instance running SQLsafe Lite.

If you want to manage all registered SQL Server instances through the Management Console, you can upgrade the SQLsafe Lite Backup Agents to the enterprise version of SQLsafe.

How do I upgrade my SQLsafe Lite license?

You can temporarily upgrade a SQLsafe Lite license to an enterprise edition license by installing a SQLsafe trial license. Note that, when the trial period has expired, your license will revert back to SQLsafe Lite.

You can then permanently upgrade a SQLsafe Lite license to an enterprise edition by purchasing a production license key and entering it in the License Key Manager.

To upgrade a SQLsafe Lite license:

1. In the Servers tree, expand the SQL Server Instances node, and then select the instance that is running the SQLsafe Freeware Edition Backup Agent.
2. Click **Enable Trial License** in the Backup/Restore Operation Status pane.

How do I upgrade my SQLsafe Freeware Edition?

You can upgrade SQLsafe Freeware Edition to SQLsafe enterprise edition by upgrading the Backup Agent on the corresponding SQL Server computer.

This installs the SQLsafe enterprise edition trial license. You can then permanently upgrade a SQLsafe Lite license to an enterprise edition by purchasing a production license key and entering it in the License Key Manager.

To upgrade a SQLsafe Freeware Edition Backup Agent:

1. Navigate to the **SQLsafe Agents** view.
2. Right-click the target SQL Server computer, and then select **Install SQLsafe Backup Agent** on the context menu.

How do I save my license keys to a file?

1. On the **Tools** menu, click **License Key Manager** .
2. Click **Save to File** , and browse to the location to which you want to save the file.
3. Enter the file name, and click **Save.**

Backup Agent configuration

How do I access the agent configuration information?

To manage your SQLsafe Backup Agents, click **SQLsafe Agents** in the navigation pane. To view information about a specific agent, click the corresponding SQL Server computer listed in the tree pane and you will be able to see the configuration information of the respective agent.

What agent configuration settings can I view?

The content pane in the SQLsafe Agents Settings view contains the agent configuration information. This information allows you to monitor and maintain the performance of each Backup Agent.

Column	Definition
Computer	Displays the name of the host computer.
Version	Displays the version number of the selected Backup Agent.
Management Server	Displays the location of the SQLsafe Management service that the Agent is configured to communicate with.
Max Load	Displays the maximum number of concurrent operations that the backup agent can perform.
Priority	Displays the Windows thread priority at which backup agent threads run.
Send Status	Displays the frequency that the agent is configured to communicate with the Management Server.
SQL Timeout	Displays the SQL DMO timeout value, which determines who long the Backup Agent will wait for a response from SQL Server before timing out.
VDI Trans. Limit	Displays the maximum size of a transfer block for the VDI operation.
VDI Buffers	Displays the number of buffers used for the VDI operation.
VDI Block Size	Displays the size of a VDI device block. All data transfers are integer multiples of this value.
VDI Timeout	Displays the timeout for configuring the VDI.

Modify Backup Agent properties

You can modify many of the SQLsafe Backup Agent properties from the Management Console and adjust performance parameters to suit your system needs.

If the SQL Server instance is running SQLsafe Lite, the Send Status every *x* seconds option is ignored. SQLsafe displays operation status information only for Backup Agents running with an enterprise edition license.

If the SQL Server instance is running SQLsafe Freeware Edition, all settings are unavailable. You must upgrade the Backup Agent to either SQLsafe Lite or the enterprise edition to make changes to the Backup Agent properties. For more information, see Manage licenses.

To change the agent properties:

1. In the navigation pane, click **SQLsafe Agents.**
2. Right-click the appropriate SQL Server instance.
3. Click **Properties** from the context menu.
4. Change the SQLsafe Agent properties to improve the performance of your backup and restore operations, or enable debug mode for troubleshooting an issue. For more information about SQLsafe Agent properties, see View agent settings.
5. Click **OK.**

You can also change the port assignment for the Backup Service.

How do I access Backup Agent properties?

To manage your SQLsafe Backup Agents, click **SQLsafe Agents** in the navigation pane. To view information about a specific agent, right-click the corresponding SQL Server computer listed in the tree pane, and then select Properties.

Why should I enable troubleshooting?

Occasionally when you contact Idera support for assistance, a representative will ask you to enable logging to get a better idea of what the issue is in your environment. SQLsafe allows you to customize your debug settings when troubleshooting an issue with your Backup Agent.

Is there a disadvantage if I leave debug mode enabled for a long period of time?

There is no disadvantage to leaving SQLsafe in debug mode for an extended period of time. If you experience an issue that occasionally and unexpectedly occurs, or you want to capture data over a long period of time, leave debug mode enabled. This settings gives you the advantage of already logging the data when the issue occurs.

How the IR Service works

The InstantRestore Service manages the following properties, which are stored in the registry:

- Max number of concurrent hydrations
- Number of driver threads
- Large raw buffer IO size
- Hydration chunk sizes
- Decompressed block cache size
- Driver active IO list size

You must use the same Windows account for the Backup Agent and InstantRestore Service. During installation, you are asked to enter credentials for only one account and the other is created with the same information. If you manually change your account information, make sure you change it in the other service as well to avoid any issues.

How do I enable or disable the InstantRestore Service?

SQLsafe includes the InstantRestore (IR) Service during an installation or upgrade. Users can enable or disable the IR components using an Agent. If an InstantRestore operation is in progress when a user attempts to disable IR components, SQLsafe returns an error.

Modify your SQL Server list

SQLsafe provides the ability to add, remove, and group SQL Server instances from within the tree pane.

To add a SQL Server instance, click **Register SQL Server** in the **Common Tasks** of the **SQLsafe Today** view. You can also find the same option by right-clicking the SQL Server instances folders on the pane tree of the **Servers** view.

To group SQL Server instances, right-click the SQL Server instances folders on the pane tree of the **Servers** View and select **Add group,** then you can Register SQL Servers to add them to the respective group. Organizing your SQL Server instances into related groups can help you verify the backup status of specify types of SQL Server instances. For example, you can categorize servers based on location, purpose, importance, platform, or any other logical category.

To remove SQL Server instances, right-click the respective instance and select **Remove SQL Server.**

In the Servers tree, the SQL Server Instances node lists all the SQL Server instances you have registered with SQLsafe. However, this list may not reflect all registered SQL Server instances across your environment. For example, when your backup or log shipping policy contains instances registered by other database administrators, SQLsafe lists these instances in the Discovered Instances node. Although you can delete this node, SQLsafe recreate the node after a policy status refreshed.

Register an instance

After creating a server group, you can add SQL Server instances to the group. Adding a SQL Server instance to SQLsafe does not affect the registered groups or SQL Server instances in SQL Server Enterprise Manager or SQL Server Management Studio.

You can also register an instance "on the fly" when you back up the hosted databases through the Management Console.

To register a SQL Server instance with SQLsafe:

1. In the navigation pane, click **Servers**.
2. Right-click on the Server Group to which you want to add the SQL Server instance.
3. Select **Register SQL Server** from the context menu.
4. In the Available Servers list in the Register SQL Servers dialog, select the instance you want to add to the Server Group.
5. Click **Add >.** SQLsafe moves the selected server to the Added Servers list.
6. Select the required authentication method used to log in to the SQL Server instance, and then click **OK**.

Understand total cost of operation (TCO)

SQLsafe provides a built-in calculator to help you calculate your monetary return on your SQLsafe investment. You can view this calculator in the Disk Space Savings pane on the SQLsafe Today view.

The calculator attempts to measure the time and monetary savings you gain through using the SQLsafe compression scheme. The Return On Investment (ROI) calculator bases your ROI on the total cost of ownership of your storage devices multiplied by the amount of disk space savings you realize using SQLsafe. SQLsafe defaults to the commonly used estimate of $200 per GB of storage. You can change this estimate to reflect your particular hardware configuration.

Manage debug settings

The Advanced Debug Settings display additional debug selections for troubleshooting the Backup Agent running on the selected SQL Server computer. You can also set the log file characteristics and maximum size depending on what issue you want to troubleshoot. It is recommended that you change these settings based on guidance from Idera support.

A rolling log allows you to create a log files that "roll" when they reach the maximum file size or the service is restarted, meaning that when the max size/restart occurs, it deletes the oldest information and logs the newest. This feature helps you avoid a large, cumbersome log file.

To change the debug settings:

1. In the navigation pane, click **SQLsafe Agents** .
2. Right-click the appropriate SQL Server instance.
3. Click Properties from the context menu.
4. Click **Advanced** .
5. Make the necessary changes, and then click **OK** .

How do I access debug settings?

To manage your debug settings, click SQLsafe Agents in the navigation pane. Right-click the name of the SQL Server instance for which you want to manage debug settings, and then select Properties. Click the Advanced button.

Once you make the appropriate changes, click OK on the Advanced Debug Settings. Make sure to select Enable Debug Mode on the SQLsafe Agent Properties, and then click OK or debugging is not enabled.

What log file settings can I change?

If you enable debug mode, SQLsafe creates a log file based on the settings in the Roll Log fields. You can choose one of the following options for the log file

No

Maintains the debug log as a single file that is unlimited in size. This option allows SQLsafe to capture diagnostic information over an extended period of time. Your log file may become very large and should be monitored to avoid any issues with file size.

Do not enable No unless absolutely necessary. Use No only when the problem being diagnosed occurs very infrequently and is not noticed in a timely manner. In almost all cases, increasing the size or number of files is sufficient for troubleshooting an issue and an unlimited file size is unnecessary.

Yes and keep *n* file(s)

Maintains the debug log as a series of files that are limited in size and quantity. This option allows SQLsafe to capture diagnostic information over a limited period of time, depending on the size and quantity of files kept. When a log file reaches the size limit or the service is restarted, SQLsafe renames the file and starts a new log file. The older the log file, the higher the digit that exists at the end of the file name. For example, file `x.log.3` is more recent than `x.log.4` . When the log file rolls over and reaches the maximum quantity, SQLsafe deletes the oldest file and the next oldest file takes its place. Because the amount of space used by the logs is limited, this setting does not require you to monitor the log files.

A Yes option is the recommended setting. Be aware that the amount of history retained is limited, and it may be possible for a problem being diagnosed to be missed. If this may be the case, first increase the quantity of files retained, then increase the size if necessary. Increasing quantity before size helps to maintain log files that are smaller and easier to view and send to Idera support.

View enterprise status for last 24 hours

The SQLsafe Today view provides an high-level record of backup and recovery operations across your enterprise.

Use this view to monitor the status of backup and restore operations and easily access the most commonly used tasks. This view automatically displays when you start the Management Console.

How do you access SQLsafe Today?

To use SQLsafe Today, click the **SQLsafe Today** globe icon in the task bar, or click **View** > **SQLsafeToday** from the menu.

What is the Status Summary?

The Status Summary provides a simple indicator to tell you at a glance whether backup and restore operations across your enterprise have been successful. The green check icon indicates success, and the red X icon indicates errors have occurred.

What are the Status Details?

The statistics pane shows the values for the following metrics:

- Number of policies whose status is OK (all operations have completed successfully)
- Number of policies whose status is not OK (includes a failed, skipped, or canceled operation)
- Number of successful operations
- Number of operation that failed (returned errors)

For more information, see How policies work.

Why are SQLsafe Today statistics different than Server statistics?

The filter used by the SQLsafe Today statistics is different than that used by the Servers statistics. SQLsafe Today shows the status for all instances and databases. Servers shows status based on your filter settings plus the currently selected node and the databases under it.

What is Disk Space Savings?

The disk space savings pane shows the disk space savings achieved by using compression on your backup sets, and, using the TCO/GB parameter set in the SQLsafe Preferences, calculates your return on investment (ROI) using SQLsafe for your SQL Server instance backups. For more information on calculating TCO, see Modify Total Cost of Operation (TCO) Preferences.

What tabs are available on the SQLsafe Today view?

There are two tabs available for you to choose on the SQLsafe Today view:

- Policies
- Backup and restore operations

What can you find on the Policies status tab?

The Policies tab displays the current status of your Backup and Log Shipping policies.

When the Policies tab is selected, all existing policies are displayed with the following columns:

Column Header	Definition
Status	Status can be ok, or display a warning or error state.
Name	Displays the policy name.
Databases Covered	Displays the number of databases covered by the policy.
Last Backup Time	Displays the start date and time of the last backup executed by the policy.
Last Backup Failure Time	Displays the start time of the last failed backup executed by the policy.

For more information, see Backup policies and How Log Shipping Policies work.

What can you find on the Backup & Restore Operation status tab?

The Backup & Restore Operations tab displays the current status of the backup and restore operations that were scheduled to run today.

When the Backup & Restore Operations tab is selected, all existing operations are displayed with the following columns:

Column Header	Definition

Progress	During an operation, the progress bar will denote the percentage of the operation completed. When the operation is complete, it will display a green bar labeled 100%. When an operation completed with errors, this column will display a red bar labeled Error. This column also indicates when the backup file has been deleted (groomed), and therefore is no longer available to be restored.
Instance	Displays the instance name that was backed up or restored by this operation.
Icon	Displays an icon if the backup includes maps containing metadata for InstantRestore and SQL virtual database. For more information about InstantRestore, see How InstantRestore works. For information about SQL virtual database, see Recover objects using SQL virtual database .
Database	Displays the database name that was backed up or restored by this operation.
Operation	Displays the operation performed. The options are Backup, Restore, and Verify.
Backup Type	Displays the type of the backup performed by the operation. The options are Full, Log, Differential, and File.
Start Time	Displays the start date and time of the operation.
Duration	Displays the number of seconds required to complete the operation.

Can you customize the columns in the grid?

You can sort by the content of any of the columns by clicking on the column header.

How do you refresh the operations status?

If a recent operation does not appear in the status view, you can refresh the status of this pane by clicking on the refresh icon in the pane title bar.

What are the Common tasks?

The Common Tasks are shortcuts to some of the more frequently performed actions in SQLsafe.

Task	Definition
Register SQL Server	Allows you to add a new SQL Server instance.
Backup Database	Starts the SQLsafe Backup Wizard, which allows you to back up one or more databases. For more information about the Backup Wizard, see Perform a manual backup.
Restore Database	Starts the SQLsafe Restore Wizard, which allows you to restore one or more databases. For more information about the Restore Wizard, see Restore a database.
Create New Policy	Starts the SQLsafe Backup Policy Wizard, which allows you to create a new backup policy. For more information about the Backup Policy Wizard, see How backup policies work.
Manage Agents	Changes the Console display to the settings view. From here, you can modify your SQLsafe Agent settings. For more information about agent settings, see View agent settings.
Attach Virtual Database	If you have installed SQL virtual database, this will launch the SQL virtual database console. For more information about SQL virtual database, see Recover objects using SQL virtual database.

View SQLServer status

The Group, Instance, and Database views display backup and restore details and operation status for all SQL Server instances registered with SQLsafe, as well as at-a-glance summaries of important administrative information. You can view information about a group of SQL Server instances, a single instance, or a database.

For this node ...	You can view ...
A server group	Displays the total number of instances in the group, the number of successful and failed operations, and the number of instances up and the number of instances not connected at the time.
An instance	Displays whether the connection to SQL Server is active, the number of successful and failed operations, whether the SQLsafe Backup Agent is running, the SQLsafe version, the license status, the number of databases on the instance, and the SQL Server version it is running. You can also find the backup and restore operations status for the last 7 days.
A database	Displays whether the database is currently online, the number of successful and failed operations, and the date of the last backup performed on the database. You can also find the backup and restore operations status for the last 7 days.

To manage your SQL Server instances, click **Servers** in the navigation pane, and then click the appropriate node in the Servers tree.

You can re-run any previous backup operation from these views. To re-run a backup, right-click the appropriate operation, and then select Back Up Again (executes backup using previous settings) or Back Up with Different Options (opens the Backup wizard). You can also quickly restore the backup files associated with a specific operation.

What SQLsafe settings are managed in the instance view?

You can install any options you did not include during your initial SQLsafe installation. Click **Settings** in the Instance Information area, and then select one of the following options, if available:

- Install SQLsafe Backup Agent / Upgrade SQLsafe Backup Agent
- Install SQLsafe Extended Stored Procedures
- Update license
- Enable/Disable SQLsafe InstantRestore
- SQLsafe Agent Properties

View backup/restore operation status

The Backup/Restore Operation Status area displays a listing of all backup and restore operations performed for the selected object for the last 7 days. To change how much status information you see, click **Filter** and then select a different date **Range** in the **Event Time** settings.

You can re-run any previous backup operation from this grid. To re-run a backup, right-click the appropriate operation, and then select Backup Again (executes backup using previous settings) or Backup with Different Options (opens the Backup wizard). You can also quickly restore the backup files associated with a specific operation.

What column information can I select?

Column	Definition
Backup Type	Displays the type of the backup performed by the operation. The types are Full, Log, Differential, and File.
Compressed	Displays the size of the backup file after compression.
Database	Displays the name of the database that was backed up or restored by this operation.
Database Size	Displays the size of the original database.
Duration	Displays the time (hours:minutes:seconds) required to complete the operation.
Encryption	Displays the type of encryption SQLsafe used during the backup operation.
End Time	Displays the end date and time of the operation.
Instance	Displays the name of the SQL Server instance that was backed up or restored by this operation.
Operation	Displays the type of operation performed. The types are Backup, Restore, and Verify.
Icon	Displays an icon if the backup includes maps containing metadata for InstantRestore and SQL virtual database. For more information about InstantRestore, see How InstantRestore works. For information about SQL virtual database, see Recover objects using SQL virtual database.
Progress	During an operation, the progress bar will denote the percentage of the operation completed. When the operation is complete, it will display a green bar labeled 100%. If an operation completed with errors, this column will display a red bar labeled Error. If an operation completed with warnings, this column will display a yellow bar labeled 100% with an asterisk. This column also indicates when the backup file has been deleted (groomed), and therefore is no longer available to be restored.
Ratio	Displays the ratio of the Uncompressed size of the database reported by SQL Server to the resulting Compressed size of the backup file created by SQLsafe.
Result Text	Displays text describing the results of the operation.
Start Time	Displays the start date and time of the operation.
Threads	Displays the number of threads SQLsafe used during the backup operation.
Uncompressed	Displays the size of data contained in the database, as reported by SQL Server.

Can I customize the columns in the grid?

Task	Action

Add or remove columns in the grid	Click Filter in the pane title bar, then select the columns you want to display in the grid.
Sort the content of a column	Click on the column header to sort the column in ascending order; click again to sort the column in descending order.
Rearrange the order of the columns	Click on the column header and drag it to a new position in the grid.
Group column headings	Click on the column header and drag it to a position beneath the column header by which it will be grouped.

How do I refresh the operations status?

If a recent operation does not appear in the status view, you can refresh the status of this pane by clicking the **Refresh** icon in the pane title bar.

Why is the Backup/Restore Operation Status grid blank?

SQLsafe only displays operation status information for Backup Agents running with an enterprise edition license. If the Backup Agent has a SQLsafe Lite or SQLsafe Freeware Edition license, this pane will be blank.

You may view the operation status for SQLsafe Lite or SQLsafe Freeware Edition Backup Agents by installing a purchased license. To use a trial before purchase, click Enable Trial License. For more information, see Manage license.

View operations status summary

The Operations status summary displays a green success icon if the most recent backup or restore operation for each of the databases in the group or instance have been completed with success. When a failed operation is followed by a successful operation on the same database, the status is given as success. The number of successes and errors noted in the Operation Status Summary will always add to the number of databases in the group or instance.

View server status details

To see the detailed results of a specific operation, click the operation in the Backup/Restore Operation Status grid, and the Details area displays below. The Details area provides the following information:

Information	Definition
Statistics	Displays the database size, the size of the uncompressed backup, the size of the compressed backup, and the compression ratio achieved with this backup. The ratio is a measure of the storage savings achieved with SQLsafe compression technology. For more information about the storage space savings you can realize using SQLsafe, see Understand your total cost of operation (TCO).
Result Text	Displays text describing the result of the operation.
Files	Displays the complete path of the backup set file for the backup or restore.
Backup Set Description	Displays the description you specified for this backup.
Storage Options	Displays the storage options you specified for this backup.

Define your Backup and Recovery Strategy

Before performing database backups within your SQL Server environment, establish a backup and restore strategy. Your strategy should consider the following points:

- Data availability needs
- Data loss impact
- Recovery model you want to use: Simple, Full, or Bulk-Logged
- Restore process you want to use: InstantRestore or normal
- Data storage space allotted to backup storage

SQLsafe supports whatever strategy you decide to implement, while allowing you to take advantage of the fastest, most efficient SQL Server backup solution available. You can create custom backup and restore policies that ensure your data is archived and recovered according to your corporate standards and Service Level Agreements (SLAs).

If your strategy includes tape backup, SQLsafe also allows you to easily integrate the third party data-protection product, Tivoli Storage Manager (TSM), into your backup strategy. For more information, see Integrate SQLsafe with TSM.

If your SQL Server environment requires FIPS compliance, see Ensure FIPS compliance.

How do I define a backup and recovery strategy?

Use the following checklist to ensure you have everything in place to successfully implement your backup strategy.

☑	**Follow these steps ...**
☐	Determine the backup types you want to perform for your different SQL Server instances.
☐	Determine what type of compression you need.
☐	Determine the type of encryption you want to use.
☐	Identify which databases should be routinely archived using backup policies.
☐	Identify which databases should be routinely recovered using restore policies.

How can I get my database up and running quickly during a restore?

SQLsafe's InstantRestore feature is the fastest way to get your database back online. Under certain conditions, InstantRestore allows you to restore your database while providing your users with quick access to the database during this process. Note that you may experience some performance issues because the restore is still running while you attempt to use the database.

How the Backup Agent works

The Backup Agent performs backup and restore operations. The agent is a service that runs on the target SQL Server instance. When you request a backup or restore operation, the Management Console wakes the previously deployed Backup Agent. Take into account that the Backup Agent must be licensed to perform any operation, if it is not licensed yet, the Agent will contact the Management Service to request a license.

While executing the backup or restore operation, the agent periodically sends messages to the Management Service.

How do I install the Backup Agent?

You can install the Backup Agent locally using the setup program or deploy the Backup Agent remotely using the Management Console. To install the agent in an environment that does not contain a SQLsafe Management Service and Repository, use the Agent Only setup type provided in the setup program. The Backup Agent will contact the Management Service to request licensing. For more information, see License Management.

How can I upgrade my Backup Agent?

You can configure SQLsafe to automatically upgrade the Backup Agent to the current software version in the SQLsafe Preferences window. For more information,see Configure your deployment.

Can I run the Backup Agent without receiving messages?

You can run the Backup Agent in silent mode. Silent mode allows you to use the Backup Agent in environments that do not require the Management Service or SQLsafe Repository.

When in silent mode, the Backup Agent does not return status information about backup and restore operations. Use this mode if you do not plan to track backup and restore status, or if you plan to perform backup and restores through the command-line interface only. This flexibility allows you to easily integrate SQLsafe into your existing backup and recovery infrastructure so you can take advantage of SQLsafe features without changing your established processes.

How to choose backup type

SQLsafe supports four standard database backup types:

- Full Backup
- Differential Backup
- Transaction Log Backup
- File Backup

You can use a backup type exclusively or combine types to fit your backup strategy.

What is a full backup?

A full backup creates a full copy of the data in a database. Full backups usually run at regularly scheduled intervals and require more storage space and time to complete. Full backups copy data and transaction log pages to the backup set. The backup is smaller than the database itself because unused space is not retained.

Full backups allow you to restore your database to its original state prior to backup. During the restoration of a full backup, the SQL Server instance being restored rolls back uncommitted transactions. Use transaction log backups to recover uncommitted transactions.

What is a differential backup?

Differential backups record only the data that changed since the last full backup. Consider using differential backups on active SQL Server instances where minimal database downtime is critical. Smaller and faster differential backups allow you to make more frequent backups with less impact on your server. Performing frequent backups helps maintain optimal database availability and minimizes data loss risks. Differential backups allow you to restore your database to the last completed differential backup.

What is a transaction log backup?

A transactional log backup creates a copy of the transaction log file. It sequentially records all database transactions that occurred since the last transaction log backup. In conjunction with a full or differential database restore, restoring a transaction log backup allows you to recover the database to the point of failure or a specific time.

Typically transaction log backups do not require intensive resource usage and can be scheduled more frequently than other backup types. Ensure you increase the frequency of your transaction log backups if your database has a high transaction rate. Also, consider storing critical transaction log backups on fault-tolerant storage devices.

While you cannot execute a transaction log backup during a full or differential backup, you can during a file backup. Ensure you create database or file backups before backing up the transaction log. The transaction log contains only the database changes made after the creation of the last backup.

What is a file or filegroup backup?
Backs up either individual files or all files in a filegroup within a database. Backing up single files or filegroups allows you to restore only corrupted files. Restoring only corrupted files increases recovery speed. Consider file and filegroup backups when your database has one or all of the following attributes:

- Database size hinders regular full or differential backups
- Database can be unavailable for short periods of time only
- Specific files are either regularly corrupted, are more critical, or change more frequently than others

You can back up files or filegroups and transaction logs at the same time.

How to choose compression and encryption

SQLsafe offers a unique combination of state-of-the-art compression and encryption technologies. These technologies set SQLsafe apart and make it unique in the SQL Server backup arena. You designate the compression rate necessary to match your storage needs, and you select the level of encryption you need to ensure data security within your environment.

For more information on the compression levels available, see Understand compression levels and Understand IntelliCompress options. For information on how selecting the appropriate compression scheme reduces your storage costs,see Understand Total Cost of Operation (TCO)

SQLsafe automatically detects whether your environment requires compliance with the Federal Information Processing Standard (FIPS), and then chooses the appropriate encryption algorithm. For more information, see Ensure FIPS compliance.

Ensure FIPS compliance

You can use SQLsafe to back up and restore SQL Server databases in environments where Federal Information Processing Standard (FIPS) compliance is required. SQLsafe automatically detects whether the target SQL Server instances require FIPS compliant encryption. When this security setting is detected, SQLsafe uses the FIPS-compliant AES encryption algorithms provided by Microsoft.

For more information about FIPS compliance, see the corresponding Microsoft TechNet Web Article and Microsoft Knowledge Base Article.

How do I know whether my environment requires FIPS compliance?

Ask your Windows security administrator whether the FIPS system cryptography setting has been enabled in the Local Security Policy or a Group Policy that applies to the SQL Server computer.

Are there additional product requirements to support FIPS?

No, FIPS compliance for SQLsafe does not require any additional software to be installed.

Understand compression levels

SQLsafe allows you to set the compression rate suited to your backup needs. You designate a default compression level during the initial setup of SQLsafe. Any time prior to initiating a backup, you can modify your compression level.

How do I choose the best compression level for my environment?

The compression level that is best for your environment depends on your storage and performance needs. Before you choose a compression level, determine whether you need maximum storage and compression (lower performance) or maximum performance (lower compression).

Compression rates and backup times depend on the following factors:

- Whether the SQL Server computer utilizes multiple processors
- Whether you are striping data to multiple backup files
- Available bandwidth on your network connections
- Current processing load, such as backing up multiple databases in the same job
- The type of data you are backing up (for example, text compresses to a smaller size than binary data)

Level 1

Low compression. Provides high execution speed and minimal server load. This compression level typically provides 75-90% compression rates on text data. This compression rate may significantly decrease if you are backing up a database that contains binary data or previously compressed data.Use this compression level if you want to perform fast backups, sometimes during business hours, at the expense of a larger size.

In environments with a slow write speed, this level will not produce backups as fast as higher levels of compression.

Level 2

Medium compression. Provides good data compression while maintaining high-speed execution. This compression level places a moderate load on your server to provide increased compression. This compression level works well in environments with a good balance between multi-processor servers (for example, a 4- to 6-way SMP server) and IO speed.

Use this compression level if your environment includes one or more of the following conditions:

- You want to increase compression without significantly impacting performance
- You can schedule backups during off-hours, if needed

Level 3

High compression. Provides a high level of compression while slightly decreasing execution speed. This compression level provides significant reduction in backed up data size, while placing a higher load on your server. This compression level works well for nightly backups in environments with a powerful multi-processor servers (for example, an 8-way SMP server) where saving space is a high priority.

Use this compression level if your environment includes one or more of the following conditions:

- You want to maximize compression without significantly impacting performance
- You can schedule backups during off-hours, if needed

Level 4

Ultra-high compression. Provides the highest level of compression, to be used when saving space is critical. This compression level places a high load on your server. To achieve acceptable run times, this level should be used on very powerful servers with 8 or more processors and generally only during off-peak periods.

Use this compression level if reduction in backed up data size is your primary objective.

Understand encryption levels

SQLsafe allows you to set the encryption level most appropriate for your backup needs. During the initial setup of SQLsafe, you can select a default encryption level. Any time before executing a backup, you can strengthen or lessen the encryption applied to the current backup.

You must have a password in order to restore an encrypted backup. For security reasons, when you generate a T-SQL or CLI script of an encrypted backup, SQLsafe does not write the specified password to the script. To successfully run the script, supply the appropriate password. SQLsafe also does not store encryption passwords and cannot recover lost or forgotten passwords.

SQLsafe automatically detects whether the target SQL Server instances require FIPS compliant encryption. When this security setting is detected, SQLsafe uses the FIPS-compliant AES encryption algorithms provided by Microsoft. For more information about FIPS compliance, see Ensure FIPS compliance .

SQLsafe encryption offers you the following encryption methods, allowing you to choose based on your security needs:

None

Provides the fastest execution speed and does not encrypt backed up data.

Advanced Encryption Standard (AES) 128-bit

Provides a strong encryption. The AES algorithm encrypts data in 128-bit blocks using a 128-bit key.

Advanced Encryption Standard (AES) 256-bit

Provides a stronger encryption. The AES algorithm encrypts data in 128-bit blocks using a 256-bit key. This method provides more secure encryption than AES 128-bit.

Understand IntelliCompress

SQLsafe offers IntelliCompress compression levels to maximize compression performance for your backups. Each time you run a backup using an IntelliCompress compression level, SQLsafe analyzes your backup data and determines the best algorithm to use. This customization optimizes the performance, no matter how the backup data may have changed since the last backup. Analyzing the data each time you run a backup provides the best compression rate for each backup, so your data is compressed in the optimal way each time, saving you time and disk space.

IntelliCompress – Optimize for Speed (iSpeed)

Provides maximum performance by automatically optimizing for speed. At each backup, SQLsafe selects a compression ratio that provides the fastest backup in that environment. This compression level meets most storage and performance needs. We recommend this compression level, particularly if you are backing up databases that contain text data.

IntelliCompress – Optimize for Size (iSize)

Provides high compression by automatically optimizing for size. At each backup, SQLsafe selects the best mix of compression and speed based on CPU power and read/write speed.

How script generation works

You can generate CLI and T-SQL scripts for backup and restore operations through the Backup and Restore wizards. SQLsafe generates the CLI or T-SQL script using the settings you specified for the backup or restore operation.

CLI scripts can be run as a batch file from the command line prompt. Generated CLI scripts use supported options for the backup and restore actions.

T-SQL scripts can be run through Query Analyzer or as a scheduled SQL Server job. Generated T-SQL scripts leverage the SQLsafe XSP to execute backups and restores.

If you need a command line or T-SQL script for your backup or restore, SQLsafe provides the Generate Script button to let you generate CLI and T-SQL scripts for these operations. When you use a wizard to run a backup or restore, SQLsafe disables this button until sufficient criteria exists to generate a script. SQLsafe generates the CLI or T-SQL script using the settings you specified for the backup or restore operation.

How do I generate script?

You can generate script through the Backup Wizard or the Restore Wizard once your settings provide SQLsafe with enough information to create the script. Click Generate Script, and SQLsafe displays command line script by default. Click the T-SQL button and SQLsafe displays the script in T-SQL format.

To retain your script in either format, click the Save to a file or Copy script to clipboard icon. SQLsafe also allows you to use normal select, cut, copy, and paste functionality directly on the displayed script.

How threads affect backups and restores

By default, SQLsafe automatically calculates the optimal number of threads necessary to process a backup or restore operation. You can calculate the number of threads for your environment based on the processors available on the computer running the SQL Server databases you want to backup. Consider performing several backups to find the appropriate number of threads for your environment. To calculate the appropriate number of threads for your environment, use the following guidelines. Also consider other loads on the SQL Server computer that may affect CPU performance and availability.

Number of CPUs	Number of Threads
Single processor	1
Multiple processors	(number of CPUs)-1

You can set the appropriate number of threads when backing up a database through the Management Console. You can customize the number of threads you want SQLsafe to use when performing a backup or restore. A similar number of threads used in each operation ensures that you achieve the same performance optimization for your backups and restores.

For SQL Server 2000 instances, selecting 12 or more threads can cause the backup operation to fail.

Recover objects using SQL virtual database

SQLsafe integrates with SQL virtual database through the Backup Wizard and Backup Policy Wizard to provide you with a more powerful recovery solution.

SQL virtual database allows you to:

- Recover any object from the backup file without having to restore the database
- Analyze and report on objects and permissions in backup files without having to restore the database
- Access backup files as though they were read-only databases

When creating a backup or backup policy, you can check the option to generate metadata for use by SQL virtual database. This metadata includes data files for each database included in your backup. Generating metadata is optional; SQL virtual database can attach SQLsafe backup files without the metadata. However, these data files improve SQL virtual database performance during the creation of the virtual database.

If you have SQL virtual database installed, click Attach Virtual Database to launch the SQL virtual database Console. From the Console, you can create virtual databases from a single full backup file or multiple backup files. You can also create multiple virtual databases from the same backup file, which allows you to make virtual databases that include data from different points in time. Once created, the virtual databases can be fully managed and queried using Microsoft SQL Server Management Studio or another database management tool.

What is SQL virtual database?

SQL virtual database is a powerful one-of-a-kind solution that lets you attach SQL Server backup files and query them like real databases. With its revolutionary, patent-pending technology, you gain instant access to critical data in a backup file without spending the time and storage previously required for restore. In minutes, you can create a virtual database and then use any native SQL Server or third party tools to query and extract the data you need.

For more information about SQL virtual database, see the SQL vdb online Help

Are there disk space recommnedations for the SQL virtual database metadata?

Use the following table to help you set aside the appropriate amount of disk space for the virtual database metadata SQLsafe generates. Typically, this metadata requires only a fraction of the disk space consumed by a fully restored backup.

Size of Backup	Additional Disk Space
1 TB	105 MB
500 GB	51 MB
100 GB	10 MB
1 GB	105 KB
500 MB	51 KB

For more information about the virtual data files that SQL virtual database creates, see the SQLvdb online Help

Automate Backups and Restores

A SQLsafe policy consists of a set of databases for which a set of disaster recovery operations will be performed according to a defined schedule.

Backup policies allow you to quickly and easily schedule backups for large sets of databases that have similar needs. Log shipping policies allow you to schedule the synchronization of transaction logs between a primary database and one or more secondary databases. Restore policies allow you to schedule the routine recovery of a specific database.

You can use policies to enforce corporate standards or Service Level Agreement (SLA) requirements.

- Create a backup policy
- Create a log shipping policy
- Create a restore policy

How do I access policies?

To view status of any policy, click **Policies** in the navigation pane, and then select the appropriate policy listed in the tree pane. SQLsafe provides an at-a-glance record of your policy statuses.

You can view information about all your policies (per type) or view the status of an individual policy. You can also create new policies or edit existing policies from these views.

Deploy maintenance plans using SQLsafe

You can use the SQLsafe log shipping, backup, and restore policies to automate and enforce your disaster recovery requirements or Service Level Agreements (SLAs). Note that SQLsafe no longer provides the Maintenance Plan Conversion Utility.

How to use log shipping policies as maintenance plans

Use the following steps to create a new log shipping policy based on an existing SQL Server Log Shipping maintenance plan.

To create a log shipping policy based on a maintenance plan:

1. Use SQL Server Management Studio to connect to the SQL Server instances for which you have a native maintenance plan.
2. Disable the backup jobs associated with the primary instance.
3. Allow all restore jobs associated with the secondary instances to complete, and then disable these jobs.
4. Start the SQLsafe Management Console, and start the Log Shipping Policy wizard.
5. On each wizard window, specify the appropriate options, and then click **Finish**. Because the selected instances were previously included in a native maintenance plan, you do not need to initialize the secondary instances.
6. Test your new log shipping policy by tracking the policy status.
7. Delete your native maintenance plan.

How to use backup policies as maintenance plans

Use the following steps to create a new backup policy based on an existing SQL Server maintenance plan.

To create a backup policy based on a maintenance plan:

1. Use SQL Server Management Studio to connect to the SQL Server instances for which you have a native maintenance plan.
2. Disable the backup jobs associated with this plan.
3. Start the SQLsafe Management Console, and start the Backup Policy wizard.
4. On each wizard window, specify the appropriate options, and then click **Finish**.
5. Test your new backup policy by tracking the policy status.
6. Open your maintenance plan and delete the tasks that performed your backups, and then enable the appropriate jobs associated with this plan. ***If your maintenance plan performed backups only***, delete your native maintenance plan.

How to use restore policies as maintenance plans

Use the following steps to create a new restore policy based on an existing SQL Server maintenance plan.

1. Create a backup policy that archives the databases you want to routinely restore.
2. Test your backup policy by running the policy jobs. This action also creates source backup files for your new restore policy.
3. Use SQL Server Management Studio to connect to the SQL Server instances that have a native maintenance plan you want to replace.
4. Disable the backup and restore jobs associated with this plan.
5. Start the SQLsafe Management Console, and start the Restore Policy wizard.
6. On each wizard window, specify the appropriate options, and then click **Finish**.
7. Test your new restore policy by tracking the policy status.
8. Open your maintenance plan and delete the tasks that performed your backups and restores, and then enable the appropriate jobs associated with this plan. ***If your maintenance plan performed backups and restores only***, delete your native maintenance plan.

Backup policies

Backup policies allow you to define backup maintenance plans across multiple SQL Server instances in your enterprise. These instances can reside on one or more physical servers.

SQLsafe offers backup policies, restore policies, and log shipping policies to address different needs.

What is a backup policy?

A backup policy consists of a list of databases you want to back up, a set of backup operations to be performed on those databases, and a set of schedules according to which the backups will be performed. You can choose to create the associated jobs to run on a specific schedule, run on demand (execute the jobs manually from the Management Console), or you can choose to define your policy for monitoring purposes only. You can then monitor the status of each backup, all from a single point of contact in the Management Console.

How do I incorporate backup strategies in my policies?

Implementing a policy requires that you have a clear understanding of your backup strategy. To determine a backup strategy to use, consider the following recovery model requirements.

Model	Full Backup?	Differential Backup?	Transaction Log Backup?	File or Filegroup Backup?
Simple Model	Required	Optional	N/A	N/A
Full Model	Required	Optional	Required	Optional
Bulk-Logged Model	Required	Optional	Required	Optional

What constitutes a good backup strategy?

Consider using all four backup types to maximize your recovery and minimize your data loss. A basic backup strategy fulfills the following needs:

1. Creation of regularly scheduled database backups
2. Creation of frequent differential backups between full backups
3. Creation of transaction log backups more frequently than differential backups

Database backup creation depends on server activity and data sensitivity. Ensure you implement a strategy and create policies that back up both user databases and system databases.

How do backup policies help me?

Backup policies allow you to plan and schedule your SQL Server backup maintenance, as well as monitor its success and failures, all from a single point of contact at the Management Console. By allowing the application and scheduling of a set of backup operations across all of your SQL Server instances enterprise-wide, SQLsafe policies make updating your maintenance plans a quick and easy process.

Create a backup policy

The SQLsafe Backup Policy wizard allows you to create backup maintenance plans across your enterprise. A SQLsafe Backup Policy is defined as a set of databases for which a set of backup operations will be performed according to a defined schedule. If you choose to create backup jobs for this policy, SQLsafe creates SQL Server jobs for the specified backups.

How do you access the Backup Policy wizard?

You can access the Backup Policy Wizard from any of the following paths:

- Go to the task bar, click **Create Policy** and then choose **Backup Policy**.
- On the Policies tab, click **Create New Policy** located on the **Operation Summary** section of the **Backup Policies Status** window. This option is only available before you create your first backup policy.
- On the Policies tab, right-click the Backup Policies folder and select **Create Backup Policy**.
- From any tab, go to the **File** menu, select **Create Policy** and then **Backup Policy**.
- You can also find this option on the **SQLsafe Today** view, by going to the **Common tasks** and then selecting **Create New Policy**.

To get started with the Backup Policy wizard:

1. Name the policy.
2. Select the databases you want to back up.
3. Select backup options.
4. Specify where you want to store the backup files.
5. Schedule when and how often you want the backup to occur.
6. Get email notifications about the policy status.

Name the policy

The General tab of the Backup Policy wizard allows you to specify the basic properties of the backup policy.

Why should I specify a name or description?

You are required to enter a unique name for each policy.

Both the name and description will appear in the status messages for your policies. Using a meaningful name and description will allow you to more easily identify problems when they occur. For example, consider specifying a description that will help you later choose the correct backup to restore during a disaster recovery situation.

Which policy action should I choose?

Choose the action that best reflects how you want to use this policy. You have two options in this section:

- Monitor and automatically create backup jobs using the SQL Server Agent
- Monitor and automatically create backup jobs using the SQLsafe Backup Agent
- Monitor only

The first option allows you to create the policy for monitoring database backups and automatically creates the backup jobs using the SQL Server Agent on your SQL Server instances. Creating jobs allows to enforce consistent backup settings across your environment.

The second option allows you to create the policy for monitoring database backups and automatically creates backup jobs using the SQLsafe Backup Agent which is in charge of executing and scheduling these policies.

The third option creates the policy only to monitor database backups and no jobs are created. By default, SQLsafe will monitor the status of any backup operation that meets the criteria of your policy.

Take into account that if you add any instance with SQL Server Express in your policy, you should choose the first option since SQL Server Express does not support the SQL Server Agent. Select the SQLsafe Backup Agent (second option) for creating your policy backup jobs.

If you choose to use the SQLsafe Backup Agent, policy data files will be stored by default at *C:\Program Files\Idera\SQLsafe\PolicyData*. You can change these settings by going to the **Policy Data** tab on the Management Console Preferences and selecting or creating the folder directory where you want to store these files.

Select databases

Use the Membership tab of the Backup Policy wizard to select which SQL Server instances and databases you want to monitor with this policy. You can also exclude one or more databases from this policy.

To make your selections, click **Add/Remove Instances**, and then choose the instances from where you want to backup databases. Then select from the different options for choosing databases (**All Databases, All User Databases, All System Databases, Specific Databases**). By choosing one of the "All" database options, the policy will automatically include the relevant databases as they are added or removed on the server.

You may select databases from different servers for one policy.

When you choose the databases you need to backup you can also specify those ones that you want to exclude from your policy, for this option move the ones you want to exclude to the list on the left.

Configure options

The Options tab of the Backup Policy wizard allows you to enter the backup types and options for each operation included the backup policy.

What information is on this tab?

For each backup operation you include in the backup policy, you can select compression, encryption, and verification options, enable object-level recovery, and set additional advanced options such as removing inactive entries from the transaction log.

What types of backup can you choose?

On the Options tab you can choose the types of backups you want for your backup policy. You can specify one, two or the three types of backup: **Full, Differential, Log**, just select the respective backup types and provide their settings.

Why can´t you see the options for all the backup types?

The options for each backup type are hidden unless the backup type is selected for the policy. For more information about backup types, see Understand backup types.

What types of compression algorithms are available?

- None
- IntelliCompress, optimize for size (iSize)
- IntelliCompress, optimize for speed (iSpeed)
- Levels 1, 2, 3, 4

Backup operations using Level 1 complete fastest but achieve the least amount of compression. Level 4 achieves maximum compression but the backup operation may take longer.

For more information about backup compression, see How to choose compression and encryption.

What types of encryption algorithms are available?

- None
- AES (128-bit)
- AES (256-bit)

If your SQL Server environment requires FIPS compliance, use the AES encryption option. For more information, see Ensure FIPS compliance.

When you choose to encrypt an archive, you must designate a password. For security reasons, SQLsafe does not store this password. Ensure you remember the password you select.

What additional options are available?

For each type of backup you select, you can also specify the following advanced options:

Options	Description
Verify the integrity of the backup when complete	Performs a data integrity check after the backup is created. SQLsafe verifies the integrity of the data files in the backup set created by this backup. Verifying the backup helps identify potential issues that could occur when restoring these data files.
Generate maps	Generates maps containing metadata for each database included in your backup file. Depending on the number of transactions completed since your last backup, generating maps may impact the performance of the backup operation. Generating maps is optional, but must exist in the backup file for InstantRestore to accept and restore that file. SQL virtual database can attach SQLsafe backup files without the metadata, but the data files improve SQL vdb performance during creation of the virtual database. For more information, see Recover objects using SQL virtual database. This option is selected by default.
Include database logins in backup file	Copies SQL login information for the selected databases, including credentials and privileges, when the backup files are written. To help ensure the security of your SQL Server database, SQLsafe encrypts the login information. This option is available for full backups only.

Thread Count	Allows you to specify how many threads you want SQLsafe to use to distribute the backup operation across multiple processors on the target SQL Server computer. Use this setting to optimize backup performance. When the resultant backup file is restored, SQLsafe uses the same thread setting to ensure consistent performance. Select **Auto** to have SQLsafe determine the optimal thread count for your environment.
Transaction Log	Removes all completed transactions, inactive entries, from the transaction log after SQLsafe finishes the backup.
Checksum: Generate	Generates a checksum for the backup file.
Checksum: Ignore Errors	Ignores any errors from the generated checksum. ***If checksum errors are encountered***, this option indicates that SQLsafe should continue to back up this database.
Backup: Copy only	Specifies a copy-only backup. This is a copy of the database and cannot be used as part of a restore strategy. It will allow you to take a "snapshot" backup of your database without interferring the LSN (log sequence number) order of your backup strategy.
Backup: Read-write filegroups	Specifies a partial backup, which includes the primary filegroup and any read-write secondary filegroups. Read-write filegroups are not supported by SQL virtual database. ***If this option is selected***, the **Generate metadata** option (Generate maps for InstantRestore and SQL virtual database) will be disabled. Additionally, backups created with the read-write filegroups option cannot be used by SQL virtual database to create virtual databases.

Select location

The Locations tab of the Backup Policy wizard allows you to specify the backup location for each operation you include in the backup policy.

What information is on the Locations tab?

For each operation you have included in the backup policy, you can specify the location type, full path in which to store the backup file, an optional housecleaning schedule for existing disk archives, and the backup file extension.

What types of backup locations can you use?

SQLsafe supports the following location types:

- Back up to a single file on the local computer or a network share
- Back up to multiple striped files on the local computer or a network share
- Back up to tape using Tivoli Storage Manager

What do you do if you don´t have an existing archive?

If you do not specify an existing archive, SQLsafe creates a new backup set with the name you specify. The location entered for each backup type must be valid for all SQL Server instances.You can choose to **Append** or **Overwrite** if the archive already exists.

What accounts can you specify to access the backup files location?

Depending whether you selected to use the SQL Server Agent or the SQLsafe Backup Agent for the scheduling of your policy, on this section you have the option to select between SQL Server Agent service account/SQLsafe Backup Agent service account respectively or a Windows account. Click **Account** and select your preferred option.

The account specified must have read and write privileges on the directory selected for your backup file location.

How do you keep my backups running despite network errors?

Select **Enable network resiliency** and then click **Configure** to change the default settings. By default, SQLsafe will retry the backup operation every 10 seconds and then fail after 5 minutes (300 seconds) of continuous errors. Also, over the course of the operation, SQLsafe allows a total of 60 minutes in which to retry the backup before stopping the operation.

This option is not available when backing up to tape using Tivoli Storage Manager.

Can you change the default file locations?

SQLsafe automatically populates the path using several available variables, depending on location type. You can modify this path to suit your needs, taking advantage of all the available variables.

For a disk backup, browse for or enter the directory in which to store the backup file. You can use the supplied macros in the way best suited to your storage needs. If you want to limit the lifetime of your backup sets created by the policy, you can select the option that removes files older than the specified time.

For a TSM backup, browse for or enter the high level directory for the tape file. You can use the supplied macros in the way best suited to your storage needs. Browse for or enter the location of the TSM configuration file.

What does removing old files do?

For backups written to a single file or mirrored files, you can choose to remove old files to prevent disk space limitations. When you select to remove files older than the specified time, backup files created with names of the same format will be deleted from that directory. You can configure SQLsafe to delete old backup files from the primary archive as well as from your mirror archives.

For backups written to a TSM Server, you can configure SQLsafe to mark these files as inactive after a specified age.

How do you mirror the backups this policy creates?

Click **Mirror Archives** , and then specify where you want the mirrored files to be stored.

For each mirror, SQLsafe creates a copy of the backup archive set. You can specify up to 2 mirrors for each backup operation.

Keep in mind that creating mirrors can impact the performance of your backup operation.

If you want to stop the backup operation when mirror location is unavailable , select **Abort backup if a mirror location reports a failure**.

You can also enable to remove files older than a specified time.

What do I specify when backing up to a TSM Server?

When a TSM location is selected, you must specify the following settings:

- high level file path
- low level file path
- the location of the TSM Client configuration file that enables generate password for authorization

You can also configure SQLsafe to mark these files as inactive after a specified age.

SQL virtual database is not available when backing up to a TSM Server.

Configure schedule

The Schedules tab of the Backup Policy wizard allows you to schedule the frequency and duration of your backup operations. For each backup type, enter the appropriate information into each of the schedule fields to satisfy your backup requirements.

What information is on the Schedules tab?

For each operation you have included in the policy, you can specify when your operation will begin, how frequently backup jobs will be executed, and the respective duration for these operations. You can also choose to run the operation "On Demand," allowing you to easily manually execute the associated jobs according to your preset options.

How do I know what frequency to set?

The schedule of your operations should be determined by how much data you can afford to lose in the event of a catastrophic failure. The schedule should be developed in concert with your backup strategy. For example, for lab or development instances, you may want to schedule on-demand or weekly backups whereas for critical production instances you may want to schedule full backups every day with transaction log backups every hour.

Can I set a different schedule for each backup operation?

Each backup operation can have a different schedule. For instance, perhaps you decide you want to run full backups monthly, differential backups once a week, and transaction logs during business hours every day.

How do I set the schedule?

You can set up a schedule by defining the following options:

Field	Description
Occurs	Unit of Frequency: On Demand, Daily, Weekly, Monthly
Daily Frequency	Time of day: • Occurs once at `HH:MM:SS AM/PM` • Occurs every `N` Hours/Minutes starting at `HH:MM:SS AM/PM`, ending at `HH:MM:SS AM/PM`
Duration	Length of time: • Start date `mm/dd/yyyy` • End date `mm/dd/yyyy` or no end date

When an operation does not occur as scheduled, the backup policy will consider it "missed" and SQLsafe can notify you about it if you configured it to do so.

Configure notifications

The Notifications tab of the Backup Policy wizard allows you to choose the backup statuses about which you want to receive alert notifications through email. Email notifications let you, and your staff, remotely monitor the status of the backups you have automated with this policy.

The status of the backup operations determine the status of your policy.When your backups are successfully completed on scheduled, the policy is considered ok.

Choose the status you want to monitor, type the email address of each recipient, select the desired alert frequency for each operation, and then click **Next.**

You must configure your mail server settings before SQLsafe can send e-mail notifications. Click **Configure E-mail** to check your settings. For more information, see Configure e-mail settings for alert notifications.

When is the email sent?

SQLsafe sends an email to the specified recipients when the selected operation status occurs. Because SQLsafe checks the status of your backup operations every minute, your alert notifications provide a real-time indication of the health of your service level agreements and disaster recovery plans for the SQL Server instances covered by this policy.

However, how often you are emailed about a specific status update depends on the notification frequency setting you select. For example, if you want to receive an email whenever a backup fails, even when the failures occur sequentially, choose to receive notifications every time the event occurs.

Review details

The Summary tab of the Backup Policy wizard provides the summary of specified values and options you have selected in the Backup Policy wizard. After you review the information on the Summary tab, click **Finish** to create the policy and corresponding backup jobs.

If you want to create the policy but not the backup jobs, return to the General tab and select the **Monitor Only** action.

View the status of all backup policies

When **Backup Policies** is selected in the **Policies** tree pane, the content pane displays information describing the overall status of all of these policies. Use this view to quickly determine whether your servers are in compliance with your corporate backup policies.

What does the Current Status mean?

The **Current Status** displays the most recent, combined status of all operations performed by your backup policies. Even though there are multiple operation statuses, the overall policy status reflects the most critical operation status. When all backups have been completed successfully according to the policy schedule, a green OK icon is displayed.

What is the Last Operation Status?

The **Last Operation Status** shows an overview of the most recent backup, restore, or log shipping operations that occurred across your enterprise. Use this view to quickly determine whether your servers are in compliance with your corporate policies.

What is the Operation Summary?

The **Operation Summary** displays a listing of all policies, providing information in the following columns:

Column Header	Definition
Status	Displays either a green OK status bar, a yellow warning status bar, or a red error status bar.
Name	Displays the policy name.
Databases Covered	Displays the number of databases being backed up by the policy.
Last Backup Time	Display the date and time of the most recent backup operation (of any type defined by the policy).
Last Backup Failure Time	Displays the date and time of the most recent backup failure (of any type defined by the policy).

How do you get details about a specific policy?

You can get more details about the status of a specific policy by double-clicking on one of the policy operations in the **Operation Summary** grid or by choosing the respective policy on the Backup Policies folder tree node.

Can you customize the columns in the grid?

You can sort by the content of any of the columns by clicking on the column header.

How do you refresh the operations status?

If a recent operation does not appear in the status view, you can refresh the status of this pane by clicking the **Refresh** icon in the pane title bar.

View status of a specific backup policy

When a specific backup policy is selected from the Backup Policies tree node, the content pane displays information describing the status of that policy. Use this view to determine which backup operations initiated by the policy have succeeded or failed.

What actions can you perform?

From the Policies tree

By right-clicking on a policy under the Backup Policies node, you can access the following shortcuts:

Action ...	What it does ...
Create Backup Policy	Opens the Backup Policy wizard, allowing you to create a new policy.
Edit Policy	Opens the Backup Policy wizard (with all options pre-set to the values used for this operation), allowing you to edit any of the options.
Delete Policy	Allows you to delete the policy. Although backup operations associated with this policy will no longer be performed, the previous backup files and status messages created by this policy will continue to be stored in the SQLsafe Repository.
Disable Policy	Allows you to disable the selected policy. Backup operations associated with this policy will no longer be performed and will turn off any email notifications you have configured to alert on the backup or restore status.
Start Jobs for Policy	Allows you to run the backup jobs associated with this policy, performing an ad-hoc backup with the options already set by the policy.
Refresh Policy List	Updates the Backup Policies node with the latest policies.

From the Current Status pane

By clicking the links available in the Current Status pane, you can access the following shortcuts:

Action ...	What it does ...
View Policy Settings	Allows you to view a summary of the policy settings.
Edit Policy	Opens the Backup Policy wizard, allowing you to change your policy settings.
Disable Policy	Disables the selected policy. Once a policy is disabled, it will no longer perform backup operations for the associated databases. To back up a database that belongs to a disabled policy, perform a manual backup using the Backup wizard.
Start Full Backups	Performs a full backup of all databases that belong to this policy by running the corresponding job. This action applies your previously defined policy settings, and is only available when your policy includes a full backup operation.
Start Diff Backups	Performs a differential backup of all databases that belong to this policy by running the corresponding job. This action applies your previously defined policy settings, and is only available when your policy includes a differential backup operation.
Start Log Backups	Performs a transaction log backup of all databases that belong to this policy by running the corresponding job. This action applies your previously defined policy settings, and is only available when your policy includes a log backup operation.

From the Operation Summary grid

By right-clicking a backup operation, you can access the following shortcuts:

Action ...	What it does ...

View Details	Shows the Details pane, providing additional information about the selected backup operation such as Statistics, Result text, Files, Backup Set Description, Storage Options.
Back up again	Runs the backup operation again, using the same settings.
Back up with Different Options	Opens the Backup wizard (with all options pre-set to the values used for this operation), allowing you to specify different options before running the operation.
Verify backup	Verifies that the backup file is "good" and can be restored with all data intact.
Restore database	Opens the Restore wizard, allowing you to restore this backup file.
Set Progress To	Allows you to change the status of the selected operation to Complete, Complete, warning, Error, Canceled, Skipped or Deleted.
Close Details	Hides the Details pane.

By right-clicking a verify operation, you can **Verify Again**, **Verify with Different Options** and **Set Progress to** different statuses.

When you select **Verify with Different Options**, the Restore Wizard opens with the Verify option enabled. Use this wizard to set specific settings for this verify operation.

What does the Current Status mean?

The Current Status displays the most recent, combined status of the backup operations performed by this policy. When there are multiple operation statuses, the policy status reflects the most critical operation status. When all backups have been completed successfully according to the policy schedule, a green ok icon is displayed.

What is the Last Operation Status?

The Last Operation Status shows an overview of the most recent backup occurred across your enterprise. Use this view to quickly determine whether your servers are in compliance with your corporate policies. The operation status is limited to backup operations performed by this policy. Click any backup operation to see more details about it, including the reasons for failed or skipped backup operations if applicable.

What are the Operation Details?

The Operation Details grid displays a listing of all backup and restore operations performed for the databases included in the selected policy for the last 7 days. This grid includes the following columns:

Column	Definition
Progress	During an operation, the progress bar will denote the percentage of the operation completed. When the operation is complete, it will display a green bar labeled 100%. If an operation completed with errors, this column will display a red bar labeled Error.
Instance	Displays the instance name that was backed up by this operation.
Icon	Displays an icon if the backup includes maps containing metadata for InstantRestore and SQL virtual database. For more information about InstantRestore, see How InstantRestore works. For information about SQL virtual database, see Recover objects using SQL virtual database.
Database	Displays the database name that was backed up by this operation.
Operation	Displays the operation performed. The options are Backup and Verify.
Backup Type	Displays the type of the backup performed by the operation. The options are Full, Transaction Log, Differential, and File.
Compressed	Displays the compressed file size of the backup.
Ratio	Displays the percentage of the data that was compressed.
Compression	Displays the type of compression that was used for this backup.
Duration	Displays the number of seconds required to complete the operation.
Start Time	Displays the start date and time of the operation.

Can I customize the columns in the Operation Details grid?

You can sort by the content of any of the columns by clicking the column header.

You can select which columns are visible in this grid, and enable column grouping, by clicking the **Filter** icon in the pane title bar.

How do I refresh the data displayed in the Operation Details grid?

Yes. If a recent operation does not appear in the status view, you can refresh the status of this pane by clicking the **Refresh** icon in the pane title bar.

What are the details?

To see the detailed results of a specific operation, click the operation in the Operation Details grid. The Details pane displays below. By default, this pane is hidden.

The Details pane provides the following information about the selected backup operation:

Tab	Description
Statistics	Displays the database size, the size of the uncompressed backup, the size of the compressed backup, and the compression ratio achieved with this backup. The ratio is a measure of the storage savings achieved with SQLsafe compression technology. For more information about the storage space savings you can realize using SQLsafe, see Understand your total cost of operation (TCO).
Result Text	Displays text describing the result of the backup.
Files	Displays the complete path of the backup set file for the backup.
Backup Set Description	plays the description you specified for this backup.
Storage Options	Displays which locations were chosen to store the backup files.

Log shipping policies

Log shipping policies allow you to ship transaction logs between multiple SQL Server instances in your enterprise, on a scheduled basis. These instances can reside on one or more physical servers.

SQLsafe offers log shipping policies, backup policies, and Restore policies to address different needs.

What is a log shipping policy?

A log shipping policy consists of primary and secondary databases you want to synchronize, a set of transaction log backup and restore operations to be performed on those databases, and a set of schedules according to which these operations will be performed. You can also choose to mirror the backup files, storing copies of the transaction logs in multiple secured locations. You can then monitor the policy status, all from a single point of contact in the Management Console.

How do log shipping policies help me?

Log shipping policies allow you to implement a disaster recovery strategy for your entire SQL Server environment. You can use log shipping polices to synchronize, or back up and restore, one database to another. Using a log shipping policy to synchronize databases also helps you save disk space and network bandwidth, and comply with security requirements, because each transaction log backup can be compressed and encrypted.

Create a log shipping policy

The SQLsafe Log Shipping Policy wizard allows you to create log shipping maintenance plans across your enterprise. A SQLsafe log shipping policy is defined as a set of primary and secondary databases whose data is synchronized by shipping transaction log backups according to a defined schedule.

How do you access the Log Shipping wizard?

You can access the Log Shipping Policy Wizard from any of the following paths:

- Go to the task bar, click **Create Policy** and then choose **Log Shipping Policy**.
- On the Policies tab, click **Create New Policy** located on the **Operation Summary** section of the **Log Shipping Policies Status** window. This option is only available before you create your first log shipping policy.
- On the Policies tab, right-click the Log Shipping Policies folder and select **Create Log Shipping Policy**.
- From any tab, go to the **File** menu, select **Create Policy** and then **Log Shipping Policy**.

To get started with the Log Shipping Policy wizard:

1. Name the policy.
2. Select the primary database that you want to back up.
3. Specify where these transaction log files should be stored.
4. Select backup options.
5. Select the secondary database you want to synchronize with the primary.
6. Get e-mail notifications about the policy status.

Name the log shipping policy

The General tab of the Log Shipping Policy wizard allows you to specify the basic properties of the log shipping policy.

Why should you specify a name or description?

You are required to enter a unique name for each policy.

Both the name and description will appear in the status messages for your policies. Using a meaningful name and description will allow you to more easily identify problems when they occur. For example, consider specifying a description that will help you later choose the correct backup to restore during a disaster recovery situation.

What options are available for creating a log shipping policy?

When you create a log shipping policy, you can choose between the two following actions:

- Create Backup and Restore Jobs using the SQL Server Agent
- Create Backup and Restore Jobs using the SQL Safe Backup Agent

How does SQLsafe determine that a log shipping policy is okay?

SQLsafe determines that the policy is okay by looking at the following statuses:

- Whether the transaction log backup on the primary database has completed on schedule
- Whether the transaction log restore on the secondary database has completed without warnings or errors
- Whether the data on the secondary database is stable

How do you control when a log shipping policy is compliant?

You can control how SQLsafe determines a missed backup by changing these options:

- Select a time limit for the log backup to occur. This is the leeway time allowed for the log backup to occur. If the log backup occurs within this period from the scheduled time, the policy is still compliant.
- Select an age limit for the secondary's data. This is the tolerance level for how old the data in the secondary database can be.

Select the primary database

Use the Primary tab of the Log Shipping Policy wizard to select which SQL Server instance will be the primary source for the log files. This is the database you will be backing up using log shipping.

What information is required on this tab?

SQL Server

The SQL Server that contains the database to be backed up. Select a registered SQL Server or click **Register** to register a new instance.

Database

Select the database from which you will ship the backup logs.

Backup Job

The schedule for how often the backup job will occur. By default, SQLsafe schedules this job to occur every day, every 15 minutes between 12:00 AM and 11:59 PM and to start on the current date. Click **Schedule** to change the frequency and start date.

Backup Options

Click **Backup Options** to change the compression and encryption methods.

The Backup Options window of the Log Shipping Policy wizard allows you to change the methods used for compression and encryption, and the number of threads used when performing a backup.

What types of compression algorithms are available?

- None
- IntelliCompress, optimize for size (iSpeed)
- IntelliCompress, optimize for speed (iSize)
- Levels 1, 2, 3, 4

Backup operations using Level 1 complete fastest but achieve the least amount of compression. Level 4 achieves maximum compression but the backup operation may take longer.

For more information about backup compression and encryption, see How to choose compression and encryption.

What types of encryption algorithms are available?

- None
- AES (128-bit)
- AES (256-bit)

If your SQL Server environment requires FIPS compliance, use the AES encryption option. For more information, see Ensure FIPS compliance.

When performing a backup, ensure the backup does not truncate the transaction logs of the database. Truncating the log will cause this log shipping policy to fail.

Select location for log shipping

The Location tab of the Log Shipping Policy wizard allows you to specify the location for the backups you are creating with this log shipping policy. Backups must be stored to a network path that all servers in the policy can write to.

What options can you set on this tab?

Access Filesystem As

This is the account SQLsafe will use to access the specified primary and mirror locations. Depending whether you selected to use the SQL Server Agent or the SQLsafe Backup Agent for the scheduling of your log policy, on this section you have the option to select between SQL Server Agent service account/SQLsafe Backup Agent service account respectively or a Windows account. Click **Account** and select your preferred option.

Enter a user account that has access rights to the target locations. The user account used must have read and write permissions to the specified resource.

You can also choose how to handle errors encountered while writing to the network during a backup by selecting **Enable network resiliency.** By default, SQLsafe will retry the backup operation every 10 seconds and then fail after 5 minutes (300 seconds) of continuous errors. Also, over the course of the operation, SQLsafe allows a total of 60 minutes in which to retry the backup before stopping the operation.

Primary Location

This is the first location where the backup files will be stored. By default, SQLsafe will ship the backup files from this location to your secondary server. When you configure the secondary database settings , you can specify an alternate location.

Enter the network path or click **Browse** to select the location of where you want the log backup archive to be kept. The destination folder must be configured as a network share.

SQLsafe detects if the Computer Browser service is not running on your computer. This service enables Windows to list other computers on the network, if this service is not running, Windows may not be able to list the computers on your network. SQLsafe allows you to start this service but keep in mind that it may take several minutes for computers to become visible.

You can also specify how long you want to keep old backup files. By default, SQLsafe will delete files older than three (3) days.

Mirror Locations

These are the locations where copies, or "mirrors", of the backup files will be saved. For each mirror location, SQLsafe creates and stores a copy of the backup files. You can specify up to 2 mirrors for each log shipping operation. Keep in mind that creating mirrors can impact the performance of your log shipping operation.

You can also specify:

- How long you want to keep old backup files. By default, SQLsafe delete files older than three (3) days
- Whether SQLsafe should cancel the backup when one of the specified mirror locations reports a failure, such as connection timeout.

How do you keep your backups running despite network errors?

Select Retry writing backup files after network errors, and then click Configure to change the default settings. By default, SQLsafe will retry the backup operation every 10 seconds and then fail after 5 minutes (300 seconds) of continuous errors. Also, over the course of the operation, SQLsafe allows a total of 60 minutes in which to retry the backup before stopping the operation.

This option is not available when backing up to tape using Tivoli Storage Manager.

Select secondary databases

Use the Secondary(s) tab of the Log Shipping Policy wizard to select the SQL Server instances and databases where the log backups will be restored.

From here, you can add, edit, or remove secondary databases. Each database can be restored with different options, schedule, recovery mode, etc. For more information about adding secondary databases, see Specify secondary database settings for the log shipping policy.

Configure secondary options

Use this window to select the SQL Server instances you want to synchronize with the log backups from the primary database.

What options are available in this window?

SQL Server

The SQL Server that contains the database to be restored. Select a registered SQL Server or click **Register** to register a new instance.

Database

Create a new database or select the database that you want to receive the transaction log restores. To create a new database, type directly the database name in the **Database** field. If you want to select an existing database, click **Select** to access the list of databases available on the instance you have selected.

Initialization

Specifies the initial state of the secondary database that receives the transaction log restores. Click **Change** to modify the type of initialization that will be performed.

By default, SQLsafe initializes the database with a newly-generated full backup.

SQLsafe detects when the primary database was previously configured to use the simple recovery model and requires for a new full backup to be performed to initialize the secondary database for the new log shipping policy. Full backups of a database using the simple recovery model lack log checkpoint information necessary for subsequent log restores.

When you click **Change** , a window for Database Initialization options opens where you can choose:

- Do not initialize. Database exists and has received most recent backup of primary database.
- Initialize database with a newly generated full backup. This will be the only option available when SQLsafe detects that the primary database was previously configured to use the simple recovery model and requires for a new full backup to initialize the secondary database.
- Initialize database with these backups. If you enable this option, you can specify the location of the backups and add encryption settings.

You can also click **Database File Locations** in this window to choose where to store your database files.

Database State

Select the recovery mode the secondary database is left in after each log restore.

This setting affects how the status appears for the secondary database. If you select **Not Accessible** (No recovery mode) , then the secondary database shows the status as "Restoring" and it is unusable. If you select **Accessible but read-only** (Standby mode) , then the database is in a read-only state. In the latter option, you can choose to disconnect users when performing restore.

Restore Job

This is how often the restore will occur. Click **Schedule** to change the frequency. By default, the restore occurs every 15 minutes every day, but you can specify other settings for your required daily frequency and duration of the job.

You can also choose to delay the restores by a number of minutes or hours. This represents the minimum time within which a secondary can be synced. For example, setting this value to 15 minutes would mean that the secondary will always be at least 15 minutes out of sync.

Restore From

Specify the location that will contain the transaction log backup files you want to restore (ship) to this secondary database.

To use the network path you previously specified for the transaction log backup location, click **Same location as backup**.

To restore from a different location, click **Different location**, and then specify the appropriate network path.

Take into account that to restore from a different location, the database must already be initialized.

Configure notifications for log shipping

The Notifications tab of the Log Shipping Policy wizard allows you to choose the log shipping statuses about which you want to receive alert notifications through email. Email notifications let you, and your staff, remotely monitor the status of the backups and restores you have automated with this policy.

The status of the log shipping operations determine the status of your policy.When your backups and restores are successfully completed on schedule, the policy is considered okay.

Choose the status you want to monitor, type the email address of each recipient, select the desired alert frequency for each operation, and then click **Next.**

You must configure your mail server settings before SQLsafe can send email notifications. Click **Configure E-mail** to check your settings. For more information, see Configure e-mail settings for alert notifications.

When is the email sent?

SQLsafe sends an email to the specified recipients when the selected operation status occurs. Because SQLsafe checks the status of your backup and restore operations every minute, your alert notifications provide a real-time indication of the health of your log shipping policy and your primary and secondary servers.

However, how often you are emailed about a specific status update depends on the notification frequency setting you select. For example, if you want to receive an email whenever a backup fails, even when the failures occur sequentially, choose to receive notifications every time the event occurs.

Review details for log shipping

The Summary tab of the Log Shipping Policy wizard provides the summary of specified values and options you have selected in the Log Shipping Policy wizard.

What do you do next?

After you have reviewed the information on the Summary tab, click **Finish** to create the policy and corresponding log shipping schedule. SQL safe opens a window with the list of tasks for your policy and verifies them.

View status of all log shipping policies

When Log Shipping Policies is selected in the Policies tree pane, the content pane displays information describing the overall status of all of these policies. Use this view to quickly determine whether your servers are in compliance with your corporate log shipping policies.

What does the Current Status mean?

The Current Status area displays the most recent, combined status of all backup and restore operations performed by your log shipping policies. Even though there are multiple operation statuses, the overall policy status reflects the most critical operation status. When all backups and restores have been completed successfully according to the policy schedule, a green okay icon is displayed.

What is the Last Operation Status?

The Last Operation Status shows an overview of the most recent backup, restore, or log shipping operations that occurred across your enterprise. Use this view to quickly determine whether your servers are in compliance with your corporate policies. Click the status to see more detail about your operations.

What is the Operation Summary?

The Operation Summary area displays a listing of all policies, providing information in the following columns:

Column Header	Definition
Status	Displays either a green Compliant status bar, or a red Non-Compliant status bar.
Name	Displays the policy name.
Databases Covered	Displays the number of databases being backed up by the policy.
Last Operation	Display the date and time of the most recent operation (of any type defined by the policy).
Last Operation Failure	Displays the date and time of the most recent failure (of any type defined by the policy).

How do you get details about a specific policy?

You can get more details about the status of a specific policy by double-clicking the policy operation in the Operation Summary grid.

Can you customize the columns in the grid?

You can sort by the content of any of the columns by clicking the column header.

How do you refresh the operations status?

If a recent operation does not appear in the status view, you can refresh the status of this pane by clicking the **Refresh** icon in the pane title bar.

View status of a specific log shipping policy

When a specific log shipping policy is selected in the tree pane, the content pane displays information describing the status of that policy. Use this view to determine which backup or restore operations initiated by the policy have succeeded or failed.

What actions can you perform?

From the Log Shipping Policies tree

By right-clicking a policy under the Log Shipping Policies node, you can access the following shortcuts:

Action ...	What it does ...
Create Log Shipping Policy	Opens the Log Shipping Policy wizard, allowing you to create a new policy.
Edit Policy	Opens the Log Shipping wizard (with all options pre-set to the values used for this operation), allowing you to edit any of the options.
Delete Policy	Allows you to delete the policy. Although backup operations associated with this policy will no longer be performed, the previous backup files and status messages created by this policy will continue to be stored in the SQLsafe Repository.
Disable Policy	Allows you to disable of the selected policy. Backup and restore operations associated with this policy will no longer be performed and email notifications configured on these jobs will be turned off.
Re-Initialize Secondary Database	Allows you to re-initialize any of the secondary databases associated with the selected policy.
Refresh Policy List	Updates the Log Shipping Policies node with the latest policies and their statuses.

From the Current Status pane

By clicking the links available in the Current Status pane, you can access the following shortcuts:

Action ...	What it does ...
View Policy Settings	Allows you to view a summary of the policy settings.
Edit Policy	Opens the Log Shipping Policy wizard, allowing you to change your policy settings.
Disable Policy	Disables the selected policy. Once a policy is disabled, it will no longer ship transaction logs to the secondary databases and it will no longer send email notifications configured for the respective jobs.
Start Log Backups	Performs a transaction log backup of the primary database that belongs to this policy by running the corresponding job. This action applies your previously defined policy settings.
Start Log Restores	Performs a transaction log restore on the secondary databases that belongs to this policy by running the corresponding job. This action applies your previously defined policy settings.

What does the Current Status mean?

The Current Status displays the most recent, combined status of the backup and restore operations performed by this policy. When there are multiple operation statuses, the policy status reflects the most critical operation status. When all backups and restores have been completed successfully according to the policy schedule, a green okay icon is displayed.

What is the Last Operation Status?

The Last Operation Status shows an overview of the most recent backup, restore, or log shipping operations that occurred across your enterprise. Use this view to quickly determine whether your servers are in compliance with your corporate policies. The operation status is limited to the operations performed by this policy.

What are the Operations Details?

The Operation Details graphic provides the following status details for the primary and secondary databases that belong to the selected policy:

Detail	Description
Icons	Indicate whether primary and secondary databases remain compliant with the backup and restore schedules defined by the policy. When compliant, the database icons are marked with a green check and the arrow icons pointing from database to database are green.
State	Indicates whether the database is online or off-line, as well as whether the database is read-only.
Last Backup	Displays the date and time when the last successful backup was performed. This detail displays for the primary database only.
Last Restore	Displays the date and time when the last successful restore was performed. This detail displays for each secondary database.
Latency	Latency measures the amount of time that has elapsed since the last successful restore operation.
Threshold (primary database)	Indicates how much time can elapse before a scheduled backup is considered missed. When a backup is missed, the policy status is non-compliant. You can change the threshold setting by editing your log shipping policy.
Threshold (secondary database)	Indicates how much time can elapse after the last successful restore operation before the database is considered stale. When the database becomes stale, the policy status is non-compliant. You can change the threshold setting by editing your log shipping policy.
Schedule	Displays how often backups are performed on the primary database and how often restores are performed on the secondary databases.

How do you refresh the Operation Details?

If a recent operation does not appear in the status view, you can refresh the status of this pane by clicking the **Refresh** icon in the pane title bar.

Restore policies

Restore policies allow you to define backup maintenance plans across multiple SQL Server instances in your enterprise. These instances can reside on one or more physical servers.

SQLsafe offers backup policies, restore policies, and log shipping policies to address different needs.

What is a restore policy?

A restore policy consists of a list of databases you want to restore, a source backup archive, and a schedule according to when the restores will be performed. You can then monitor the status of each recurring restore, all from a single point of contact in the Management Console.

How do restore policies help me?

Restore policies allow you to plan and schedule your SQL Server restore maintenance, as well as monitor its success and failures, all from a single point of contact at the Management Console.

Can I select InstantRestore for my restore policy?

No. InstantRestore is available only when performing a manual restore.

Create a restore policy

The SQLsafe Restore Policy wizard allows you to create restore maintenance plans across your enterprise. A SQLsafe restore policy is defined as a set of databases for which restore operations will be performed according to a defined schedule. By default, SQLsafe creates the SQL Server jobs for the specified restores.

You can create a restore policy for any database that belongs to a backup policy and has a full backup.

How do you access the Restore Policy wizard?

You can access the Restore Policy Wizard from any of the following paths:

- Go to the task bar, click **Create Policy** and then choose **Restore Policy**.
- On the Policies tab, click **Create New Policy** located on the **Operation Summary** section of the **Restore Policies Status** window. This option is only available before you create your first restore policy.
- On the Policies tab, right-click the Restore Policies folder and select **Create Restore Policy**.
- From any tab, go to the **File** menu, select **Create Policy** and then **Restore Policy**.

To get started with the Restore Policy wizard:

1. Name the policy.
2. Select the source database which contains the data you want to restore.
3. Select the target database where the data will be restored.
4. Get email notifications about the policy status.

Name the restore policy

The General tab of the Restore Policy wizard allows you to specify the basic properties of the restore policy.

Why should you specify a name or description?

You are required to enter a unique name for each policy.

Both the name and description will appear in the status messages for your policies. Using a meaningful name and description will allow you to more easily identify problems when they occur. For example, consider specifying a description that will help you later choose the correct restore operation to monitor during a disaster recovery situation.

What options do you have for creating a restore policy?

When you create a restore policy, you can choose from between the two following options:

- Create Restore Jobs using the SQL Server Agent
- Create Restore Jobs using the SQL Safe Backup Agent

Select the database you want to restore

The Source tab of the Restore Policy wizard allows you to specify the database you want to restore, the location of the corresponding backups, and which account SQLsafe should use to access these files.

To choose the location of your backup, click **Select** and choose one of the locations displayed. SQLsafe will automatically restore the latest backup found in that location each time your restore policy runs.

SQLsafe requires the selected database to belong to a backup policy since it will get the backup file location from a corresponding backup policy for the source database. ***If you choose a database that does not have a backup policy***, SQLsafe will prompt you to create a new backup policy for this database.

How do you keep your restores running despite network errors?

Select **Enable Network Resiliency** and then click **Configure** to change the default settings. By default, SQLsafe will retry the restore operation every 10 seconds and then fail after 5 minutes (300 seconds) of continuous errors. Also, over the course of the operation, SQLsafe allows a total of 60 minutes in which to retry the restore before stopping the operation. You can change these settings according to your requirements.

What accounts can you specify to access the backup files?

Depending whether you selected to use the SQL Server Agent or the SQLsafe Backup Agent for the scheduling of your restore policy, on this section you have the option to select between SQL Server Agent service account/SQLsafe Backup Agent service account respectively or another account with the respective credentials.

The specified user account must have read and write privileges on the selected directory for the backup file location.

Select the target database

The Target tab of the Restore Policy wizard allows you to specify the database that you want to keep updated with routine restores.

What can you do on this tab?

You can perform the following actions:

- Select the instance where your target database is
- Select the database you want to update using this restore operation
- Specify the location of the data and log files associated with this database
- Choose the appropriate recovery state for the database (Fully Accessible, Accessible but read-only or Not Accessible).
- Schedule when the Backup Agent should execute the restore job
- Select the applicable restore options

How do you change the location of your database files?

If SQLsafe does not display the correct path for the location where you want to restore a file, click **Select** in the Database File Locations section, and then select the proper location.

The Database File Locations window allows you to manage the paths where SQLsafe restores new data files and log files. SQLsafe creates the file name automatically using the file type and destination database name for easy identification.

How do you set the restore schedule?

You can click **Schedule** on the Restore Job option and set the frequency and the duration of your restore policy job.

How do you restore the SQL logins for this database?

You can recover SQL logins associated with this database by selecting the **Restore database logins** option in the Restore options. SQLsafe applies this option when the source backup files contain login information. To capture login information, configure your backup policy to include the database logins.

What do you do if your instance is not listed?

If your instance is not displayed in the SQL Server drop-down list, you can choose to add a new instance by clicking the **Register** SQL Server butt on. For more information, see Register an instance.

What do you do if you have users connected to the database?

You can instruct SQLsafe to disconnect users from the database before performing the restore. To do so, select the **Disconnect users** option from the restore options.

Configure notifications for restore policy

The Notifications tab of the Restore Policy wizard allows you to choose the restore statuses from which you want to receive alert notifications through email. Email notifications let you, and your staff, remotely monitor the status of the restores you have automated with this policy.

The status of the restore operations determine the status of your policy.When your restores are successfully completed on scheduled, the policy is considered okay.

Choose the status you want to monitor, type the email address of each recipient, select the desired alert frequency for each operation, and then click **Next**.

You must configure your mail server settings before SQLsafe can send email notifications. Click **Configure E-mail** to check your settings. For more information, see Configure e-mail settings for alert notifications.

When is the email sent?

SQLsafe sends an email to the specified recipients when the selected operation status occurs. Because SQLsafe checks the status of your restore operations every minute, your alert notifications provide a real-time indication of the health of your service level agreements and disaster recovery plans for the SQL Server instances covered by this policy.

However, how often you are emailed about a specific status update depends on the notification frequency setting you select. For example, if you want to receive an email whenever a restore fails, even when the failures occur sequentially, choose to receive notifications every time the event occurs.

Review details for restore policy

The Summary tab of the Restore Policy wizard provides the summary of specified values and options you have selected in the Restore Policy wizard.

What do I do next?

After you have reviewed the information on the Summary tab, click **Finish** to create the policy and corresponding restore jobs.

View status of all restore policies

When Restore Policies is selected in the Policies tree pane, the content pane displays information describing the overall status of all of these policies. Use this view to quickly determine whether your servers are in compliance with your corporate restore policies.

What does the Current Status mean?

The Current Status displays the most recent, combined status of all operations performed by your restore policies. Even though there are multiple operation statuses, the overall policy status reflects the most critical operation status. When all restores have been completed successfully according to the policy schedule, a green okay icon is displayed.

What is the Last Operation Status?

The Last Operation Status shows an overview of the most recent backup, restore, or log shipping operations that occurred across your enterprise. Use this view to quickly determine whether your servers are in compliance with your corporate policies. Click the status to see more detail about your operations.

What is the Operation Summary?

The Operation Summary displays a listing of all policies, providing information in the following columns:

Column Header	Definition
Status	Displays either a green okay status bar, a yellow warning status bar, or a red error status bar.
Name	Displays the policy name.
Databases Covered	Displays the number of databases being restored by the policy.
Last Operation	Display the date and time of the most recent restore operation.
Last Operation Failure	Displays the date and time of the most recent restore failure.

How do you get details about a specific policy?

You can get more details about the status of a specific policy by double-clicking a policy operation in the Operation Summary grid.

Can you customize the columns in the grid?

You can sort by the content of any of the columns by clicking the column header.

How do you refresh the operations status?

If a recent operation does not appear in the status view, you can refresh the status of this pane by clicking the **Refresh** icon in the pane title bar.

View status of a specific restore policy

When a specific restore policy is selected from the Restore Policies tree node, the content pane displays information describing the status of that policy. Use this view to determine which restore operations initiated by the policy have succeeded or failed.

What actions can I perform?

From the Policies tree

By right-clicking a policy under the Restore Policies node, you can access the following shortcuts:

Action ...	What it does ...
Create Restore Policy	Opens the Restore Policy wizard, allowing you to create a new policy.
Edit Policy	Opens the Restore Policy wizard (with all options pre-set to the values used for this operation), allowing you to edit any of the options.
Delete Policy	Allows you to delete the policy. Although restore operations associated with this policy will no longer be performed, the previous status messages returned by this policy will continue to be stored in the SQLsafe Repository.
Disable Policy	Allows you to disable of the selected policy. Restore operations associated with this policy will no longer be performed.
Start Jobs for Policy	Allows you to run the restore job associated with this policy, performing an ad-hoc restore with the options already set by the policy.
Refresh Policy List	Updates the Restore Policies node with the latest policies.

From the Current Status pane

By clicking the links available in the Current Status pane, you can access the following shortcuts:

Action ...	What it does ...
View Policy Settings	Allows you to view a summary of the policy settings.
Edit Policy	Opens the Restore Policy wizard, allowing you to change your policy settings.
Disable Policy	Disables the selected policy. Once a policy is disabled, it will no longer perform restore operations for the associated databases. To recover a database that belongs to a disabled policy, perform a manual restore using the Restore wizard.
Start Restore	Performs a full restore of all databases that belong to this policy by running the corresponding job. This action applies your previously defined policy settings.

From the Operation Summary grid

By right-clicking on an operation, you can access the following shortcuts:

Action ...	What it does ...
View Details	Shows the Details pane, providing additional information about the selected operation.
Restore again	Runs the restore operation again, using the same settings.
Restore with different options	Opens the Restore wizard (with all options pre-set to the values used for this operation), allowing you to specify different options before running the operation.
Set Progress To	Allows you to change the status of the selected operation.
Close Details	Hides the Details pane.

What does the Current Status mean?

The Current Status displays the most recent, combined status of the restore operations performed by this policy. When there are multiple operation statuses, the policy status reflects the most critical operation status. When all restores have been completed successfully according to the policy schedule, a green ok icon is displayed.

What is the Last Operation Status?

The Last Operation Status shows an overview of the most recent backup, restore, or log shipping operations that occurred across your enterprise. Use this view to quickly determine whether your servers are in compliance with your corporate policies. The operation status is limited to restore operations performed by this policy.

What are the Operation Details?

The Operation Details grid displays a listing of all restore operations performed for the databases included in the selected policy for the last 7 days. This grid includes the following columns:

Column	Definition
Progress	During an operation, the progress bar will denote the percentage of the operation completed. When the operation is complete, it will display a green bar labeled 100%. If an operation completed with errors, this column will display a red bar labeled Error.
Instance	Displays the instance name that was restored by this operation.
Database	Displays the database name that was restored by this operation.
Operation	Confirms that a restore operation was performed.
Backup Type	Displays the type of backup restored by the operation. Currently, only the recovery of full backups is supported by the restore policy.
Compressed	Displays the compressed file size of the backup used in this restore.
Ratio	Displays the percentage of the data that was compressed in the associated backup.
Compression	Displays the type of compression that was used for the associated backup.
Duration	Displays the number of seconds required to complete the restore operation.
Start Time	Displays the start date and time of the restore operation.

Can you customize the columns in the Operation Details grid?

You can sort by the content of any of the columns by clicking the column header.

You can select which columns are visible in this grid, and enable column grouping, by clicking the **Filter** icon in the pane title bar.

How do you refresh the data displayed in the Operation Details grid?

If a recent operation does not appear in the status view, you can refresh the status of this pane by clicking the **Refresh** icon in the pane title bar.

What are the details?

To see the detailed results of a specific operation, right-click the operation in the Operation Details grid and select **View Details**. The Details pane displays below. By default, this pane is hidden.

The Details pane provides the following information about the selected backup operation:

Tab	Description
Statistics	Displays the database size, the size of the uncompressed backup, the size of the compressed backup, and the compression ratio achieved with this backup. The ratio is a measure of the storage savings achieved with SQLsafe compression technology. For more information about the storage space savings you can realize using SQLsafe, see Understand your total cost of operation (TCO).
Result Text	Displays text describing the result of the restore.
Files	Displays the complete path of the backup set file for the restore.
Backup Set Description	Displays the description you specified for this restore.

Storage Options	Displays which locations were chosen to store the backup files associated with the restore.

Need more help? Search the Idera Customer Support Portal

View last operation status

After a policy runs, the Policies tree content pane displays information describing the overall status of all of these operations. The Last Operation Status shows an overview of the most recent backup, restore, or log shipping operations that occurred across your enterprise. Use this view to quickly determine whether your servers are in compliance with your corporate policies.

If your operations are successful, SQLsafe displays a list of these operations and their associated messages. If an operation was unsuccessful for any reason, the Last Operation Status also allows you to rerun the operation from this view instead of requiring you to access the appropriate wizard.

You can rerun any previous operation from this grid. To rerun an operation, check the box to the left of the appropriate operation, and then click Run Selected Operations Again . This request executes the backup or restore using the previous settings.

What is the operation summary box?

The operation summary box displays a list of all operations for the selected topic, such as Backups were canceled by user. SQLsafe provides information in the following columns:

Column Header	Definition
Instance	Displays the instance name.
Database	Displays the database name.
Operation	Displays the type of operation performed.
Start Time	Displays the start date and time of the most recent operation.

Can I rerun more than one operation?

Yes, you can quickly rerun one or more operations through the Last Operation Status. Check the boxes next to all appropriate operations, and then click Run Selected Operations Again. To select all of the displayed operations, check the box next to the Instance column title.

How can I capture the provided information?

SQLsafe allows you to copy the list summary and the related messages using the copy buttons to the left of the operation summary box and the messages box. You can then paste this information in another application, such as Notepad. Use the upper copy button to capture the status, instance, database, operation, and start time. Use the lower copy button to capture the same information, but also include the message.

Perform a Manual Backup

The SQLsafe Backup Wizard allows you to:

- Back up multiple databases on different SQL Server instances
- Back up multiple databases on the same SQL Server instance
- Back up individual databases

SQLsafe executes all of these operations in parallel.

To successfully back up data on a SQL Server instance, SQLsafe requires that you deploy a Backup Agent to the target instance. You can remotely deploy a Backup Agent through the Backup Wizard by registering the target instance.

If SQLsafe detects that your instances is not licensed, go to **License Key Manager** and enable the license for that instance.

To back up multiple databases on a routine schedule, use a backup policy to maintain an up-to-date archives of your databases.

How do you create an archive using the Backup Wizard?

The Backup Wizard guides you through the steps required to archive your database content into backup sets. You can back up a single database, multiple databases, or an entire SQL Server instance.

To create a backup with the Backup Wizard:

1. In the navigation pane, click **Servers.**
2. In the Servers tree, select the SQL Server instance or database you want to backup.
3. Select **Backup Database** from the right-click context menu or click the **Backup** option on the Management Console menu bar. Additionally you can find this **Backup** option on the **File** menu.
4. On the Databases tab, verify that the correct SQL Server instance and databases are selected, and then click **Next** . For more information, see Select the database to back up.
5. On the General tab, select the Backup Type, and select **Create a copy-only backup** or **Verify Backup** if appropriate. Enter a name for the backup and a description. For more information, see Specify the type of backup. Click **Next.**
6. On the Location tab, select the Location Type from **Single File**, **Striped Files** or **Tape** (Tivoli Storage Manager).
7. For any location type, choose to overwrite or append to an existing archive. For more information, see Select a location for the backup . You can also choose how to handle errors encountered while writing to the network during a backup by clicking **Enable network resiliency**.
8. On the Location tab, you can also set up to two mirror locations for your backup. Click **Next**.
9. On the Options tab, select the appropriate compression and encryption options, and any advanced objects that are appropriate for your environment. For more information, see Specify compression and encryption options. ***If your SQL Server environment requires FIPS compliance***, use the AES encryption option. Click **Next**.
10. On the Notifications tab, select the email address to which you want to send alert notifications. For more information, see Configure e-mail notification for the backup .
11. On the Summary tab, review your selections. For more information, see Review the details of the backup.

Select databases for manual backup

The Databases tab of the SQLsafe Backup wizard allows you to specify the instance that hosts the databases, and the specific databases you want to back up.

If your instance is not licensed, SQLsafe displays a warning message. Go to **License Key Manager** to enable the license for your instance.

What can you do on the Databases tab?

You can select the instance that hosts your target databases.

After you select the instance, the database list is populated. From the database list, select the databases you want to back up.

If you want to ...	Select this option ...
Back up all databases on the selected SQL Server instance	All Databases
Back up only User databases on the selected SQL Server instance	All User Databases
Back up only System databases on the selected SQL Server instance	All System Databases (master, model, msdb, distribution)
Back up only the databases you specify on the selected SQL Server instance	Specific Databases, and then choose the appropriate databases

Why isn´t the target instance listed?

The instance list only includes SQL Server instances that have been registered with SQLsafe. If the instance is not in the drop-down list, you can choose to add a new instance by clicking **Register SQL Server.** For more information, see Register an instance.

You can click **Refresh** to update the list of your databases if you do not see the current information.

Select backup type

The General tab of the SQLsafe Backup wizard allows you to specify the backup type, name, and description of the backup you are creating.

What types of backups can you choose?

SQLsafe supports the standard SQL Server database backup types:

- Full Backup
- Differential Backup
- Transaction Log Backup
- File Backup

What should you do for your initial backup?

If you are backing up the database for the first time, select **Full Backup.** A full backup will provide a comprehensive data set, and is required to perform differential backups or transaction log backups later on. For more information about backup types, Understand backup types.

When should you specify a description?

You should provide a description to identify important details about this operation so you can easily identify which backup sets should be restored later. The backup description will appear in the status view of past and current backups, and will allow you to more easily identify problems when they occur.

How do you verify the integrity of your backup?

You can choose to verify the backup. When this option is selected, SQLsafe performs a data integrity check after the backup has been created. SQLsafe only verifies the integrity of the data files in the backup set created by this backup.

Verifying the backup helps identify potential issues that could occur when restoring these data files.

What is a copy-only backup?

A copy-only backup is a copy of the database, not a true backup, and cannot be used as a part of a restore strategy or restore chain. It is a backup that does not affect the log sequence numbers (LSN) of the database.

Select location for manual backup

The Locations tab of the SQLsafe Backup wizard allows you to specify the backup location you want to use to store the backup set. For a TSM backup, you can change the TSM connections settings to override the values set in the client options file if you need to write the backup files to a TSM Server other than the TSM Server already specified in the dsm.opt file.

What information is on the Locations tab?

You can select the location type and the UNC or full path of an existing archived backup set.

What do you do if you don´t have an existing archive file?

If you do not have an existing archive file, SQLsafe creates a new archive file that includes this backup set, using the name you specified.

What do you do if you do have an existing archive?

You can **Append** to an existing archived backup set or choose to **Overwrite** it.

How do you specify a UNC path?

To specify a UNC, type the UNC path directly in the field. You cannot specify a UNC when using the browse option.

Using a UNC path allows you to restore backups to a different or new server from the original archive.

Where can you store your backup set?

SQLsafe supports the following location types:

- Single File
- Striped Files
- Tape (using Tivoli Storage Manager)

What actions can you take with the location types?

Location Type	Action
Single File	Enter the name of the backup archive.
Striped Files	Enter as many backup archive names as the number of striped files you want. When backing up SQL Server 2000 databases, consider using as few striped files as possible since a high number of striped files can significantly degrade performance due to SQL Server memory allocation.
Tape	Enter the path of the TSM configuration file and the Object Name.

What are striped files?

If you want to take advantage of distributing I/O overhead for a large database, select striped files, and select backup locations on different local disks.

When backing up SQL Server 2000 databases, consider using as few striped files as possible since a high number of striped files can significantly degrade performance due to SQL Server memory allocation.

How do you handle errors encountered while writing to the network during a backup?

Click **Enable Resiliency** and access the **Network Resiliency Settings** window where you can specify how often you want to retry when errors occur and after how much time the operation will fail. You can also configure how much time is allowed for the total retry time of the backup.

How do you mirror your backups?

Click **Mirroring Archives**, and then specify where you want the mirror copies to be stored.

For each mirror, SQLsafe creates a copy of the backup archive set. You can specify up to 2 mirrors for each backup operation. Keep in mind that creating mirrors can impact the performance of your backup operation.

If you want to stop the backup operation when the mirror location is unavailable, select the corresponding option.

How do I keep my backup running despite network errors?

Select **Retry writing backup files after network errors**, and then click **Configure** to change the default settings. By default, SQLsafe will retry the backup operation every 10 seconds and then fail after 5 minutes (300 seconds) of continuous errors. Also, over the course of the operation, SQLsafe allows a total of 60 minutes in which to retry the backup before stopping the operation.

This option is not available when backing up to tape using Tivoli Storage Manager.

What do I specify when backing up to a TSM Server?

When a TSM location is selected, you must specify the following settings:

- high level file path
- low level file path
- the location of the TSM Client options file that enables generate password for authorization

You can change the TSM connections settings to override the values set in the client options file. You can also configure SQLsafe to mark these files as inactive after a specified age.

Note that SQLsafe accepts up to 260 characters for the TSM file path name.

Can I store backup files in a different TSM Client file space?

Yes. Under **TSM Client Settings**, specify the name of the node you want to use and the password required to access the node.

What settings can I change in the TSM Client options file?

Click **Change** to specify the node name, the password required to access the node, and the TCP/IP Server address and port.

Configure options for manual backup

The Options tab of the SQLsafe Backup wizard allows you to select additional options, such as compression and encryption, to use for the current backup operation.

What types of compression algorithms are available?

- None
- IntelliCompress, optimize for size (iSize)
- IntelliCompress, optimize for speed (iSpeed)
- Levels 1, 2, 3, 4

A backup operation using Level 1 completes fastest but achieves the least amount of compression. Level 4 achieves maximum compression but the backup operation may take longer.

For more information about backup compression, see How to choose compression and encryption.

What types of encryption algorithms are available?

- None
- AES (128-bit)
- AES (256-bit)

If your SQL Server environment requires FIPS compliance, use the AES encryption option. For more information, see Ensure FIPS compliance.

Does encryption require a password?

When you choose to encrypt an archive, you must designate a password. For security reasons, SQLsafe does not store this password. Ensure you remember the password you select.

What are the advanced options?

The following options are available as Advanced Options:

Options	Description
Number of threads	Allows you to specify how many threads you want SQLsafe to use to distribute the backup operation across multiple processors on the target SQL Server computer. Use this setting to optimize backup performance. Select **Auto** to have SQLsafe determine the optimal thread count for your environment.
Remove inactive transaction log entries	Removes all completed transactions from the transaction log after SQLsafe finishes the backup. This option is only available for Log backups
Generate maps	Generates maps containing metadata for each database included in your backup file. Depending on the number of transactions completed since your last backup, generating maps may impact the performance of the backup operation. Generating maps is optional, but must exist in the backup file for InstantRestore to accept and restore that file. SQL virtual database can attach SQLsafe backup files without the metadata, but the data files improve SQL vdb performance during creation of the virtual database. For more information, see Recover objects using SQL virtual database. This option is selected by default.
Include database logins in backup file	Copies SQL login information for the selected databases, including credentials and privileges, when the backup files are written. To help ensure the security of your SQL Server database, SQLsafe encrypts the login information. This option is available for full backups only.

What are the advanced options for SQL Server 2005 and later?

The following options are available as Advanced Options for SQL Server 2005 and later:

Options	Description
Generate checksums	Generates a checksum for the backup file.

Ignore checksum errors	Select this option to ignore any errors from the generated checksum. ***If checksum errors are encountered***, this option indicates that SQLsafe should continue to back up this database.
Read-write filegroups	Specifies a partial backup, which includes the primary filegroup and any read-write secondary filegroups. Read-write filegroups are not supported by SQL virtual database. ***If this option is selected***, the **Generate metadata** option will be disabled. Additionally, backups created with the read-write filegroups option cannot be used by SQL virtual database to create virtual databases.

What does the option Generate Script do?

You can generate a T-SQL or CLI script that will execute the backup you have defined in the wizard. For more information about generating scripts, see How script generation works.

What do you do next?

After you complete the Options tab, you can click **Next** to continue with the Backup Wizard, select any previously visited tab to modify that information, or click **Generate Script** to create a T-SQL or CLI script.

Configure notifications for manual backup

The Notifications tab of the SQLsafe Backup wizard allows you to email a status notification to the appropriate database administrators about this backup. Email notifications let you, and your staff, remotely monitor the status of your backups.

Choose the status you want to monitor, type the email address of each recipient, and then click **Next**.

You must configure your mail server settings before SQLsafe can send email notifications. Click **Configure E-mail** to check your settings. For more information, see Configure e-mail settings for status notifications.

When is the email sent?

SQLsafe sends an email to the specified recipients only when the selected backup status occurs. For example, if you chose to monitor whether the backup fails, you will not be emailed if the backup is skipped. Because you are performing a manual backup, you will receive one status notification.

Review details for manual backup

The Summary tab of the SQLsafe Backup wizard provides the summary of specified values and options you have selected in the Backup Wizard.

What do you do next?

After you have reviewed the information on the Summary tab, click **Backup** to submit the backup job immediately, or click **Generate Script** to create a script you can use to run the job at a later time. For more information about generating scripts, see How script generation works.

How do you verify the status of your backup?

If you chose to run the backup job immediately, and want to verify a successful run, you can view its status using the **Instance View**. For more information, see View backup/restore operation status.

What actions can you perform on the Summary tab?

Action	Steps
Immediately backup databases	Click **Backup**, and then highlight the instance or database in the tree pane to see the status of the operation.
Create a CLI backup script	Click **Generate Script**, and then click **Command Line**. To **Save the script to a file**, click the saving icon or the **Copy script to clipboard** i con respectively. SQLsafe creates a backup script using the settings you specified for the selected databases. You can use this script to perform future backups of any system or user database you selected. Click **Close** to return to the Backup Wizard.
Create a T-SQL backup script	Click **Generate Script**, and then click **T-SQL**. To **Save the script to a file**, click the saving icon or the **Copy script to clipboard** icon respectively. SQLsafe creates a backup script using the settings you specified. You can use this script to perform future backups of any system or user database you selected. Click **Close** to return to the Backup Wizard. This script requires the SQLsafe XSP. For more information on installing the SQLsafe XSP, see Deploy the SQLsafe XSP. For more information about how to use the SQLsafe XSP, see the sample scripts available from the Programs menu.

Perform a Manual Restore

SQLsafe allows you to restore multiple databases or files to any SQL Server instance you have registered. Ensure each registered instance is running the SQLsafe Backup Agent. Depending on your needs, you can restore databases from specific backup sets, or use the intuitive user interface to select specific points in time for each database you want to restore. When you select a time, SQLsafe automatically selects the appropriate backup sets that contain the data to be restored.

The Restore wizard will walk you through the restore process. Use the following checklist to ensure you have everything in place to restore your databases to the correct locations and to the correct points in time.

☑	**Follow these steps ...**
☐	Determine the location of the databases you want to restore to the SQL Server instance in question.
☐	Determine which SQL Server instance should host the recovered databases.
☐	For each database you need to recover, decide whether you will be restoring data from a specific backup set, or if you will restore data to a specific point in time. you can select the specifics in the Restore wizard.
☐	Determine whether you want and are able to use InstantRestore.

To restore a database on a routine schedule, use a restore policy to maintain an up-to-date copy of your database.

What does the Restore wizard do?

The SQLsafe Restore wizard allows you to simultaneously restore multiple databases on different SQL Server instances, restore multiple databases on the same SQL Server instance, or restore individual databases. SQLsafe also allows you to verify the integrity of a backed up database without restoring it.

What is InstantRestore?

InstantRestore allows you to quickly come back on line while restoring your database. It is important to understand InstantRestore fully before undertaking this type of database restore. Make sure you know the supported restore information before attempting to use the InstantRestore feature. Note that InstantRestore supports only complete database restores and does not support file or filegroup restores.

How do I restore a backup using the Restore wizard?

1. In the navigation pane, click **Servers**.
2. In the Servers tree, select the SQL Server instance or specific database you want to restore.
3. Select the appropriate restore operation (**Database (s)** or **Database (s) Files**) from the right-click context menu, the **Restore** option on the Management Console menu bar, or go to the **File** menu and look for the **Restore** option.
4. On the Target tab, choose the instance to which you want to restore the database. You can disconnect any users before you restore the database. For more information, see Select the instance to restore. On this section, you can also choose to verify the integrity of a backup up database instead of restoring it. On the Advanced Options, you can select the number of threads for decompressing data. After making you choices, click **Next**.
5. On the Databases tab, select the database or backup file you want to use for the restore. If you want to restore a backup that has moved or has no history, you can still select it using one of the file system tabs (Repository, File System, Target Server, TSM). For more information,see Select the database you want to restore. Click **Next**.
6. On the Backup Sets tab, for each database you have chosen to restore, select either the time to restore to or the backup set to restore from. On this section you can also configure options for encryption settings, editing file paths, and enabling network resiliency options. For more information, see Select a backup set for the restore. Click **Next**.
7. On the Database Files tab, configure the appropriate settings for each database you are restoring. On this section you can verify the database name and data file locations. For more information, see Enter the database files for the restore.
8. Click **Next**.
9. On the Recovery State tab, select the appropriate recovery state for each individual database (Fully accessible, Not accessible, Accessible but read-only). For more information, see Choose the recovery state for the restore.
10. Click **Next**.
11. On the Restore Type tab, select the appropriate restore type. You can select from normal SQLsafe restore or InstantRestore. For more information, see Choose the type for the restore.
12. On the Notifications tab, select for which events to receive notifications about and specify the email addresses of those who will receive these notifications. In order for SQLsafe to send email notifications, you must configure your mail sever settings first. For more information go to Configure e-mail settings.
13. On the Summary tab, review your selections. For more information, see Review the details of the restore.
14. Click **Restore**.

SQL safe is a high-performance backup and recovery solution for your SQL Servers. Learn more > >

Idera Website	Products	Purchase	Support	Community	About Us	Resources	Legal

How InstantRestore works

SQLsafe InstantRestore is a powerful new restore technology that allows you to bring a database online quickly while the restore occurs in the background. SQLsafe enables the SQL Server to immediately begin the transactional part of a database restore, deferring the data file (MDF) restoration until after the database is online. SQL Server continues to handle all transaction log (LDF) restoration activity.

When the restore process is complete and the database is online, SQLsafe takes over and restores the remaining data to the data files in the background. If SQL Server needs data not yet restored, SQLsafe delivers the data to SQL Server directly from the backup. Because SQLsafe never interferes in the SQL Server log operations, ACID (Atomicity, Consistency, Isolation and Durability) compliance for your databases is not affected. When SQLsafe completes data file restoration, it removes itself from all I/O activity of the database and leaves behind a database identical to one restored with a traditional restore process. As a result, SQLsafe is no longer required to access the database.

You cannot use the InstantRestore feature on any version of the Windows 2000 operating system and Microsoft SQL Server 7.

Beginning with version 7.0, SQLsafe includes a mini-filter driver to support the InstantRestore feature. The driver, named SQLsafeFilterDriver, allows SQL Server to access database data while SQLsafe is performing an instant restore. The driver is only used during an instant restore and is no longer necessary once the database is completely restored.

How to enable InstantRestore

You first must enable the InstantRestore feature. Because some users may feel uneasy installing a device driver on their systems, InstantRestore is disabled by default. You can enable or disable the InstantRestore feature quickly depending on what task you are performing:

- ***If you are viewing your SQL Server instances in the Servers tree*** , right-click the instance you want to restore, and then select **Enable SQLsafe InstantRestore** or **Disable SQLsafe InstantRestore**.
- ***If you are in the SQLsafe Database Restore wizard*** , complete the wizard up to the Restore type tab where you will find the option for enabling InstantRestore.

If an InstantRestore operation is in progress when a user attempts to disable these components, SQLsafe displays a warning message.

Eligible backups

The InstantRestore feature is available for only a database backup that is:

- **A SQLsafe backup archive with backup metadata (maps).** Because InstantRestore allows SQL Server to immediately access the data in a backup, the process needs additional information about the backup which is not present in a native backup file. Please note that this information is also missing in SQLsafe backups that are written directly to Tivoli Storage Manager (TSM).
- **A complete database restore.** InstantRestore can restore a database using any normal restore chain starting with a full backup. InstantRestore does not support partial restores such as file restores or restoring a database with the NO RECOVERY or STANDBY options.

Monitoring your instant restores

As SQLsafe performs an instant restore, you can monitor its progress using the SQLsafe Management Console or via alerting. InstantRestore is a new type of restore operation and appears in the Management Console status grid like traditional backup or restore operations.

The InstantRestore operation is tracked with the following two operation types:

InstantRestore

The InstantRestore operation tracks the progress of the entire database restore process. The progress bar increments to 100% for the initial restore progress until the database comes online. When the initial restore completes and the database is online, the status changes to **Online** and the cell changes to light green. SQLsafe then displays a new line for the Hydrate operation.

Hydrate

The Hydrate operation tracks the progress of the background restore process. The progress bar increments to 100% for the background restore progress until the restore is complete. When the database restore is complete, the status of both the InstantRestore and Hydrate operations changes to **Complete** and the cell changes to dark green.

Instant Restore operations include the following two statuses to indicate important milestones of the operation:

Online

The Online status indicates that the database is online and ready for use.

Halted

The Halted status indicates that an event interrupted the InstantRestore process. A network issue between SQLsafe and the backup archive can interrupt an instant restore. Because InstantRestore allows changes to the database while the restore is occurring, the database is not deleted if an issue occurs during Hydration. If such an event occurs, the database transitions to a read-only state to prevent the system and users from

writing additional data to the database. At this point, you can restore access to the backup archives and the instant restore can safely resume.

Handling errors during Hydration

If the hydration process is interrupted for any reason:

- The InstantRestore and Hydration operations transition to the Halted state.
- SQLsafe displays an error message stating that hydration is interrupted.

If an error occurs during the InstantRestore operation prior to the beginning of the Hydrate process, SQLsafe displays only the InstantRestore operation with an error status, and includes the error message for the failure.

> The InstantRestore operation has two phases. In the first phase, the T-SQL restore command runs and after the database is online, hydration starts. If an error is encountered in the first phase (i.e. the T-SQL restore command) and the database remains in SQL Server, SQLsafe does not delete the database.

SQLsafe includes the following failure scenarios that may occur during an instant restore.

Component	Failure	Resolution
Server	Crashes	If the server suffers a catastrophic crash and is no longer available, no recovery is available.
Server	Reboots	If the server reboots because of a power failure, automatic software update, or other similar situation, and comes back online correctly, the SQLsafe Filter Service restarts and then resumes hydration.
Server	Runs out of resources	If the server runs out of memory or other resources, and the SQLsafe Filter Service cannot allocate the additional resources during hydration, SQLsafe uses the following steps: 1. ***If the offending process is identified*** : a. The user must stop the process. b. The user can manually restart the SQLsafe Filter Service (if stopped). c. If hydration does not resume once the SQLsafe Filter Service restarts, the user can manually restart the operation. 2. ***If the offending process is not identified*** , the user may reboot the server.
Server	Suffers a disk failure	If the database or InstantRestore support files is corrupted by a disk failure, no recovery is available.
Service	Restarts	If one or all of the following items restarts, hydration should resume after the restart is complete: • SQL Server • SQLsafe Backup Agent • SQLsafe Filter Service If the database did not go into Suspect mode during this process, hydration resumes from the point where it left off when the SQLsafe Filter Service restarted. If the database is in Suspect mode, the SQLsafe Filter Service brings the database out of Suspect mode, and then resumes hydration.

Filter Service	Crashes	If the SQLsafe Filter Service crashes, hydration resumes once the service restarts. If the SQLsafe Filter Service crashes again, you may need to recover any new data added since the first crash.
Backup file	Is corrupt	If the backup file is corrupt or there is a read problem when accessing the network, the SQLsafe Filter Service fails to decompress during hydration. If the backup file is corrupt, and you have another copy of the backup file, you can restart hydration using the non-corrupt backup file. If the issue is a read problem when accessing the network, you can restart hydration once you address the network issue.
Backup file	Is inaccessible due to a network failure	If the backup file is inaccessible due to a network failure, InstantRestore attempts a retry. If the retry fails, and the maximum retry attempts is reached, the Hydration operation status transitions to the Failure state. Once you correct the network issue or relocate the backup file, you can resume hydration. If the Hydration fails, you may need to restart InstantRestore.
Backup file	Is inaccessible due to a lack of access permissions	If the SQLsafe Filter Service restarts and is unable to open the backup file because the account attempting to read the file does not have the proper permissions, you must provide the account permission, and then resume hydration.

Does SQLsafe include new characteristics specific to the InstantRestore feature?

Yes, there are new details in SQLsafe to support InstantRestore. For supported platforms, the following components were added to SQLsafe to support InstantRestore:

SQLsafe Filter Service (SQLsafeFilterService.exe)

The SQLsafe Filter Service is responsible for handling I/O requests from SQL Server and performing the background database restore (hydration).

SQLsafe Filter Driver (SQLsafeFilterDriver.sys)

The SQLsafe Filter Driver is responsible for intercepting I/O requests for databases that have active InstantRestore operations under way. When an instant restore completes the driver totally disengages from all I/O activity of the database and is no longer needed. This device driver utilizes the Microsoft mini-filter driver technology.

Do you have to use the console for InstantRestore?

No, the Console is not the only place where you can use the InstantRestore feature. You can execute an InstantRestore via T-SQL script using either the SQLsafe CLI or XSP commands. To use the XSP InstantRestore command, see the sample XSP scripts available from the Programs menu.

Example CLI code snippets that use the InstantRestore command

You can also perform an instant restore through the CLI. Additional options can be set in the SQLsafe Restore wizard, from which you can generate a CLI script that includes the specified wizard settings.

```
SQLsafeCmd.exe InstantRestore <database> <full_backup> -diff <diff_backup> -log <log_backup>
```

The following three options are specific to a backup set:

- `BackupFile` (if the backup set is striped)
- `BackupSet`
- `Password` (or `EncryptedRestorePassword`)

Where these options appear in the command determines to which backup set they are applied. When you encounter one of these options, it is applied to the full if no -Diff/-Log option is yet encountered, otherwise it is applied to the most recent -Diff/-Log. For example, if you want to instantly restore the following backups:

- Full backup, 2 stripes, backupset 2, encryption key "full"
- Diff backup, 2 stripes, backupset 3, encryption key "diff"
- Log backup, 2 stripes, backupset 4, encryption key "log"

Use the command:

```
SQLsafeCmd InstantRestore Northwind "C:\Backup\Northwind_Full (1 of 2).safe" -BackupFile
"C:\Backup\Northwind_Full (2 of 2).safe" -BackupSet 2 -Password "full" -Diff "C:\Backup\Northwind_Diff (1
of 2).safe" -BackupFile "C:\Backup\Northwind_Diff (2 of 2).safe" -BackupSet 3 -Password "diff" -Log
"C:\Backup\Northwind_Log (1 of 2).safe" -BackupFile "C:\Backup\Northwind_Log (2 of 2).safe" -BackupSet 4
-Password "log"
```

For more information about available instant restore options, see the usage statements in the CLI Help.

Select target instance for restore

The Target tab of the Restore wizard allows you to you select the instance to where you will restore the database.

What information is on the Target tab?

On the Target tab, you can select the instance to where you will restore the selected databases.

What do you do if your instance is not listed?

If your instance is not displayed in the **SQL Server** drop-down list, you can choose to add a new instance by clicking **Register SQL Server**. For more information, see Register an instance.

What do you do if you have users connected to the database?

You can instruct SQLsafe to disconnect users from the databases before performing the restore. To do so, select the **Disconnect users before the restore** option.

What does "verify only" mean?

This restore option helps you ensure your backup operations are successful without actually restoring your data. Consider using this restore verification option on all critical backups after executing the backup operation.

What other Advanced Options do you have on this section?

You can specify the number of threads for decompressing data or you can choose the **Auto** option so that SQLsafe calculates the optimum number of threads for your operation.

Select the databases you want to restore

The Databases tab of the Restore wizard allows you to specify the databases you want to restore and the general location of the corresponding archive files. You can select:

- Whether the backup file resides in your repository. Choose the SQL Server where the database(s) to be restored were backed up, then select the Databases you want to restore.
- Whether the archive file was written to the local File System. Enter a file from the network share or local drive. This path must be accessible by the Backup Agent installed on the Agent Computer.
- Whether a network share is available on a remote file system (Target Server)
- Whether the backup was performed using TSM

When restoring from a TSM Server, browse for the correct database archive. You can change the TSM connections settings to override the values set in the client options file.

Select the backup set for the restore

The Backup Sets tab of the Restore wizard allows you to choose which backup sets you want to use to restore the selected databases.

What information is on the Backup Sets tab?

For each database you have selected to restore, the backup set listing is populated with the available backup sets from the Repository. You can choose the specific backup sets you want to restore, or you can select a point in time to which you want to restore data. To restore more than one database, select a backup set for each database.

> If your backups have been done locally in a server that is different from the the restore server, you may need to specify manually the location of these backup sets.

What do you do on the Backup Sets tab?

For each database you are restoring, you can choose one of three methods to select the appropriate backup sets:

- Time slider
- Manual selection of a specific point-in-time
- Manual selection of the backup set

What is the benefit of using the point-in-time slider?

When you select a point in time by clicking in the time slider, the corresponding backup sets are automatically selected. This ensures you are using the appropriate backup sets and files to restore the data you need. SQLsafe does not restore data time-stamped with dates later than the point in time you specify.

How do you use the point-in-time slider?

Depending on where you click, you can control which backups are used in this restore.

Click location	Result
Within a full backup marker	Selection of the full backup set.
Within a differential backup marker	Selection of the last known full backup, as well as the differential backup.
Above a transactional log marker	Slider snaps to the end of that log file and you will select the last known full backup and the entire transactional log file.
Within a transactional log marker	Selection of the last known full backup and all the transactions up to the specific point-in-time you clicked on.

> You can set the amount of information displayed on the point-in-time slider by choosing information from the Last 30 days, Last 14 days, Last 7 days, Yesterday & Today, Today, and Custom Date Range.

Why would you select a specific point-in-time instead of using the slider?

Because the precision of the slider may not suit your needs, you can manually enter the specific point in time to restore in the **Selection Options**. This automatically selects the appropriate backup sets while providing pin-point time accuracy.

How do you manually select backup sets?

You can also choose to manually select which backup sets to restore. If you choose this option, you must also select the specific backup set to restore. To pick specific backup files, click the Backup Files from the list of Backup Set Names.

How do you select where your backup files are located?

Click **Edit File Paths** to display a list of backup files that you can use to restore the selected backup set. The Backup File Locations window displays the list of backup files SQLsafe uses to restore your backup sets. By clicking on the filename, you can edit it. You can also edit the path by clicking the button to the right of the path you want to change. Mirrored files also appear in the dropdown list if available. Click **OK** to apply your changes.

What are the encryption settings?

The option for **Encryption Settings** will be available when you choose a backup set where you have used the encryption option during its backup. Use this option to access these encryption settings.

How do you keep your restores running despite network errors?

Select **Enable network resiliency** , and then click **Configure** to change the default settings. By default, SQLsafe will retry the restore operation

every 10 seconds and then fail after 5 minutes (300 seconds) of continuous errors. Also, over the course of the operation, SQLsafe allows a total of 60 minutes in which to retry the restore before stopping the operation.

Why is the Generate Script button enabled?

You can generate a T-SQL or CLI script that will execute the restore operation with the settings you have defined in this wizard. For more information about generating scripts, see How script generation works.

How do you use a mirrored file?
In some situations, SQLsafe creates a mirrored version of a backup file. You can use this file when the database you want is mirrored, and you cannot find the original because it was moved or deleted.

When SQLsafe tests file paths for a restore, and does not find the information it is looking for, a dialog box opens asking if you want to choose the same path and try again, or if you want to choose a different location for these files. If you choose to find a different path, SQLsafe displays the path of the failed file and allows you to choose another location. SQLsafe displays an icon to the left of the file name that alerts you of any file that failed the access test. Select the appropriate path, and then click **OK**.

Specify a file name and location

The Database Files section of the Restore wizard allows you to rename a database by changing the name or move the location by editing the data file locations of the restored files.

What information is on the Database Files tab?

For each database you have selected to restore, you are required to specify the name for the restored database, and the filename to which you will restore the database.

What do I do on the Database Files tab?

For each database you are restoring, you have several ways to select the restored database name and path. You can:

- Select target database from drop-down list of existing databases
- Enter a new database name
- Enter a new database path
- Select restore options for these files
- Edit the filename of the restoring file

When you select a database name from the drop-down list, or edit the field, the **Restore As Filename** is automatically updated to reflect the new name, but you can edit this field by directly typing on the grid. You can also change the database path by simply editing the filename in the grid.

What actions can I perform on the Database Files tab?

Action	Steps
Create a new database to restore.	Type a new database in the **Restore As** text box.
Change the path of the target database	Enter a new path in the **Change path** field.
Ensure the selected backup files are restored, even if that means overwriting an existing database.	Select the **Force Restore** option (replace).
Restore the SQL logins associated with the selected databases	Select the **Restore database logins** option. This option is available when you are restoring a full backup that contains the database login information.
Ignore any errors from the generated checksum. ***If checksum errors are encountered***, SQLsafe should continue to restore the backup file.	Select the **Ignore checksum** errors option.
Retain the settings used when the selected databases were replicated.	Select the **Preserve replication** settings option.

Can I overwrite an existing database?

To restore a database over an existing database, select the **Force Restore** option to ensure SQLsafe writes the selected backup files over the existing database.

Select recovery state

The Recovery State tab of the Restore wizard allows you to choose the recovery state each database should be left in after the restore.

Fully accessible is the only recovery state supported by the InstantRestore feature. If you choose a partial recovery state, you cannot restore your database using InstantRestore. For additional information about performing an InstantRestore, see How InstantRestore works .

Which recovery states are supported?

SQLsafe supports the following recovery states:

- **Fully Accessible**. Leaves the database operational. No additional transaction logs can be restored. Note that you must use this fully-operational recovery state to use InstantRestore.
- **Not Accessible** (no recovery mode). Leaves the database non-operational, but able to restore additional transaction logs.
- **Accessible but read-only** (standby mode). Leaves the database read-only and able to restore additional transaction logs. You can specify an **Undo file** for this option.

Select restore type

The Restore Type section of the Restore wizard allows you to choose whether you want to use the InstantRestore option when restoring your database.

InstantRestore is not available for all restores as not all properties are supported; for example, you cannot restore a SQLsafe backup from a TSM Server. Also note that InstantRestore supports only complete database restores and does not support file or filegroup restores. Additionally, InstantRestore can only work when you choose a Fully Accessible recovery state.

What is the benefit of using InstantRestore?

In most cases, InstantRestore allows you to use the database almost immediately after starting the restore. If you have large databases that you need to access very quickly, this may be the best option for you, but take into account that there may be some performance issues if your users are making changes to the database while the restore is in progress.

InstantRestore will bring the database online quickly allowing you to access your data while SQLsafe continues to restore the database in the background.

What options do you have available on this section?

You can choose between a Normal SQLsafe Restore and a SQLsafe InstantRestore. If you choose the first one, SQLsafe will restore the database using the traditional restore engine and the database will become available when the restore completes. If you choose the InstantRestore option, the database will become available in a fraction of the time that a normal restore normally takes.

Configure notifications for manual restore

The Notifications section of the Restore wizard allows you to email a status notification to the appropriate database administrators about the restore operation. Email notifications let you, and your staff, remotely monitor the status of your restores.

Choose the status you want to monitor, type the email address of each recipient, and then click **Next**.

You must configure your mail server settings before SQLsafe can send email notifications. Click **Configure E-mail** to check your settings. For more information, see Configure e-mail settings for status notifications.

When is the email sent?

SQLsafe sends an email to the specified recipients only when the selected restore status occurs.

Review details for manual restore

The Summary tab of the restore wizard provides the summary of specified values and options you have selected in the Restore Wizard.

What do I do next?

After you have reviewed the information on the Summary tab, click **Restore** to submit the restore job immediately, or click **Generate Script** to create a script you can use to run the job at a later time.

If you choose to run the restore job immediately, and want to verify a successful run, you can view its status in the Instance view. For more information, see View backup/restore operation status.

What actions can I perform on the Summary tab?

Action	Steps
To immediately restore databases	Click **Restore**, and then highlight the instance or database in the tree pane to see the status of the operation.
To create a CLI restore script	Click **Generate Script**, and then click **Command Line**. To save the script to a file, click the save icon or the copy script to clipboard icon. SQLsafe creates a restore script using the settings you specified for the selected databases. You can use this script to perform future restores of any system or user database you selected. Click **Close** to return to the Restore Wizard.
To create a T-SQL restore script	Click **Generate Script**, and then click **T-SQL**. To save the script to file, click the save to a file icon or the copy script to clipboard icon. SQLsafe creates a restore script using the settings you specified. You can use this script to perform future restores of any system or user database you selected. Click **Close** to return to the Restore Wizard. This script requires the SQLsafe XSP. For more information on installing the SQLsafe XSP, see Deploy the SQLsafe XSP. For more information about how to use the SQLsafe XSP, see the sample scripts available from the Programs menu.

How do I verify the status of my restore?

If you want to verify that your restore operation successfully ran, you can view its status using the Instance view. For more information, see View backup/restore operation status.

Report on Backup and Restore Operations

SQLsafe Reports (Reports) provides several built-in reports that allow you to quickly and access backup and restore information. Each report gives detailed information about backups and restores performed by SQLsafe.

Available reports

You can generate any of the following reports. These reports help you better understand and track backup and restore operations, such as measuring the performance of individual backups or monitoring storage consumption. Use these reports to proactively identify and meet the needs of your changing SQL Server environment.

SQLsafe – Backup Owners

This report lists the backups and associated owners for all SQL Server instances and databases registered with SQLsafe. Use this report to monitor backup activity and enforce database security. For example, you can verify that the appropriate database administrators are executing backup operations on the databases they own.

SQLsafe – Backup Performance

This report provides backup performance statistics for the selected SQL Server instances and databases. Use this report to track and compare backup performance.

SQLsafe – Backup Size Chart

This report charts SQLsafe backup sizes for a specific database over time. Use this report to track how the backup size for a particular database has changed.

SQLsafe – Backup Store Utilization

This report indicates how much backup storage space is currently used by the selected SQL Server instances and databases.

SQLsafe – Large Backup

This report lists any SQLsafe backup that is larger than the specified size. Use this report to identify backups that could compromise storage policies.

SQLsafe – Last Backup

This report provides details about the last database backup executed on the selected SQL Server instances and databases. Use this report to monitor or troubleshoot recent backup operations.

SQLsafe restored databases

This report provides details about all database restore activity that occurred in a given date range. Use this report to track restore operations across your SQL Server environment.

SQLsafe storage savings report

This report summarizes the storage cost savings you have gained by using SQLsafe. This savings is calculated using the following formula: (saved MB)/(1024 x cost per MB). Use this report to understand one of the many benefits of using SQLsafe.

Customize reports

You can customize any of the built-in SQLsafe reports or develop new reports that fit your unique needs. If you decide to customize these reports, consider the following best practices:

- Saving your new and modified reports to a separate folder
- Using a different file name for modified reports

For more information about developing custom reports, see the Reporting Services Books Online.

How reports work

Reports seamlessly integrates into Microsoft SQL Server Reporting Services (Reporting Services). For each built-in SQLsafe report, the Reports Installer utility deploys Report Definition Language (RDL) files to the Report Server computer. The RDL files define the report layout and parameters, using the data source (SQLsafe Repository) you specified during install. Reporting Services automatically acknowledges these files, allowing you to immediately generate and view reports on imported data using the Report Manager Web interface.

For more information about the Reporting Services architecture, see the Reporting Services Books Online.

How to run reports

With the appropriate permissions, you can generate and view data directly from the Report Manager Web interface.

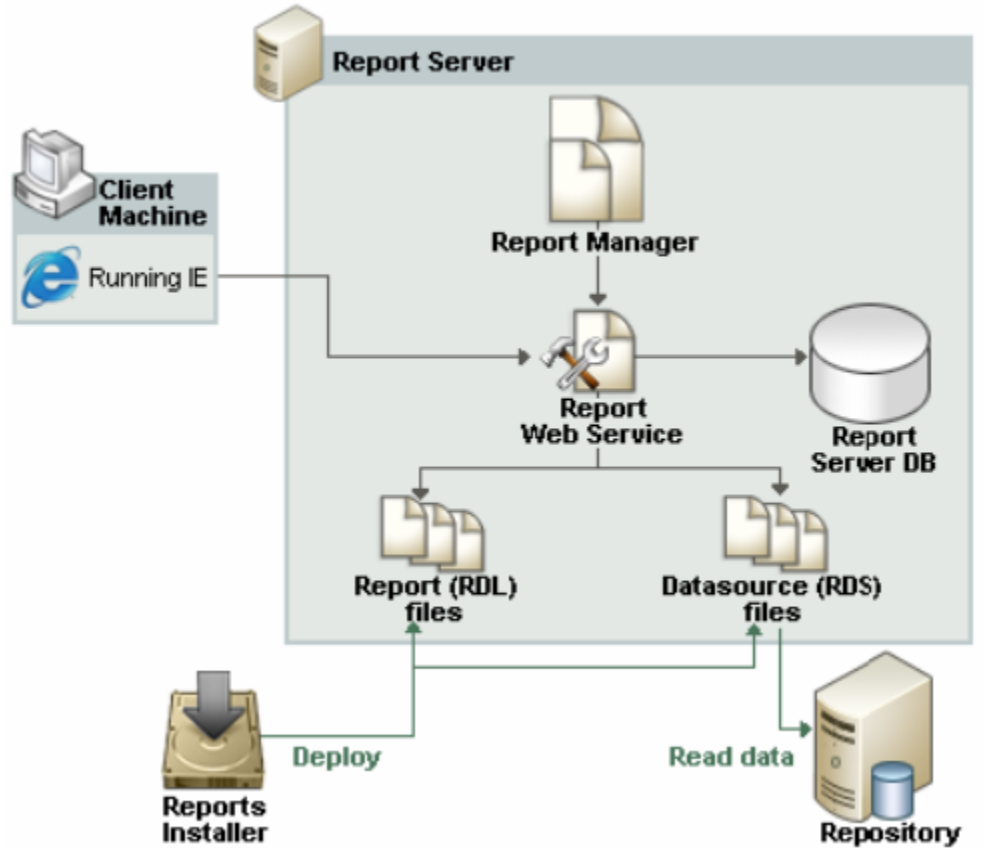
To use Report Manager to run reports:

1. Start Internet Explorer, and then type `http://ReportServerName/Reports` in the Address field. For example, if you are running Reporting Services on the `lab01` server computer, type `http://lab01/Reports`.
2. On the Reporting Services home page, click **SQLsafe**.
3. Click the report you want to run.

> In order to configure Microsoft SQL Server Reporting Services on your computer, you can refer to Reporting Services Configuration Manager (Native Mode).

Deploy reports

You can implement Reports on any computer running Microsoft SQL Server 2000 Reporting Services (Reporting Services) or later. The following installation scenario illustrates how you can implement Reports in an existing SQL Server environment that uses a dedicated Report Server.



Install reports

The Reports setup program installs and runs the Reports Installer utility. The Reports Installer utility allows you to specify the proxy user account credentials and select which built-in SQLsafe reports you want to deploy.

Users with 64-bit installations must follow different steps to install reports. For more information, see Idera solution 3891: Where do I find the SQLsafe reports? in our knowledge base wiki.

The following procedure guides you through a local installation of Reports. However, you can also deploy Reports remotely.

To install reports:

1. Log on with an administrator account to the Report Server computer.
2. Run `Setup.exe` in the root of the installation kit.
3. Read the Welcome window, and then click **Next**.
4. Review and accept the license agreement by selecting **I accept the terms in the license agreement**, and then click **Next**.
5. Accept the default folder for your Reports installation, or click **Change** to specify a different folder, and then click **Next**.
6. Click **Install**.
7. On the Idera SQLsafe Reports Installer window, specify the following configuration settings, and then click **Next**.
   - Report Server Web Service URL. SQLsafe will display the default Reporting Services URL.
   - Name of the computer that hosts the Report Server
   - Name and location of the target SQLsafe Repository
   - Credentials of the Windows account the Report Server should use to connect to the repository database. The specified account should have read permissions on this database.
8. Select which SQLsafe reports you want to deploy to this Report Server, and then click **Next**.
9. Click **Install**.

To successfully deploy reports using this utility, your logon account must have Content Manager rights on the Report Server. For more information, see the Reporting Services Books Online.

Change the report data source

You can change the Reports data source to pull data from a different Repository location. Use the Report Manager to change the data source connection link. For more information, see the Reporting Services Books Online.

Reports permissions and requirements

Reports leverages the existing role-based security model provided with Reporting Services. Reports supports Windows Authentication only (mixed mode on SQL Server).

Reports requires the following permissions and rights to successfully generate reports on your backup and restore data. Assign the appropriate role on the SQLsafe folder in the Report Manager. The individual report files inherit the permissions you set.

By default, the Reports Installer utility deploys the report files to `Program Files\Idera\SQLsafe Reporting Services` on the Report Server computer.

Account	Action	Requirements
Proxy user (specified in data source)	Connect to the SQLsafe Repository and read data per report parameters	Read access to the SQLsafe Repository database
Administrator	Configure reports and set security, run Installer utility	Content Manager role
End user (auditor or manager)	Generate and view reports	Browse role

For more information, on how to access the Report Manager, click Report Manager (SSRS Native Mode) .

Reports requirements

SQLsafe leverages Microsoft SQL Server Reporting Services (Reporting Services) to provide on-the-spot reporting on your backup and restore data. The Report Server computer should meet or exceed the hardware and software requirements recommended by Microsoft to run and manage the Reporting Services components.

SQLsafe supports Reporting Services version 1.0 or later and requires Microsoft Internet Explorer version 6.0 or later. You can generate SQLsafe reports on both 32-bit and 64-bit Report Servers.

Integrate SQLsafe with TSM

Use this TSM Guide to integrate SQLsafe into your existing TSM-based backup and recovery processes. SQLsafe interfaces with the TSM Client API, allowing you to backup and restore directly to the TSM Server while using the SQLsafe user interfaces. By integrating SQLsafe with your TSM deployment, you can immediately receive the benefits of fast, compressed, secure backups as well as several enterprise storage management features – without retooling your current archival workflow.

TSM integration checklist

☑	**Follow these steps ...**
☐	Install the SQLsafe components, and review the supported TSM Client versions.
☐	Install the SQLsafe Backup Agent on each SQL Server instance on which backups will be performed.
☐	Install the TSM Client on the same SQL Server instances, and then configure each TSM Client to connect to the TSM Server. For more information, see the IBM TSM Backup-Archive Clients Installation and User's Guide.
☐	Ask your TSM Administrator to create a new management class for SQLsafe. For more information, see the IBM Tivoli Storage Manager for Windows Administrator's Guide.
☐	Perform a test backup and restore using SQLsafe with TSM settings.
☐	Create policy jobs to enforce consistent backup operations across your TSM environment.

How SQLsafe works with TSM

When you perform a TSM backup, the SQLsafe Backup Agent sends the data files directly to the TSM Server using the TMS Client API, which handles the final storage and management of the backup archives. The SQLsafe Backup Agent uses the TSM Client API options file to locate the TSM Server.

During the backup operation, SQLsafe compresses and optionally encrypts the data files before sending them to the TSM Server, minimizing the impact on your network and storage requirements. The SQLsafe user interfaces expose several TSM parameters, such as retention periods and storage locations, that can help you and the TSM Administrator more easily manage your backup archives. For more information about specific TSM functions, see the IBM TSM Backup-Archive Clients Installation and User's Guide.

How TSM data retention works

Because both SQLsafe and TSM play very important but different roles in determining data file retention, some advance planning and configuration is required before you begin using SQLsafe with TSM.

First, determine your data retention requirements. For example, you may want to groom (delete) backup archive sets after 7 days. Your TSM Administrator will need to create a new management class for SQLsafe and configure the desired data retention period in TSM (such as, retain all backup files for one week).

When configuring TSM, note that SQLsafe accepts up to 260 characters for the TSM file path name.

Once TSM has been configured, backups can now be performed automatically using SQLsafe policies or manually using the SQLsafe CLI or XSP. When you perform a backup, you can define how long SQLsafe should retain a backup archive. Backup archives that age beyond the specified time period will not be available to restore through the SQLsafe user interfaces. However, keep in mind that these data files will be available on the TSM Server until TSM grooms the backup archives according to the retention time.

Setting data retention in SQLsafe Backup Policy jobs

When using the Management Console, you can configure the SQLsafe retention period (Remove files older than) option on the Location tab of the Policy wizard. This option specifies how long SQLsafe should keep this backup archive available for restore. The SQLsafe Backup Agent will automatically mark these data files as inactive on the TSM Server, which allows the files to be groomed (deleted) by TSM. This expiration processing is based on the retention values configured for the SQLsafe management class.

Setting data retention through the CLI

When using the SQLsafe CLI, use the -delete backup option to specify when SQLsafe should make a backup archive as inactive.

For example:

```
sqlsafecmd backup northwind TSM -tsmhighlevel BACKUP -tsmmanagementclass SQLsafe -delete 1weeks
```

You do not need to specify the Low Level filename when grooming files through SQLsafe. The Low Level filename is automatically generated in the following format: `<instance name>_<database name>_<backup type>_<timestamp>.safe`

After the designated time period, SQLsafe marks the backup archives as "deleted" in the Management Console, signaling they are no longer available to restore. However, these backup archives are simply inactive until they are permanently groomed from the TSM Server. You can manually browse inactive backup archives using the TSM Browse command and then manually restore the backup archive

Setting Data Retention through the XSP

When using the XSP, use the `@delete` parameter. This parameter functions in the same way as the `–delete` backup option in the CLI. For more information, see the sample XSP scripts available from the Programs menu.

Back up to the TSM Server

You can use the SQLsafe Backup wizard in the Management Console or the backup command in the CLI or XSP to send a backup directly to your TSM Server.

TSM is case sensitive so special care should be taken when specifying the High Level and Low Level settings. Note that SQLsafe accepts up to 260 characters for the TSM file path name.

Backup wizard

Start the Backup wizard and follow the tabs, setting the appropriate options. On the Locations tab, select **Tape** (Tivoli Storage Manager), and then specify the following required fields:

- High Level
- Low Level
- Management class (optional)
- Client Options File (dsm.opt file)
- Connection Settings

If your backup set is located on a TSM Server other than the server included in the dsm.opt file, you can change the TSM connections settings to override the values set in the client options file. Click **Change** on this option and specify: Node Name, Node Password, Server Address and Server Port.

You can also configure SQLsafe to mark these files as inactive after a specified age.

Example CLI code snippets that use the backup command

You can also perform a backup through the CLI. Additional backup options can be set in the SQLsafe Backup wizard, from which you can generate a CLI script that includes the specified wizard settings. For example:

```
SQLsafeCmd Backup Northwind TSM -TsmClientOwnerName tsmclient -TsmClientOwnerPassword password
-TsmConfigFile "C:\Program Files\Tivoli\TSM\baclient\dsm.opt" -TsmHighLevel Backup -TsmLowLevel
%instance%_%database%_%backuptype%_%timestamp%.safe -TsmManagementClass mclass1 -TsmTcpServerAddress
tsmserver -TsmTcpPort 1500
```

You can use the CLI to change the TSM connections settings for the client options file. The `TsmTcpServerAddress` and `TsmTcpPort` options are compatible with any command that supports TSM.

For more information about available backup options, see the usage statements in the CLI Help.

XSP

You can perform backups using the XSP. The XSP backup parameters function in the same way as backup options in the CLI. For more information, see the sample XSP scripts available from the Programs menu.

Restore a backup from a TSM Server

You can use the SQLsafe Restore wizard in the Management Console or the restore command in the CLI or XSP to restore a backup file directly from your TSM Server.

TSM is case sensitive so special care should be taken when specifying the High Level and Low Level settings. Note that SQLsafe accepts up to 260 characters for the TSM file path name

Restore wizard

Start the Restore wizard and follow the tabs, setting the appropriate options. On the Sources tab, specify where the backup files are located. You can specify the location using either action:

- On the Repository tab, select the database you originally backed up.
- On the Tivoli Storage Manager tab, select the backup files.

Example CLI code snippets that use the restore command

You can also perform a restore through the CLI. Additional restore options can be set in the SQLsafe Restore wizard, from which you can generate a CLI script that includes the specified wizard settings.

```
SQLsafeCmd Restore Northwind TSM -InstanceName SQL2000 -TsmHighLevel Backup -TsmLowLevel
SQLSAFEDEV01_SQL2000_Northwind_Full_200805301028.safe
```

```
SQLsafeCmd Restore Northwind Tsm -InstanceName SQL2000 -TsmHighLevel Backup -TsmLowLevel
SQLSAFEDEV01_SQL2000_Northwind_Log_200805301030.safe
```

You can use the CLI to change the TSM connections settings for the client options file. The `TsmTcpServerAddress` and `TsmTcpPort` options are compatible with any command that supports TSM.

For more information about available restore options, see the usage statements in the CLI Help.

XSP

You can restore data files using the XSP. The XSP restore parameters function in the same way as restore options in the CLI. For more information, see the sample XSP scripts available from the Programs menu.

Automate backups to your TSM Server

Once the SQL Server computer has been properly configured to send and receive information from the TSM Server, you can then create policy jobs that instruct SQLsafe to write backup files directly to the TSM Server.

Start the Backup Policy Wizard and follow the tabs, setting the appropriate options. On the Locations tab, select **Tape** (Tivoli Storage Manager).

SQLsafe will skip any invalid backup types or options. For example, SQLsafe will skip databases that are off-line, will not perform T-Log backups of databases that are in simple mode, and will ignore the object level recovery option when backing up system databases.

Browse archives on the TSM Server

The available backup archives can be viewed (browsed) by right-clicking the target SQL Server instance in the **Servers** navigation pane and selecting **Browse TSM Archives**.You can also view this information through the SQLsafe Restore wizard, CLI, or XSP. You can view a list of all available files including those flagged as inactive.

To browse the TSM Server through the Restore wizard, select **Tivoli Storage Manager** on the Source tab, and then click **Browse**.

To use the XSP browse command, see the sample XSP scripts available from the Programs menu.

Example CLI code snippets that use the browse command

To browse all active files:

```
SQLsafeCmd Browse TSM
```

To browse all active and inactive files:

```
SQLsafeCmd Browse TSM -TSMIncludeInactive
```

To browse all active and inactive files in a Highlevel called BACKUP:

```
SQLsafeCmd Browse TSM -TSMIncludeInactive -TSMHighLevel BACKUP
```

TSM is case sensitive. Be careful when specifying the High Level and Low Level file set.

Extract archives from the TSM Server

You can extract any active backup archive from the TSM Server using the command line interface (CLI). For more information about how to use the TSM commands and options in the CLI, see the usage statements in the CLI Help.

An example CLI codee snippet that uses the extract command

```
SQLsafeCmd extract TSM -BackupFile c:\NW_full.safe -TSMHighLevel Backup -TSMLowLevel
SQLSAFEDEV01_SQL2000_Northwind_Full_2005300847.safe
```

TSM is case sensitive. Be careful when specifying the High Level and Low Level file set.

Mark SQLsafe backup files inactive

You can manually mark any SQLsafe backup that is stored on your TSM Server as inactive using the command line interface (CLI). For more information about how to use the TSM commands and options in the CLI, see the usage statements in the CLI Help.

An example CLI code snippet that uses the expire command

```
SQLsafeCmd expire TSM -BackupFile c:\NW_full.safe -TSMHighLevel Backup -TSMLowLevel
SQLSAFEDEV01_SQL2000_Northwind_Full_2005300847.safe -age 7 days.
```

TSM is case sensitive. Be careful when specifying the High Level and Low Level file set.

SafeToSQL Utility

Use this SafeToSQL Guide to install and use the SafeToSQL utility. This utility helps you easily convert your SQLsafe archive files for use with Microsoft SQL Server. With SafeToSQL, you can use a simple command line statement to save your archive files in `.bak` format, ensuring they are stored in an industry-wide format.

How SafeToSQL works

SafeToSQL provides a quick and easy way to convert SQLsafe archive files to the format used by Microsoft SQL Server. The conversion SafeToSQL performs is useful when you are sending your archive files to someone who may not have SQLsafe installed, and needs to access the archive files for troubleshooting or data migration purposes.

You can execute this conversion though a simple command-line statement from the command shell or in a batch file. When SafeToSQL converts the `.safe` file, the utility appends the name of the backup set index to the `.bak` file name.

How does the utility handle multi-threaded backup sets?

SQLsafe has the capability of creating multi-threaded backup set to multiple virtual devices. When that backup set is converted using SafeToSQL, multiple SQL Server backup files will be created, one for each virtual device.

Why does the utility output multiple backup files from a single SQLsafe archive?

SQLsafe uses multiple processing threads to apply compression and encryption settings during a backup operation. During the backup, SQL Server divides the data between separate backup devices. SQLsafe then writes the finished backup from all of these devices into a single archive file. When SafeToSQL converts the `.safe` file to native format, a separate `.bak` file is created for each device or thread that was used during the original backup. This approach ensures the information can be restored to SQL Server using the same number of devices that were used for the backup. This is a SQL Server requirement.

Deploy the SafeToSQL utility

Use the following information and instructions to successfully deploy the SafeToSQL utility in your production SQL Server environment.

Requirements

Installing and running SafeToSQL requires .NET Framework 2.0, but does not require that you install SQLsafe. Because SafeToSQL will expand your SQLsafe backups to the same size as native backups, you should ensure adequate disk space is available for the converted backups.

How to install SafeToSQL

You can install the SafeToSQL utility from the main setup program.

To install SafeToSQL:

1. Log on with an administrator account to the computer on which you want to install SafeToSQL.
2. Run `Setup.exe` in the root of the installation kit or click **SafeToSQL Utility** on the Install section of the Welcome window.
3. Read the Welcome window, and then click **Next**.
4. Review and accept the license agreement by selecting **I accept the terms in the license agreement**, and then click **Next**.
5. Choose the destination folder, and then click **Next**.
6. Click **Install**.

Create the SafeToSQL command

To use the SafeToSQL utility, run the Command Prompt, and then type the appropriate command syntax for the conversion you need to execute. Use the following descriptions to choose the options you need.

Command syntax

Use the following syntax when converting a SQLsafe archive file:

```
SafeToSQL source_file_path [-backupfile file_name] [ -backupset #] [-password pwd] [-list]
```

Where the following option is mandatory:

source_file_path

Defined as the complete directory path and file name of the SQLsafe archive containing the backup set to convert to Microsoft SQL Server backup format.

Options

The SafeToSQL utility provides the following options.

-backupfile filename

Provides the names of additional files in multi-file archives. You must specify each file in a multi-file archive and provide the complete path to the file.

-backupset #

Specifies the index (1-based) of the backup set in an archive containing multiple backup sets. ***If you do not specify the backup set index,*** the backup set defaults to 1, the index of the first backup set in the archive.

-password pwd

Specifies the password for decrypting an encrypted backup set. ***If the backup set is encrypted,*** provide the password you specified during backup.

-list

Prints out the complete contents of the archive specified by source_file_path.

Output file name format

SafeToSQL uses the following file naming convention for SQLsafe backup files it converts to Microsoft SQL Server backup files:

```
filename_#.bak
```

Where the file name components are as follows:

filename

Specifies the name of the source archive file.

#

Specifies the name of the backup set index.

Example SafeToSQL commands

Use the following example scenarios to create SafeToSQL commands that fit your conversion needs.

Convert an archive with a single backup set

To convert an encrypted archive that contains the *pubs* database as the single backup set, type the following command at the command prompt:

```
SafeToSQL "d:\sqlsafe_backup\LT1_pubs_01_enc.safe" -password my_password
```

The output path and name of the converted file is:

```
d:\sqlsafe_backup\LT1_pubs_01_enc_1.bak
```

Convert an archive with multiple backup sets

To convert an archive that contains the *northwind* database as the second backup set in the archive, type the following command at the command prompt:

```
SafeToSQL "d:\sqlsafe_backup\LT1_multi_01.safe" -backupset 2
```

The output path and name of the converted file is:

```
d:\sqlsafe_backup\LT1_multi_01_2.bak
```

To list the contents of the archive, type the following command at the command prompt:

```
SafeToSQL "d:\sqlsafe_backup\LT1_multi_01.safe" –list
```

Convert an archive saved across multiple files

To convert an archive saved in the directory in two files, type the following command at the command prompt:

```
SafeToSQL "d:\sqlsafe_backup\pubs_a.safe" –additionalfile "d:\sqlsafe_backup\pubs_b.safe"
```

The output path and names of the converted files are:

```
d:\sqlsafe_backup\pubs_a_1.bak
```

```
d:\sqlsafe_backup\pubs_b_1.bak
```

Availability Groups

AlwaysOn Availability Groups are part of an integrated solution, introduced in SQL Server 2012 with the goal of achieving the highest level of data availability and disaster recovery for organizations. Availability Groups grant DBAs the ability to automatically or manually failover a group of databases as a single unit with support for up to four secondary replicas. For additional information on availability groups, see the Microsoft document, Overview of AlwaysOn Availability Groups (SQL Server).

SQLsafe supports SQL Server Availability Groups and allows you to perform backup and recovery strategies on your primary and secondary replicas.

Keep in mind that an agent needs to be installed on all nodes in the availability group that will be considered for backups.

Backup policies with Availability Groups

SQLsafe allows you to configure backup policies with availability groups. The policy includes all the databases in the Availability Group that you want to backup and you can determine which Availability Group members you would like to be taken into account.

Keep in mind that in Availability Groups:

- On primary replicas you can perform full, differential, and log backups
- On secondary replicas, full backups must be copy only, differential backups are not supported, and log backups must NOT be copy only

When SQLsafe performs the backup operation, it detects the preferred replica for the backup operation and it skips the non-preferred ones. Please take into account that if you add a new node as the preferred replica and it is not part of the policy, you will need to add the respective database to the policy.

Restores on Availability Groups

SQLsafe assembles all the necessary files for a restore operation even though the backups were taken from different Availability Group members. You can select which one of the Availability Group members (primary or replica) will be restored.

The **Backup Sets** section in the Restore wizard shows you backups taken from primary and secondary replicas for an Availability Group database.