

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.

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`.

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](#).

TIP 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

Hardware requirements

SQLsafe™

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

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.

TIP *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	Windows administrator permission on the Management Console computer and target database server
	Allows you to install SQLsafe components	
	Allows you to perform SQLsafe tasks, such as executing a backup or restore operation, using standard Windows authentication	Windows administrator permission on the target computer
	Allows you to create the SQLsafe Repository database	db_owner or db_backupoperator role on each user or system database on the registered SQL Server instance
	Allows you to read and write backup files	Create Database Rights on the target SQL Server instance
	Allows you to access the SQLsafe Repository	Windows account credentials with read and write permission on the volume or 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	db_owner or db_backupoperator role on each user or system database on the registered SQL Server instance
	Allows you to create the SQLsafe Repository database	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

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.

TIP 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.

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.

TIP You cannot use the InstantRestore feature on any version of the Windows 2000 operating system or Microsoft SQL Server 7.

General Software Requirements

- Microsoft Data Access Components (MDAC) 2.8 or later
- Microsoft .NET Framework version 2.0 SP1 or later. **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.
- Internet Explorer 7.0 or later (to use the online Help)

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.

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

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.

- Windows 2000 SP4 (Excludes InstantRestore feature support)
- Windows XP Professional SP3 or later
- Windows Server 2003 SP2 or later
- Windows Server 2008 SP1
- Windows Server 2008 R2
- Windows Vista SP1
- Windows 7
- SQL Server 7 (Excludes InstantRestore feature support)
- SQL Server 2000 SP4
- SQL Server 2005 SP1 or later
- SQL Server 2005 Express

SQLsafe supports the following versions of the TSM Client application.

- 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.

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

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

- Repository and Management Service on each node of the Windows cluster
- Management Console on your workstation (can also be installed on the cluster nodes)
- Backup Agent on each cluster node hosting the SQLsafe installation, as well as on any additional virtual SQL Server instances you want to include in your disaster recovery strategy

For more information, see [Deploy Backup Agent to a virtual SQL Server](#) and [Install SQLsafe on clustered Windows servers](#).

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)

TIP 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.

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](#)

TIP 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 **INSTALL** on the Welcome window.
5. Click **INSTALL SQLsafe** on the Install window.
6. On the Welcome 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.

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 on **Install SQLsafe Backup Agent** from the context menu.
4. Choose whether you want to install the SQLsafe XSP.
5. Click **OK**.

Use the following instructions to deploy the SQLsafe Backup Agent to your virtual SQL Server instances. 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. For more information on implementation, see Idera Solution 1394 "How to install the SQLsafe Backup Agent on a clustered SQL Server" in the knowledge base at our [Customer Service Portal](http://www.idera.com/support) (www.idera.com/support).

How to deploy the Backup Agent on a Windows 2003 cluster

1. On each node (computer) in the target cluster, verify that a resource group exists for your target SQL Server cluster. *If the target cluster does not have a SQL Server resource group*, create one.
2. On each node, run the SQLsafe setup program to install the Backup Agent. When prompted to enter service account credentials, specify a Windows account that meets the [permissions requirements](#).
3. Change the Backup Agent service properties to require a manual start.
 - a. Start the Windows Services tool.
 - b. Stop the SQLsafe Backup Service.
 - c. On the **General** tab of the Service Properties window, set the **Startup type** to `Manual`.
4. Log onto the currently active cluster node (primary node) using an administrator account, and then start the Microsoft Cluster Administrator tool.
5. Assign a shared path to the drive being used by the target instance on this node. The target instance is the SQL Server instance that hosts databases you want to back up and restore.
 - a. In the left navigation pane, expand the **Groups** node.
 - b. Select the cluster resource group to which the target instance belongs.
 - c. Use Windows Explorer to create a folder on the physical disk you identified for this resource group.
 - d. Start the Registry Editor and navigate to the `HKLM\SOFTWARE\Idera\SQLsafekey`. For this key, add a **String Value** named `Shared Path` and set it to directory path for the new folder.
6. Create an IP Address resource for the SQLsafe Backup Agent service. *If a Network Name resource already exists*, skip this step.
 - a. Select the cluster resource group for the SQL Server instance you want to back up and restore.
 - b. Create a Network Name resource that will map to the TCP/IP address.
 - c. Add the TCP/IP address as a dependency.
7. Create the Generic Service resource for the SQLsafe Backup Agent service (`SQLsafeBackupService.exe`).
 - a. Select the cluster resource group for the SQL Server instance you want to back up and restore.
 - b. Add a Generic Service resource named SQLsafe Backup Service and specify the following dependencies:
 - The name of the disk used by the SQL Server resource cluster group.
 - This root registry key: `SOFTWARE\Idera\SQLsafe`.
8. In Windows Services, bring the SQLsafe Backup Agent service resource online.

How to deploy the Backup Agent on a Windows 2008 cluster

1. On each node (computer) in the target cluster, verify that a resource group exists for your target SQL Server cluster. *If the target cluster does not have a SQL Server resource group*, create one.
2. On each node, run the SQLsafe setup program to install the Backup Agent. When prompted to enter service account credentials, specify a Windows account that meets the [permissions requirements](#).

Use the following instructions to deploy SQLsafe in a clustered SQL Server environment. When deployment is complete, you can back up and recover databases hosted on your virtual instances. This deployment lets you ensure SQLsafe continues running despite hardware failure or other failover conditions. If you have a clustered environment hosting multiple instances, you must manually deploy the SQLsafe Backup Agent on each node. You cannot remotely deploy the SQLsafe Backup Agent to a cluster server from the console. For more information on implementation, see Idera Solution 1394 "How to install the SQLsafe Backup Agent on a clustered SQL Server" in the knowledge base at our [Customer Service Portal](http://www.idera.com/support) (www.idera.com/support).

Install the SQLsafe Management Service on a clustered Windows server

1. On each node, run the SQLsafe setup program to perform a typical install.
 - o When prompted to enter service account credentials, specify a Windows account that meets the [permissions requirements](#).
 - o When prompted to enter a location for your backup files, choose a UNC path (for example, \\MyServer-MyBackups).
 - o During each install, ensure you specify the same virtual SQL Server instance for the Repository location.
2. Change the properties of the Management Service to require a manual start.
 - a. Start the Windows Services tool.
 - b. Stop the SQLsafe Management Service.
 - c. On the **General** tab of the Service Properties window, set the **Startup type** to `Manual`.
3. Start the Microsoft Cluster Administrator tool, and navigate to the cluster where you have installed SQLsafe.
4. Create a resource group for SQLsafe on that cluster and ensure it contains the following items. For more information about how to create a cluster resource group, see the Microsoft Windows cluster documentation.
 - o A Network Name resource
 - o A Physical Disk resource
 - o A TCP/IP address that was added as a dependency
5. **If you are using a Windows 2003 cluster**, assign a shared path to the drive being used by the SQLsafe cluster resource group, and then continue with step 7.
 - a. In the left navigation pane, expand the **Groups** node.
 - b. Select the SQLsafe cluster resource group.
 - c. Create a folder on the physical disk of this resource group.
 - d. Start the Registry Editor and navigate to the `HKLM\SOFTWARE\Idera\SQLsafe` key. For this key, add a **String Value** named `Shared Path` and set it to directory path for the new folder.
6. **If you are using a windows 2008 cluster**, assign a shared path to the drive being used by the target instance on this node. The target instance is the SQL Server instance that hosts databases you want to back up and restore.
 - a. In the left navigation pane, expand the appropriate domain node, and then expand **Services and Applications**.
 - b. Select the cluster resource group to which the target instance belongs, expand **Disk Drives** in the right pane.
 - c. Create a folder on the physical disk of this resource group.
 - d. Start the Registry Editor and navigate to the `HKLM\SOFTWARE\Idera\SQLsafe` key. For this key, add a **String Value** named `Shared Path` and set it to directory path for the new folder.

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.

- [Configure e-mail settings for alert notifications](#)
- [Configure Management Console preferences](#)
- [Configure the Management Service](#)
- [Import archived backup sets](#)
- [Manage your licenses](#)
- [Modify Backup Agent properties](#)
- [Modify your SQL Server list](#)
- [Register your SQL Server instances with SQLsafe](#)
- [Understand your total cost of operations](#)
- [Upgrade a SQLsafe Lite or Freeware Edition Backup Agent](#)
- [View Backup Agent settings](#)

You can enable SQLsafe to send e-mail 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, or by selecting **E-mail Notification Settings** from the Tools menu.

What e-mail settings can I change?

If you enable e-mail alert notifications, you can configure how the e-mail will appear in your Inbox.

Sender Name

Enter the name that will appear as the sender of the e-mail.

Reply-to Address

Enter the e-mail 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 e-mail alerts.

What mail server information is required?

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

Server Address

Enter the address of your mail server.

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.

SQLsafe allows you to modify many of the default settings of the application, and you can change your Management Console preferences at any time. Reconfiguring these preferences allows you to modify settings in the following categories:

- Backup
- Agent Deployment
- User Experience

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 filenames
- Whether SQLsafe will continue to retry a backup operation if it encounters network errors while writing the backup file
- Number of threads employed in a backup

What agent deployment settings can I change?

On the Agent Deployment tab, you can identify the host of the Management Service for the deployed Backup Agents and the 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 set the display parameters for the console, set the Total Cost of Ownership parameter necessary to calculate your return on investment, and configure troubleshooting settings.

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.

TIP 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 e-mail alerts.

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?

Click **Repository and Management Service Settings** on the Tools menu to configure Management Service settings.

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

TIP 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 source tab of the Restore Wizard.

To import backup archives from a local folder:

1. In the Import window, click on **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 Import window, click on **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 Import window, click on **Browse TSM**.
2. Select the appropriate TSM options file.
3. Enter a High Level and Low Level search parameters.
4. From the **Results** textbox, select the found files to be imported.
5. Review the displayed backup set information and click **OK**.

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

- View the license key associated with each SQL Server instance
- Add or remove license keys

Backup Agents and their associated SQL Server instances are the only licensed components in the SQLsafe architecture. You can also view the current license for a Backup Agent in the Information pane of the Instance View.

How do I manage my licenses?

You may need to add a license if you exhaust your trial license, or if you need to install more SQL Server instances.

To upgrade a trial license to a permanent license:

1. On the Tools menu, click **License Key Manager**.
2. On the License Key Manager window, click **Add**
3. On the Add License Key window, enter the instance name and the license key, separated by a comma.
4. Specify a license key for each instance by pressing **ENTER** after each entry.
5. Click **OK**. The license keys will display in the License Key Manager window.
6. *If you want to save the list to a file*, click **Save to a File** and save the file to your desired location.

What are the terms of the trial license?

By default, SQLsafe installs with a limited time, unlimited instance trial license key. After you install the SQLsafe components using the Typical or Custom setups, the Management Console lists your trial license under Result in the Details pane. You cannot manage the default trial license. This license key is stored in the SQLsafe Repository.

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 these licenses with the License Key Manager. The SQLsafe enterprise edition 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.

The Settings view displays the configuration settings of the Backup Agent running on the selected SQL Server computer. To update settings for a Backup Agent deployed to a specific computer, right-click the computer, and then select **Properties** from the context menu.

How do I access agent settings?

To manage your SQLsafe Backup Agents, click SQLsafe Agents in the navigation pane. To view information about a specific agent, click on the corresponding SQL Server computer listed in the tree pane.

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 how 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.

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**.

TIP 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 would 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.

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 SQLsafe Today view. To group or remove SQL Server instances, right-click the server instance or group in the Server pane. 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.

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.

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.

TIP 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**.

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.

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 license status, the number of databases on the instance, and the SQL Server version it is running.
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.

On each view, you can track the following information:

- [Operations Summary](#)
- [Backup/Restore Operation Status](#)
- [Server Details](#)

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

TIP 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 this 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](#)
- [Install SQLsafe Extended Stored Procedures](#)
- [Enable/Disable SQLsafe InstantRestore](#)
- [SQLsafe Agent Properties](#)

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 **Time-frame** settings.

TIP 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%. <i>If an operation completed with errors</i> , this column will display a red bar labeled Error. <i>If an operation completed with warnings</i> , 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 on 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](#).

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.

To see the detailed results of a specific operation, click on 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.

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.

<input checked="" type="checkbox"/>	Follow these steps ...
<input type="checkbox"/>	Determine the backup types you want to perform for your different SQL Server instances.
<input type="checkbox"/>	Determine what type of compression you need.
<input type="checkbox"/>	Determine the type of encryption you want to use.
<input type="checkbox"/>	Identify which databases should be routinely archived using backup policies .
<input type="checkbox"/>	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.

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. While executing the requested 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. This install requires the SQLsafe license key. For more information, see [Manage license](#).

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.

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.

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](#).

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](http://technet.microsoft.com) (technet.microsoft.com) and [Microsoft Knowledge Base Article #811833](http://support.microsoft.com/kb/811833) (http://support.microsoft.com/kb/811833).

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.

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.

TIP 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.

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.

TIP 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.

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.

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.

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.

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

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 [SQLvdb online Help](#).

Are there disk space recommendations 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](#).

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.

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.

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.

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 e-mail notifications about the policy status.](#)

The Options tab 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.

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 types of compression algorithms are available?

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

TIP 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](#).

Why can't I 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 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.

The Notifications tab allows you to choose the backup statuses about which you want to receive alert notifications through e-mail. E-mail 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**.

TIP 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 e-mail sent?

SQLsafe sends an e-mail 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 e-mailed about a specific status update depends on the notification frequency setting you select. For example, if you want to receive an e-mail whenever a backup fails, even when the failures occur sequentially, choose to receive notifications every time the event occurs.

The Summary tab 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.

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 I 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.

Can I 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 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 on the **Refresh** icon in the pane title bar.

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 I 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.
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.
Disable Policy	Allows you to disable of the selected policy. Backup operations associated with this policy will no longer be performed.
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 ...
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.
View Policy Settings	Allows you to view a summary of the policy settings.

From the Operation Summary grid

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

Action ...	What it does ...
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.
View Details	Shows the Details pane, providing additional information about 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 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, 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 backup operations performed by this policy. Click the status to see more detail about your operations.

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%. <i>If an operation completed with errors</i> , 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, 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 on the column header.

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

What are the details?

To see the detailed results of a specific operation, click on 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	Displays the description you specified for this backup.
Storage Options	Displays which locations were chosen to store the backup files.

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 then monitor its 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 policies 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.

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.

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.](#)

The General tab allows you to specify the basic properties of the log shipping 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.

How does SQLsafe determine that this policy is ok?

SQLsafe determines that the policy is ok 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 stale

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.

Use the Primary tab 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.

Schedule

The schedule for how often the backups will occur. Click **Schedule** to change this frequency.

Backup Options

Click **Backup Options** to change the compression and encryption methods. For more information, see [Change backup options for the log shipping policy](#) .

The Location tab allows you to specify the location for the backups you are creating with this log shipping policy.

What information is required on this tab?

Network Path

This is the location where the backup will be stored. 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.

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

Access As

This is the account SQLsafe will use to access the specified folder. Enter a user account that has access rights to the target location for the backup archive.

TIP The user account used must have read and write permissions to the specified resource.

How do I keep my 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.

The Backup Options window 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

TIP 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](#).

Use the Secondary(s) tab 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. For more information about adding secondary databases, see [Specify secondary database settings for the log shipping policy](#).

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

What information is required 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

Select the database which will receive the transaction log restores.

Initialization

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

By default, SQLsafe will initialize the database with a newly generated full backup.

Database State

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

This setting will affect how the status appears for the secondary database. If you select Not Accessible (No recovery), then the secondary database will show the status as "Restoring" and it will be unusable. If you select Accessible (Standby), then the database will be in a read-only state.

Restore Job

This is how often the restore will occur. Click **Schedule** to change the frequency.

By default, the restore will occur every 15 minutes every day.

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.

The Notifications tab allows you to choose the log shipping statuses about which you want to receive alert notifications through e-mail. E-mail 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 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**.

TIP 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 e-mail sent?

SQLsafe sends an e-mail 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 e-mailed about a specific status update depends on the notification frequency setting you select. For example, if you want to receive an e-mail whenever a backup fails, even when the failures occur sequentially, choose to receive notifications every time the event occurs.

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 which 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](#).

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.

TIP You can create a restore policy for any database that belongs to a [backup policy](#) and has a full backup.

To get started with the Restore Policy wizard:

1. [Name the policy.](#)
2. [Select the target database where the data will be restored.](#)
3. [Select the source database which contains the data you want to restore.](#)
4. [Get e-mail notifications about the policy status.](#)

The General tab allows you to specify the basic properties of the restore 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 restore operation to monitor during a disaster recovery situation.

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

What can I do on this tab?

You can perform the following actions:

- Select the database you want to update using this restore operation
- Specify the location of the data and log files associated with this database
- Select the applicable restore options
- Choose the appropriate recovery state for the database
- Schedule when the Backup Agent should execute the restore job

How do I restore the SQL logins for this database?

You can recover SQL logins associated with this database by selecting the **Restore database logins** option. 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 I do if my 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** button. For more information, see [Register an instance](#).

What do I do if I 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.

The Source tab 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.

TIP SQLsafe requires the selected database to belong to a backup policy. *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 I keep my restores running despite network errors?

Select **Retry reading backup files after network errors**, 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.

The Notifications tab allows you to choose the restore statuses about which you want to receive alert notifications through e-mail. E-mail 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 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**.

TIP 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 e-mail sent?

SQLsafe sends an e-mail 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 e-mailed about a specific status update depends on the notification frequency setting you select. For example, if you want to receive an e-mail whenever a restore fails, even when the failures occur sequentially, choose to receive notifications every time the event occurs.

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.

TIP 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 I 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 button on the Management Console menu bar.
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 the Copy-only, or Verify Backup check box 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 the drop-down list.
7. For any location type, choose to overwrite or append to an existing archive. If you choose to overwrite, you will be prompted to verify your intent to overwrite. For more information, see [Select a location for the backup](#). Click **Next**.
8. 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**.
9. On the Notifications tab, select the e-mail address to which you want to send alert notifications. For more information, see [Configure e-mail notification for the backup](#).
10. On the Summary tab, review your selections. For more information, see [Review the details of the backup](#).

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

What can I 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 the **Register SQL Server**. For more information, see [Register an instance](#).

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

What types of backups can I choose?

SQLsafe supports the standard SQL Server database backup types:

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

What should I do for my initial backup?

If you are backing up the database for the first time, select a 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 I 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 I verify the integrity of my 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 of the database.

The Locations tab 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 I do if I 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 I do if I do have an existing archive?

You can append to an existing archived backup set or choose to overwrite it.

How do I 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.

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

Where can I store my backup set?

SQLsafe supports the following location types:

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

What actions can I 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.

The Options tab 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

TIP 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.
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

The Notifications tab allows you to e-mail a status notification to the appropriate database administrators about this backup. E-mail 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**.

TIP 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 status notifications](#).

When is the e-mail sent?

SQLsafe sends an e-mail 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 e-mailed if the backup is skipped. Because you are performing a manual backup, you will receive one status notification.

The Summary tab provides the summary of specified values and options you have selected in the Backup Wizard.

What do I 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 I verify the status of my 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 I 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 file, click the save to file icon or the copy script to clipboard. 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 file, click the save to file icon or the copy script to clipboard. 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.

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.

<input checked="" type="checkbox"/>	Follow these steps ...
<input type="checkbox"/>	Determine the location of the databases you want to restore to the SQL Server instance in question.
<input type="checkbox"/>	Determine which SQL Server instance should host the recovered databases.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Determine whether you want and are able to use InstantRestore .

TIP 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 file-group 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 from the right-click context menu or the Restore menu on the Management Console menu bar.
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](#). Click **Next**.
5. On the Databases tab, select the database or backup file you want to use for the restore. 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. 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. For more information, see [Enter the database files for the restore](#). Click **Next**.

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 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 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.

TIP You cannot use the InstantRestore feature on any version of the Windows 2000 operating system and Microsoft SQL Server 7.

TIP SQLsafe 7.0 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.

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

The Target tab allows you to you select the instance to which you will restore the database.

What information is on the Target tab?

On the Target tab, you can select the instance to which you will restore the selected databases.

What do I do if my 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** button. For more information, see [Register an instance](#).

What do I do if I 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 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.

The Databases tab allows you to specify the databases you want to restore and the general location of the corresponding archive files. You can select:

- Whether the archive file was written to the local file system
- Whether a network share is available on a remote file system
- 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.

The Backup Sets tab 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.

What do I 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 I 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.

Why would I 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 to. This automatically selects the appropriate backup sets while providing pin-point time accuracy.

How do I 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** button.

How do I keep my restores running despite network errors?

The Database Files tab allows you to enter the database files information for 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 restore-as filename

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. When you change the database path, you must click Apply in order for the changes to be reflected in the grid. You can also simply edit 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
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. <i>If checksum errors are encountered</i> , SQLsafe should continue to restore the backup file.	Select the Ignore checksum errors 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.

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.

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

<input checked="" type="checkbox"/>	Follow these steps ...
<input type="checkbox"/>	Install the SQLsafe components, and review the supported TSM Client versions .
<input type="checkbox"/>	Install the SQLsafe Backup Agent on each SQL Server instance on which backups will be performed.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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.
<input type="checkbox"/>	Perform a test backup and restore using SQLsafe with TSM settings.
<input type="checkbox"/>	Create policy jobs to enforce consistent backup operations across your TSM environment

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)**.

TIP 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.

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
```

TIP TSM is case sensitive. Be careful when specifying the High Level and Low Level file set.

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 code snippet that uses the extract command

```
SQLsafeCmd extract TSM -BackupFile c:\NW_full.safe -TSMHighLevel Backup -TSMLowLevel SQLSAFE-  
DEV01_SQL2000_Northwind_Full_2005300847.safe
```

TIP TSM is case sensitive. Be careful when specifying the High Level and Low Level file set.

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 SQLSAFE-DEV01_SQL2000_Northwind_Full_2005300847.safe -age 7 days
```

TIP TSM is case sensitive. Be careful when specifying the High Level and Low Level file set.

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.

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 through 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.

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.
3. On the Install screen, click **Install SafeToSQL Utility**.
4. Read the Welcome window, and then click **Next**.
5. Review and accept the license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.
6. Choose the destination folder, and then click **Next**.
7. Click **Install**.

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.

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
```