User Guide

STORSTATE
ONLINE BACKUP & RECOVERY®

User Guide

Doc Version: 8.16.09
App Version: 5.5.3.x

Copyright Notice

Trademarks

Disclaimer

Table of Contents

1 Overview

1.1 Highlights

- Easy Backup & Recovery of
  - All file types (MS Office documents, QuickBooks databases, image/bare metal backups, etc)
  - Microsoft Exchange Server 2000 / 2003 / 2007
  - Microsoft SQL Server 7.0 / 2000 / 2005 / 2008
  - Lotus Domino/Notes 5.0 or above
  - Oracle 8i or above
  - MySQL 3.2.4 or above
  - Windows System State for Windows 2000 / XP / 2003
  - Windows Complete System Backup for Windows 2008 and Windows Vista Business / Enterprise / Ultimate edition
  - Bare-metal backup using StorageCraft ShadowProtect
  - One-click selection of important personal files and settings (Outlook/Outlook Express/Windows Mail, My Documents, Desktop, Favorites, etc)
  - Backs up only changes within a file (using Byte-Level Delta technology)
- Supports backing up of open files on Windows (Volume Shadow Copy)
- Supports backing up of Windows NTFS access privileges, Linux access privileges and modes, Mac OS X metadata and resource forks
- Easy to use, deploy and maintain

1.2 Features

- Runs on Windows, Mac OS X, Linux, NetWare, Unix and all other platforms supporting a Java2 Runtime Environment
- Supports both full backup (database backup) and incremental backup (transaction log backup) for Microsoft SQL Server, Microsoft Exchange Server, Lotus Domino/Notes, and Oracle
- Access backup data anytime, anywhere by using a web browser
- Continuous Data Protection – Backup files when they're modified
- Byte-Level Delta backup (backs up only the changes within files – fast and efficient)
- Volume Shadow Copy backup (backup files even when they are exclusively open, ex. Outlook.pst)
- Customizable backup schedule allows backups to be scheduled at any time
- Encryption up to 256-bit with multiple algorithm and mode choices
- Backup and restore Microsoft Exchange individual email, contacts, calendars, tasks etc
- Support for local backup, off-site backup, or both
- Auto Upgrade Agent to automatically upgrade the backup software
- Off-line backup mode and logout backup reminders
- Compresses and encrypts data automatically before sending to the Data Vaulting Center (only compressed and encrypted data is stored)
- Support for increment and differential backup strategies
- Can integrate with external "Open File Manager" to provide open file backup support to all open files
- Comprehensive backup reporting by email lists all files backed up
- Backup data is CRC validated before storage in the Data Vaulting Center
- Fully user customizable data retention policy allows users to have access to deleted or modified files using the least possible storage space in the Data Vaulting Center
- Select source backup files easily by using a backup filter, ex. selecting all *.doc and *.xls in your computer in a single operation
- Run any custom OS commands before/after a backup job
- Choose whether to restore "file permissions" during restore
- Periodic backup file validation at the Data Vaulting Center ensures backup files are 100% valid and fully restorable when needed.

1.3 Security

- 128-bit point-to-point SSL data transfer
- Support for HTTP/HTTPS Proxy and Socks v4/v5 firewall
- Data is encrypted up to 256-bit before leaving your computer and while stored in the Data Vaulting Center
- Choice of different encryption algorithms, ex. Twofish, Triple DES, Advanced Encryption Standard (AES)
- Choice of different encryption modes, ex. Electronic Cook Book (ECB) and Cipher Block Chaining (CBC)
- Random initializing vector, salt and iteration count generated automatically when encrypting each file
- Restrict online access to files based on IP address

1.4 System Requirements

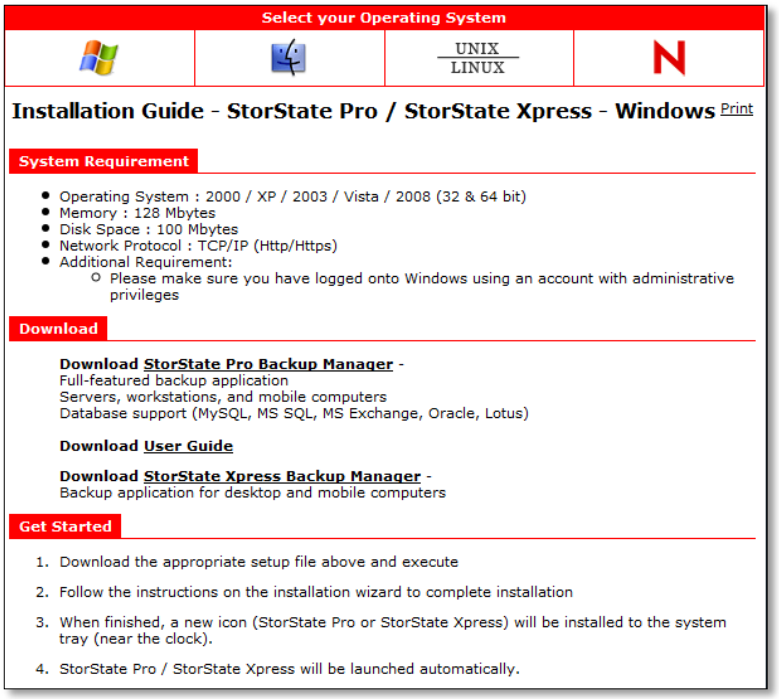
Backup & Recovery Applications			
	Supported Platforms	Application Compatibilities	Hardware Requirements
STORSTATE BACKUP MANAGER® PRO	• Windows 95 / 98 / ME / NT / 2000 / XP / 2003 / Vista / 2008 • Linux kernel 2.4 or above • NetWare 5.2 or above • Solaris 2.x or above • AIX • HP-UX • FreeBSD • Mac OS X 10.3 or above • All other operating systems that support Java2 Runtime Environment 1.4.2 or above	• All file types • Unlimited backup sets • Microsoft Exchange Server 2000 / 2003 / 2007 • Microsoft SQL Server 7.0 / 2000 / 2005 / 2008 • Lotus Domino / Lotus Notes 5.0 or above • Oracle 8i or above • MySQL 3.2.4 or above • Windows System State for 2000, XP, 2003 • Windows Full System Backup for Vista / 2008 • Bare-metal backup using StorageCraft ShadowProtect (sold separately)	• Memory: o 128MB (minimum) o 256MB (recommended) • Disk Space: o 110MB • Network Protocol: o TCP/IP (http/https)
STORSTATE BACKUP MANAGER® PRESS	• Windows 2000 / XP / 2003 / Vista / 2008 • Mac OS X 10.3 or above	• All file types • 1 backup set	• Memory: o 128MB (minimum) o 256MB (recommended) • Disk Space: o 110MB • Network Protocol: o TCP/IP (http/https)

2 Installing StorState Backup Manager

Before you can start backing up data to the StorState Data Vaulting Center, you need to install the StorState Pro/Xpress Backup Manager onto your computer.

2.1 Installing StorState Backup Manager for Windows

1. Download the appropriate StorState Backup Manager installer from the Online Installation Guide: http://www.storstate.com/installguide



2. Follow the instructions on the installation wizard to complete installation

3. When finished, a new icon (StorState Pro or StorState Xpress) will be installed to the system tray (near the clock) and will be launched automatically.

4. The Data Vaulting Center host name is listed in the [Address] field. Only change the host name if instructed so by StorState Support. Click the [Next] button.

5. If you don't have a backup account, register for a trial account:
   i. Enter the [Login Name], [Password] and [Confirm Password] of your choice
   ii. Enter your [Email] in the text field provided
   iii. Press the [Submit] button
   iv. If the [Login Name] of your choice is already taken by another user, please try a different login name
6. If you have a backup account already, select [already a user?] and logon to the Data Vaulting Center with your existing username and password.

7. If this is your first time logging into the server, you will be guided to create a backup set:
   i. Enter a backup set name of your choice in the [Name] field and choose the type of backup set in the [Type] field
   ii. Select the files that you want to backup
   iii. Setup the backup schedule by pressing the [Add] button. You can add multiple backup schedules to

a backup set.

iv. Setup the encryption setting for your backup set. IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!

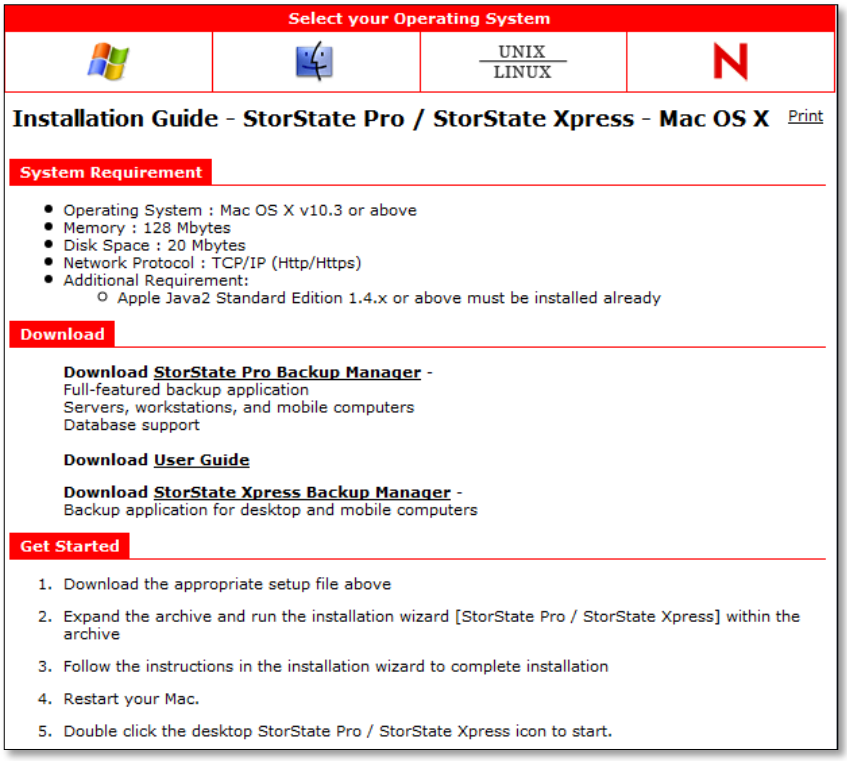
v. Press the [OK] button to complete the configuration of the backup set. Scheduled backups will run automatically if you leave your computer on.

IMPORTANT: If this isn't the first time this StorState account has been used and it has pre-existing backup sets, you will be prompted to setup the encryption for each existing backup set. It is important to use the same key and settings that were used when the set was created. Otherwise, files backed up in the future will use different encryption than existing files, complicating restore operations.

8. To run a backup immediately, click the [Backup] button on the left panel, select the backup set (Pro only) and press the [OK] button.

2.2 Installing StorState Backup Manager for Mac OS X

1. Download the appropriate StorState Backup Manager installer from the Online Installation Guide: http://www.storstate.com/installguide



2. Expand the archive and run the installer within the archive. Follow the on screen instructions to install.

3. After installation, restart your Mac if prompted, then double-click the desktop StorState Pro or Xpress icon to start.

4. The Data Vaulting Center host name is listed in the [Address] field. Only change the host name if instructed so by StorState Support. Click the [Next] button.

5. If you don't have a backup account, register for a trial account:
   i. Enter the [Login Name], [Password] and [Confirm Password] of your choice
   ii. Enter your [Email] in the text field provided
   iii. Press the [Submit] button
   iv. If the [Login Name] of your choice is already taken by another user, please try a different login name
6. If you have a backup account already, select [already a user?] and logon to the Data Vaulting Center with your existing username and password.

7. If this is your first time logging into the server, you will be guided to create a backup set:
   i. Enter a backup set name of your choice in the [Name] field and choose the type of backup set in the [Type] field
   ii. Select the files that you want to backup
   iii. Setup the backup schedule by pressing the [Add] button. You can add multiple backup schedules to a backup set.
   iv. Setup the encryption setting for your backup set. IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on

your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!

v. Press the [OK] button to complete the configuration of the backup set. Scheduled backups will run automatically if you leave your computer on.

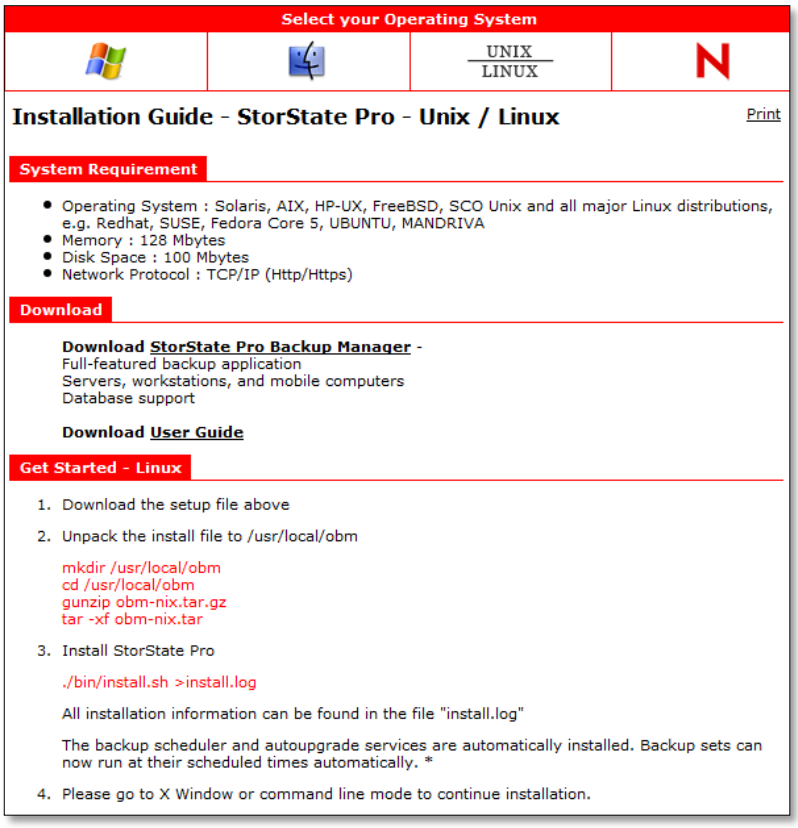
IMPORTANT: If this isn't the first time this StorState account has been used and it has pre-existing backup sets, you will be prompted to setup the encryption for each existing backup set. It is important to use the same key and settings that were used when the set was created. Otherwise, files backed up in the future will use different encryption than existing files, complicating restore operations.

8. To run a backup immediately, click the [Backup] button on the left panel, select the backup set (Pro only) and press the [OK] button.

2.3 Installing StorState Backup Manager for Linux/Unix/Solaris

Linux

1. Download the StorState Pro Backup Manager installer from the Online Installation Guide: http://www.storstate.com/installguide



2. Unpack the install file to /usr/local/obm

```
# mkdir /usr/local/obm
# cd /usr/local/obm
# gunzip obm-nix.tar.gz
# tar -xf obm-nix.tar
```

3. Install StorState Pro

```
# ./bin/install.sh >install.log
```

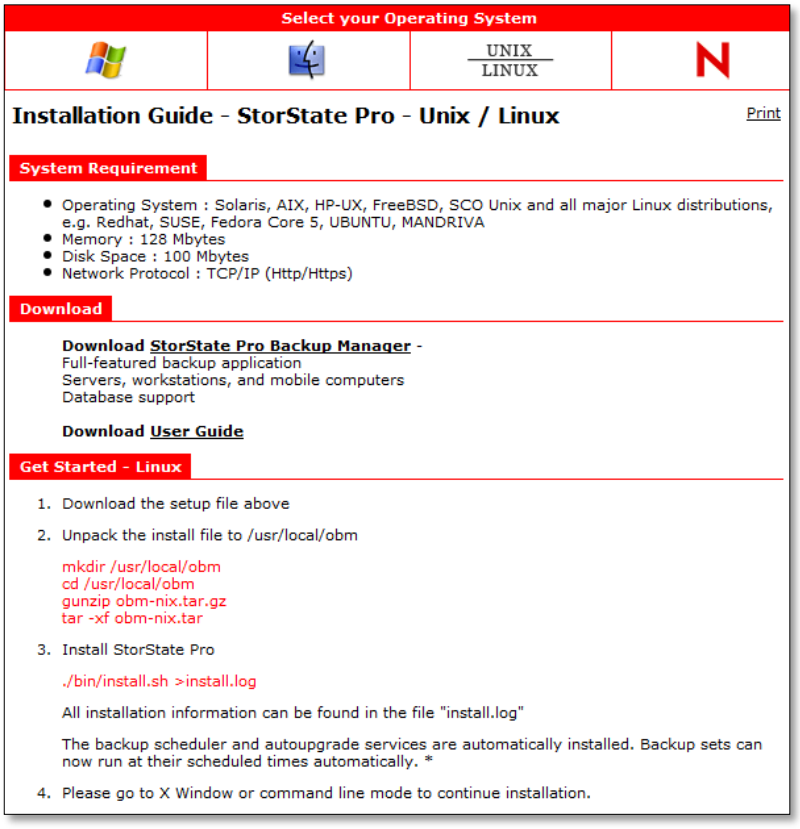
All installation information can be found in the file "install.log"

The backup scheduler and autoupgrade services are automatically installed. Backup sets can now run at their scheduled times automatically.

4. Please go to X Window or Command Line Mode to continue installation.

Solaris

1. Download the StorState Pro Backup Manager installer from the Online Installation Guide: http://www.storstate.com/installguide



2. Unpack the install file to /usr/local/obm

```
# mkdir /usr/local/obm
# cd /usr/local/obm
# gunzip obm-nix.tar.gz
# tar -xf obm-nix.tar
```

3. Remove the bundled jvm

```
# rm -rf /usr/local/obm/jvm
```

4. Install J2SE Java Runtime Environment (JRE) 1.4.x or later to /usr/java

5. Create a symbolic link for JRE

```
# ln -s /usr/java /usr/local/obm/jvm
```

6. Set the JAVA_HOME environment variable

```
# JAVA_HOME=/usr/java; export JAVA_HOME
```

7. Install StorState Pro

```
# ./bin/install.sh >install.log
```

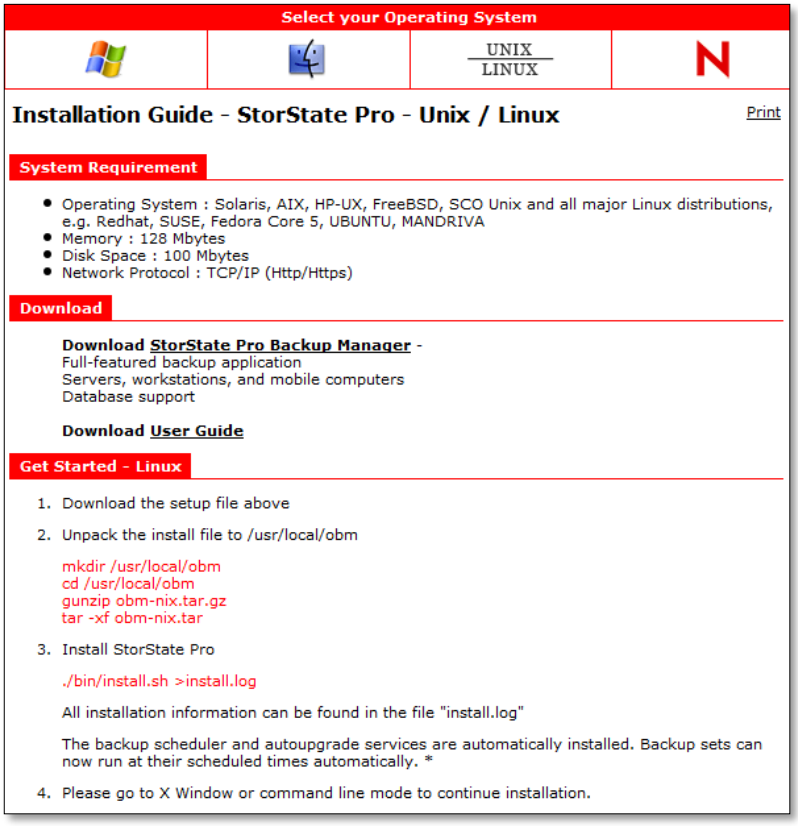
All installation information can be found in the file "install.log"

The backup scheduler and autoupgrade services are automatically installed. Backup sets can now run at their scheduled times automatically.

8. Please go to X Window or Command Line Mode to continue installation.

BSD

1. Download the StorState Pro Backup Manager installer from the Online Installation Guide: http://www.storstate.com/installguide



2. Unpack the install file to /usr/local/obm

```
# mkdir /usr/local/obm
# cd /usr/local/obm
# gunzip obm-nix.tar.gz
# tar -xf obm-nix.tar
```

3. Remove the bundled jvm

```
# rm -rf /usr/local/obm/jvm
```

4. Download J2SE Java Runtime Environment (JRE) 1.4.x or later

Depending on your platform and BSD release, download the corresponding JRE and dependant packages. For example, we are using FreeBSD 6.1 i386 for installation:

Download javavmwrapper-2.3.tbz and diablo-jre-freebsd5.i386.1.5.0.07.01.tbz from the following links.

http://www.freebsd-fr.org/ports/java.html#javavmwrapper-2.3
http://www.freebsdfoundation.org/downloads/java.shtml
http://www.freebsd.org/ports/java.html#diablo-jre-1.5.0.07.01_3 (See package dependency of your machine)

5. Install J2SE Java Runtime Environment (JRE) 1.4.x or later to /usr/local/diablo-jre1.5.0

   Use following commands to install the packages
   # pkg_add javavmwrapper-2.3.tbz
   # pkg_add diablo-jre-freebsd5.i386.1.5.0.07.01.tbz

6. Create a symbolic link for JRE

   # ln -s /usr/local/diablo-jre1.5.0 /usr/local/obm/jvm

   If you are using csh as your shell, you need to type "rehash" and hit enter to make the symbolic link take effect.

   # setenv JAVA_HOME /usr/local/obm/jvm

7. Verify the installed JRE

   $JAVA_HOME/bin/java –version

   Check for warnings in the output:

   With warning

   Java HotSpot(TM) Client VM warning: Can't detect initial thread stack location java version "1.4.2_12"
   Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_12-b03)
   Java HotSpot(TM) Client VM (build 1.4.2_12-b03, mixed mode)

   Without warning

   java version "1.5.0"
   Java(TM) 2 Runtime Environment, Standard Edition (build diablo-1.5.0-b01)
   Java HotSpot(TM) Client VM (build diablo-1.5.0_07-b01, mixed mode)

8. Install StorState Pro

   # ./bin/install.sh >install.log

   All installation information can be found in the file "install.log"

9. Install the backup scheduler and autoupgrade services

   Add two entries to system file /etc/rc.conf for auto starting backup scheduler and autoupgrade agent.

   # obmaua_enable="YES"
   # obmscheduler_enable="YES"

   Restart computer or run the following scripts

   # /usr/local/etc/rc.d/obmscheduler start &
   # /usr/local/etc/rc.d/obmaua start &

   Backup sets can now run at their scheduled times automatically.

10. Please go to X Window or Command Line Mode to continue installation.

X-Windows

1. Set the DISPLAY environment variables

   Linux / Unix (sh, bash): DISPLAY=IP_ADDRESS_OF_XTERMINAL[:0.0]; export DISPLAY

   For example:
   DISPLAY=:0.0; export DISPLAY
   or DISPLAY=127.0.0.1; export DISPLAY
   or DISPLAY=127.0.0.1:0.0; export DISPLAY
   or DISPLAY=192.168.0.2; export DISPLAY
   or DISPLAY=192.168.0.2:0.0; export DISPLAY

   BSD (csh): setenv DISPLAY IP_ADDRESS_OF_XTERMINAL[:0.0]

   For example:
   setenv DISPLAY :0.0
   or setenv DISPLAY 127.0.0.1
   or setenv DISPLAY 127.0.0.1:0.0
   or setenv DISPLAY 192.168.0.2
   or setenv DISPLAY 192.168.0.2:0.0

2. Run StorState Pro Backup Manager

   # sh /usr/local/obm/bin/RunOBC.sh &

3. The Data Vaulting Center host name is listed in the [Address] field. Only change the host name if instructed so by StorState Support. Click the [Next] button.

4. If you don't have a backup account, register for a trial account:
   i. Enter the [Login Name], [Password] and [Confirm Password] of your choice
   ii. Enter your [Email] in the text field provided
   iii. Press the [Submit] button
   iv. If the [Login Name] of your choice is already taken by another user, please try a different login name
5. If you have a backup account already, select [already a user?] and logon to the Data Vaulting Center with your existing username and password.

6. If this is your first time logging into the server, you will be guided to create a backup set:
   i. Enter a backup set name of your choice in the [Name] field and choose the type of backup set in the [Type] field
   ii. Select the files that you want to backup
   iii. Setup the backup schedule by pressing the [Add] button. You can add multiple backup schedules to a backup set.
   iv. Setup the encryption setting for your backup set. IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!
   v. Press the [OK] button to complete the configuration of the backup set. Scheduled backups will run automatically if you leave your computer on.

   IMPORTANT: If this isn't the first time this StorState account has been used and it has pre-existing backup sets, you will be prompted to setup the encryption for each existing backup set. It is important to use the same key and settings that were used when the set was created. Otherwise, files backed up in the future will use different encryption than existing files, complicating restore operations.

7. To run a backup immediately, click the [Backup] button on the left panel, select the backup set and press the [OK] button.

Command Line Mode

1. Login to your Web Management Console to add, update and remove backup sets:
   https://www.storstate.com/login/
   i. If you want to update a backup set, make changes to the backup set and press the [Update] button
   ii. If you want to add a new backup set, click the [Add] link
   iii. If you want to remove a backup set, select the backup set to be removed and click the [Remove] link
2. Use the Backup Configurator to configure your computer

   ```
   # sh /usr/local/obm/bin/Configurator.sh
   ```

3. Enter your Login Name, Password, Data Vaulting Center URL and proxy setting if needed

   ```
   Login Name: userXXX
   Password: ********************
   Data Vaulting Center URL: dvc1.storstate.com
   Which Protocol ? (1) Http (2) Https : 1
   Use proxy ? (Y)es or (N)o : Y
   Proxy Type ? (1) Http/Https Proxy (2) SOCKS : 1
   Enter proxy server : aaa.bbb.com
   Enter proxy port : xxx
   Enter proxy username (optional) : administrator
   Enter proxy password (optional) : ********************
   ```

   If you have created a new backup set using the Web Management Console, you set the encrypting key, the encrypting algorithm and the encryption mode of this backup set by following the instructions below.

   IMPORTANT: If this isn't the first time this StorState account has been used and it has pre-existing backup sets, you will be prompted to setup the encryption for each existing backup set. It is important to use the same key and settings that were used when the set was created. Otherwise, files backed up in the future will use different encryption than existing files, complicating restore operations.

   THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!

   ```
   Found new backup set 'xxx'
   Please enter the following values for this backup set:

   Encrypting Algorithm ?
   (1) Twofish (2) AES (3) Triple DES (4) No encryption : 1
   Encrypting Key: ********************
   Re-Enter Encrypting Key: ********************
   Encrypting Mode ? (1) ECB (2) CBC : 1
   Run scheduled backup on this computer ? (Y)es or (N)o : Y
   ```

4. If you want to make any changes to the settings above, you can use the main menu below to do so.

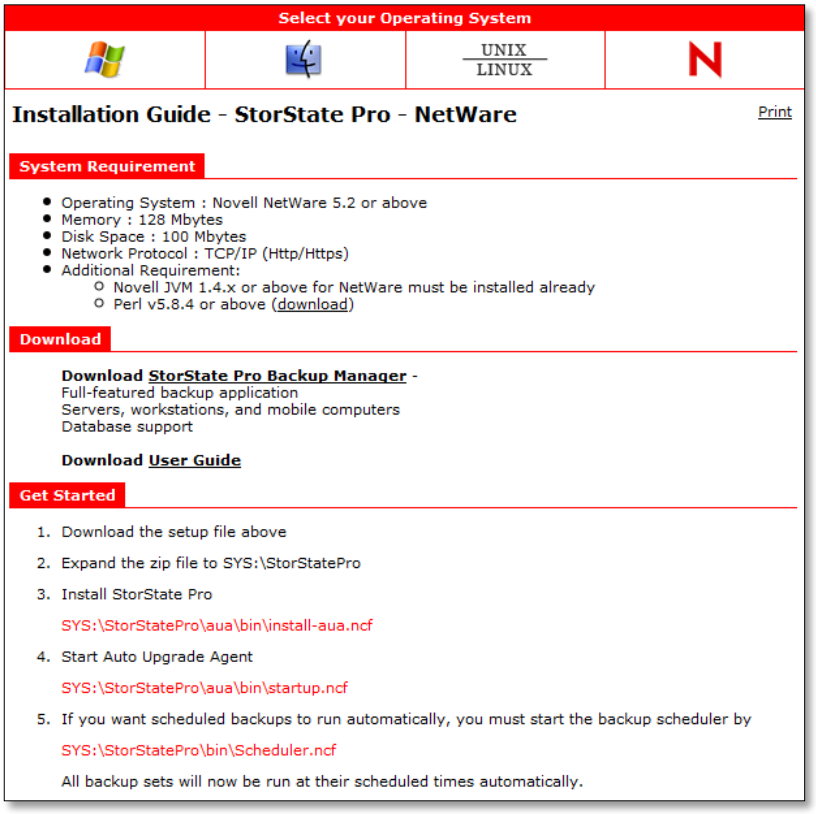
   ```
   Main Menu:
   ------------
   (1). List Backup Setting
   (2). Change Password
   (3). Change Network Setting
   (4). Change run scheduled backup setting
   (5). Toggle Masked Field (Password, Encryption Key)
   (6). Generate Configuration Report (text format)
   (7). Quit

   Your Choice:
   ```

5. You can then run a backup by executing the command below, where [BACKUP_SET] is the backup set to run.

   ```
   # sh /usr/local/obm/bin/RunBackupSet.sh [BACKUP_SET]
   ```

2.4 Installing StorState Backup Manager for Netware

1. Download the StorState Pro Backup Manager installer from the Online Installation Guide: http://www.storstate.com/installguide



2. Expand the zip file to SYS:\StorStatePro

3. Install StorState Pro

   SYS:\> SYS:\StorStatePro\aua\bin\install-aua.ncf

4. Start Auto Upgrade Agent

   SYS:\> SYS:\StorStatePro\aua\bin\startup.ncf

5. Start the backup scheduler

   SYS:\> SYS:\StorStatePro\bin\Scheduler.ncf

   All backup sets will now be run at their scheduled times automatically.

6. Open StorState Pro by running SYS:\StorStatePro\bin\RunBackupManager.ncf

9. The Data Vaulting Center host name is listed in the [Address] field. Only change the host name if instructed so by StorState Support. Click the [Next] button.

10. If you don't have a backup account, register for a trial account:
    i. Enter the [Login Name], [Password] and [Confirm Password] of your choice
    ii. Enter your [Email] in the text field provided

iii. Press the [Submit] button

iv. If the [Login Name] of your choice is already taken by another user, please try a different login name

11. If you have a backup account already, select [already a user?] and logon to the Data Vaulting Center with your existing username and password.

12. If this is your first time logging into the server, you will be guided to create a backup set:

    i. Enter a backup set name of your choice in the [Name] field and choose the type of backup set in the [Type] field

    ii. Select the files that you want to backup

    iii. Setup the backup schedule by pressing the [Add] button. You can add multiple backup schedules to a backup set.

    iv. Setup the encryption setting for your backup set. IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!

    v. Press the [OK] button to complete the configuration of the backup set. Scheduled backups will run automatically if you leave your computer on.

IMPORTANT: If this isn't the first time this StorState account has been used and it has pre-existing backup sets, you will be prompted to setup the encryption for each existing backup set. It is important to use the same key and settings that were used when the set was created. Otherwise, files backed up in the future will use different encryption than existing files, complicating restore operations.

13. To run a backup immediately, click the [Backup] button on the left panel, select the backup set and press the [OK] button.

3 Uninstalling StorState Backup Manager

This section describes the steps required to uninstall the StorState Pro/Xpress Backup Manager from your computer.

3.1 Uninstalling StorState Backup Manager for Windows

1. Open [Start] -> [Control Panel] -> [Add/Remove Programs]
2. Select [StorState Pro/Xpress Backup Manager] from the list and press the [Remove] button

3.2 Uninstalling StorState Backup Manager for Mac OS X

1. Remove all program files by running

   ```
   # cd $OBM_HOME/bin
   # sudo ./uninstall.sh
   ```

2. Remove all backup setting by removing ~/.obm

   ```
   # rm –rf ~/.obm
   ```

3. Restart your computer

3.3 Uninstalling StorState Backup Manager for Linux/Unix/Solaris

1. Run the uninstall script

   ```
   # sh /usr/local/obm/bin/uninstall.sh

   Removing Scheduler from service using script name obmscheduler
   Using init script path /etc/init.d
   Using run level script path /etc/rc.d
   Removing symbolic link from run levels
   Removing script file obmscheduler from /etc/init.d
   Shutting down AutoUpdateAgent
   Waiting 5 seconds for AutoUpdateAgent to clean up
   Removing AutoUpdateAgent from service using script name
   Using init script path /etc/init.d
   Using run level script path /etc/rc.d
   Removing symbolic link from run levels
   Removing script file obmaua from /etc/init.d
   Online Backup Manager uninstall service is complete!
   It is now safe to remove files from /usr/local/obm
   ```

2. Remove installed files and all application data

   ```
   #rm -rf /usr/local/obm
   #rm -rf ~/.obm
   ```

3.4 Uninstalling StorState Backup Manager for Netware

1. Stop the running backup scheduler by running

   ```
   SYS:\> touch SYS:\StorStatePro\ipc\Scheduler\stop
   ```

2. Stop the running auto upgrade agent by running

   ```
   SYS:\> SYS:\StorStatePro\aua\bin\shutdown.ncf
   ```

3. Remove all program files by removing the directory SYS:\StorStatePro

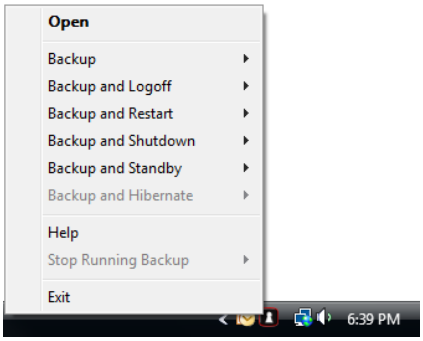
4. Remove all backup settings by removing the directory SYS:\.OBM

4 Using StorState Backup Manager

This chapter will describe all the features available in StorState Pro/Xpress Backup Manager and outline how you can use StorState to meet various backup needs.

4.1 System Tray Launcher (Windows Only)

After you have successfully installed StorState Backup Manager onto your computer, a StorState icon will be added to the system tray area (next to your system clock) automatically.

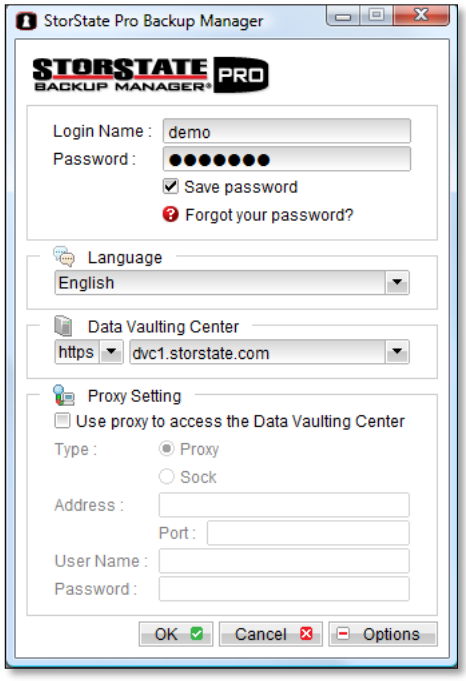


This icon is the entry point to StorState Backup Manager. Right clicking the icon will show a menu that provides the following functions:

Menu Item	What it does
Open	Run StorState Backup Manager
Backup	Runs a specific backup set (or all backup sets) chosen from the sub-menu in silent background mode.
Backup and Logoff	Runs a specific backup set (or all backup sets) chosen from the sub-menu in silent background mode and then logoff from Windows when finished.
Backup and Restart	Runs a specific backup set (or all backup sets) chosen from the sub-menu in silent background mode and restart Windows when finished.
Backup and Shutdown	Runs a specific backup set (or all backup sets) chosen from the sub-menu in silent background mode and shutdown the computer when finished.
Backup and Standby	Runs a specific backup set (or all backup sets) chosen from the sub-menu in silent background mode and enter the Standby mode of Windows.
Backup and Hibernate	Runs a specific backup set (or all backup sets) chosen from the sub-menu in silent background mode and enter the Hibernate mode of Windows.
Help	Shows a help dialog
Stop running backup	Interrupts a running backup set (or all backup sets) chosen from the sub-menu.
Exit	Close this system tray launcher application.

4.2 Logon Dialog

Before you can use StorState Backup Manger, you must be authenticated by the Data Vaulting Center first. Enter your username and password.



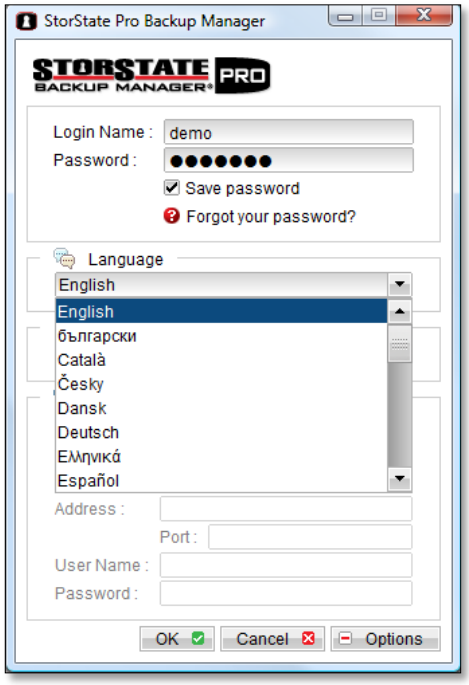
For secure communications, we recommend you use SSL (Secure Socket Layer) by selecting the [https] option.

The [Address] field shows the network address of the Data Vaulting Center to which StorState Backup Manager will connect to authenticate your username and password. Please leave the default address, or enter the address provided to you by StorState Support.

If you need to connect to the server through proxy, enter your proxy setting in the [Proxy Setting] section. For [SOCKS] proxy, both v4 and v5 without user authentication are supported.

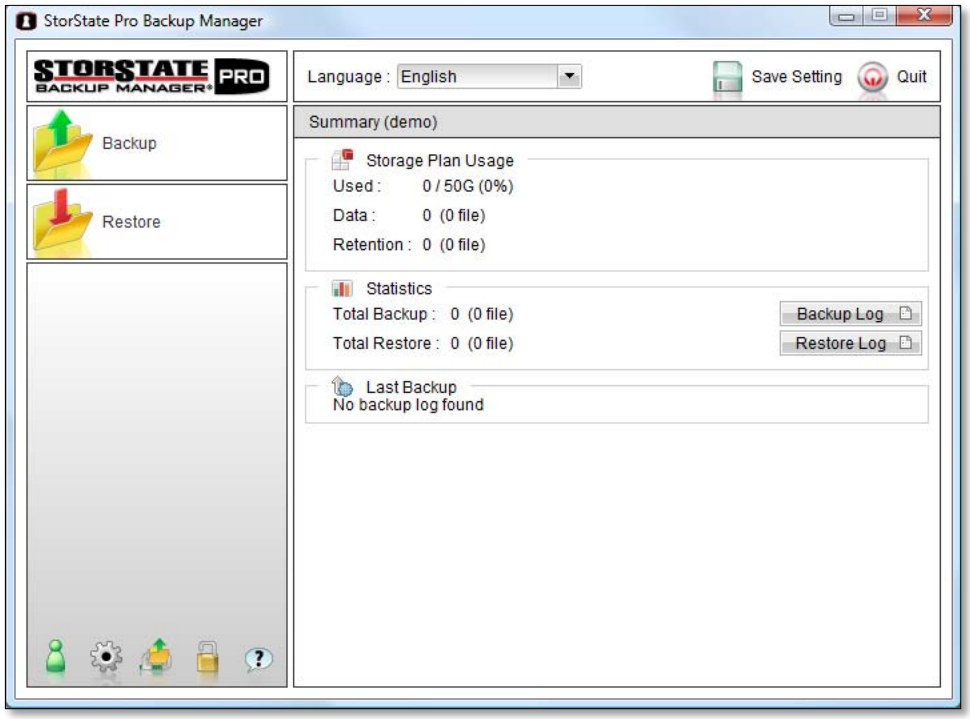
4.3 Language Selection

You can switch the language of the StorState Backup Manager user interface by choosing the desired language available from the [Language] drop down list.



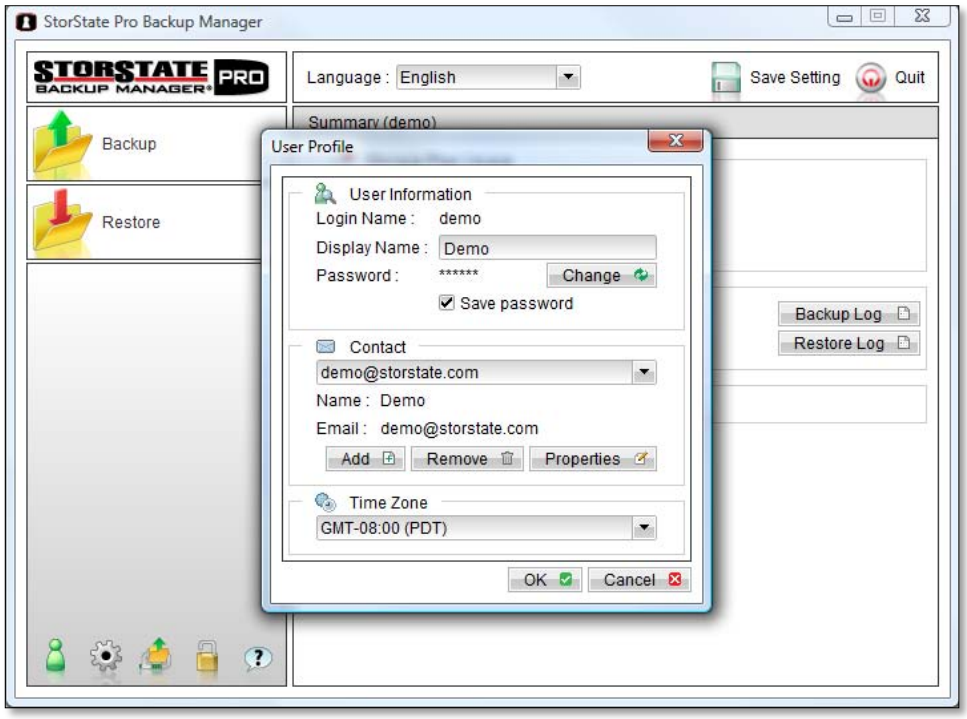
4.4 Main Window

Press [OK] to logon. After authentication, the StorState Backup Manager main window appears.



4.5 User Profile

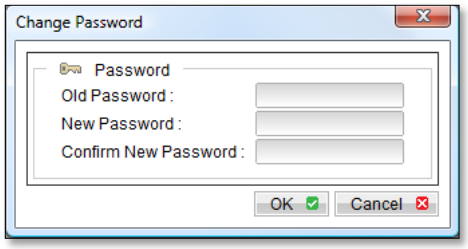
You can then use StorState Backup Manager to update your user profile. Press the button to open the [User Profile] dialog.



To change your [Display Name], enter the new display name in the [Display Name] field and press [OK].

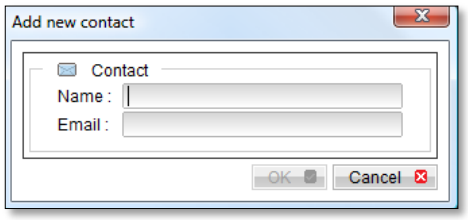
To change your account password, press the [Change] button next to the password field. A [Change Password] dialog will appear. Enter your original password and new password into the text field of this dialog and press [OK].

PLEASE NOTE: This changes the User Account password only, not the encryption/decryption key for any backup sets. Backup Set encryption keys cannot be changed once created.



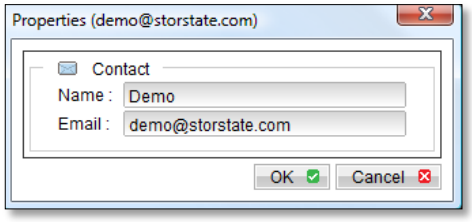
To change your [Time Zone], select your time zone from the drop down list next to the time zone entry.

To add a new contact to this account, press the [Add] button in the [Contact] section. A [Add New Contact] dialog will appear. Enter a name and an email address in the text fields provided and then press the [OK] button.



To remove a contact, select the email address that is to be removed from the list and press the [Remove] button. Press [OK] to confirm the removal.

To update a contact email address, select the email address that is to be updated from the list and press the [Properties] button. A [Properties] dialog will appear. After you have made the changes that you want, press the [OK] button.



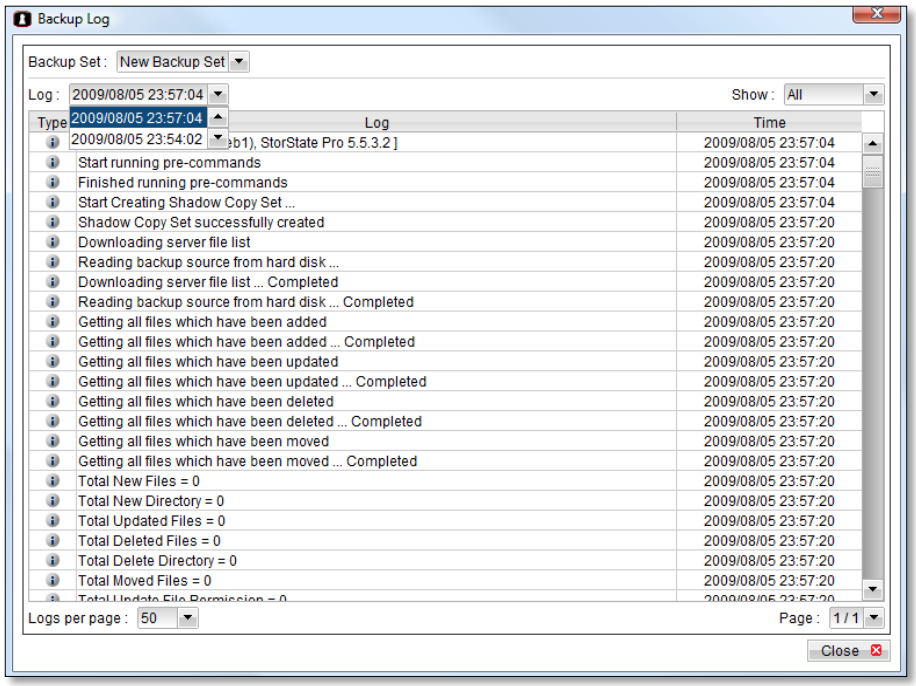
4.6 Backup Logs

All backup activities are logged to backup activity log files. They are available for review from within StorState Backup Manager. To review backup jobs:

1. Press the [Backup Log] button on the StorState Backup Manager main window.

2. Select the Backup Set you want to review from the [Backup Set] drop down list.

3. Select the Backup Job you want to review from the [Log] drop down list.

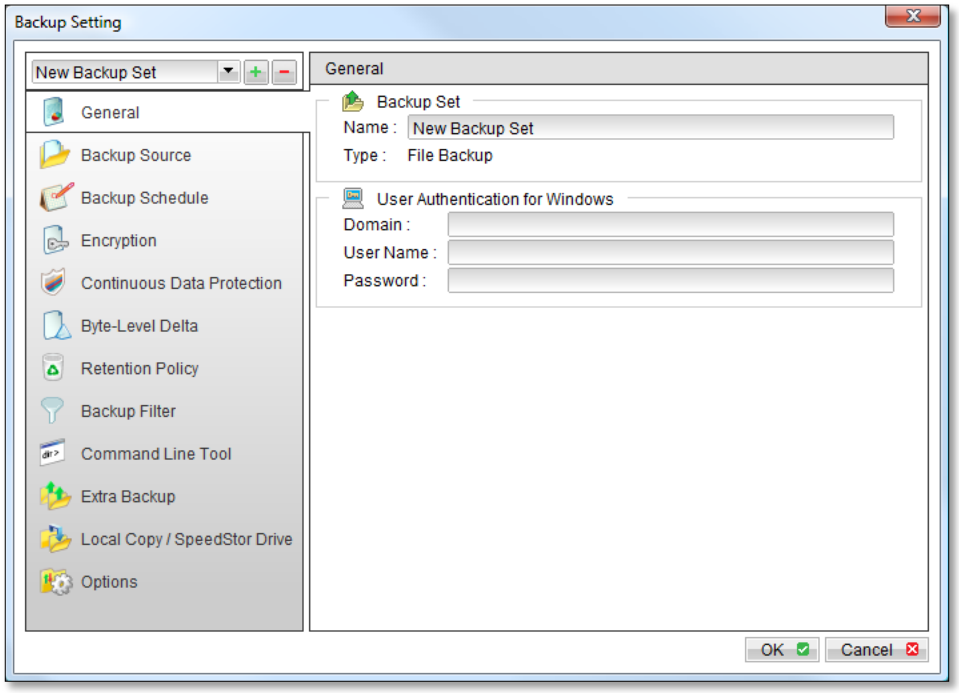


5 Setting Up Backup Sets

A backup set contains all backup settings for a backup operation. This section will describe all features available within a backup set.

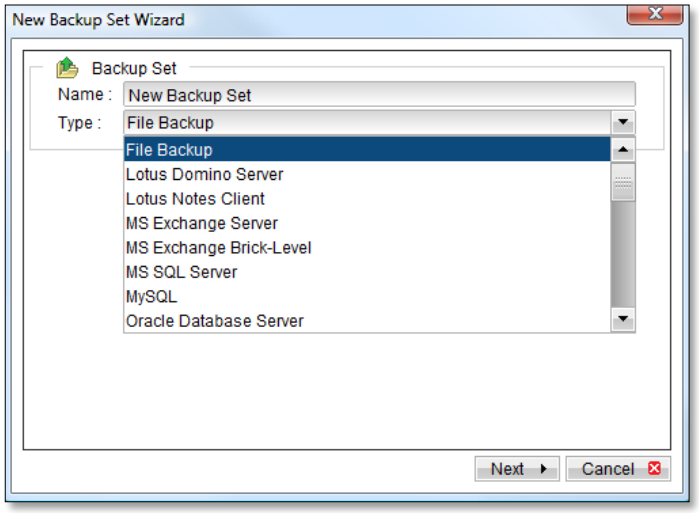
StorState Pro allows multiple backup sets while StorState Xpress allows one backup set. Each backup set is an individual and independent entity. For example, you may have one backup set for user files and another for MS Exchange data. StorState Pro contains plugins for many server types while StorState Xpress is limited to File Backup. The setup instructions below pertain to StorState Pro, setup for StorState Xpress is similar.

To add a backup set, click the button to open the [Backup Setting] dialog. As an example, let's create a "New Backup Set" for the rest of this chapter.



On the left panel, press the button to create a new backup set.

5.1 Backup Set Type



A backup set can be of one of the following types:

Backup Type	Description
File Backup	Backup common files/directories
Lotus Domino/Notes	Backup Lotus Domino/Notes
MS Exchange Server	Backup Microsoft Exchange Server 2000 / 2003 / 2007
MS Exchange Brick-Level	Backup individual emails, contacts, calendars, tasks, etc from Microsoft Exchange Server 2000 / 2003 / 2007
MS SQL Server	Backup Microsoft SQL Server 7.0 / 2000 / 2005
MySQL	Backup MySQL Server
Oracle Database Server	Backup Oracle databases
Windows System State	Backup Microsoft Windows System State for 2000 / XP / 2003
ShadowProtect System Backup	Bare-Metal backup using StorageCraft ShadowProtect (must purchase separately)
MS Windows System Backup	Complete System Backup for Windows 2008 and Windows Vista Business / Enterprise / Ultimate edition

Backup set type is defined at backup set creation and cannot be modified. If you want to change the backup set type, you have to create a new backup set.

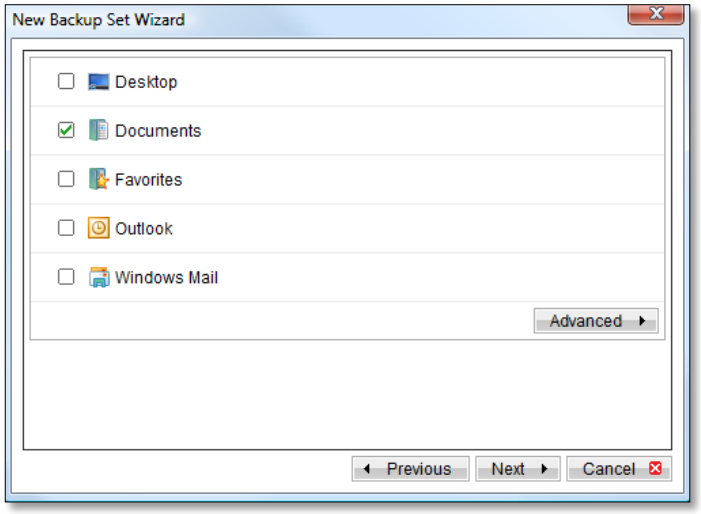
5.2 Backup Source

A “Backup Source” defines the files/directories that are to be included in a backup set. There are two types of backup sources: Selected and Deselected. Selected backup source defines files/directories that are to be included in a backup set while deselected backup source defines files/directories that are to be excluded from a backup set. StorState Backup Manager will generate appropriate backup source setting for you automatically when you make your backup source selection.

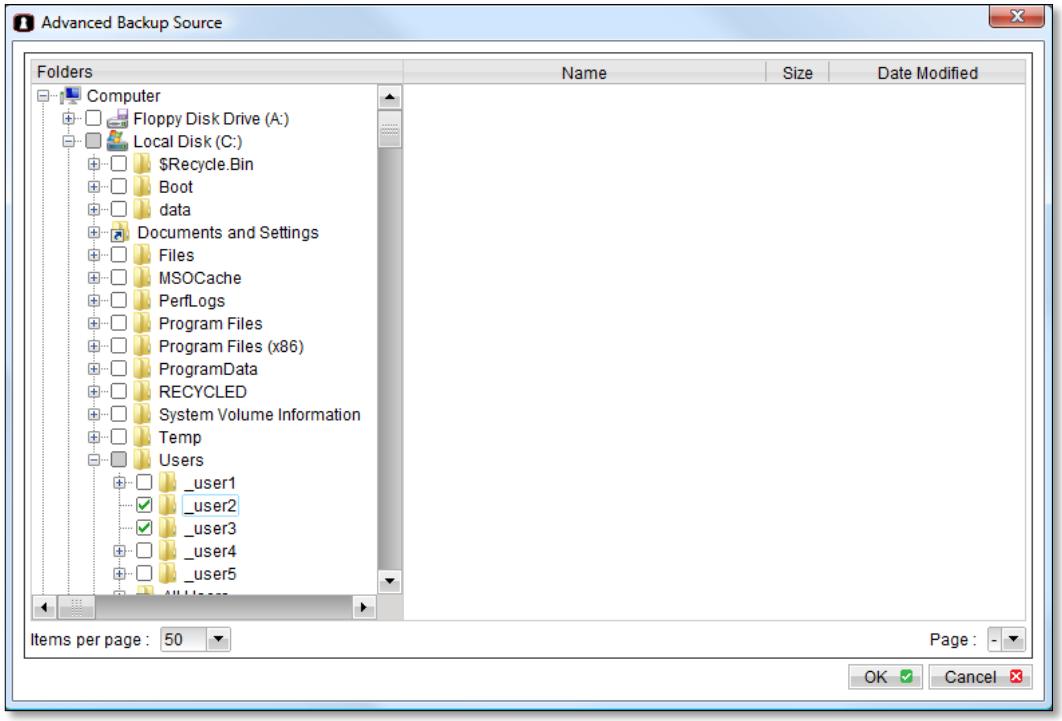
Please note that for Windows operating systems, if the “Hide protected operating files (Recommended)” setting is enabled for the file explorer, system folders/files will not be shown in the backup source. By selecting the parent folders however, all subfolders (including system folders/files) will be included in the backup set. Thus if you want to exclude system folders (ex. Recycle Bin) from the backup, please select the desired folders/files directly rather than selecting the parent folder. Alternatively, you can enter the corresponding system path in the [Exclude List] of the backup set using your Web Management Console.

On the first screen of the dialog, you can easily select the following common folders to be backed up:

1. "Desktop" folder
2. "My Documents" folder
3. "Favorites" folder
4. "Outlook", "Outlook Express" and "Windows Mail" mail store folder



By clicking the [Advanced] button, you can select specific folders to be backed up as well.



The checkbox next to files/directories shown above can be in one of the following modes:

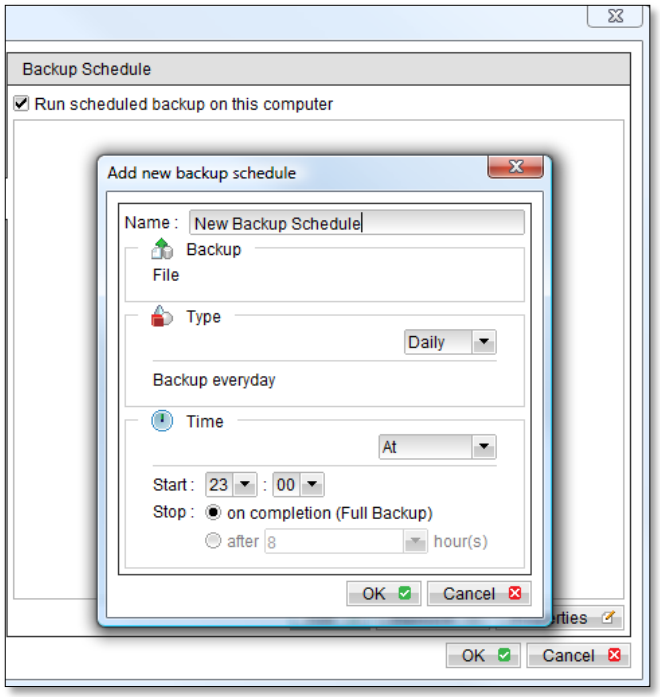
Mode	Description
☑	All files/directories (recursively) under this directory will be backed up
☑	All files/directories (recursively), except those explicitly excluded, under this directory will be backed up. If you add files/directories to this directory in the future, they will be backed up as well.
☐	Only the checked files/directories under this directory will be backed up. If you add files/directories to this directory in the future, they will NOT be backed up.
☐	Nothing under this directory will be backed up.

By clicking on the boxes, you can change the modes of each file/directory, in order to create a set of files to be backed up.

You can change the backup source anytime after creating the backup set by clicking the [Backup Source] button of the left panel on the [Backup Setting] dialog.

5.3 Backup Schedule

A "Backup Schedule" defines the frequency and time that backups should run automatically.



A backup schedule can be one of the following types:

Type	Description
Daily	Backup Job will run everyday
Weekly	Backup Job will run on the specified day(s) of every week
Monthly	Backup Job will run on the specified day or on a day with a given criteria (ex. first weekend, last weekday) of every month
Custom	Backup job will run once on a particular date and time

Backups will run at the scheduled time for a maximum of the duration specified, or until all data is backed up if [Stop on backup completion] option is chosen. If a backup job does not finish within the maximum duration specified, it will be interrupted.

Please note that you can have more than one schedule for a backup set. For example, you can have a daily backup schedule that runs at 13:00, and another daily backup schedule that runs at 00:00 midnight. The combination of these schedules creates a backup schedule that runs every day at 00:00 and 13:00.

You can change backup schedules anytime after creating the backup set by clicking the [Backup Schedule] button on the left panel of the [Backup Setting] dialog.

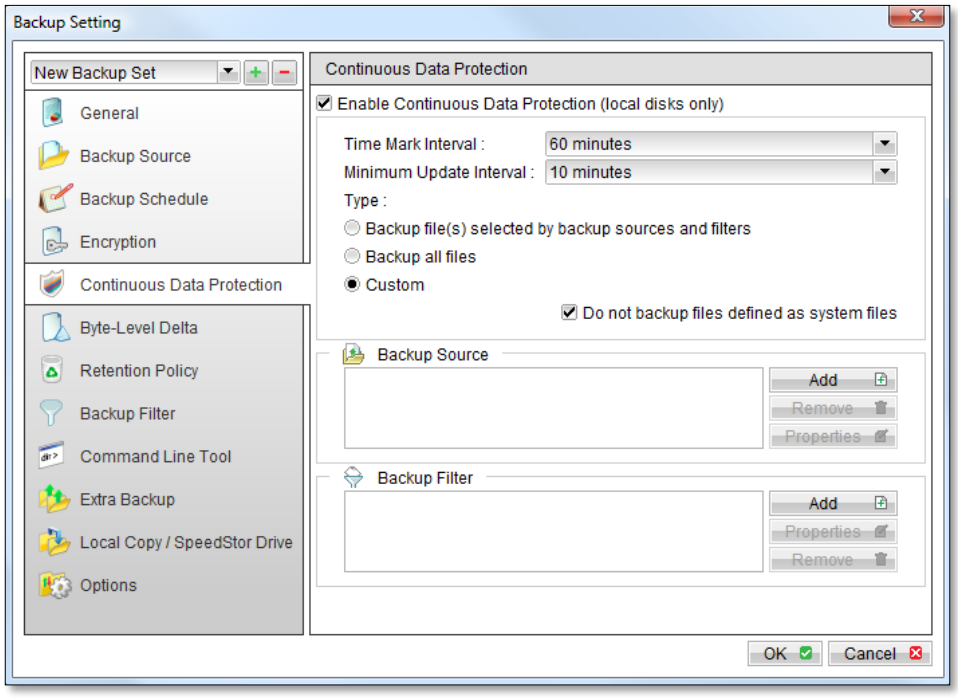
5.4 Continuous Data Protection (CDP)

The StorState Backup Manager Continuous Data Protection (CDP) feature enables files to be backed up automatically when changes are made to files on local hard disks. The benefits of using CDP are:

1. All intra-day interim changes are backed up automatically without waiting for a scheduled backup. Even if the computer crashes before scheduled backups run, the latest changes are backed up after files are modified. Snapshots of frequently changing files are captured for reference or rollback.

2. Occasionally users do not save their data in folders selected in a backup set, and thus data is not backed up when the scheduled backup runs. CDP can be configured to track all changes to files on local hard disk automatically, backing up files wherever they are. This makes defining a backup set a much easier task for both administrators and users.

Although CDP is a very helpful feature, it does have some drawbacks. For example, it is a memory resident program which tracks file changes to the file system and backs up files continuously in background, consuming both CPU and memory resources. This can potentially slow down a computer. For application servers, ex. Microsoft Exchange Server or Microsoft SQL Server, that do not require CDP features (you can use transaction log backup intervals as frequent as every 1 minute to mimic a continuous backup strategy instead), you can disable CDP by changing the startup method of the service: [Control Panel] -> [Administrative Tools] -> [Services] -> [Continuous Data Protection (StorState Backup Manager)] -> [General] -> [Startup type] to “manual”.

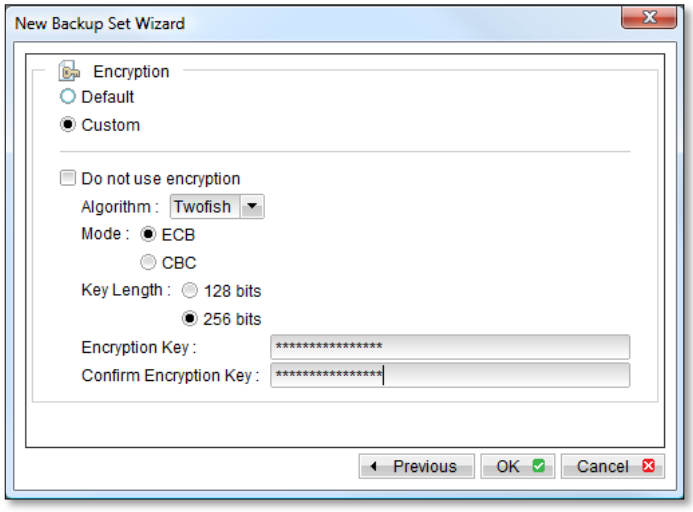


The following table explains all CDP parameters available within a backup set.

Parameter	Description
Enable Continuous Data Protection (local disks)	Defines whether CDP is enabled in this backup set. CDP will only backup files on local hard disks, not floppy drives, removable drives or network mapped drives.
Time Mark Interval	Defines the interval of point-in-time views generated by CDP. For example, if this setting is set to “60 minutes”, the point-in-time views selectable from the StorState Backup Manager Restore Wizard or the StorState Web Management Console File Explorer will be “00:00”, “01:00”, “02:00” etc, for each day.
Minimum Update Interval	Defines the minimum interval that repeatedly updated files are backed up again. For example, if a file is updated every minute and the [Minimum Update Interval] is set to “10 minutes”, CDP backs up this file every 10 minutes instead of every minute. If you want all changes to be backed up instead, please change this setting to “Always”. However, since StorState keeps only 1 snapshot of a file within a single point-in-time view (“Time Mark Interval”), only the last backup file within each point-in-time view is restorable. All other interim backup files are overwritten automatically without notice. Please note that this applies to all full file backups only, not to files that are backed up incrementally by Byte-Level Delta. To maintain a valid Byte-Level Delta chain for incremental delta files, StorState will not delete incremental delta files automatically. If you want to restore any of these snapshots, you can use the [Show all files] view to display all interim incremental backup files.
Type	[Backup file(s) selected by backup sources and filters] – CDP will only back up changed files selected in this Backup Set Backup Source and Filter settings [Backup all files] – CDP will back up all changed files [Custom] – CDP will only back up changed files selected in CDP Backup Source and CDP Backup Filter settings
Do not backup files defined as system files	CDP will exclude the following files from its backup: 1. '[WINDOWS_DIR]' (e.g. C:\WINDOWS*) 2. '[PROGRAM_DIR]' (e.g. C:\Program Files*) 3. '[RECYCLE_BIN_DIR]' (e.g. C:\RECYCLER, D:\$Recycle.Bin) 4. '[ALL_LOCAL_DRIVE]:\Pagefile.sys' (e.g. C:\Pagefile.sys, D:\Pagefile.sys) 5. '[ALL_LOCAL_DRIVE]:\hiberfil.sys' (e.g. C:\hiberfil.sys, D:\hiberfil.sys) 6. '[ALL_LOCAL_DRIVE]:****.tmp' (e.g. C:\xxx\abc.tmp, D:\yyy\abc.tmp) 7. '[ALL_LOCAL_DRIVE]:\System Volume Information' (e.g. C:\System Volume Information, D:\System Volume Information) 8. '[APP_DATA]\Microsoft' 9. '[APP_DATA]\Kaspersky Lab' 10. '[APP_DATA]\Symantec' 11. '[APP_DATA]\Avg7' 12. '[APP_DATA]\Avg8' 13. '[APP_DATA]\McAfee' 14. '[APP_DATA]\McAfee.com' 15. '[APP_DATA]\Sophos' 16. '*\ntuser.dat' 17. '*\Application Data\Mozilla*' 18. '*\Local Settings\Application Data\Microsoft*' 19. '*\Application Data\Macromedia*' 20. '~$*.(doc|dot|ppt|xls|DOC|DOT|PPT|XLS)' 21. '*\Local Settings\(Temp|Temporary Internet Files|History)*' 22. '*\LOCALS~1\(Temp|Tempor~1|History)*' Where: [APP_DATA] = "C:\Documents and Settings\All Users\Application Data\" (XP) or "C:\ProgramData" (Vista)
Backup Source	This option is only available when [Custom] CDP type is selected. When this option is used, CDP will only backup the files under the paths defined and all other files are ignored.
Backup Filter	Defines whether a file will be backed up by CDP. When CDP type is [Backup all files], it is only possible to exclude files from CDP backup. CDP backup filter is similar to backup set filter, please refer to Backup Filter section for more info.

5.5 Encryption

Before your files are sent to the StorState Data Vaulting Center, all files are compressed and encrypted using your choice of encryption algorithm, mode and key.



The following table explains all encryption parameters available within a backup set.

Parameter	Description
Encryption Algorithm	Defines the encryption algorithm used to encrypt your backup files. [AES] Advanced Encryption Standard algorithm [DESede] Triple DES algorithm [Twofish] Twofish algorithm AES is the default encryption algorithm.
Encryption Mode	Defines the encryption mode used to encrypt your backup files. [ECB] Electronic Cook Book Mode [CBC] Cipher Block Chaining Mode ECB is the default encryption mode.
Encryption Key Length	Defines the encryption key length used to encrypt your backup files. [128 bits] [256 bits] 256 bits is the default encryption key length.
Encryption Key	The key used to encrypt all files within a backup set. The [Default] setting uses your account login password as your encryption key. **Keep it in a safe place. If the key is lost, you will not be able to decrypt your backup files.**

Unless you would like to customize your encryption settings, it is recommended to use [Default] encryption. By selecting [Default], the Encryption Key for the backup set will be set to your current account login password, AES for the Algorithm, ECB for the Mode, and 256 bits for the Key Length. Please consult references on Cryptography for more information about encryption algorithms, modes and key lengths.

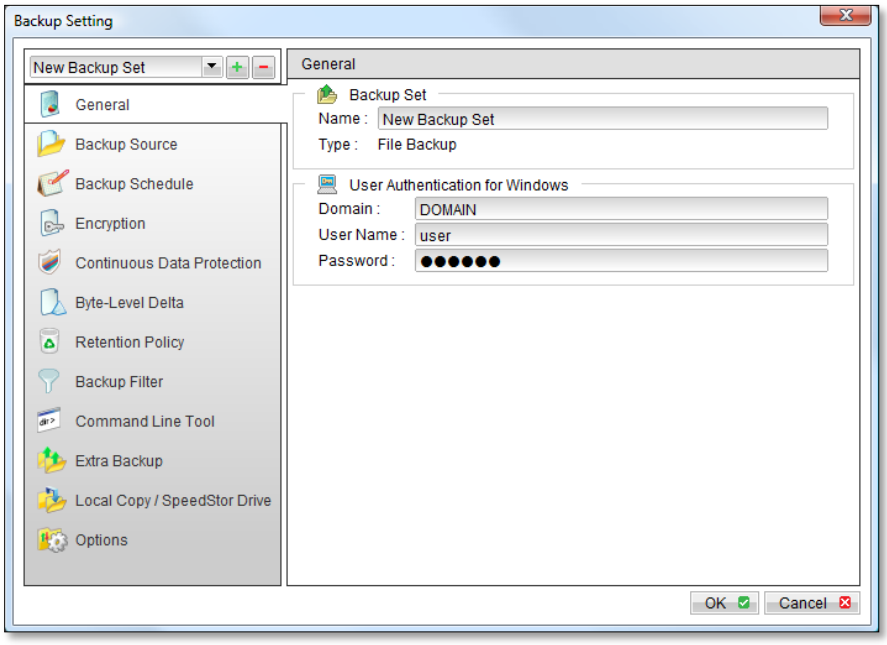
THE ENCRYPTION KEY AND SETTINGS CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!

5.6 Mapped Network Drive

If you need to backup a mapped network drive in Windows, you must enter your Window's domain, username and password into the [Network Resources Authentication for Windows] section as shown below. It is required because scheduled backups will always run under the context of Window's "Local System" account (which does not have the privileges required to access network resources) by default. StorState Backup Manager needs to collect your Windows username, password and domain name to authenticate itself to the Windows domain controller to acquire the required access privileges for the network files to be backed up. If you don't supply a username and password, StorState Backup Manager will have problems accessing network resources during its scheduled backup jobs.

If you need to backup mapped network drives in scheduled backup:

i. Select the backup set from the drop down list at the top of the left panel



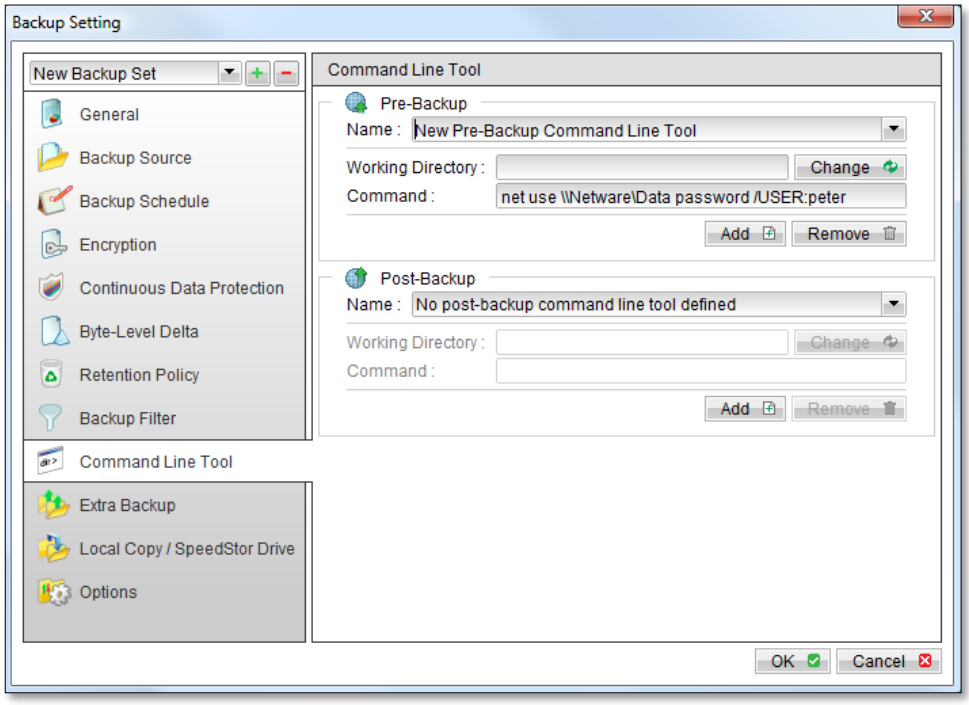
ii. Enter your Windows domain, username and password into the right panel

iii. Press the [OK] button to save.

The steps above apply only to computers running in a Windows domain. If you don't have a Windows domain, and are using a workgroup or NetWare server, please use the "net use" command to authenticate the running backup process against the computer hosting the mapped drive. Otherwise, you will get "Access Denied" error from the backup report.

For example, if you want to backup \\SERVER\SHARE that is located on a NetWare server (or another computer in a Windows workgroup) and you are getting a "Network drive is not accessible" error message, try adding the following command as a [Pre-backup command]:

net use \\SERVER\SHARE [PASSWORD] /USER:[DOMAIN | MACHINE_NAME]\[USERNAME]



Ex: Enter one of the following commands into the Pre-Backup Command field:

net use \\Netware\Data password /USER:peter
net use \\WorkgroupComputer1\Data password /USER:WorkgroupComputer1\peter

This will authenticate the current process with the NetWare server (or another computer in a Windows workgroup) and the backup will then run correctly.

5.7 Backup Filter

A “Backup Filter” defines the file selection rules that allow you to easily include/exclude files into/from the backup set by applying criteria(s) to the file names or directory names.

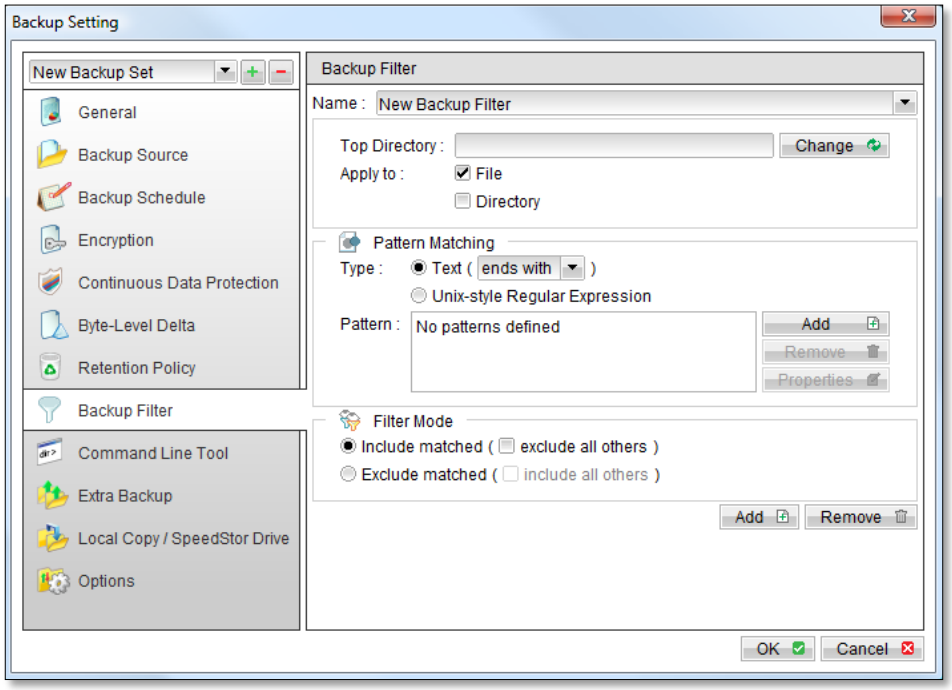
There are some basic rules regarding backup filters:

i. Filters are checked in creation order. Once inclusion/exclusion has been identified, the remaining filters won't be checked.

ii. Inclusion/Exclusion made by filter always takes precedence over backup source selections

iii. If all filters do not apply to a particular file, this file is then checked for inclusion/exclusion in the backup source selections

To add a new filter, press the [Add] button at the bottom of the right panel.



Key	Description
Name	The name of the filter
Top Directory	The top level directory to which this filter is applied. Filtering rules will be applied to all files and/or directories under this directory.
Apply To	Define whether to apply the filtering rule to files and/or directories
Pattern Matching	Defines the filtering rules of a filter. A filtering rule can be of one of the following types: [Starts With] Include/Exclude all files/directories with names starting with a certain pattern. For example: You can use B* to match all files with names starting with a 'B' character [Contains] Include/Exclude all files/directories with names containing a certain pattern. For example: You can use *B* to match all files with names containing a 'B' character [Ends With] Include/Exclude all files/directories with names ending with a certain pattern. For example: You can use *.doc to match all files with names ending with '.doc' (all Word documents) [Regular Expression] Include/Exclude all files/directories with names matching a regular expression. To add a new pattern, press the [Add] button in the [Pattern Matching] area.
Filter Mode	Defines whether you want to include or exclude matched files into/from the backup set. Also, for those unmatched files, you can choose to exclude (if include filter type) or include (if exclude filter type) them into/from the backup set.

Example 1:
If you want to backup only Word, Excel and PowerPoint documents in your document directory (ex. C:\My Documents), you should setup your backup filter as follows.

Top Directory = C:\My Documents
Apply To = File (true)
Matching Type = End With
Matching Patterns = *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx
Filter Mode = Include
Exclude all others = True

Example 2:
If you want to backup all files, excluding all *.exe, *.dll and *.tmp, in C:\Applications, you should setup your backup filter as follows.

Top Directory = C:\Applications
Apply To = File (true)
Matching Type = End With
Matching Patterns = *.exe,*.dll, *.tmp
Filter Mode = Exclude
Include all others = True

Example 3:
If you have made your selection of files (all under C:\) from the backup source setting but you want to exclude all images (ex. *.jpg and *.gif) from your selection, you should setup your backup filter as follows.

Top Directory = C:\
Apply To = File (true)
Matching Type = End With
Matching Patterns = *.jpg, *.gif
Filter Mode = Exclude
Include all others = false

Please note that the [Include all others] setting is not enabled because you don't want to include all other files (NOT *.jpg, *.gif) under C:\ into the backup set.

Example 4: (advanced)

If you want to include everything, except the "log" directory, under C:\Applications into a backup set, you should setup your backup filter as follows.

Top Directory = C:\Applications
Apply To = Directory (true)
Matching Type = Regular Expression
Matching Patterns = ^log$
Filter Mode = Exclude
Include all others = True

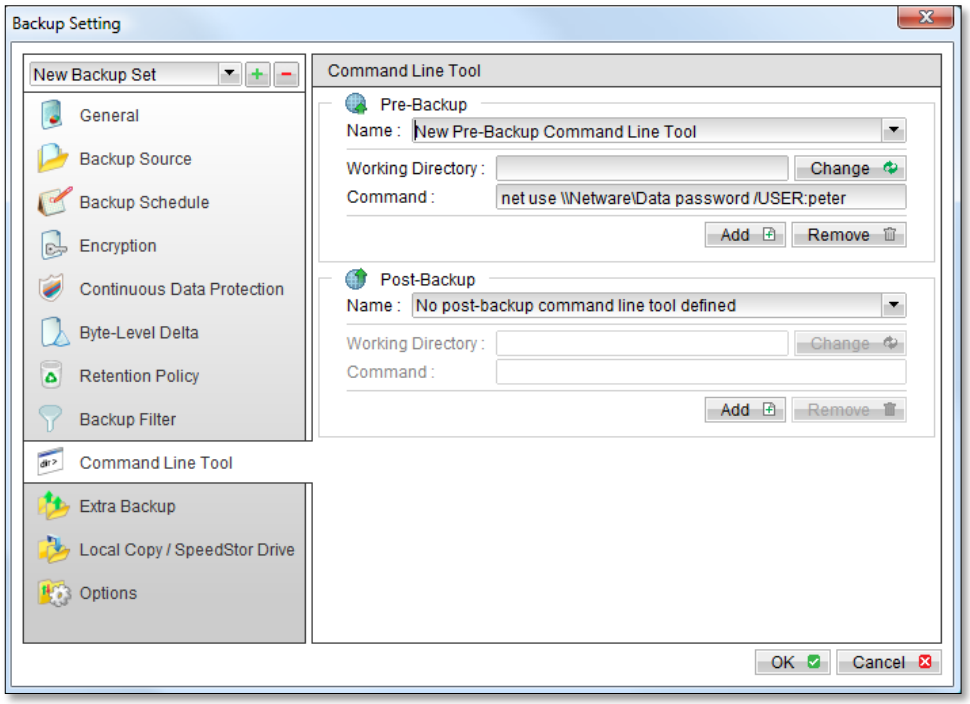
Example 5: (advanced)

If you want to include all directories named "log" from the backup set files with file name starting with "B" and ending with "*.doc" under C:\My Documents into the backup set, you can use a regular expression of "^B.*\.doc$" to do your selection. The filter backup can then be setup as follows.

Top Directory = C:\My Documents
Apply To = File (true)
Matching Type = Regular Expression
Matching Patterns = ^B.*\.doc$
Filter Mode = Include
Exclude all others = True

5.8 Pre/Post-Backup Command

The [Command Line Tool] feature has two major components, the [Pre-Backup] command and the [Post-Backup] command. You can use the [Pre-Backup] or [Post-Backup] commands to run any native OS (operating system) commands before or after running a backup job.



Both [Pre-Backup] and [Post-Backup] commands comprise of the following parameters:

Key	Description
Name	Name of this command
Command	The command to be run (ex. C:\My Documents\Application.exe or C:\My Documents\BatchJob.bat)
Working Directory	The directory at which this command will run

The backup set type affects the time at which [Pre-Backup] and [Post-Backup] commands run. The following table outlines when [Pre-Backup] and [Post-Backup] commands will run in different types of backup sets.

Backup Set Type	When Pre-Backup Commands run?	When Post-Commands run?
File Backup	Before uploading backup files	After uploading all backup files
Non-File Backup Sets (ex. Microsoft SQL Server)	Before spooling backup files to temporary directory	After spooling backup files to temporary directory (i.e. before the first backup file is uploaded)

Note: You should never backup an application while it is running as this can result in inconsistent and unusable files getting backed up. Please use the “Volume Shadow Copy” feature if you’re running Windows, or make use of the Pre-Backup Command feature to shutdown your application before running a backup job and use the Post-Backup Command feature to restart your application after the backup job has completed.

For Example

If want to stop Microsoft Outlook using the Pre-Backup Command and restart it after backup using the Post-Backup Command, create the two following text files and assigned the files to the Pre-Backup and Post-Backup Command.

1. Create a text file named “OutlookClose.vbs” using notepad with the following two lines:

```
Set objOLK = createObject("Outlook.Application")
objOLK.quit
```

2. Create a text file named “OutlookStart.bat” using notepad with the following line:

```
"C:\Program Files\Microsoft Office\OFFICE11\OUTLOOK.EXE"
```

5.9 Temporary directory

If you are running a file backup job with Byte-Level Delta enabled or a database type backup job, StorState Backup Manager will generate temporary files and the directory that will be used to store these files is defined by [Options] -> [Temporary directory for storing backup files]. Please set this to a non-system disk partition that has enough free space to avoid problems.

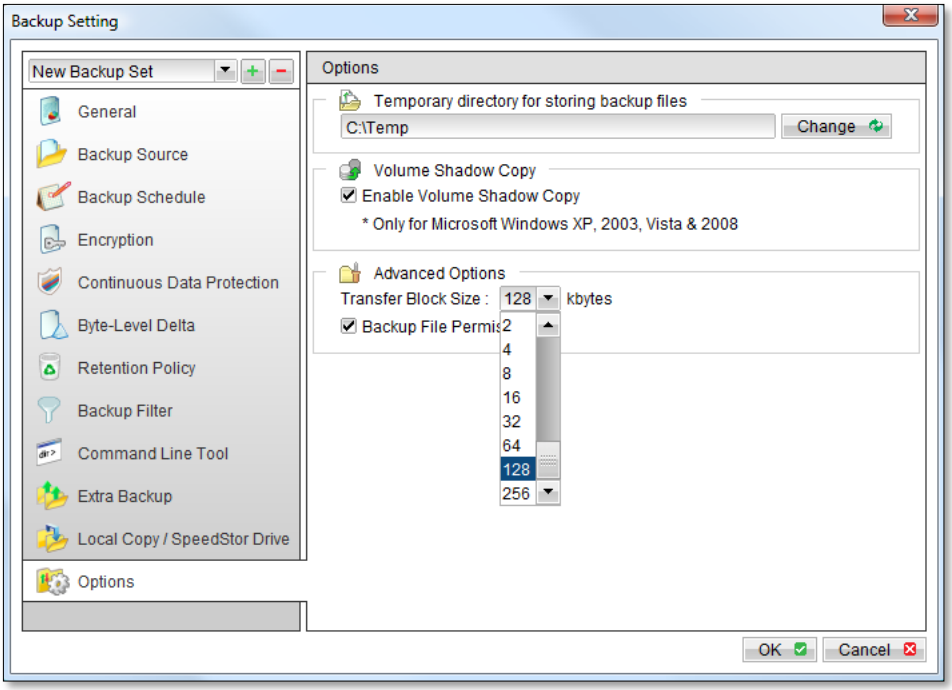
You can set the [Temporary directory for storing backup files] to a mapped network drive. If you choose to do this, please use a UNC path (ex. \\SERVER\SHARE) and don’t forget to configure the [Backup Set] -> [Network Resources Authentication for Windows] setting.

5.10 Transfer Block Size

Transfer block size defines the block size StorState Backup Manager will use to transfer your backup blocks. Generally, backup jobs using a larger block size will have better performance because of the smaller number of connections involved.

However, some firewalls or proxy servers may block out-going network traffic (HTTP/HTTPS POST method) with large block sizes for security reasons. If you are in a network with this type of restriction, please lower the transfer size value and try again.

To change the transfer block size of any backup set, please select the [Options] button on the left panel and then you can make changes to the [Transfer Block Size] under [Advanced Options]. After you have made your changes, press the [OK] button to save.



5.11 Follow Symbolic Link (Linux/Unix/Mac only)

Under Unix/Linux/Mac, users can create a symbolic link to link a file/directory to another directory. This setting defines whether you want StorState Backup Manager to traverse any symbolic links encountered in your backup path.

To change the option to follow symbolic links in any backup set, please select the [Options] button on the left panel. You can then make changes to the [Follow Symbolic Link] option by checking or un-checking the box. After you have made your changes, press the [OK] button to save.

5.12 Microsoft's Volume Shadow Copy Service (VSS)

Microsoft Volume Shadow Copy Service (VSS) allows you to backup files that are exclusively opened. Without VSS, you will get the error message "The process cannot access the file because another process has locked a portion of the file" if you are trying to backup a file that is exclusively opened (ex. Outlook PST files).

Please note that VSS is only available on Windows XP or later and you must have administrative privileges to start the VSS service on a computer. Also VSS will only work if at least one of your partitions is formatted using NTFS.

If you are running Windows 2003, please install the Windows 2003 VSS hot fix available from http://support.microsoft.com/default.aspx?scid=kb;en-us;887827 before running VSS.

If you are running into problems with VSS running on Windows XP / 2003, Microsoft's recommendation is to try re-registering the Volume Shadow Copy Service. Simply run the script in [StorState Home]\bin\RegisterVSS.bat to do so.

For more information, please reference the following page for a technical introduction to Volume Shadow Copy Services (VSS):
http://technet.microsoft.com/en-us/library/cc785914(WS.10).aspx

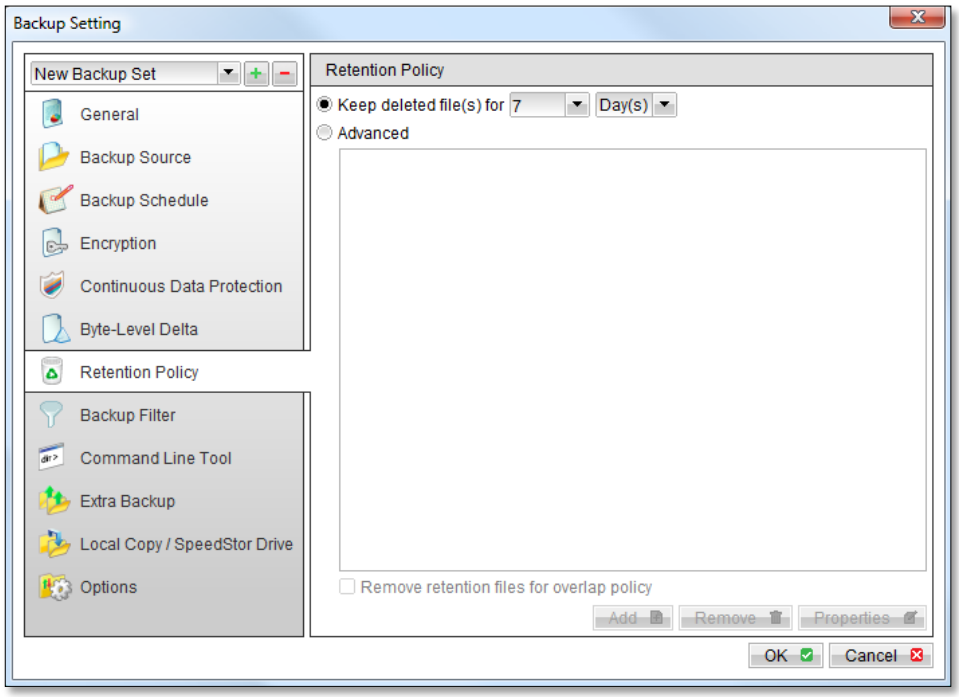
5.13 Retention Policy

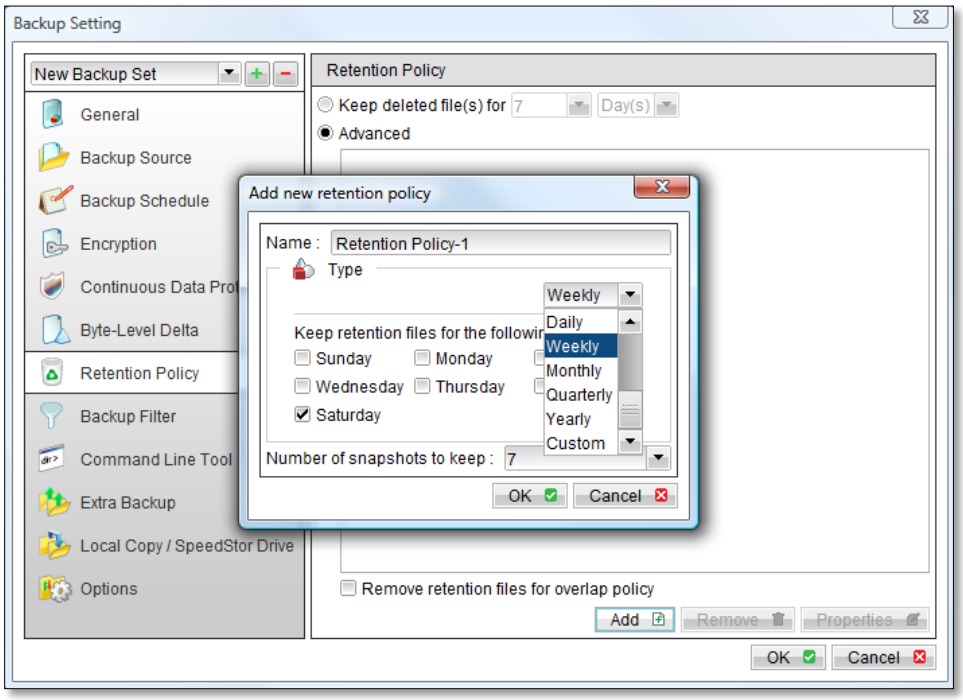
During a backup, if StorState Backup Manager finds that you have deleted a file (or updated a file) on your computer, it will put the corresponding deleted (or updated) file already backed up in the Data Vaulting Center into a retention area. The retention policy setting of a backup set defines how long files inside the retention area will be kept in the vaulting center before they are deleted automatically.

The retention policy will only affect "retained" files (i.e. files that have already been deleted or updated on your computer and thus are moved to the retention area in the Data Vaulting Center). For those files that have not been updated on your computer, the backup of these files is kept in the data area in the Data Vaulting Center and won't be affected by the settings of the retention policy. The backup files of unchanged files will stay in the Data Vaulting Center forever until the original files are removed (or updated) from your computer.

Standard Retention Policy

The standard retention policy deletes retained files automatically after a pre-defined number of days or after a pre-defined number of backup jobs. To change the retention policy setting of any backup set, please select the [Retention Policy] button on the left panel. You can then make changes to your retention policy under the [Retention Policy] section on the right. After you have made your changes, press the [OK] button to save.





Advanced Retention Policy

The [Advanced] retention policy allows you to configure a more flexible policy, retaining backup snapshots based on the time of the backup job. For example, you can configure the advanced retention policy to keep the following sets of backup snapshots similar to an old-style tape rotation scheme:

- All files available within the last 7 days

- All files available on the last 4 Saturdays within the last 28 days
- All files available on the 1st day of each month within the last 3 months
- All files available on the 1st day of each quarter within the last 12 months
- All files available on the 1st day of each year within the last 7 years

To do so, you need to setup your advanced retention policy as follows:

- Type = Daily; Number of snapshots to keep = 7
- Type = Weekly; Frequency = Saturday; Number of snapshots to keep = 4
- Type = Monthly; Frequency = Day 1; Number of snapshots to keep = 3
- Type = Quarterly; Frequency = Day 1 of Jan, Apr, Jul, Oct; Number of snapshots to keep = 4
- Type = Yearly; Frequency = Date 01-01; Number of snapshots to keep = 7

Assuming today is 17-Jan-2009, if [Remove retention files for overlap policy] is NOT enabled, a total of 22 snapshots will be kept on the server (provided you have run backups daily for more than 7 years) i.e.:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2009	14-Jan-2009	01-Jan-2009	01-Jan-2009	01-Jan-2009
15-Jan-2009	07-Jan-2009	01-Dec-2008	01-Oct-2008	01-Jan-2008
14-Jan-2009	31-Dec-2008	01-Nov-2008	01-Jul-2008	01-Jan-2007
13-Jan-2009	24-Dec-2008		01-Apr-2008	01-Jan-2006
12-Jan-2009				01-Jan-2005
11-Jan-2009				01-Jan-2004
10-Jan-2009				01-Jan-2003

If [Remove retention files for overlap policy] is enabled, only the following snapshots are kept:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2009	14-Jan-2009	~~01-Jan-2009~~	~~01-Jan-2009~~	01-Jan-2009
15-Jan-2009	07-Jan-2009	~~01-Dec-2008~~	~~01-Oct-2008~~	01-Jan-2008
~~14-Jan-2009~~	~~31-Dec-2008~~	~~01-Nov-2008~~	~~01-Jul-2008~~	01-Jan-2007
~~13-Jan-2009~~	~~24-Dec-2008~~		~~01-Apr-2008~~	01-Jan-2006
~~12-Jan-2009~~				01-Jan-2005
~~11-Jan-2009~~				01-Jan-2004
~~10-Jan-2009~~				01-Jan-2003

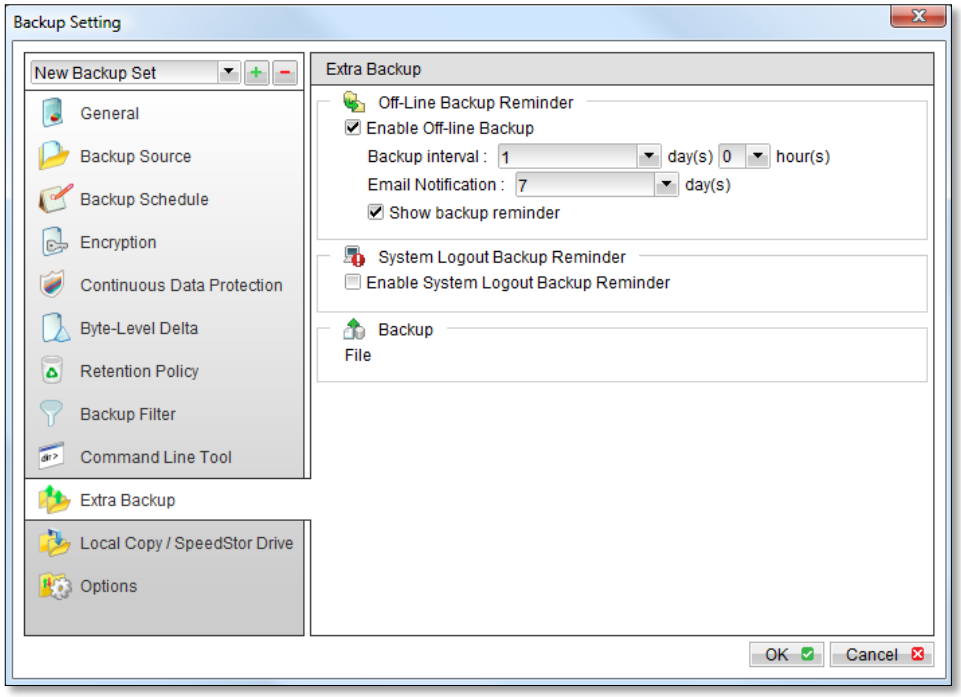
The weekly policy overrides the daily policy so snapshots from 10-Jan-2009, 11-Jan-2009, 12-Jan-2009, 13-Jan-2009 and 14-Jan-2009 are removed. The monthly policy overrides the weekly policy so snapshots from 24-Dec-2008 and 31-Dec-2008 are removed. The same applies to the monthly, quarterly and yearly policy for a total of 11 snapshots.

5.14 Extra Backup (Off-Line backup, Logout Reminder)

Off-line backup is basically designed for notebook users who are off-line most of the time and cannot rely on the backup schedule to backup regularly. The "Backup Interval" setting allows notebook users to specify the interval that they would like their data to backup. When the machine is online and this interval has elapsed, a backup will run automatically. If [Off-Line Backup Alert] is enabled, a popup message box will ask the user to confirm starting the backup.

The [Email Notification] setting is the number of days since the last backup that triggers the Data Vaulting Center to send email notifications to remind you to run an off-line backup.

When the [System Logout Backup Reminder] setting is enabled, a popup message box will ask the user to start a backup before logging out or shutting down Windows.

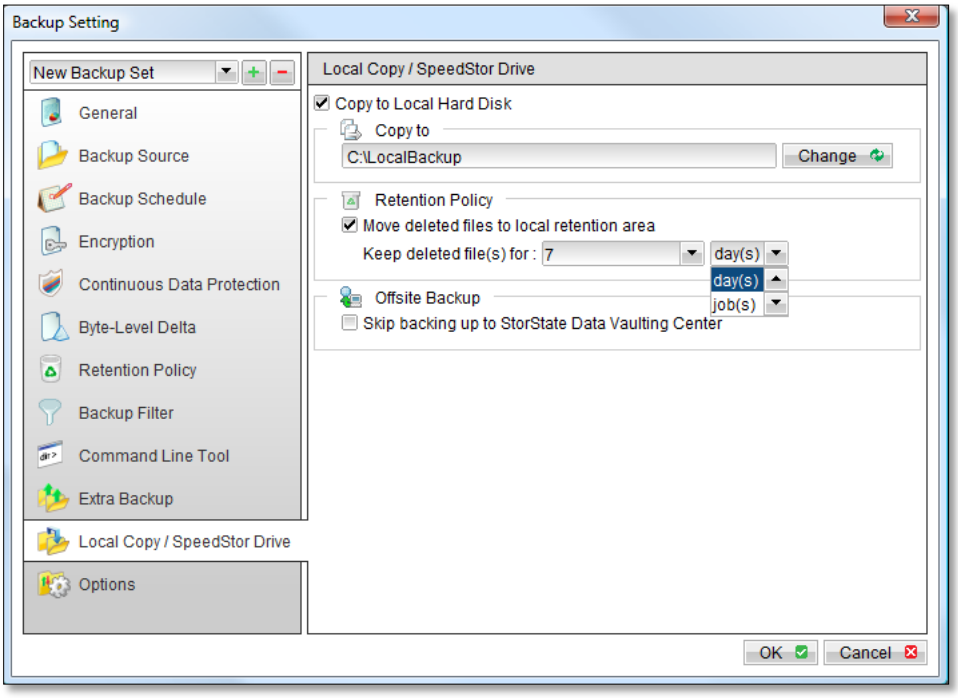


5.15 Byte-Level Delta

Please refer to the Byte-Level Delta section for information on this topic.

5.16 Local Copy / SpeedStor Drive

To save an additional copy of backup data on a SpeedStor Drive or local hard disk (in addition to a copy of backup data stored in the Data Vaulting Center) for the most rapid file-restoration and/or to provide an extra level of redundancy, you can do the following:



Select [Local Copy / SpeedStor Drive] under your backup set from the left panel and check the [Copy to Local Hard Disk] checkbox. Enter the SpeedStor Drive letter or a directory to where you want the extra copy of your backup files to be stored in the [Copy to] field provided. An extra copy of the backup will be saved in the [Copy to] directory when your backup job runs. Backup files are stored in a compressed and encrypted format for security, and must be decrypted with the backup set encryption key before use.

Computer in a Windows Workgroup or NetWare Server

To make a local copy to a directory located on a NetWare server or another computer in a Windows workgroup, and you are getting a "Network drive is not accessible" error message, please try adding the following command as a [Pre-backup command]

net use \\SERVER\SHARE [PASSWORD] /USER:[DOMAIN | MACHINE_NAME]\[USERNAME]

Ex:

C:\> net use \\Netware\Data password /USER:peter
C:\> net use \\WorkgroupComputer1\Data password /USER:WorkgroupComputer1\peter

This will authenticate the current process with the NetWare server (or another computer in a Windows workgroup). The backup will then be allowed to run correctly.

How to restore "Local Copy / SpeedStor Drive" files

"Local Copy / SpeedStor Drive" files are stored in the [Copy to] directory in a compressed and encrypted format for security. To restore backup files, please do the followings:

i. Press the button on the main page of the StorState Backup Manager screen.

ii. Select the required [Backup Set] from the list and press [Next] to proceed.

iii. Select the backup job you wish to restore from the [Show files as of Job] drop-down box, or leave "Latest" to restore from the latest backup. Select [Show all files] to view all snapshots of files stored on your local drive.

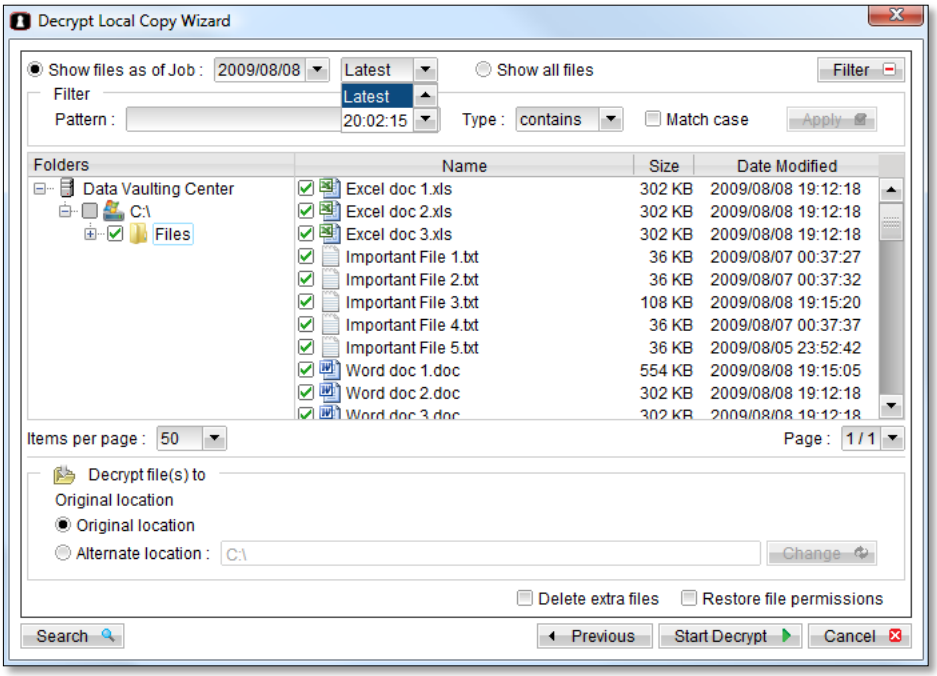
iv. Optional - Click the Filter button on the top right corner to filter the files/folders view based on your criteria.

v. Optional - Click the Search button on the bottom left corner to search for files/folders based on your criteria.

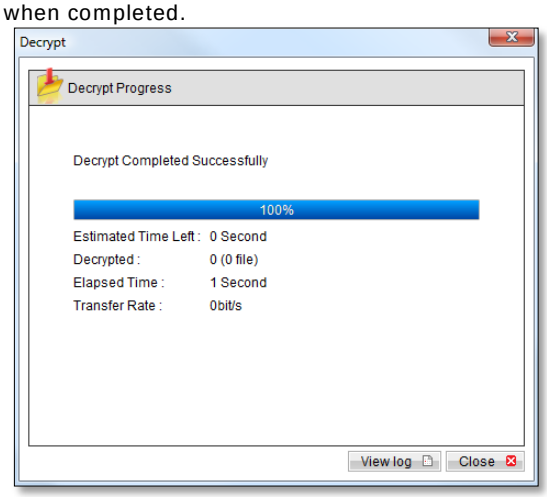
vi. In the "Decrypt file(s) to" section, leave the setting to "Original location" to restore files and folders to the same location as when backed up. Select "Alternative location" to specify a different folder to restore to.

vii. Select the "Delete extra files" checkbox to synchronize the restore location with the backup files/folders being restored. This setting will delete existing files/folders from the restore location that were not part of the backup.

viii. Select the "Restore file permissions" checkbox to restore file permissions to files as they are restored.



ix. Click [Start Decrypt] to start the restore operation. A dialog will display the progress and alert you when completed.

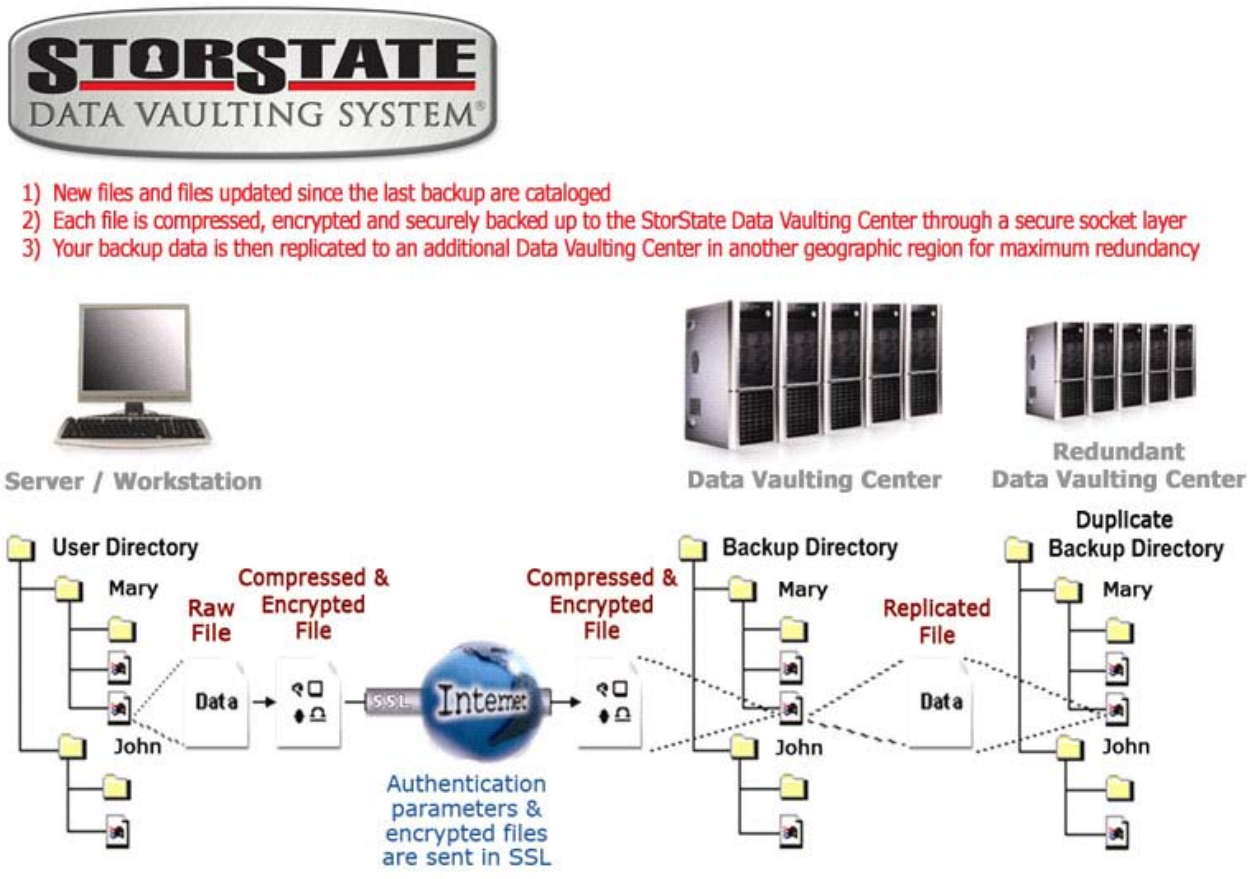


6 Backing Up Files

This chapter describes how files are backed up by StorState Backup Manager to the Data Vaulting Center

6.1 How files are backed up

The diagram below describes how the StorState Data Vaulting System works.



Run backups at scheduled times automatically

Once you set a backup scheduled, the backup job will be started automatically. Backup jobs can be scheduled as often as you like (ex. twice a day or hourly during office hours).

Incremental Backup

Unchanged files are already backed up to the vaulting center and do not need to be backed up again. StorState Backup Manager will find new or updated files from your backup set files and upload only these files to the vaulting center. This significantly reduces the time required to perform a backup operation since most users update less than 5% of their total data each day.

Compresses and encrypts data automatically

Data is compressed and encrypted before being uploaded to the Data Vaulting Center. Not only does this reduce the storage space required for your backup files, it also ensures the privacy of your data.

File Retention Policy

Customizable file retention policies allows you to access multiple versions of the same file or deleted files from your backup set. Modified or deleted files are put into a retention area before they are removed from the vaulting center, and retained according to the policy you define. This feature is particularly useful when you have accidentally deleted a file or incorrectly updated a file and need to roll backup to a previous version.

6.2 Backup files directly to the Data Vaulting Center

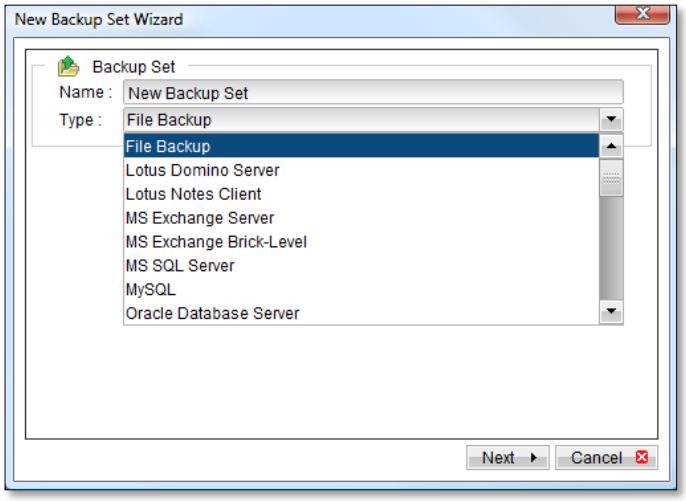
You can backup your data to the StorState Data Vaulting Center by following the instructions below.

i. Open the StorState Backup Manager.

a. To configure backup sets, click the button to open the [Backup Setting] dialog.

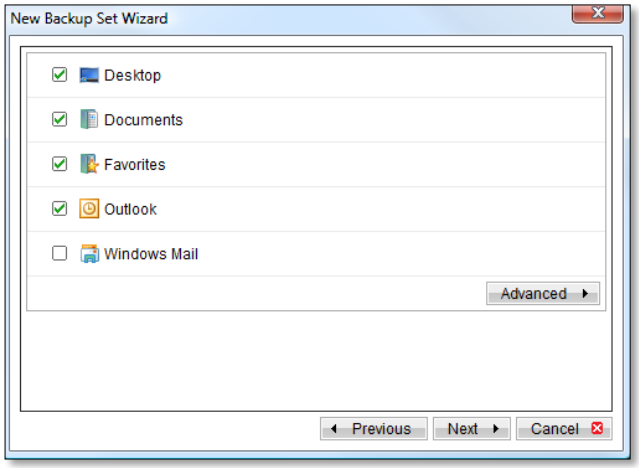
b. On the left panel, press the button to create a new backup set.

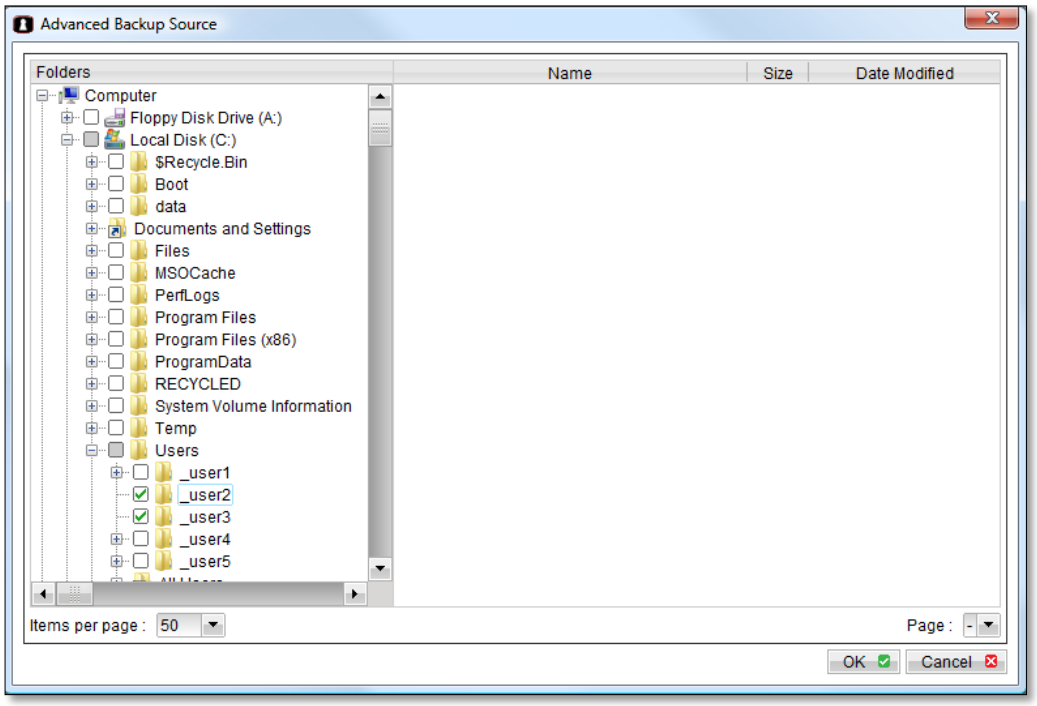
c. Enter a name for your backup set.



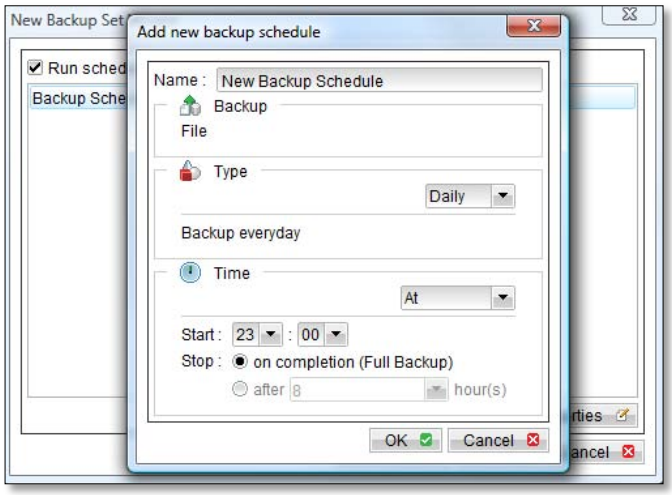
d. Select the files/directories you want to backup.

e. Press [Advanced] to add more files to the backup set.

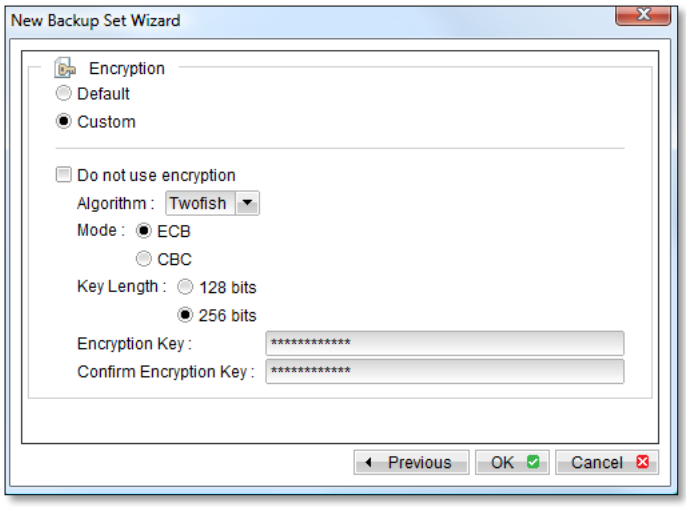




f. Set the backup schedule (Note: You can have more than one schedule in a backup set).



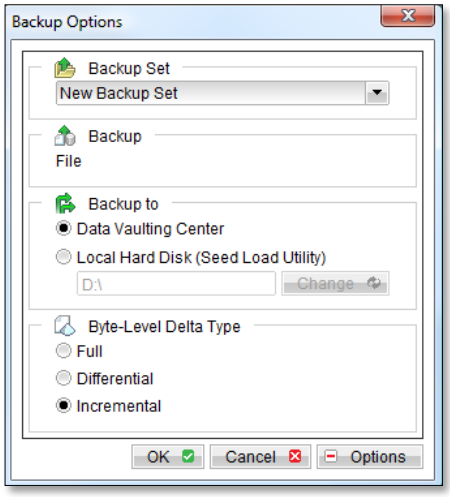
g. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set. The [Default] option sets your encryption key to be the same as your backup account password. Press [OK] to return to the StorState Backup Manager main screen.



ii. Run Backup

a. Press the [Backup] button on the main screen of StorState Backup Manager.

b. Select the backup set you want to run and click [OK] to start the backup job.



IMPORTANT NOTES:

1) You can have more than one backup set in a StorState Pro backup account. StorState Xpress is limited to one File Backup set.

2) Keep your encryption key in a safe place. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!

3) The default encryption setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set.

6.3 Backup files to removable hard disk (seed loading)

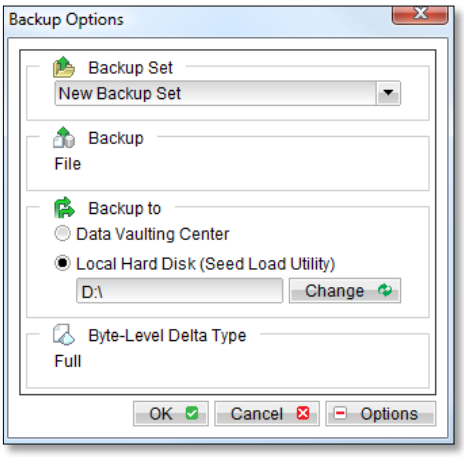
If you have a lot of data (ex. 300GB+) to backup to the Data Vaulting Center, it can take a considerable amount of time to perform the first full backup over the Internet. Alternatively, for your first backup you can use the Seed Loading Utility, backing up your data to a removable/mobile hard disk (instead of directly to the Data Vaulting Center) and ship the disk to StorState. StorState engineers can then load the backup files from your removable hard disk into your data vault. This could save days (even weeks) in performing your first full backup. Since subsequent backups will be incremental (only new or updated files will be uploaded to the server) you should have no problems uploading your backup data over the Internet.

To perform seeding loading, please do the following:

i. Open StorState Backup Manager.

ii. Setup your backup set(s) (see previous sections for details).

iii. Select the backup set you wish to run, click the [Options] button on the bottom right corner and select [Local Hard Disk (Seed Load Utility)]. Click the [Change] button and select the device you wish to use.



iv. Please make sure you have enough free space on the device specified.

Press the [OK] button to start the backup job. The Backup Progress window will load and display the backup activity.

v. The message “Backup Completed Successfully” will be shown when the backup job is completed.

vi. Contact StorState Support for shipping information. You will be given an SL Routing # to include on the outside of the package.

7 Restoring Files

This chapter describes the ways backup files can be restored.

Backup files can only be restored with the encryption key used when creating the backup set

7.1 Restore backup files directly from the Data Vaulting Center

You can use either StorState Backup Manager or the Web Management Console to restore backup files from the Data Vaulting Center.

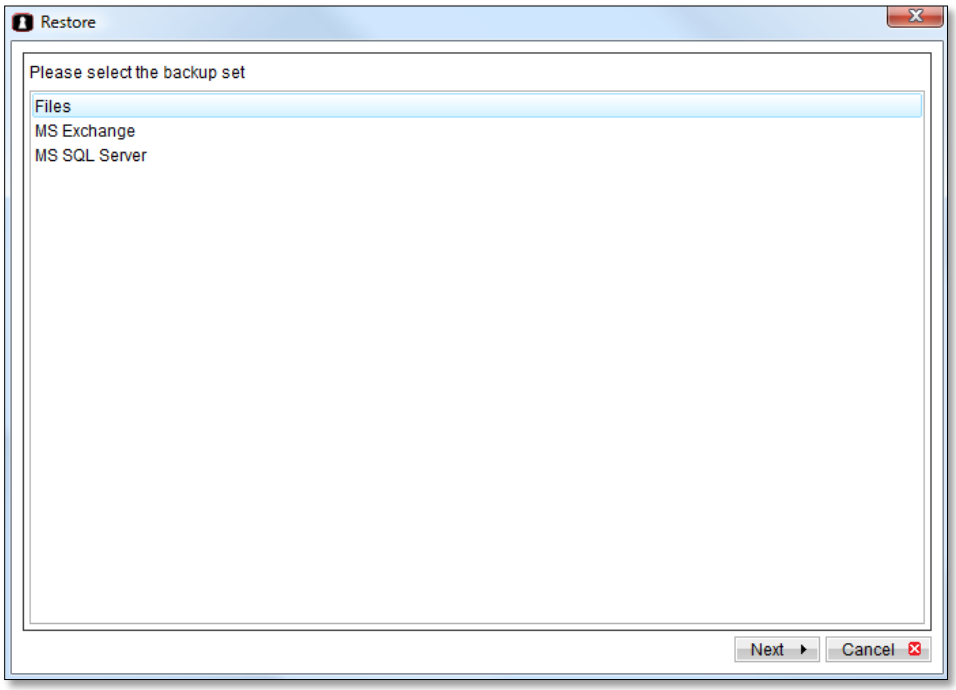
Restoring with StorState Backup Manager

You can restore your data from the Data Vaulting Center by following the instructions below.

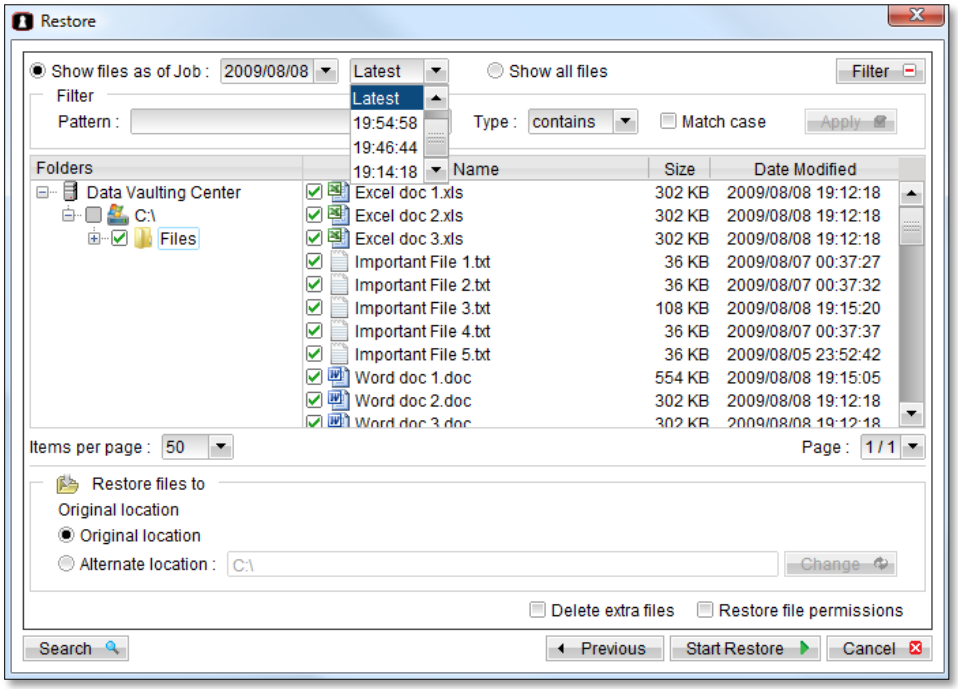
i. Open StorState Backup Manager.

ii. Press the [Restore] button on the left of the main screen of StorState Backup Manager.

iii. Select the required [Backup Set] from the list and press [Next] to proceed.



iv. Select the backup job you wish to restore from the [Show files as of Job] drop-down box, or leave on "Latest" to restore from the latest backup. Select [Show all files] to view all snapshots of files stored in your data vault.



v. Optional - Click the Filter button on the top right corner to filter the files/folders view based on your criteria.

vi. Optional - Click the Search button on the bottom left corner to search for files/folders based on your criteria.

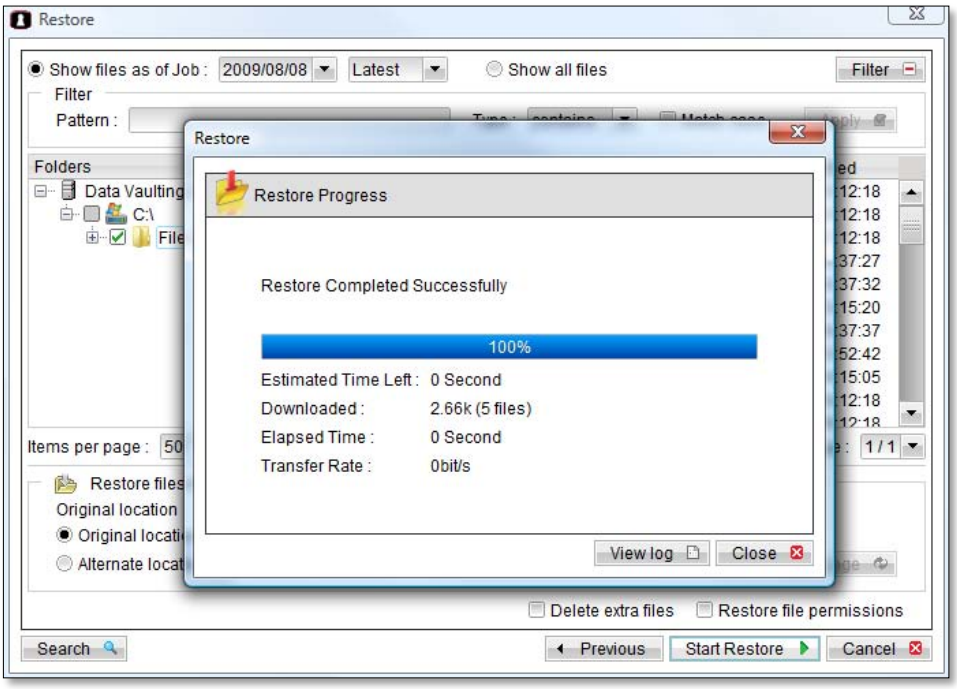
vii. Select the files/folders you would like to restore. A file won't be downloaded from your data vault if an identical file exists in the restore path already.

viii. In the "Restore files to" section, leave the setting to "Original location" to restore files and folders to the same location as when backed up. Select "Alternative location" to specify a different folder to restore to.

ix. Select the "Delete extra files" checkbox to synchronize the restore location with the backup files/folders being restored. This setting will delete existing files/folders from the restore location that were not part of the backup.

x. Select the "Restore file permissions" checkbox to restore file permissions to files as they are restored.

xi. Click [Start Restore] to start the restore operation. A dialog will display the progress and alert you when completed.

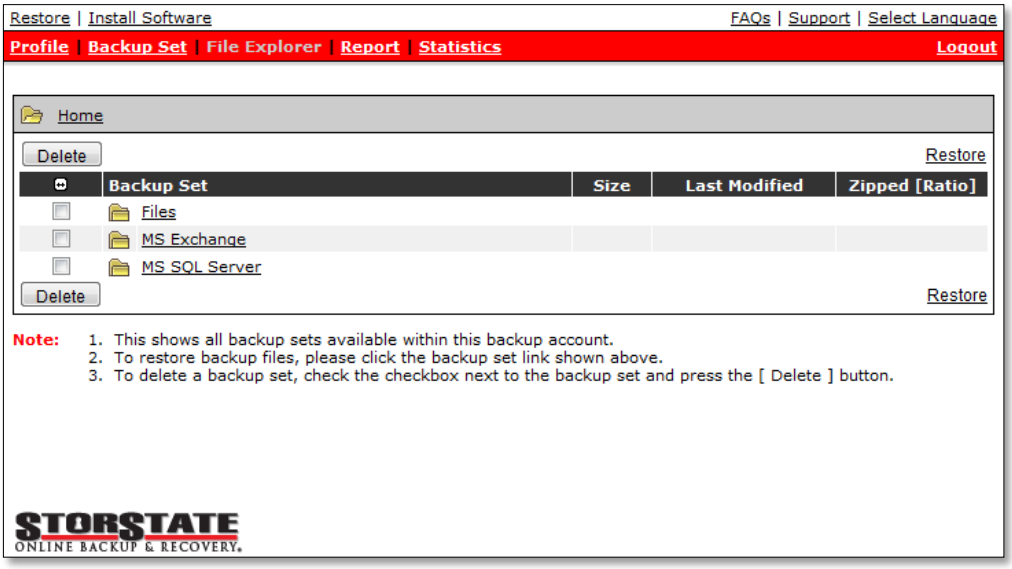


Restoring with the Web Management Console

You can restore data from the StorState Web Management Console by following instructions below.

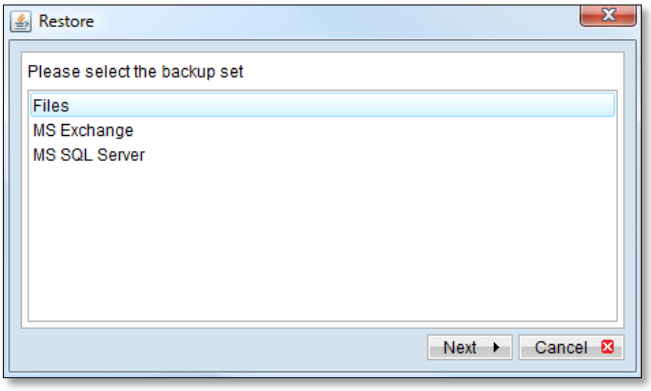
i. Logon to your Web Management Console: https://www.storstate.com/login/

ii. From the top left menu, click [Restore] to go to the [File Explorer] page.

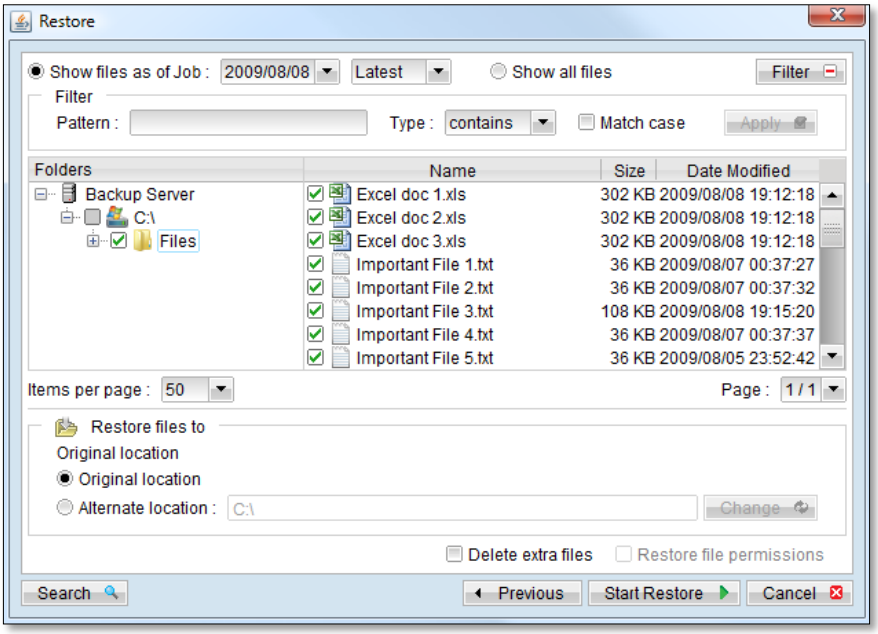


iii. Click [Restore] on far right side to open the Java Restoration Applet.

iv. Select the required [Backup Set] from the list and press [Next] to proceed.



v. Select the backup job you wish to restore from the [Show files as of Job] drop-down box, or leave on "Latest" to restore from the latest backup. Select [Show all files] to view all snapshots of files stored in your data vault.



vi. Optional - Click the Filter button on the top right corner to filter the files/folders view based on your criteria.

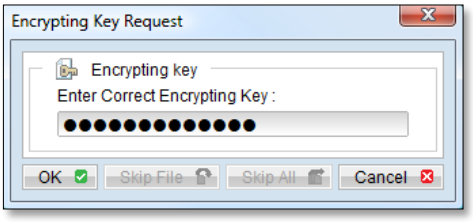
vii. Optional - Click the Search button on the bottom left corner to search for files/folders based on your criteria.

viii. Select the files/folders you would like to restore. A file won't be downloaded from your data vault if an identical file exists in the restore path already.

ix. In the "Restore files to" section, leave the setting to "Original location" to restore files and folders to the same location as when backed up. Select "Alternative location" to specify a different folder to restore to.

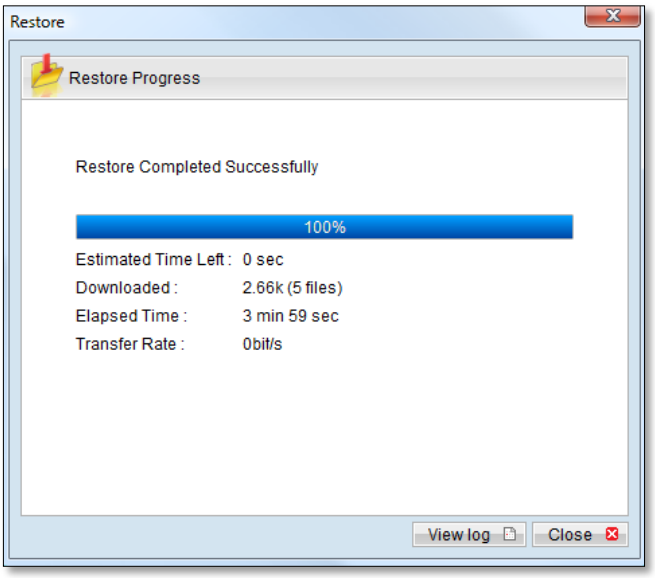
x. Select the "Delete extra files" checkbox to synchronize the restore location with the backup files/folders being restored. This setting will delete existing files/folders from the restore location that were not part of the backup.

xi. Click [Start Restore] to start the restore operation. The Encrypting Key Request window will open.



xii. Enter the Encryption Key used when the backup set was created and click [OK].

xiii. The Restore Progress window will display the restoration progress and alert you when completed.



7.2 Restore backup files from Local Copy / SpeedStor Drive

"Local Copy / SpeedStor Drive" files are stored in the [Copy to] directory in a compressed and encrypted format for security. To restore backup files, please do the followings:

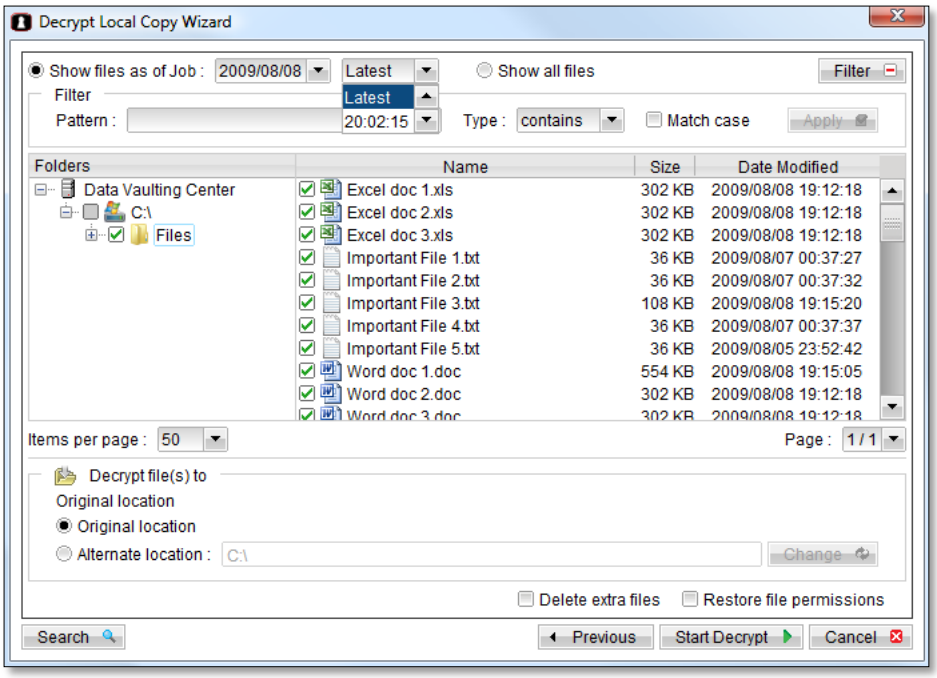
i. Press the button on the main page of the StorState Backup Manager screen.

ii. Select the required [Backup Set] from the list and press [Next] to proceed.

iii. Select the backup job you wish to restore from the [Show files as of Job] drop-down box, or leave "Latest" to restore from the latest backup. Select [Show all files] to view all snapshots of files stored on your local drive.

iv. Optional - Click the Filter button on the top right corner to filter the files/folders view based on your criteria.

v. Optional - Click the Search button on the bottom left corner to search for files/folders based on your criteria.

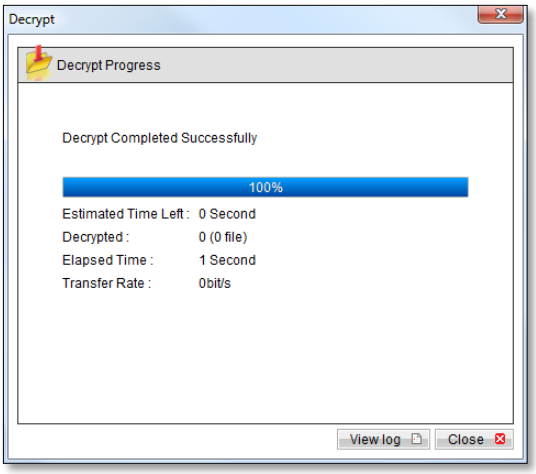


vi. In the “Decrypt file(s) to” section, leave the setting to “Original location” to restore files and folders to the same location as when backed up. Select “Alternative location” to specify a different folder to restore to.

vii. Select the “Delete extra files” checkbox to synchronize the restore location with the backup files/folders being restored. This setting will delete existing files/folders from the restore location that were not part of the backup.

viii. Select the “Restore file permissions” checkbox to restore file permissions to files as they are restored.

ix. Click [Start Decrypt] to start the restore operation. A dialog will display the progress and alert you when completed.



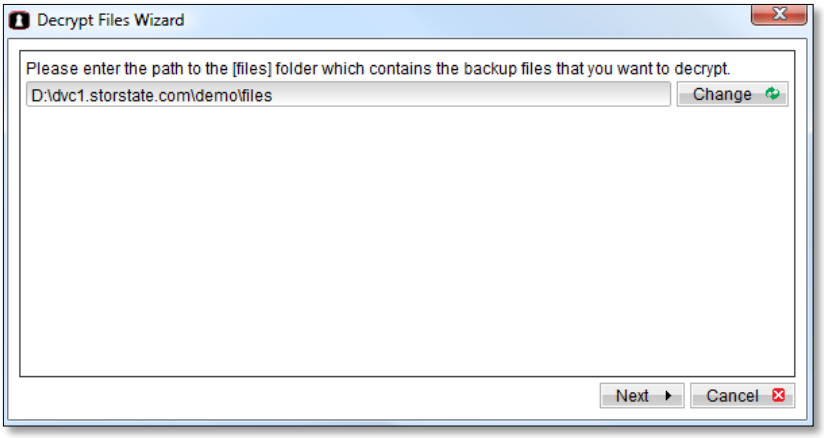
7.3 Restore backup files from other locations/devices

If you want to restore files from another location or device, for example, restoration from media provided by StorState, please follow the directions below. Keep in mind all backup files are encrypted and must be decrypted using the encryption key used when the backup set was created before use.

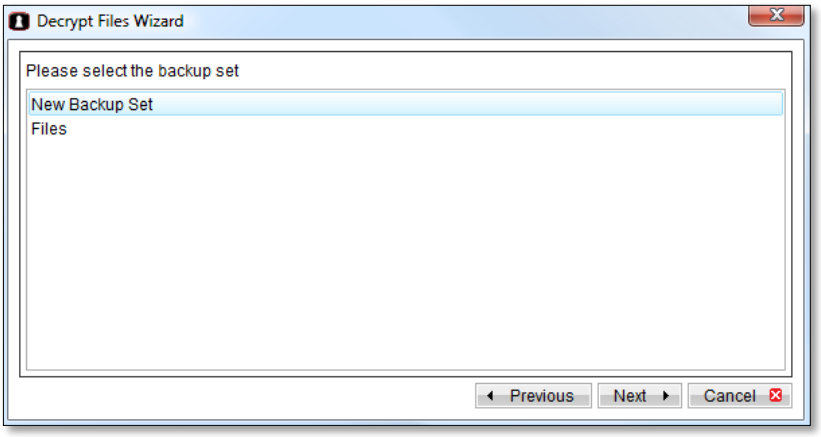
i. Open StorState Backup Manager.

ii. Press the button to start the [Decrypt Files Wizard].

iii. Click the [Change] button, and navigate to the "files" subfolder of the backup files location.



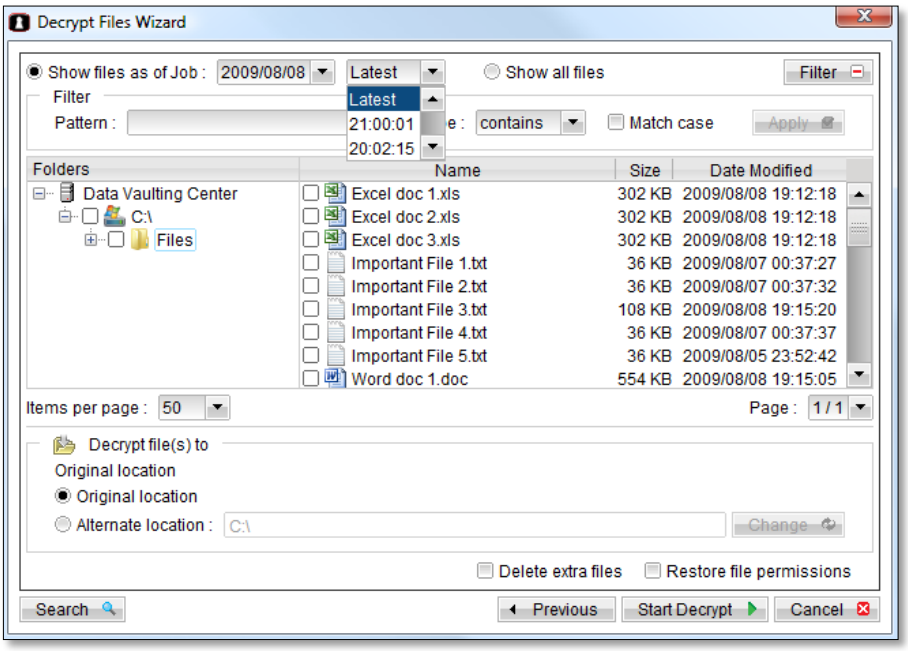
iv. Select the required [Backup Set] from the list and press [Next] to proceed.



v. Select the backup job you wish to decrypt from the [Show files as of Job] drop-down box, or leave on "Latest" to decrypt the latest backup. Select [Show all files] to view all snapshots of files stored on the backup media.

vi. Optional - Click the Filter button on the top right corner to filter the files/folders view based on your criteria.

vii. Optional - Click the Search button on the bottom left corner to search for files/folders based on your criteria.



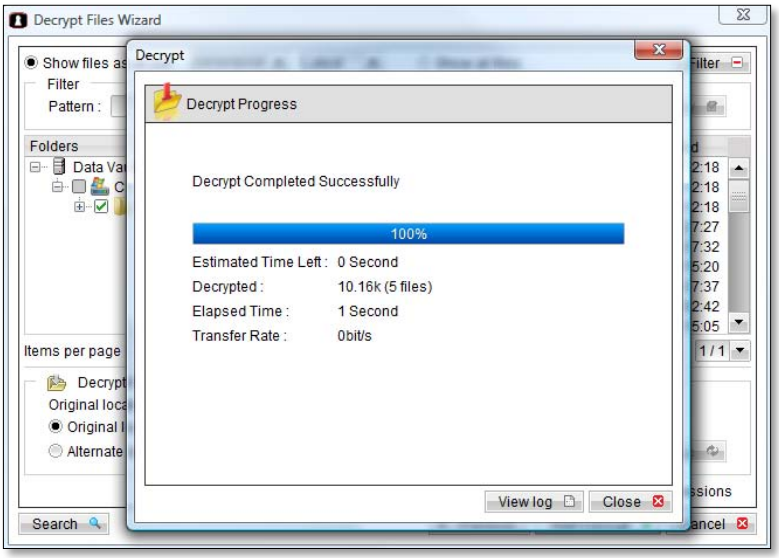
viii. Select the files/folders you would like to decrypt. A file won't be decrypted if an identical file exists in the decrypt path already.

ix. In the "Decrypt files to" section, leave the setting to "Original location" to decrypt files and folders to the same location as when backed up. Select "Alternative location" to specify a different folder to decrypt to.

x. Select the "Delete extra files" checkbox to synchronize the decrypt location with the backup files/folders being decrypted. This setting will delete existing files/folders from the decrypt location that were not part of the backup.

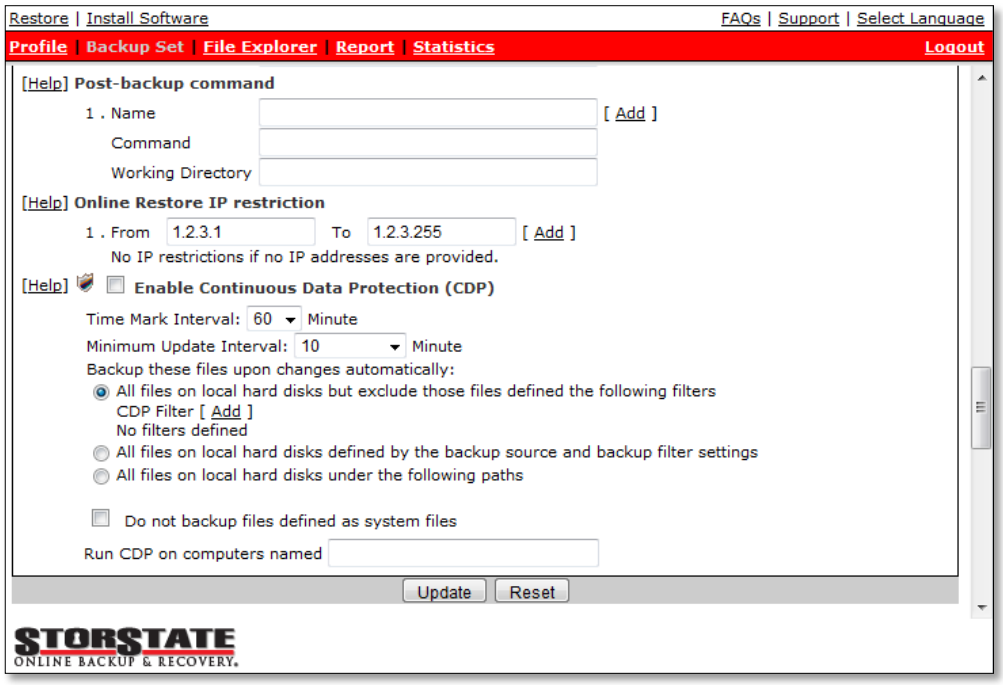
xi. Select the "Restore file permissions" checkbox to restore file permissions to files as they are decrypted.

xii. Click [Start Decrypt] to start the decryption operation. A dialog will display the progress and alert you when completed.



7.4 IP address restriction for online restore

Online file restore operation can be restricted to authorized IP addresses only. To setup IP restriction, login to your Web Management Console and click the [Backup Set] button on the top left menu. Scroll down to the [Online Restore IP Restriction] section, fill in the IP range to be allowed, and click the [Add] button. Multiple IP address ranges may be added.



8 Byte-Level Delta Technology

The chapter describes what Byte-Level Delta technology is and how Byte-Level Delta can be used to backup large files (ex. a 10GB Outlook.pst file) without uploading the whole file every backup.

8.1 Overview

Byte-Level Delta technology is an advanced data block matching algorithm which can find changes (delta) of file content between two files. Using this algorithm, regular backup of large files over low-speed internet connections is possible, because only the changes in information since the last backup are sent over the internet.

The following is an example of a 10GB Outlook.pst file backed up by StorState Backup Manager with Byte-Level Delta technology.

i. During the first backup, the whole file (10GB), along with its checksum file, are backed up to the Data Vaulting Center. This can be done directly through the internet or by using the seed loading utility to copy to a removable hard disk.

ii. When backup runs next, StorState Backup Manager will download a checksum listing of all data blocks of the full backup file (or last incremental backup file) from the Data Vaulting Center and use it to find all changes that have been made to the current Outlook.pst file.

iii. Changes detected are then saved in a delta file which is uploaded to the Data Vaulting Center. A new checksum file is generated and is also uploaded.

iv. Subsequent backups of this Outlook.pst file will go through step ii & iii again. Only a small delta file and checksum file will be uploaded to the Data Vaulting Center.

v. With Byte-Level Delta technology, regular backups of large files over low-speed internet connection is possible.

Incremental Byte-Level Delta type

Incremental Delta will facilitate the quickest backup operation. The delta is generated by comparing the latest uploaded full or delta file. The delta file generated is the smallest possible and uses the least bandwidth during backup. For restoration, the full file and all delta files up to the required point-in-time is required to restore the file to a specific point-in-time.

Example: You add around 100MB of changes to a 10GB Outlook.pst everyday.

After the first full backup job, StorState Backup Manager will generate and upload delta files instead of uploading the full file until either one of the following two rules are true:

a) The number of deltas generated since the last full backup is greater than the [No. of Delta] setting.

b) The delta ratio (the ratio of the delta file size against the full file size) is greater than the [Delta Ratio] setting.

Using incremental delta, the delta generated by comparing the current file with the latest uploaded full or delta file is around 100MB.

Since the delta file size is around 100MB daily, the delta ratio (around 1%) will not trigger a full file upload. Instead StorState Backup Manager will continue to generate and upload delta files until day 102 (assuming the full file was uploaded on day 1) when the number of deltas generated exceeds the [No. of Delta] setting (assuming the default setting of 100) and triggers the upload of the full Outlook.pst file. You can disable the [No. of Delta] and [Delta Ratio] if you don't want to upload the full file.

All delta files are generated with respect to changes made since the last incremental or full backup. This means that the last full backup file and **ALL** incremental delta backup files are required to restore the latest snapshot of a backup file.

Differential Byte-Level Delta type

Differential Delta will facilitate the quickest restore. The delta is generated by comparing with the latest uploaded full file. The delta file generated grows daily and uses more bandwidth during backup. For restoration, the full file and a single delta file is required to restore the file to a specific point-in-time.

Example: You add around 100MB of changes to a 10G Outlook.pst everyday.

After the first full backup job, StorState Backup Manager will continue to generate and upload delta files instead of uploading the full file until either one of the following two rules are true:

a) The number of deltas generated since the last full backup is greater than the [No. of Delta] setting.

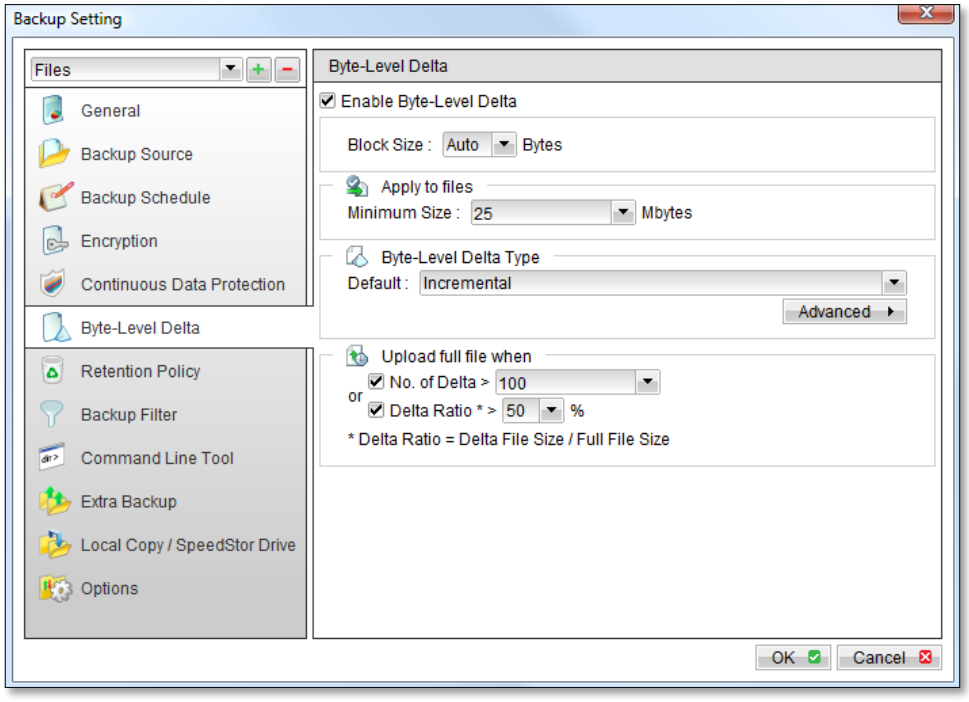
b) The delta ratio (the ratio of the delta file size against the full file size) is greater than the [Delta Ratio] setting.

Using differential delta, the delta generated by comparing the current file with the latest uploaded full file is around 100MB for the 1st delta, 200MB for the 2nd delta, 300MB for the 3rd delta and so on.

Since the delta file grows by 100MB daily, the delta ratio for day 52 (delta file size is approximately 51x100= 5.1GB, assuming the full file was uploaded on day 1) being over 50% exceeds the default [Delta Ratio] setting and triggers the upload of the full Outlook.pst file. You can disable the [No. of Delta] and [Delta Ratio] if you don't want to upload the full file.

All delta files are generated with respect to changes made since the last full backup file (i.e. differential backup). This means that only last full backup file and the last delta file are required to restore the latest snapshot of a backup file. Other intermediate delta files are only required if you want to restore other snapshots of a backup file.

Differential Byte-Level Delta backup has the benefit that a corrupted delta file would only make one particular version of a backup file non-recoverable and all other backups created by other delta files of the same file would still be intact.



8.2 Block Size

The block size setting defines the size of the data block being used to detect the changes between the last full or delta backup file and the current file on the local computer. In general, the smaller the block size, the more likely a matching data block can be found between the last backup file and the file on the local computer. It therefore produces a smaller delta file but would require more processing power to detect the changes. On the other hand, Byte-Level Delta backup running with larger block size will run faster but will generally produce a larger delta file.

In most cases, the default [Auto] setting is best, choosing the optimal block size for each file based on the file size.

8.3 Minimum File Size

The [Minimum Size] setting defines the smallest file size a file must have before Byte-Level Delta backup is used.

If the size of a file that is being backed up is smaller than the [Minimum Size] setting, Byte-Level Delta backup technology will not be used, and the entire file will be uploaded to the Data Vaulting Center. It is not advantageous to perform Byte-Level Delta backup on small files because backing up the whole file doesn't take long, delta processing time isn't needed, and restoration time will be reduced.

8.4 Uploading full file again

No. of Delta

The [No. of delta] setting defines the maximum number of delta files from the same backup file to be generated and backed up to the Data Vaulting Center before a full backup (the whole file) is uploaded to the Data Vaulting Center instead. The default value is 100.

For example, if you have created 100 delta files from the full backup file already and the [No. of delta] setting is set to 100, the next backup will upload a full backup file (the whole file) instead of just the delta file. However, if the [No. of delta] rule is disabled, it will keep generating delta files and uploading them to the Data Vaulting Center until the other delta rule forces a full backup (i.e. delta ratio exceeded).

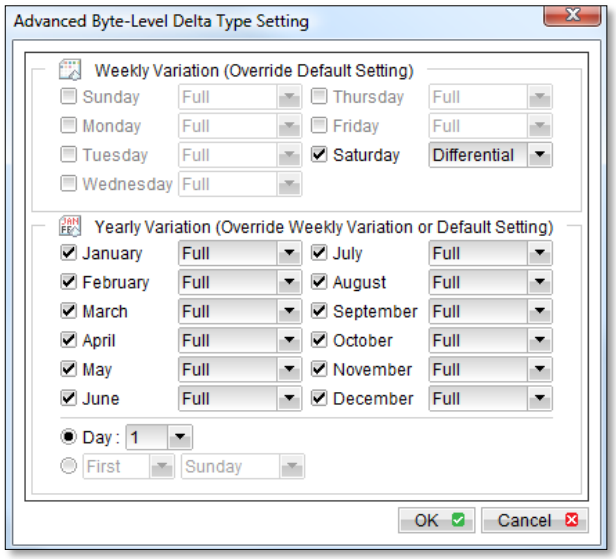
Delta Ratio

The [Delta Ratio] setting defines the highest percentage of changes allowed, between the last full backup file and the current file, before the full backup file will be uploaded to the Data Vaulting Center. The default value is 50%.

If the delta ratio calculated from the size of the generated delta file and the size of the full backup file is greater than the [Delta Ratio] setting, the whole file, instead of just the delta file, will be backed up to the Data Vaulting Center. Uploading the whole file reduces the time required to restore the file.

8.5 Advanced Byte-Level Delta type

The [Byte-Level Delta Type] -> [Advanced] setting allows users to override default Byte-Level Delta type on a schedule. This is useful if for example, you want most Byte-Level Delta backups to be incremental but you want to do a differential Byte-Level Delta backup on Saturdays, as well as full file backups on the 1st day of every month.



With the settings above, all backup Jobs on Saturdays will be differential Byte-Level Delta backups, and backups on the 1st day of each month will be full backups. This ensures that all backup files will be backed up in full at a regular interval. The benefits are a faster restore time due to less delta merging, and the risk of a corrupted incremental delta file resulting in data loss is lower because a full backup is always available periodically.

9 Backup/Restore Oracle Database

This chapter will describe in detail how StorState Pro Backup Manager backs up your Oracle Database Server, and how you can restore an Oracle database using the backup files.

9.1 Requirements

i. StorState Pro Backup Manager must be installed onto a computer that can connect to your Oracle Database Server using the TCP/IP protocol.

ii. Data from Oracle databases will be backed up to a temporary directory before they are sent to the Data Vaulting Center. Please make sure you have sufficient space on your computer to store the data when you run the backup job.

iii. The database must be in archived log mode.

To switch the database to archived log mode, please do the following:

a. Set the parameters below in the PFILE to enable automatic archiving

LOG_ARCHIVE_DEST = [*directory where archive redo logs will be stored*]
LOG_ARCHIVE_FORMAT = 'log%t_%s_%r.arc'
LOG_ARCHIVE_START = TRUE

b. Set ORACLE_SID to your database's System Identifier (SID)

```
export ORACLE_SID=GDB1
```
(assuming your database's SID is *GDB1*)

c. Run SQL Plus and connect to database as SYSDBA

For Oracle 9i/10g/11g

```
sqlplus "/ as sysdba"
```

For Oracle 8i

```
connect internal;
```

d. Shutdown database

```
shutdown immediate
```

e. Start and mount database

```
startup mount
```

f. Switch database to archived log mode

```
alter database archivelog;
```

g. Open database

```
alter database open;
```

Oracle 10g Example:

```
$ export ORACLE_SID=GDB1

$ sqlplus "/ as sysdba"

SQL*Plus: Release 10.2.0.1.0 - Production on Thu Nov 8 15:08:57 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options
```

```
SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.

SQL> startup mount
ORACLE instance started.

Total System Global Area  285212672 bytes
Fixed Size                 1218992 bytes
Variable Size             96470608 bytes
Database Buffers         184549376 bytes
Redo Buffers               2973696 bytes
Database mounted.

SQL> alter database archivelog;

Database altered.

SQL> alter database open;

Database altered.
```

iv. Grant the JAVASYSPRIV role to the system account

You can grant this role to system account by executing:

h. Grant permission to system account

For Oracle 9i/10g/11g

```
SQL> grant javasyspriv to system;
```

For Oracle 8i

```
SVRMGRL> connect internal
SVRMGRL> @?/javavm/install/initjvm.sql;
SVRMGRL> @?/rdbms/admin/catalog.sql;
SVRMGRL> @?/rdbms/admin/catproc.sql;
SVRMGRL> @?/javavm/install/initdbj.sql;
SQL> grant javasyspriv to system;
```

Oracle 9i/10g/11g Example:

```
SQL> grant javasyspriv to system;

Grant succeeded.
```

9.2 Overview

StorState Pro Backup Manager will backup your Oracle database by taking the following steps.

i. Connect to the Oracle database using SQL*NET over TCP/IP

ii. Run all Pre-Commands of this backup set

iii. If the backup type to run is [Database Backup type],

a. all data files in each of the tablespace(s) selected are copied to the temporary directory specified by this backup set

b. if there are temporary files in the database, the script to re-create the temporary files is generated to a file located in the temporary directory specified by this backup set

c. all non-default initialization parameters will be spooled to an initializing file located in the temporary directory specified by this backup set

d. all control files will be copied to the temporary directory specified by this backup set

e. all archived log files will be copied to the temporary directory specified by this backup set

iv. If the backup type to run is [Archived Log Backup type],

a. all archived log files will be copied to the temporary directory specified by this backup set

v. Run all Post-Commands of this backup set

vi. Upload all files copied to the temporary directory to the StorState Data Vaulting Center

vii. Remove temporary files from the temporary directory

Note:
If your Oracle database is running on Windows, please install StorState Pro Backup Manager in the computer running the Oracle database. This will shorten the time required to backup the Oracle database.

9.3 How to backup an Oracle Database (Physical Backup)

Please follow the instructions below to backup your Oracle database to the Data Vaulting Center.

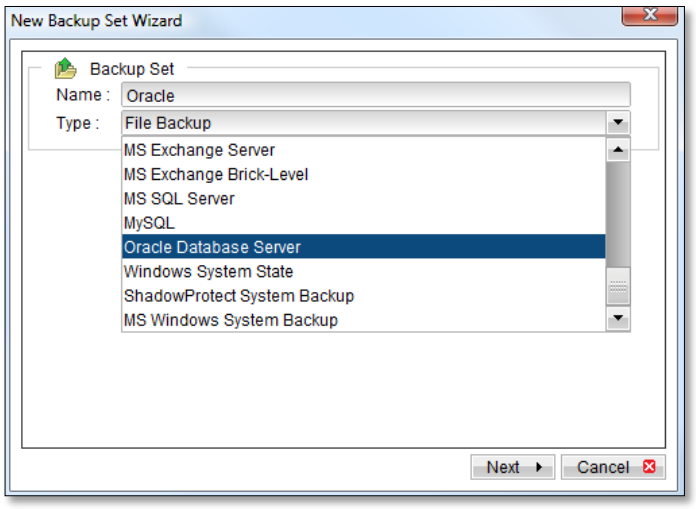
i. Open StorState Pro Backup Manager.

ii. Create a new backup set.

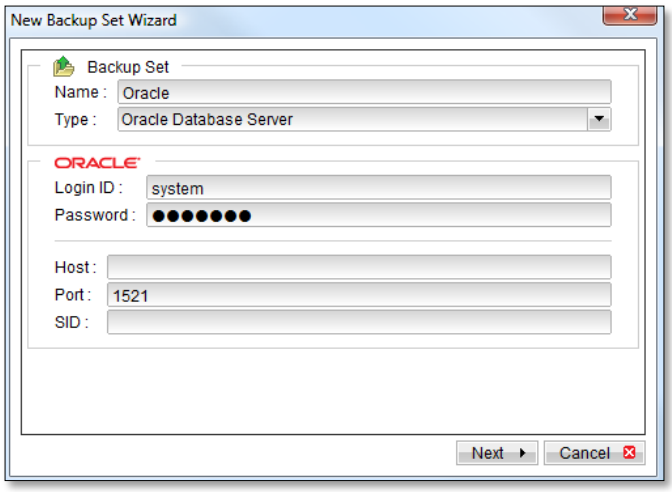
a. To setup backup sets, click the button to open the [Backup Setting] page.

b. On the left panel, press the button to create a new backup set.

c. On the dialog, choose [Oracle Database Server] as the [Type].

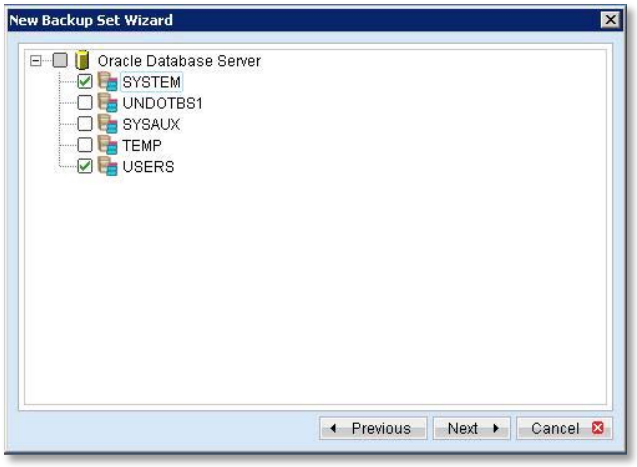


d. Enter a name for your backup set.

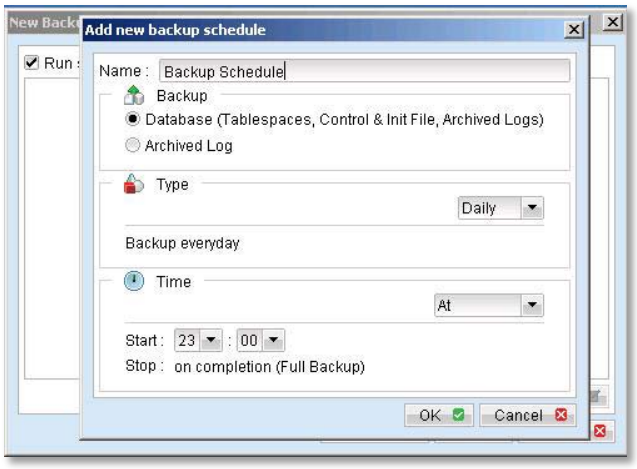


e. Enter the system password, the Oracle Database Server Host Name, TNS Port and SID.

f. Select the tablespace(s) you wish to backup.



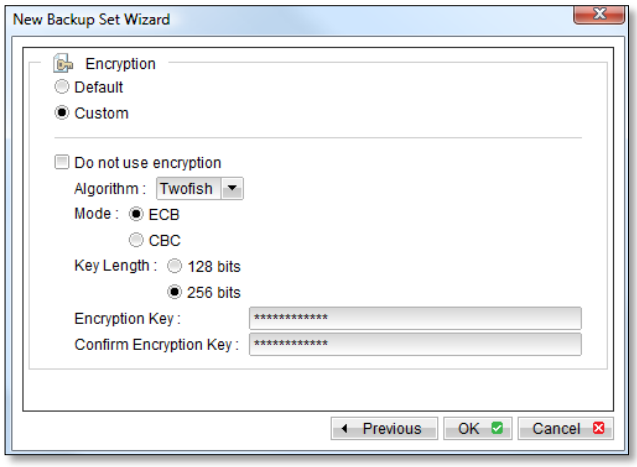
g. Setup the backup schedule for database backup and archived log backup.



Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day

transaction log backups by adding multiple daily transaction log backup schedules to your backup set.

h. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave on default.

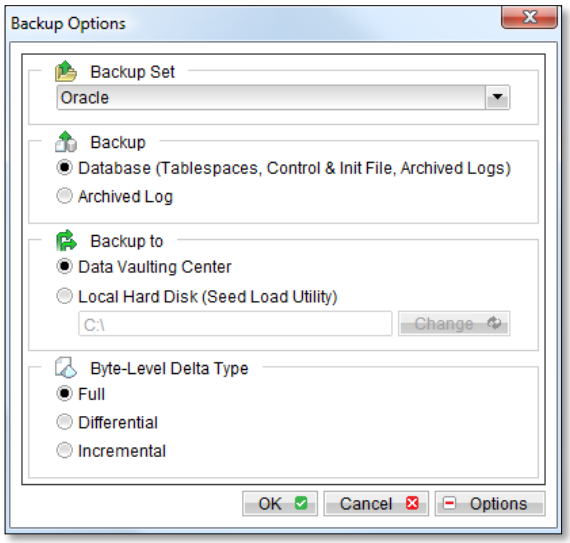


IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!

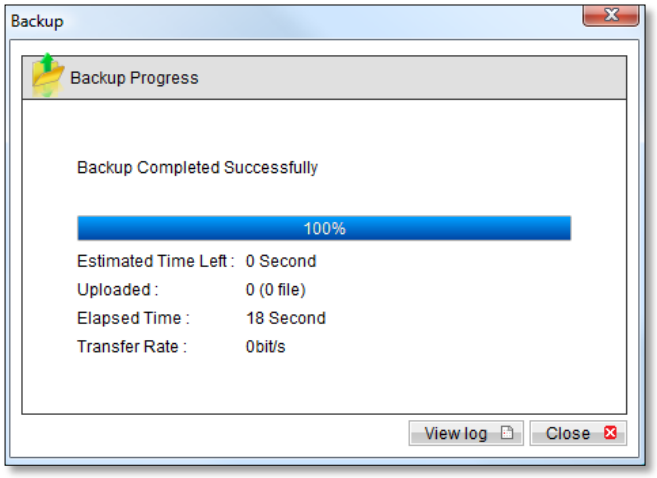
iii. Run Backup.

a. Press the [Backup] button on the main page of StorState Pro Backup Manager.

b. Select your Oracle backup set from the [Backup Set] list. Select the [Backup] type (Full Database Backup or Archived Log Backup) you would like to perform. If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.



9.4 How to restore an Oracle Database

Please follow the instructions below to restore your Oracle 9i/10g/11g databases.

i. Download the backup files from the Data Vaulting Center to a temporary folder, or decrypt backup files from a local copy.

ii. <u>To restore an existing database</u>

Shutdown the database

To shutdown the database, please do the following:

a. Set ORACLE_SID to your database's System Identifier (SID)

```
$ export ORACLE_SID=GDB1
```
(assuming your database's SID is *GDB1*)

b. Run SQL Plus and connect to database as SYSDBA

```
$ sqlplus "/ as sysdba"
```

c. Shutdown database

```
SQL> shutdown immediate
```

Oracle 9i/10g/11g Example:

```
$ export ORACLE_SID=GDB1

$ sqlplus "/ as sysdba"

SQL*Plus: Release 10.2.0.1.0 - Production on Thu Nov 8 17:04:57 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
```

To recover a database that currently does not exist
Create a password file

```
$ orapwd file=$ORACLE_HOME/dbs/orapwGDB1 password=pwd123
```

(assuming your database's SID is *GDB1*, and password is *pwd123*)

Oracle 9i/10g/11g Example:
`$ orapwd file=/oracle/OraHome1/dbs/orapwGDB1 password=pwd123`

iii. Put all downloaded backup files into place

Control files, data files and archived logs are stored in your data vault along with their full path information. Put all these files back to their original locations when performing a database restore.

For example:

```
/oracle_restore/Oracle Database Server/oracle/product/10.2.0/db_1/admin/GDB1/
/oracle_restore/Oracle Database Server/oracle/product/10.2.0/db_1/dbs/initGDB1.ora
/oracle_restore/Oracle Database Server/oracle/product/10.2.0/db_1/dbs/spfileGDB1.ora
/oracle_restore/Oracle Database Server/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/
/oracle_restore/Oracle Database Server/oracle/product/10.2.0/db_1/oradata/GDB1/
```

Move to

```
/oracle/product/10.2.0/db_1/admin/GDB1/
/oracle/product/10.2.0/db_1/dbs/initGDB1.ora
/oracle/product/10.2.0/db_1/dbs/spfileGDB1.ora
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/
/oracle/product/10.2.0/db_1/oradata/GDB1/
```

iv. Rename database files (**Only for restoring database to a new location**)

Rename your database files by doing the following:

a. Modify the PFILE to update file path

Open the PFILE (*$ORACLE_HOME/dbs/initGDB1.ora*), change every file path to the new location, and then save it.

For example:

```
background_dump_dest = /oracle/OraHome1/admin/GDB2/bdump

control_files = (/oracle/OraHome1/oradata/GDB2/control01.ctl,
                 /oracle/OraHome1/oradata/GDB2/control02.ctl,
                 /oracle/OraHome1/oradata/GDB2/control03.ctl)

core_dump_dest = /oracle/OraHome1/admin/GDB2/cdump

user_dump_dest = /oracle/OraHome1/admin/GDB2/udump
```

Change to

```
background_dump_dest = /new_db_location/OraHome1/admin/GDB2/bdump

control_files = (/new_db_location/OraHome1/oradata/GDB2/control01.ctl,
                 /new_db_location/OraHome1/oradata/GDB2/control02.ctl,
                 /new_db_location/OraHome1/oradata/GDB2/control03.ctl)

core_dump_dest = /new_db_location/OraHome1/admin/GDB2/cdump

user_dump_dest = /new_db_location/OraHome1/admin/GDB2/udump
```

b. You may need to quote the values of dispatchers as a single argument.

Add double quotation marks

```
dispatchers = "(PROTOCOL=TCP) (SERVICE=GDB1XDB)"
```

c. Delete the SPFILE

Delete the SPFILE (*$ORACLE_HOME/dbs/spfileGDB1.ora*)

d. Set ORACLE_SID to your database's System Identifier (SID)

$ export ORACLE_SID=GDB1 (assuming your database's SID is *GDB1*)

e. Run SQL Plus and connect to database as SYSDBA

```
$ sqlplus "/ as sysdba"
```

f. Start and mount database

```
SQL> startup mount
```

g. Create a backup of the control file to trace file

```
SQL> alter database backup controlfile to trace as '/New_DB_Location/control.trc' reuse;
```
(assuming you create a trace file to */New_DB_Location/*)

h. Rename each data file, log file and tempfile

Open the trace file just created, and then check for the filename of each datafile, log file and tempfile.

Please do the following to rename each of the files:

```
SQL> ALTER DATABASE RENAME FILE 'xxx' TO 'yyy';
where xxx is the old filename found in the trace file, and yyy is the new filename with updated path
```

For example:

```
SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/system01.dbf' TO
'/new_db_location/oradata/GDB1/system01.dbf';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/undotbs01.dbf' TO
'/new_db_location/oradata/GDB1/undotbs01.dbf';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/sysaux01.dbf' TO
'/new_db_location/oradata/GDB1/sysaux01.dbf';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/users01.dbf' TO
'/new_db_location/oradata/GDB1/users01.dbf';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/TS1' TO
'/new_db_location/oradata/GDB1/TS1';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/redo01.log' TO
'/new_db_location/oradata/GDB1/redo01.log';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/redo02.log' TO
'/new_db_location/oradata/GDB1/redo02.log';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/redo03.log' TO
'/new_db_location/oradata/GDB1/redo03.log';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/temp01.dbf' TO
'/new_db_location/oradata/GDB1/temp01.dbf';
```

Oracle 9i/10g Example:

```
$ export ORACLE_SID=GDB1

$ sqlplus "/ as sysdba"

SQL*Plus: Release 10.2.0.1.0 - Production on Fri Nov 9 17:50:30 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Connected to an idle instance.
```

```
SQL> startup mount

ORACLE instance started.

Total System Global Area  285212672 bytes
Fixed Size                 1218992 bytes
Variable Size             92276304 bytes
Database Buffers         188743680 bytes
Redo Buffers              2973696 bytes
Database mounted.

SQL> alter database backup controlfile to trace as '/new_db_location/control.trc' reuse;

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/system01.dbf' TO
'/new_db_location/oradata/GDB1/system01.dbf';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/undotbs01.dbf' TO
'/new_db_location/oradata/GDB1/undotbs01.dbf';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/sysaux01.dbf' TO
'/new_db_location/oradata/GDB1/sysaux01.dbf';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/users01.dbf' TO
'/new_db_location/oradata/GDB1/users01.dbf';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/TS1' TO
'/new_db_location/oradata/GDB1/TS1';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/redo01.log' TO
'/new_db_location/oradata/GDB1/redo01.log';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/redo02.log' TO
'/new_db_location/oradata/GDB1/redo02.log';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/redo03.log' TO
'/new_db_location/oradata/GDB1/redo03.log';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/temp01.dbf' TO
'/new_db_location/oradata/GDB1/temp01.dbf';

Database altered.
```

v. Restore Database

Use Recovery Manager to restore your database by doing the following:

For Oracle 9i/10g/11g

a. Set ORACLE_SID to your database's System Identifier (SID)

```
$ export ORACLE_SID=GDB1
```
(assuming your database's SID is *GDB1*)

b. Run Oracle Recovery Manager (rman) and connect to the target database

```
$ rman target /
```

c. Start and mount database

```
RMAN> startup mount
```

d. Reapply all transactions from the archived log files to the last sequence

```
RMAN> recover database until sequence=4 thread=1;
```

(assuming the sequence number of your last archived redo log is *3*)

Sequence numbers are named in the filename of archived redo log

ex. `/oracle/OraHome1/dbs/o1_mf_1_2_3m5h1svs_.arc`
`/oracle/OraHome1/dbs/o1_mf_1_3_3m5h1yby_.arc`
in this case, the sequence number of archived redo log is **4**.

e. Open database

```
RMAN> alter database open resetlogs;
```

Oracle 9i/10g/11g Example:

```
$ export ORACLE_SID=GDB1

$ rman target /

Recovery Manager: Release 10.2.0.1.0 - Production on Thu Nov 8 17:46:27 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

connected to target database (not started)

RMAN> startup mount

Oracle instance started
database mounted

Total System Global Area    285212672 bytes

Fixed Size                  1218992 bytes
Variable Size             113247824 bytes
Database Buffers          167772160 bytes
Redo Buffers                2973696 bytes

RMAN> recover database until sequence=4 thread=1;

Starting recover at 08-NOV-07
Starting implicit crosscheck backup at 08-NOV-07
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=157 devtype=DISK
Finished implicit crosscheck backup at 08-NOV-07

Starting implicit crosscheck copy at 08-NOV-07
using channel ORA_DISK_1
Finished implicit crosscheck copy at 08-NOV-07

searching for all files in the recovery area
cataloging files...
cataloging done

List of Cataloged Files
=======================
File Name:
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1_3_3m5h1y
by_.arc

using channel ORA_DISK_1

starting media recovery

archive log thread 1 sequence 2 is already on disk as file
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1_2_3m5h1s
vs_.arc
archive log thread 1 sequence 3 is already on disk as file
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1_3_3m5h1y
by_.arc
archive log
filename=/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1
_2_3m5h1svs_.arc thread=1 sequence=2
archive log
filename=/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1
_3_3m5h1yby_.arc thread=1 sequence=3
media recovery complete, elapsed time: 00:00:01
Finished recover at 08-NOV-07

RMAN> alter database open resetlogs;

database opened
```

For Oracle 8i

a. Set ORACLE_SID to your database's System Identifier (SID)

```
$ export ORACLE_SID=GDB1
```
(assuming your database's SID is *GDB1*)

b. Run Oracle Server Manager (svrmgrl)

```
$ svrmgrl
```

c. Connect to the target database

```
SVRMGRL> connect internal
```

d. Start and mount database

```
SVRMGRL> start mount;
```

e. Reapply all transactions from the archived log files

```
RMAN> recover database using backup controlfile
```

f. Open database

```
RMAN> ALTER DATABASE OPEN RESETLOGS;
```

Oracle 8i Example:

```
$ svrmgrl

SVRMGRL> connect internal

SVRMGR> startup mount;
ORACLE instance started.
Total System Global Area               95874448 bytes
Fixed Size                                64912 bytes
Variable Size                          52744192 bytes
Database Buffers                       40960000 bytes
Redo Buffers                            2105344 bytes
Database mounted.

SVRMGRL> recover database using backup controlfile
ORA-00279: change 419671 generated at 06/14/03 02:51:49 needed for thread 1
ORA-00289: suggestion : /data/ora815/vin/archive/ARCH0000000225.LOG
ORA-00280: change 419671 for thread 1 is in sequence #225
ORA-00278: log file '/data/ora815/vin/archive/ARCH0000000224.LOG' no longer needed for this
recovery
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
AUTO
Log applied.
. . . . . .
ORA-00279: change 547222 generated at 06/18/03 19:58:26 needed for thread 1
ORA-00289: suggestion : /data/ora815/vin/archive/ARCH0000000384.LOG
ORA-00280: change 547222 for thread 1 is in sequence #384
ORA-00278: log file '/data/ora815/vin/archive/ARCH0000000383.LOG' no longer needed for this
recovery
ORA-00308: cannot open archived log '/data/ora815/vin/archive/ARCH0000000384.LOG'
ORA-27037: unable to obtain file status
Linux Error: 2: No such file or directory
Additional information: 3

SVRMGR> recover database using backup controlfile until cancel
ORA-00279: change 547222 generated at 06/18/03 19:58:26 needed for thread 1
ORA-00289: suggestion : /data/ora815/vin/archive/ARCH0000000384.LOG
ORA-00280: change 547222 for thread 1 is in sequence #384
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
CANCEL
Media recovery cancelled.
SVRMGR> alter database open resetlogs;
Statement processed.
```

vi. (**Optional**) Create Net Service Name and Database Service Listener

To create Net Service Name
Start **Net Manager** by running the command **netmgr**

```
$ netmgr
```

→ expand [**Oracle Net Configuration**]

→ expand [**Local**]
→ select [**Service Naming**]
→ click "**+**" icon on the toolbar
→ Net Service Name Wizard will be launched to guide you through creating a net service name
→ click [**File**] on the menu bar
→ [**Save Network Configuration**] on the menu bar

To create Database Service Listener
Start **Net Manager** by running the command **netmgr**
```
$ netmgr
```
→ expand [**Oracle Net Configuration**]
→ expand [**Local**]
→ expand [**Listeners**]
→ select [**LISTENER**]
→ select [**Database Services**] from combo box
→ click [**Add Database**]
→ input Global Database Name and SID
→ click [**File**] on the menu bar
→ [**Save Network Configuration**] on the menu bar

9.5 How to restore a single tablespace

Restoring a tablespace requires a backup of datafiles consistent with the existing archived logs and control files, as redo will be applied during the restore operation.

Please follow the instructions below to restore a tablespace.

i. Download the backup files from the Data Vaulting Center to a temporary folder, or decrypt backup files from a local copy.

ii. Set ORACLE_SID to your database's System Identifier (SID)

```
$ export ORACLE_SID=GDB1
```
(assuming your database's SID is *GDB1*)

iii. Run SQL Plus and connect to database as SYSDBA

```
$ sqlplus "/ as sysdba"
```

iv. Shutdown database

```
SQL> shutdown immediate
```

v. Copy your tablespace datafiles into place

Datafile names and paths can be found by using the REPORT SCHEMA command.

a. Set ORACLE_SID to your database's System Identifier (SID)

```
$ export ORACLE_SID=GDB1
```
(assuming your database's SID is *GDB1*)

b. Run Oracle Recovery Manager (rman) and connect to the target database

```
$ rman target /
```

c. Start and mount database

```
RMAN> startup mount
```

d. List the names of all datafiles and tablespaces

```
RMAN> report schema;
```

For example:

```
Report of database schema
File K-bytes     Tablespace  RB segs Datafile Name
---- ---------- ----------- ------- -------------------
1         419840 SYSTEM      ***     /oracle/OraHome1/oradata/GDB1/system01.dbf
2         204800 UNDOTBS1     ***    /oracle/OraHome1/oradata/GDB1/undotbs01.dbf
3          20480 CWMLITE     ***     /oracle/OraHome1/oradata/GDB1/cwmlite01.dbf
4          20480 DRSYS       ***     /oracle/OraHome1/oradata/GDB1/drsys01.dbf
5         141440 EXAMPLE     ***     /oracle/OraHome1/oradata/GDB1/example01.dbf
6          25600 INDX        ***     /oracle/OraHome1/oradata/GDB1/indx01.dbf
7          20480 ODM         ***     /oracle/OraHome1/oradata/GDB1/odm01.dbf
8          10240 TOOLS       ***     /oracle/OraHome1/oradata/GDB1/tools01.dbf
9          25600 USERS       ***     /oracle/OraHome1/oradata/GDB1/users01.dbf
10         39040 XDB         ***     /oracle/OraHome1/oradata/GDB1/xdb01.dbf
11             0 TS1         ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf
12             0 TS1         ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf
13             0 TS1         ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf
```

e. Copy all backups of datafiles that constitute the tablespace to the listed location

For example:

/oracle_restore/Oracle Database Server/oracle/OraHome1/oradata/GDB1/*TS1_datafile1.dbf*

/oracle_restore/Oracle Database Server/oracle/OraHome1/oradata/GDB1/*TS1_datafile2.dbf*

/oracle_restore/Oracle Database Server/oracle/OraHome1/oradata/GDB1/*TS1_datafile3.dbf*

Move to

/oracle/OraHome1/oradata/GDB1/*TS1_datafile1.dbf*

/oracle/OraHome1/oradata/GDB1/*TS1_datafile2.dbf*

/oracle/OraHome1/oradata/GDB1/*TS1_datafile3.dbf*

vi. Restore tablespace

`RMAN> recover tablespace TS1;` (assuming your tablespace is *TS1*)

If your datafiles are consistent with the database, you should see:

Oracle 9i/10g Example:

```
RMAN> recover tablespace TS1;

Starting recover at 19-JUL-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=156 devtype=DISK

starting media recovery

archive log thread 1 sequence 1 is already on disk as file D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_1_39Y98F0H_.ARC
archive log thread 1 sequence 2 is already on disk as file D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_2_39Y98JSD_.ARC
archive log thread 1 sequence 3 is already on disk as file D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_3_39Y9SW4D_.ARC
archive log filename=D:\ORACLE\PRODUCT\10.2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELO
G\2007_07_19\O1_MF_1_1_39Y98F0H_.ARC thread=1 sequence=1
media recovery complete, elapsed time: 00:00:01
Finished recover at 19-JUL-07
```

If your datafiles are not consistent with the database, you should see:

Oracle 9i/10g Example:

```
RMAN> recover tablespace TS1;

Starting recover at 19-JUL-07
```

```
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=156 devtype=DISK
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of recover command at 07/20/2007 12:24:49
RMAN-06163: some datafiles cannot be recovered, aborting the RECOVER command
RMAN-06166: datafile 7 cannot be recovered
RMAN-06166: datafile 6 cannot be recovered
RMAN-06166: datafile 5 cannot be recovered
```

In this case, you need to find the consistent datafiles in order to restore the tablespace.

If there are archive logs missing, you should see:

Oracle 9i/10g Example:

```
RMAN> recover tablespace TS1;

Starting recover at 20-JUL-07
using channel ORA_DISK_1

starting media recovery

archive log thread 1 sequence 12 is already on disk as file D:\ORACLE\PRODUCT\10
.2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_18\O1_MF_1_12_39VF4JNJ_.ARC
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of recover command at 07/20/2007 12:28:52
RMAN-06053: unable to perform media recovery because of missing log
RMAN-06025: no backup of log thread 1 seq 13 lowscn 660617 found to restore
```

In this case, you need to find the missing archive log files in order to restore the tablespace.

vii. Open database

```
RMAN> alter database open;
```

Oracle 9i/10g Example:

```
$ export ORACLE_SID=GDB1

$ rman target /

Recovery Manager: Release 9.2.0.1.0 - Production

Copyright (c) 1995, 2002, Oracle Corporation.  All rights reserved.

connected to target database (not started)

RMAN> startup mount

Oracle instance started
database mounted

Total System Global Area    235999352 bytes

Fixed Size                    450680 bytes
Variable Size              201326592 bytes
Database Buffers            33554432 bytes
Redo Buffers                  667648 bytes

RMAN> report schema;

using target database control file instead of recovery catalog
Report of database schema

using target database controlfile instead of recovery catalog
Report of database schema
File K-bytes    Tablespace         RB segs Datafile Name
---- ---------- ------------------ ------- ------------------
1       419840 SYSTEM             ***     /oracle/OraHome1/oradata/GDB1/system01.dbf
2       204800 UNDOTBS1           ***     /oracle/OraHome1/oradata/GDB1/undotbs01.dbf
3        20480 CWMLITE            ***     /oracle/OraHome1/oradata/GDB1/cwmlite01.dbf
4        20480 DRSYS              ***     /oracle/OraHome1/oradata/GDB1/drsys01.dbf
5       141440 EXAMPLE            ***     /oracle/OraHome1/oradata/GDB1/example01.dbf
6        25600 INDX               ***     /oracle/OraHome1/oradata/GDB1/indx01.dbf
7        20480 ODM                ***     /oracle/OraHome1/oradata/GDB1/odm01.dbf
8        10240 TOOLS              ***     /oracle/OraHome1/oradata/GDB1/tools01.dbf
9        25600 USERS              ***     /oracle/OraHome1/oradata/GDB1/users01.dbf
10       39040 XDB                ***     /oracle/OraHome1/oradata/GDB1/xdb01.dbf
11           0 TS1                ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf
12           0 TS1                ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf
13           0 TS1                ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf
```

```
List of Temporary Files
=======================
File Size(MB) Tablespace          Maxsize(MB) Tempfile Name
---- -------- -------------------- ----------- --------------------
1    20       TEMP                 32767       D:\ORACLE\PRODUCT\10.2.0\ORADATA\
GDB1\TEMP01.DBF

RMAN> recover tablespace TS1;

Starting recover at 30-AUG-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=11 devtype=DISK

starting media recovery
media recovery complete

Finished recover at 30-AUG-07

RMAN> alter database open;

database opened
```

9.6 Export and Import a Database (Logical Backup)

While physical backup of database files permit the full reconstruction of a database, logical backup is a useful supplement to physical backup for some purposes. For instance, logical backup using the export and import utilities are the only method that Oracle supports for moving an existing database from one platform to another.

Please follow the instructions below to backup a database:

i. Export the full database to a dump file

```
$ exp system/pwd123 FULL=y FILE='/oracle/data.dmp' LOG='/oracle/export.log'
```

(assuming your system password is *pwd123*, the name of the dump file is */oracle/data.dmp* and the name of the log file is */oracle/export.log*)

Oracle 9i/10g Example:

```
$ exp system/pwd123 FULL=y FILE='/oracle/data.dmp' LOG='/oracle/export.log'

Connected to: Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options
Export done in WE8MSWIN1252 character set and AL16UTF16 NCHAR character set

About to export the entire database ...
. exporting tablespace definitions
. exporting profiles
. exporting user definitions
. exporting roles
. exporting resource costs

                    //////////////////////
                    // ... exporting ... //
                    //////////////////////

. exporting dimensions
. exporting post-schema procedural objects and actions
. exporting user history table
. exporting default and system auditing options
. exporting statistics
Export terminated successfully without warnings.
```

ii. Backup the exported dump file with StorState Backup Manager using a File Backup.

Please follow the instructions below to restore a database:

iii. Download the backup files from the Data Vaulting Center to a temporary folder, or decrypt backup files from a local copy.

iv. Import the full database from the downloaded backup of the dump file

```
$ imp system/pwd123 FULL=y FILE='/oracle/data.dmp' LOG='/oracle/import.log'
```

(assuming your system password is *pwd123*, the name of the dump file is */oracle/data.dmp* and the name of the log file is */oracle/import.log*)

Oracle 9i/10g Example:

```
$ imp system/pwd123 FULL=y FILE='/oracle/data.dmp' LOG='/oracle/import.log'

Connected to: Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

Export file created by EXPORT:V10.02.01 via conventional path
import done in WE8MSWIN1252 character set and AL16UTF16 NCHAR character set
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS
. importing SYSMAN's objects into SYSMAN
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS

         //////////////////////
         // ... importing ... //
         //////////////////////

. importing OLAPSYS's objects into OLAPSYS
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS
. importing SYSMAN's objects into SYSMAN
. importing SCOTT's objects into SCOTT
Import terminated successfully without warnings.
```

10 Backup/Restore Microsoft SQL Server

This chapter will describe in detail how to use StorState Pro Backup Manager to backup your Microsoft SQL Server 7.0 / 2000 / 2005 / 2008 server and how you can restore your Microsoft SQL Server using the backup files.

10.1 Requirements

i. StorState Pro Backup Manager must be installed onto the computer running Microsoft SQL Server.

ii. The “recovery model” setting for databases to be backed up must be set to “Full”.

iii. Data from Microsoft SQL Server will be backed up to a temporary directory before being sent to the Data Vaulting Center. Please make sure you have sufficient space on your computer to store this data when you run the backup job.

10.2 Overview

StorState Pro Backup Manager will backup your Microsoft SQL Server database(s) by taking the following steps:

iv. Before running any backup activities all Pre-Commands of the backup set will run.

v. For each database that is to be backed up, StorState Pro Backup Manager will issue a database / transaction log backup command to Microsoft SQL Server to backup each database to a Microsoft SQL Server database backup file (*.bak file) and save it in the temporary directory specified.

vi. After all *.bak files have been spooled to the temporary directory, all Post-Commands of the backup set will run.

vii. All files copied to the temporary directory are uploaded to the Data Vaulting Center.

viii. Temporary files are removed from the temporary directory.

10.3 How to backup Microsoft SQL Server database(s)

Please follow the instructions below to backup your Microsoft SQL Server databases using StorState Pro Backup Manager.

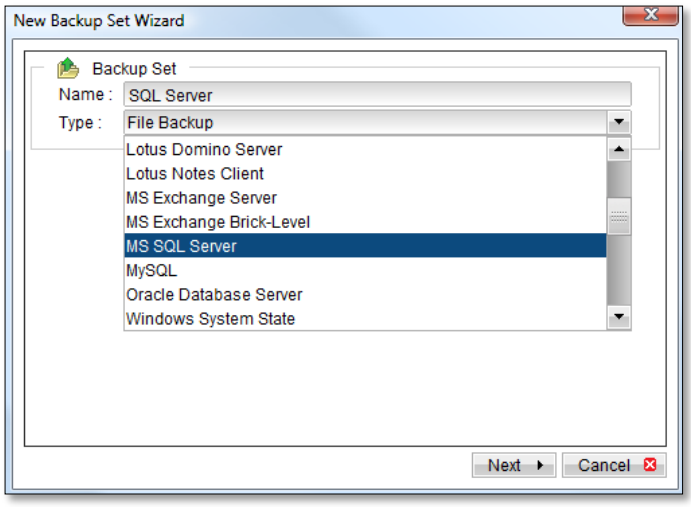
i. Open StorState Pro Backup Manager.

ii. Create a new backup set

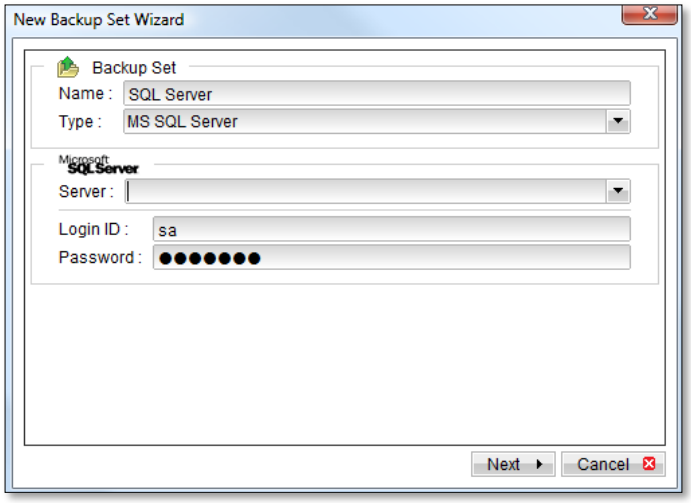
a. To setup backup sets, click the  button to open the [Backup Setting] page.

b. On the left panel, press the  button to create a new backup set.

c. On the dialog, choose [MS SQL Server] as the [Type].

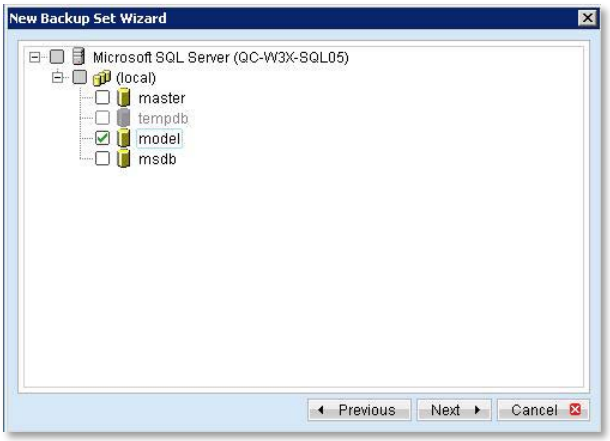


d. Enter a name for your backup set

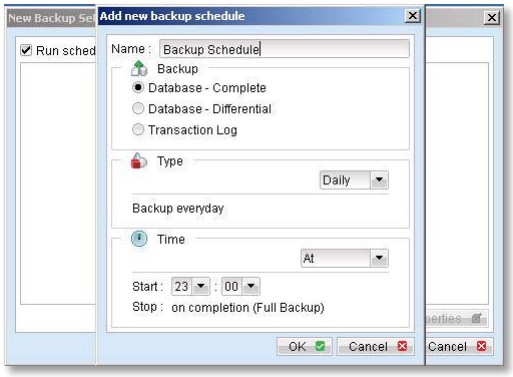


e. Enter the Microsoft SQL Server administrator username and password

f. Select the database(s) you want to backup

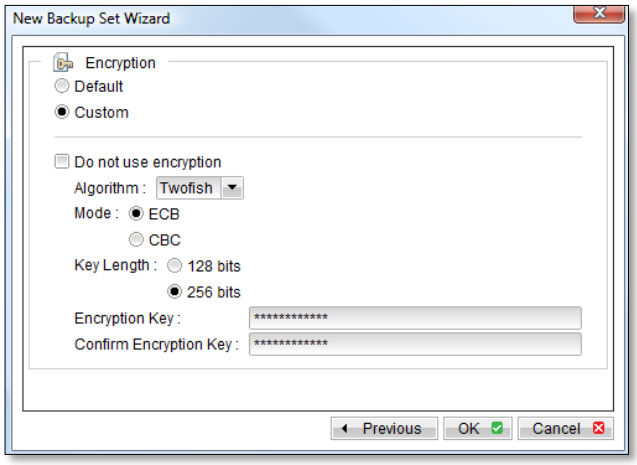


g. Setup the backup schedule for full database backups and transaction log backups.



(Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day transaction log backups by adding multiple daily transaction log backup schedules to your backup set)

h. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave at the default setting.

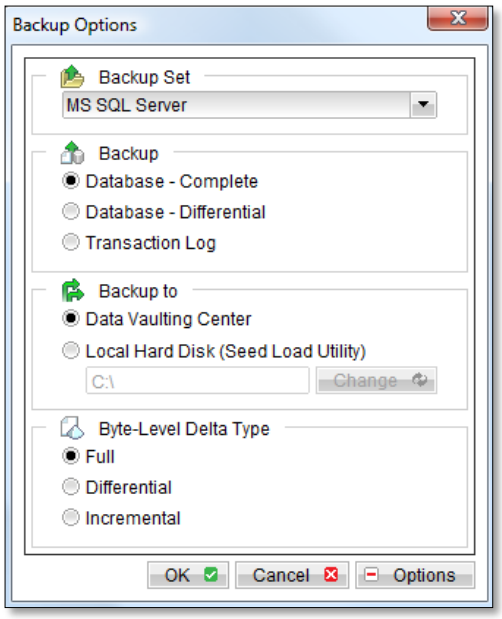


IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!

iii. Run Backup

a. Press the [Backup] button on the main StorState Pro Backup Manager screen.

b. Select your MS SQL Server [Backup Set] from the list. Select the [Backup] type (ex. Complete, Differential, Transaction Log) you would like to perform. If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

10.4 How to restore Microsoft SQL Server database(s)

Please follow the instructions below to restore your Microsoft SQL Server databases.

i. Download the backup files (.bak) from the Data Vaulting Center to a temporary folder, or decrypt backup files from a local copy

ii. Open Microsoft SQL Enterprise Manager

You can open Microsoft SQL Enterprise Manager from [Start Menu] -> [Program] -> [Microsoft SQL Server] -> [Enterprise Manager]

iii. (Optional) Restore "master" database

You need to restore the "master" database if you:

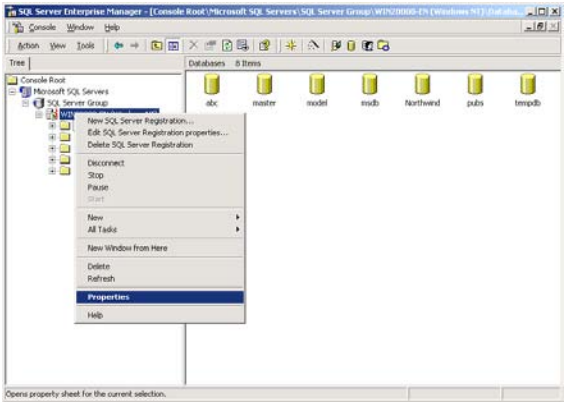
a. are rebuilding all of your databases from scratch
b. have changed any server-wide or database configuration options
c. have added logins or other login security-related operations.
d. have created or removed logical backup devices.
e. have configured the server for distributed queries and remote procedure calls, such as adding linked servers or remote logins.

You do not need to restore your master database if you just want to restore a user database. For more information on Microsoft SQL Server "master" database, please visit http://www.microsoft.com/sql/.

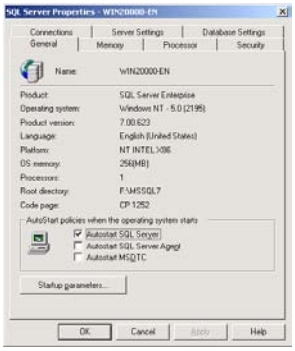
To restore the "master" database, please do the following:

a. Start Microsoft SQL Server in "Single User Mode"

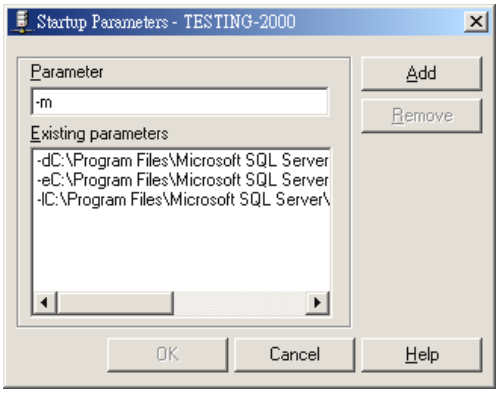
1. Right click your Microsoft SQL Server and select [Properties].



2. Press the [Startup Parameters] button.

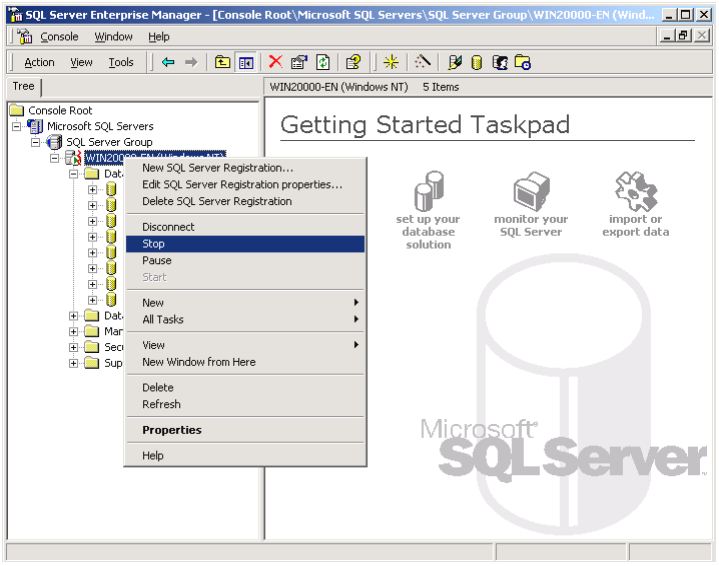


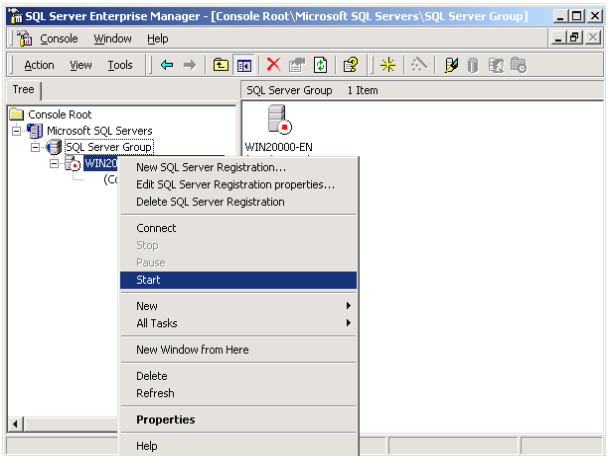
3. Add a “-m” parameter to the [Startup Parameters].



4. Restart Microsoft SQL Server.

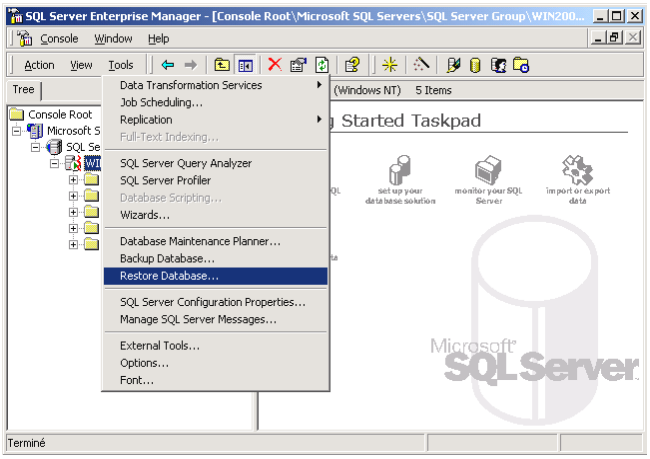
   From [Enterprise Manager], right click on Microsoft SQL Server and select [Stop] and then [Start].





b. Restore “master” database

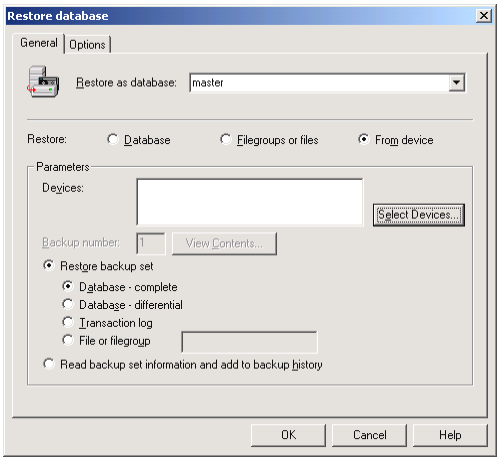
1. From [Enterprise Manager] -> [Tools] -> [Restore Database].



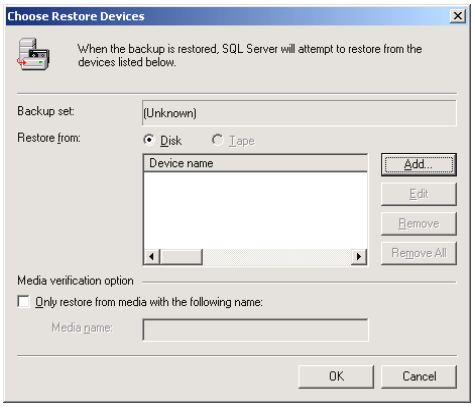
2. Select [master] in the [Restore as database] drop down list.

3. Select the [From device] radio button.

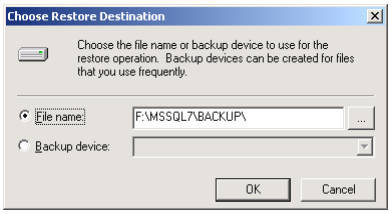
4. Press the [Select Devices] button.



5. From the [Choose Restore Devices], press the [Add] button.



6. From the [Choose Restore Destination] panel, press the [...] button to choose your master backup (*.bak) from your backup files.



7. Press the [OK] button, to start restoring the “master” database.

c. Restart Microsoft SQL Server in “Normal Mode”

1. Remove “-m” parameter from the [Startup Parameters] as in previous step.

2. Restart your Microsoft SQL Server as in previous step.

iv. (Optional) Restore “model”, “msdb” and “distribution” databases

You need to restore “model” database if you have changed the database template of your SQL Server.

You need to restore “msdb” database if you have changed the scheduling information or you want to restore the backup and restore history of your databases.

You need to restore “distribution” database if you are running the replication components of SQL Server.

You do not need to restore these databases if you just want to restore a user database. For more information on Microsoft SQL Server “model”, “msdb” and “distribution” databases, please visit http://www.microsoft.com/sql/.

You need to restore each of these databases one by one. To restore any of these databases, please do the following:

a. From [Enterprise Manager] -> [Tools] -> [Restore Database].

b. Select the database to be restored in the [Restore as database] drop down list.

c. Select the [From device] radio button.

d. Press the [Select Devices] button.

e. Press the [...] button to choose your backup files (*.bak) for the database to be restored.

f. Press the [OK] button.

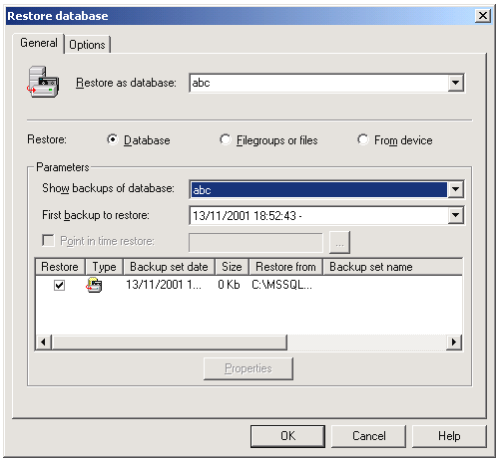
v. Restore user database(s)

For each of the databases you would like to restore,

a. From [Enterprise Manager] -> [Tools] -> [Restore Database].

b. Select the database to be restored in the [Restore as database] drop down list.

c. Select the [Database] radio button.



d. From the [Show backups of database] drop down list, select the database to be restored

e. From the [First backup to restore] drop down list, select the snapshot of the database you would

like to restore to.

You can restore your database to any backup snapshot from the time of your last full backup to your most recent backup.

f. Change the [Restore From] entry

If your backup files (*.bak) are not in the default directory, you need to change to the full path to your backup files by pressing the [Properties] button.

g. Press the [OK] button

vi. All database(s) should be restored successfully

11 Backup/Restore Lotus Domino / Notes

This chapter will describe in detail how to use StorState Pro Backup Manager to backup your Lotus Domino Server / Notes client 5 / 6 / 6.5, and how you can restore your Lotus Domino Server / Notes client from the backup files.

11.1 Requirements

i. StorState Pro Backup Manager must be installed onto the computer running Lotus Domino Server / Notes client.

ii. Data from Lotus Domino Server / Notes client will be backed up to a temporary directory before being sent to the Data Vaulting Center. Please make sure you have sufficient disk space to store this data when you run the backup job.

iii. Lotus Domino Server must run with archive transaction logging enabled

To set up transaction logging in archive style, please do the following:

a. Ensure that all databases to be logged reside in the Domino data directory, either at the root or in subdirectories.

b. From the Domino Administrator, click the Configuration tab.

c. In the "Use Directory on" field, choose the server's Domino directory.

d. Click Server Configuration, and then click Current Server Document.

e. Click the Transactional Logging tab.

f. Complete these fields, and then save the document.

Field	Enter
Transactional Logging	Choose Enabled. The default is Disabled.
Log path	Path name location of the transaction log. The default path name is \LOGDIR in the Domino data directory, although it is strongly recommended to store the log on a separate, mirrored device, such as a RAID (Redundant Array of Independent Disks) level 1+ device with a dedicated controller. The separate device should have at least 1GB of disk space for the transaction log. If you are using the device solely for storing the transaction logs, set the "Use all available space on log device" field to Yes.
Logging style	Choose Archive. The default is Circular.
Maximum log space	The maximum size, in MB, for the transaction log. Default is 192MB. Maximum is 4096MB (4GB). Domino formats at least 3 and up to 64 log files, depending on the maximum log space you allocate.
Use all available space on log device	Choose one: • "Yes" to use all available space on the device for the transaction logs. This is recommended if you use a separate device dedicated to storing the logs. If you choose "Yes", you don't need to enter a value in the "Maximum log space" field. • "No" to use the default or specified value in the "Maximum log space" field.
Automatic fixup of corrupt databases	Choose one: • Enabled (default). If a database is corrupt and Domino cannot use the transaction log to

	recover it, Domino runs the Fixup task, assigns a new DBIID, and notifies the administrator that a new database backup is required. • Disabled. Domino does not run the Fixup task automatically and notifies the administrator to run the Fixup task with the -J parameter on corrupt logged databases.
Runtime / Restart performance	This field controls how often Domino records a recovery checkpoint in the transaction log. This setting affects server performance. To record a recovery checkpoint, Domino evaluates each active logged database to determine how many transactions would be necessary to recover each database after a system failure. When Domino completes this evaluation, it: • Creates a recovery checkpoint record in the transaction log, listing each open database and the starting point transaction needed for recovery • Forces database changes to be saved to disk if they have not been saved already Choose one: • Standard (default and recommended). Checkpoints occur regularly. • Favor runtime. Domino records fewer checkpoints, which requires fewer system resources and improves server run time performance. • Favor restart recovery time. Domino records more checkpoints, which improves restart recovery time because fewer transactions are required for recovery.

Notes:
You can only run a transaction log backup if you have transaction logging enabled and you are using archive mode. A forced backup will not run if you have transaction logging enabled but not in archive mode or if transaction logging is disabled.

11.2 Overview

StorState Pro Backup Manager will backup your Lotus Domino Server / Notes client by taking the following steps:

i. Run all Pre-Commands of the backup set

ii. If the [Backup] type is set to [Database],

   a. all file(s) / database(s) selected are copied to the temporary directory specified in this backup set

   b. the notes.ini file, if selected, will be copied to the temporary directory

   c. only filled log extents will be copied to the temporary directory, and the Domino Server is notified of their availability for reuse (for Domino Server only)

iii. (for Domino Server only) If the [Backup] type is set to [Transaction Log],

   a. only filled log extents will be copied to the temporary directory, and the Domino Server is notified of their availability for reuse

iv. Run all Post-Commands of the backup set

v. Upload all files copied to the temporary directory to the Data Vaulting Center

vi. Remove temporary files from the temporary directory

11.3 How to backup Lotus Domino / Notes database(s) / file(s) on Windows

Please follow the instructions below to backup your Lotus Domino Server / Notes client databases / files.

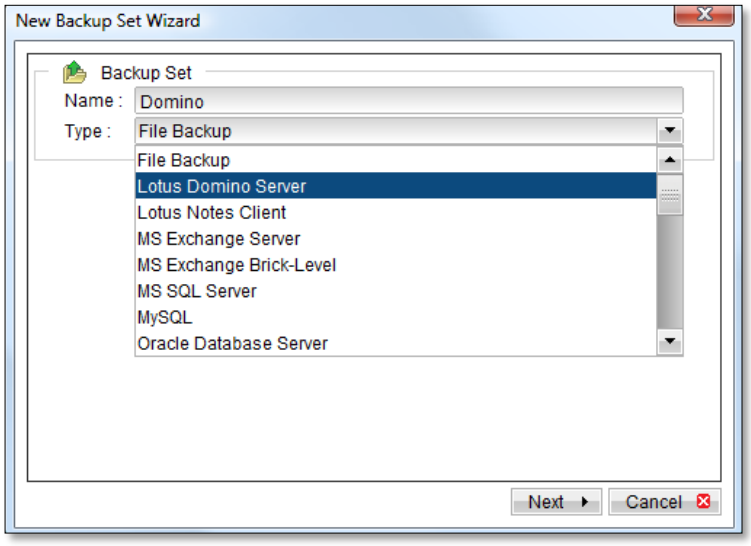
i. Open StorState Pro Backup Manager

ii. Create a new backup set

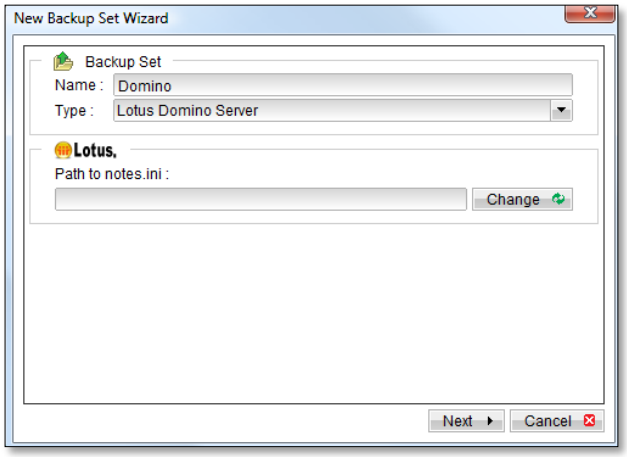
b. To setup backup sets, click the button to open the [Backup Setting] page.

c. On the left panel, press the button to create a new backup set.

d. On the dialog, choose [Lotus Domino Server] or [Lotus Notes Client] as the [Type].

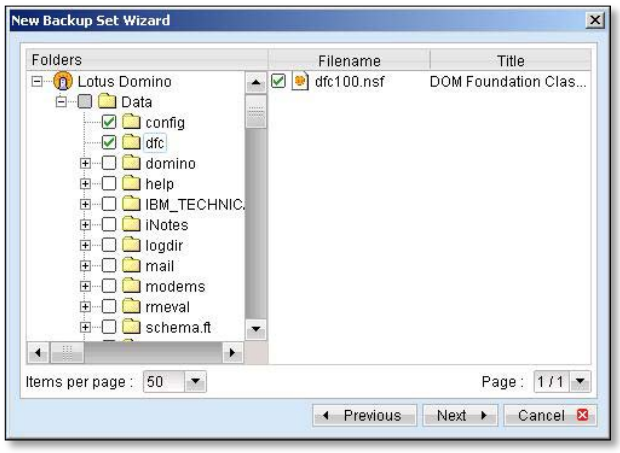


e. Enter a name for your backup set.

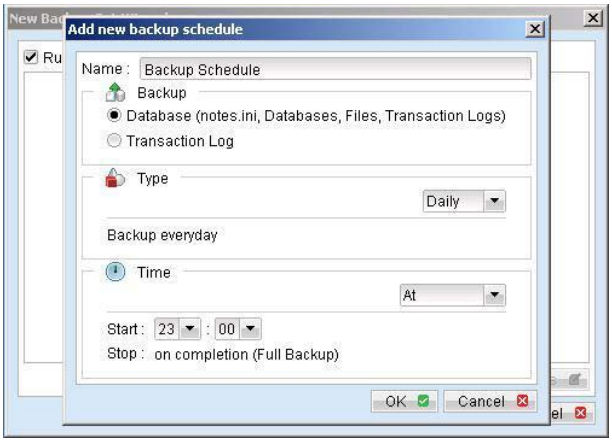


f. Select the location of the “note.ini” file.

g. Select the database(s) / file(s) you want to backup



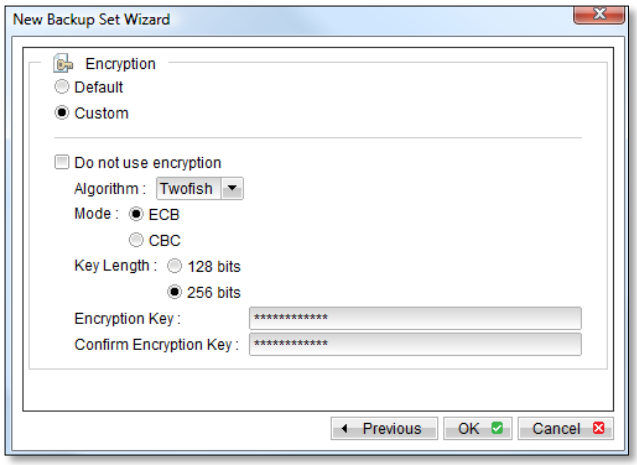
h. Setup backup schedules for [Database] and [Transaction Log] backups (Log backup for Domino Server only)



(Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day transaction log backups by adding multiple daily transaction log backup schedules to your backup set)

i. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave the default setting.

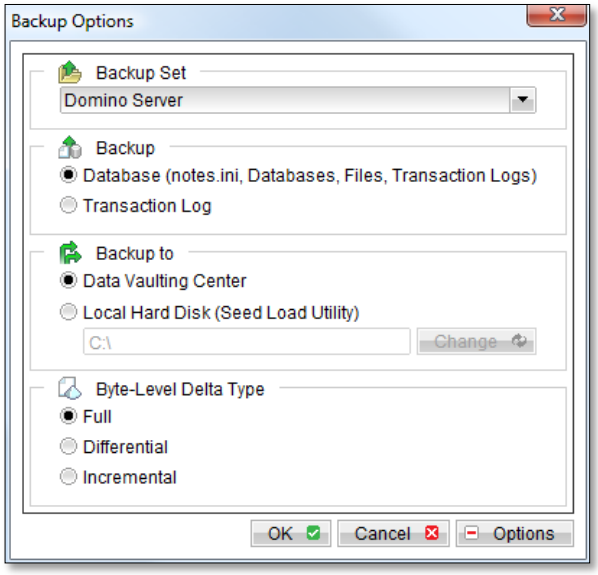
IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!



iii. Run Backup

a. Press the [Backup] button on the main screen of StorState Pro Backup Manager.

b. Select your Domino Server or Notes backup set from the [Backup Set] list. Select the [Backup] type (Database or Transaction Log) you would like to perform (Log backup for Domino Server only). If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

11.4 How to restore Lotus Domino / Notes database(s) / file(s) on Windows

Please follow the instructions below to restore Lotus Domino Server / Notes client database(s) / file(s).

i. Shutdown the Lotus Domino Server

ii. If you want to perform a full Domino restore (restore all databases and files):

a. Download the backup files from the Data Vaulting Center or decrypt backup files from a local copy and save them back to their original location. This includes "notes.ini", all backup files from the Lotus Domino data directory and all archived transaction logs

b. Modify the "DominoRecover.bat" file located under the bin directory of the StorState Pro Backup Manager installation to reflect your setup. You need to specify the Lotus executable directory.

For example change the PROGRAM_DIR to:
PROGRAM_DIR=C:\Lotus\Domino

c. Run "DominoRecover.bat" and press 'Y' to continue.
For example: C:\Program Files\StorState Pro\bin\DominoRecover.bat

This will run media recovery for all databases (*.nsf and mail.box) found under the Lotus data directory (e.g. C:\Lotus\Domino\Data). You should see something similar to the screen below.

Media Recovery Example:

```
C:\Program Files\StorState Pro\bin>DominoRecover.bat
Media Recovery Utility for Lotus Domino 5.0 or above

Please make sure that you have done the following:
1. Reinstall Lotus Domino on this computer in the same directory
2. Restore Notes.ini to the Lotus Domino installation directory
   (e.g. C:\Lotus\Domino)
3. Restore Domino Data directory back to the directory defined
   in Notes.ini (e.g. C:\Lotus\Domino\Data)
4. Restore all archived transaction logs to the directory defined
   in Notes.ini (e.g. C:\Lotus\Domino\Data\logdir)

Continue ? (Y) or (N) y
Running media recovery ...
Please wait, creating new transaction logs in directory: C:\logdir\
02/12/2003 14:39:19   Recovery Manager: Restart Recovery complete. (0/0
databases needed full/partial recovery)
Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
02/12/2003 14:39:22   Recovery Manager: Media Recovery complete for
C:\Lotus\Domino\Data\admin4.nsf, last update applied .

 Backup file C:\Lotus\Domino\Data\admin4.nsf recovered.

……

Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
02/12/2003 14:40:57   Recovery Manager: Media Recovery complete for
C:\Lotus\Domino\Data\statrep.nsf, last update applied .

 Backup file C:\Lotus\Domino\Data\statrep.nsf recovered.

C:\Program Files\StorState Pro\bin>
```

d. Content of all database(s) is now rolled forward to the last committed transaction found in the last archived transaction log

e. Restart Lotus Domino Server

iii. If you want to restore a single database:

a. Download the database file to be restored from the Data Vaulting Center or decrypt the database file from a local copy and save it back to its original location

b. (optional) If you need to perform media recovery on this database, please download all archived transaction logs and save them back to their original location

c. Modify the "DominoRecover.bat" file located under the bin directory of the StorState Pro Backup Manager installation to reflect your setup.

For example we will recover the "admin4.nsf" and have restored the file to C:\restore\notesdata,

change the tags to:

PROGRAM_DIR=C:\Lotus\Domino
INPUTFILE=C:\restore\notesdata\admin4.nsf
RESTOREDB=C:\Lotus\Domino\Data\admin4.nsf
RECDATE=18/01/2007
RECTIME=00:02

d. Run "DominoRecover.bat".

You should see something similar to the screen below.

Media Recovery Example:

```
C:\Program Files\StorState Pro\bin>DominoRecover.bat
Media Recovery Utility for Lotus Domino 5.0 or above

Running media recovery ...
Restart Analysis (0 MB): 100%
18/01/2007 14:42:15   Recovery Manager: Restart Recovery complete. (0/0
databases needed full/partial recovery)
Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
18/01/2007 14:42:17   Recovery Manager: Media Recovery complete for
C:\Lotus\Domino\data\admin4.nsf, last update applied .

 Backup file C:\Lotus\Domino\data\admin4.nsf recovered.


C:\Lotus\Domino>
```

e. All content of the database is now rolled forward to the last committed transaction found in the last archived transaction log.

f. Restart Lotus Domino Server

11.5 How to backup Lotus Domino / Notes database(s) / file(s) on Linux

Please make sure that the user running StorState Pro Backup Manager has sufficient privileges to read and write to the "notesenv" file located in the "bin" subdirectory of where StorState Pro Backup Manager is installed. This file is used by StorState Pro to store the location of the Domino/Notes application executables. Use chmod to set read, write & execute permissions:

```
# cd /usr/local/obm/bin
# chmod 777 notesenv
```

Please follow the instructions below to backup your Lotus Domino Server / Notes client databases / files.

i. Open StorState Pro Backup Manager by typing the following in a terminal

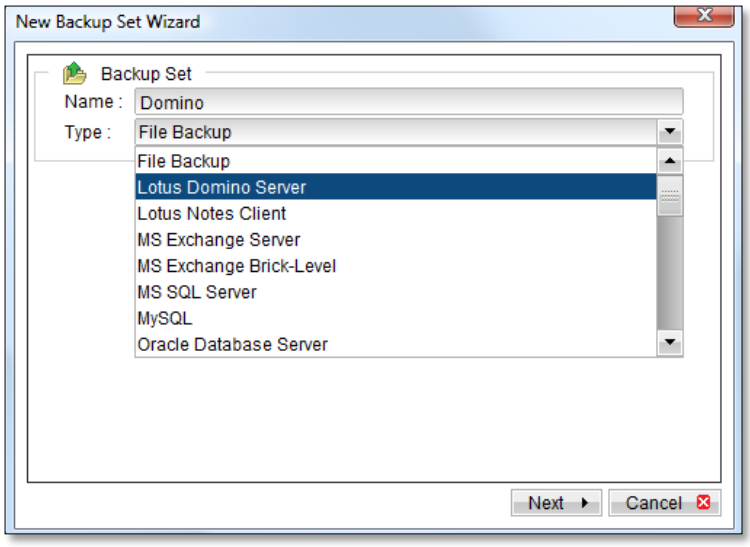
```
# cd /usr/local/obm
# ./bin/RunOBC.sh
```

ii. Create a backup set

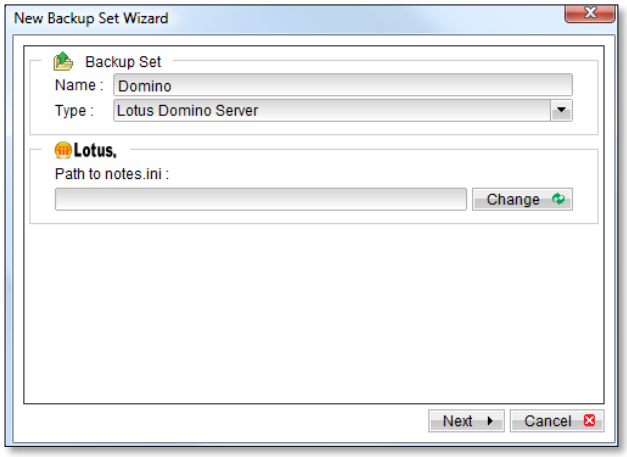
a. To setup backup sets, click the  button to open the [Backup Setting] page.

b. On the left panel, press the button to create a new backup set.

c. On the dialog, choose [Lotus Domino Server] or [Lotus Notes Client] as the [Type].

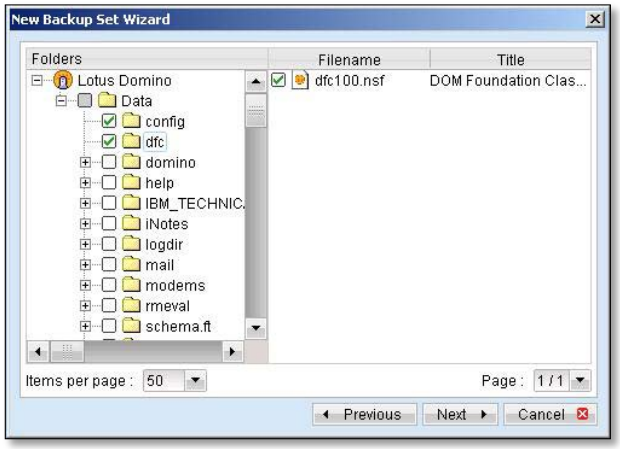


d. Enter a name for your backup set.

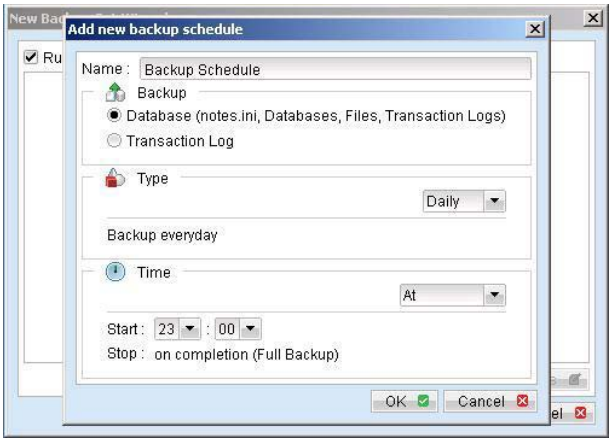


e. Select the location of the “note.ini” file. The default location is in the /local/notesdata folder.

f. Select the database(s) / file(s) you want to backup



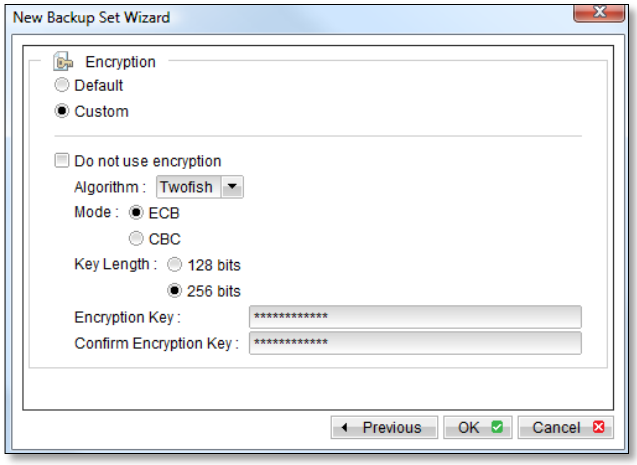
g. Setup backup schedules for [Database] and [Transaction Log] backups (Log backup for Domino Server only)



(Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day transaction log backups by adding multiple daily transaction log backup schedules to your backup set)

h. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave the default setting.

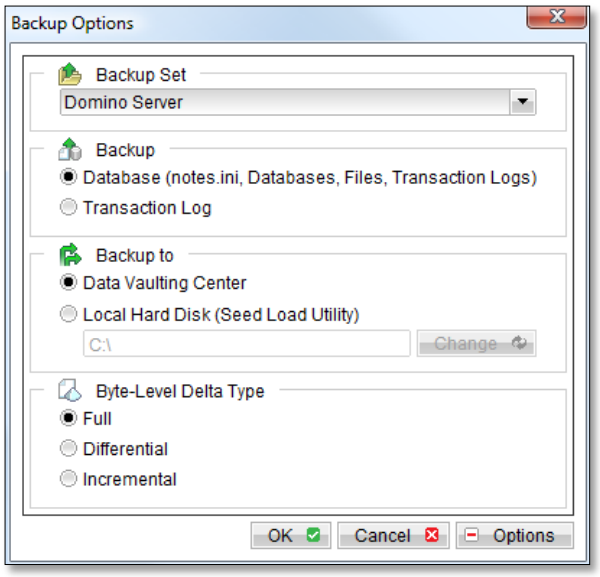
IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!



iii. Run Backup

a. Press the [Backup] button on the main screen of StorState Pro Backup Manager.

b. Select your Domino Server or Notes backup set from the [Backup Set] list. Select the [Backup] type (Database or Transaction Log) you would like to perform (Log backup for Domino Server only). If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

11.6 How to restore Lotus Domino / Notes database(s) / file(s) on Linux

Please follow the instructions below to restore Lotus Domino Server / Notes client database(s) / file(s).

i. Shutdown the Lotus Domino Server

ii. If you want to perform a full Domino restore (restore all databases and files):

a. Download the backup files from the Data Vaulting Center or decrypt backup files from a local copy, and them back to their original location. This includes notes.ini, all backup files from the Lotus Domino data directory and all archived transaction logs. If you encounter any access problems, please try restoring using the "root" user.

b. Make sure that the owner and group permissions of the restored files are the notes user.

For example: # chown –R notes:notes /local/notesdata

This will assign the "notes" owner and group to all files and directories within /local/notesdata.

c. Modify the "DominoRecover.sh" file located under the bin directory of the StorState Pro Backup Manager installation to reflect your setup. You need to specify the data directory and the Lotus executable directory.

For example change the DATA_DIR and LOTUS tags to:
DATA_DIR=/local/notesdata
LOTUS=/opt/ibm/lotus

d. Make sure the current user is the notes user before running the "DominoRecover.sh".

e. Run "DominoRecover.sh" and press 'Y' to continue.

For example: #./usr/local/obm/bin/DominoRecover.sh

This will run media recovery for all databases (*.nsf and mail.box) found under the Lotus data directory (ex. /local/notesdata). You should see something similar to the screen below.

Media Recovery Example:

```
bash-3.00$ cd /usr/local/obm/bin
bash-3.00$ ./DominoRecover.sh
Media Recovery Utility for Lotus Domino 5.0 or above

Please make sure that you have done the following:
1. Reinstall Lotus Domino on this computer in the same directory
2. Restore Notes.ini to the Lotus Domino installation directory
   (e.g. /local/notesdata)
3. Restore Domino Data directory back to the directory defined
   in Notes.ini (e.g. /local/notesdata)
4. Restore all archived transaction logs to the directory defined
   in Notes.ini (e.g. /local/notesdata/logdir)

Continue ? (Y) or (N) y

Running media recovery ...
directory /local/notesdata// already exists
Please wait, creating new transaction logs in directory: /local/notesdata/logdir/
02/01/2009 11:38:43 AM  Recovery Manager: Restart Recovery complete. (0/0 databases
needed full/partial recovery)
02/01/2009 11:38:45 AM  Recovery Manager: Assigning new DBIID for
/local/notesdata/names.nsf (need new backup for media recovery).
Media Recovery Replay (0 MB): 100%
02/01/2009 11:38:45 AM  Recovery Manager: Media Recovery complete for
/local/notesdata/dfc/dfc100.nsf, last update applied .

 Backup file /local/notesdata/dfc/dfc100.nsf recovered.
Media Recovery Replay (0 MB): 100%
02/01/2009 11:38:46 AM  Recovery Manager: Media Recovery complete for
/local/notesdata/help/decsdoc.nsf, last update applied .

…

 Backup file /local/notesdata/iNotes/help70_iwa_en.nsf recovered.
Media Recovery Replay (0 MB): 100%
02/01/2009 11:38:50 AM  Recovery Manager: Media Recovery complete for
/local/notesdata/mail/notes.nsf, last update applied .

 Backup file /local/notesdata/mail/notes.nsf recovered.
bash-3.00$
```

f. All content of all database(s) is now rolled forward to the last committed transaction found in the last archived transaction log.

g. Restart Lotus Domino Server.

iii. If you just want to restore a single database:

a. Download the database file from the Data Vaulting Center or decrypt the file from a local copy, and save the file back to its original location.

b. (optional) If you need to perform media recovery on this database, please download all archived transaction logs and save them back to their original location.

c. Modify the “DominoRecover.sh” file located under the bin directory of the StorState Pro Backup Manager installation to reflect your setup.

For example we will recover the “admin4.nsf” and have restored the file to /restore/local/notesdata, change the tags to:

DATA_DIR=/local/notesdata
LOTUS=/opt/ibm/lotus
INPUTFILE=/restore/local/notesdata/admin4.nsf
RESTOREDB=/local/notesdata/admin4.nsf
RECDATE=18/01/2009
RECTIME=22:41

d. Make sure the current user is the notes user before running “DominoRecover.sh”.

e. Run “DominoRecover.sh”.

For example: #./usr/local/obm/bin/DominoRecover.sh

You should see something similar to the screen below.

Media Recovery Example:

```
bash-3.00$ cd /usr/local/obm/bin
bash-3.00$ ./DominoRecover.sh
Media Recovery Utility for Lotus Domino 5.0 or above

directory /local/notesdata// already exists

 Recovering backup file ...

Restart Analysis (0 MB): 100%
18/01/2009 03:35:56 PM  Recovery Manager: Restart Recovery complete. (0/0 databases
needed full/partial recovery)
Media Recovery Replay (1 MB): 30% 50% 80% 100%
18/01/2009 03:35:57 PM  Recovery Manager: Media Recovery complete for /local/res
tore/local/notesdata/admin4.nsf, last update applied .

 Backup file /local/restore/local/notesdata/admin4.nsf recovered.

 Taking database /local/notesdata/admin4.nsf offline ...


 Restoring database /local/notesdata/admin4.nsf
  from recovered backup file /local/restore/local/notesdata/admin4.nsf ...
Database file /local/notesdata/admin4.nsf restored from /local/restore/local/not
esdata/admin4.nsf

 Bringing database /local/notesdata/admin4.nsf online ...


Program completed successfully.
bash-3.00$
```

f. All content of the database is now rolled forward to the last committed transaction found in the last archived transaction log.

g. Restart Lotus Domino Server.

12 Backup/Restore Microsoft Exchange Server

This chapter will describe in detail how to use StorState Pro Backup Manager to backup your Microsoft Exchange Server 2000 / 2003 / 2007 and how you can restore your Microsoft Exchange Server from the backup files.

12.1 Requirements

i. Microsoft Exchange Server 2000 with Services Pack 3 and post-SP3 update rollup installed. Please refer to http://www.microsoft.com/exchange/ for more information.
Or
Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007.

ii. StorState Pro Backup Manager must be installed on the computer running Microsoft Exchange Server.

iii. Data from Microsoft Exchange Server will be backed up to a temporary directory before being sent to the Data Vaulting Center. Please make sure you have sufficient space on your computer to store this data when you run the backup job.

12.2 Overview

Microsoft Exchange Server 2000/2003/2007 stores its data in the Windows Active Directory as well as in its databases. To fully backup a Microsoft Exchange Server 2000/2003/2007, you need to backup the following components:

i. **Windows System State**

The Windows System State contains information about your Windows system, including Windows Active Directory. A Microsoft Exchange Server 2000 / 2003 / 2007 stores some of its configuration, ex. email accounts and mailbox properties, inside Windows Active Directory. It is important that Windows Active Directory is backed up properly when backing up a Microsoft Exchange Server.

Active Directory is stored on the server running as the Windows domain controller. If your Exchange Server is a domain controller, you can simply backup the Windows System State of your Exchange Server. If your Exchange Server is running as a member server, you will need to install another copy of StorState Pro Backup Manager on the domain controller to backup the Windows System State.

ii. **Microsoft Information Store**
Exchange Server stores all emails and documents inside its databases, which are grouped together as storage groups inside Microsoft Information Store. It is important that Microsoft Information Store is fully backed up when backing up your Exchange Server.

iii. **Microsoft Site Replication Service**
Microsoft Site Replication Service is installed automatically when Exchange Server site replication feature is enabled. Microsoft Site Replication stores its runtime and configuration information inside its own database. If you are running your Exchange Server with Site Replication Service enabled, please make sure that you backup the site replication database as well.

iv. **Microsoft Key Management Service (Exchange 2000 only)**
Similarly, if you have setup your Exchange Server with Key Management Services enabled, please make sure that you backup the key management database as well.

StorState Pro Backup Manager will backup your Microsoft Exchange Server by taking the following steps:

i. Run all Pre-Commands for this backup set

ii. If the backup type is set to [Database] backup,

a. Windows System State will be backed up to a temporary directory specified in the backup set

b. All Exchange databases selected are backed up to a temporary directory specified in the backup

set

iii. If the backup type is set to [Transaction Log] backup,

a. New transaction log extents generated since the last backup will be copied to the temporary directory

iv. Remove transaction log extents backed up from the Exchange Server

v. Run all Post-Commands for the backup set

vi. Upload all backup files from the temporary directory to the Data Vaulting Center

vii. Remove temporary files from the temporary directory

12.3 How to backup Microsoft Exchange Server

Please follow the instructions below to backup your Microsoft Exchange Server:

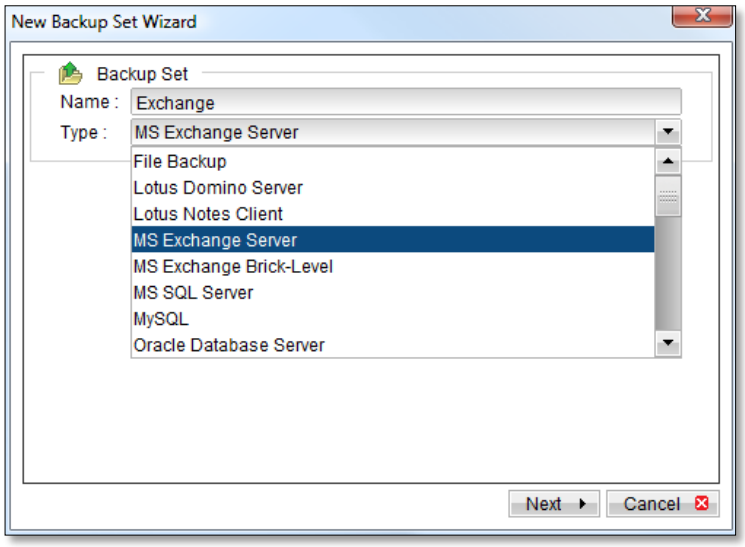
i. Open StorState Pro Backup Manager

ii. Create a new backup set:

a. To setup backup sets, click the button to open the [Backup Setting] page.

b. On the left panel, press the button to create a new backup set.

c. On the dialog, choose [MS Exchange Server] as the [Type].



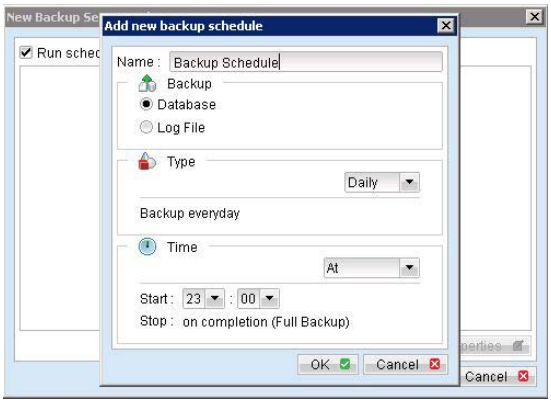
d. Enter a name for your backup set.

e. Select the database(s) to be backed up.

If this Exchange Server is also the domain controller, select the [System State] checkbox as well. Otherwise, please install StorState Pro Backup Manager on the domain controller and select the [System State] checkbox on that computer.

f. Enter a temporary directory for storing the backup files before being sent to the Data Vaulting Center.

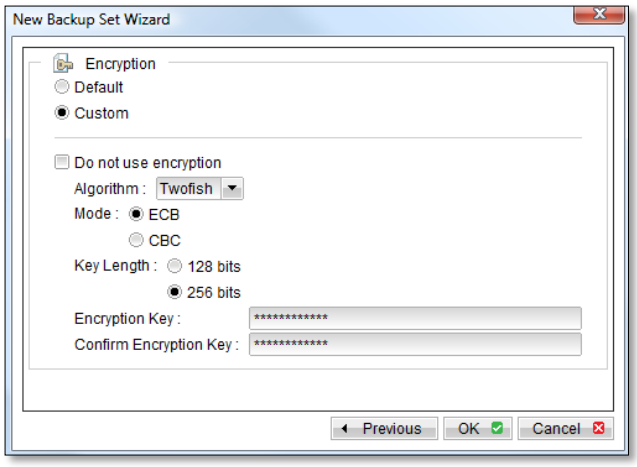
g. Setup backup schedules for [Database] and [Transaction Log] backups



(Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day transaction log backups by adding multiple daily transaction log backup schedules to your backup set)

h. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave the default setting.

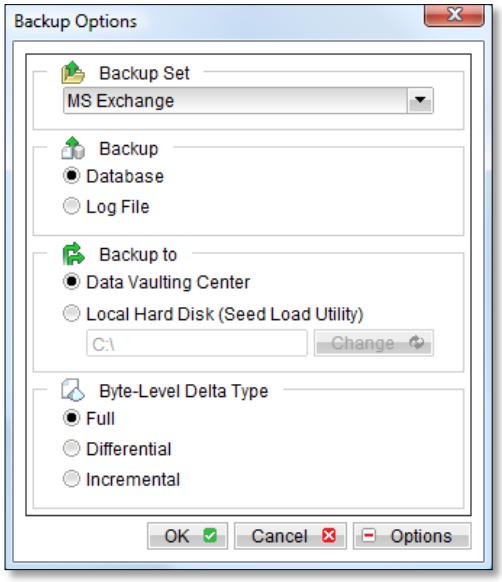
IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!



iii. Run Backup

a. Press the [Backup] button on the main screen of StorState Pro Backup Manager.

b. Select your Exchange Server backup set from the [Backup Set] list. Select the [Backup] type (Database or Log File) you would like to perform. If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

12.4 How to restore Microsoft Exchange Server

Please follow the instructions below to restore Microsoft Exchange Server.

i. Prepare the system for your Exchange Server (if required)

Install the original version of Windows and Exchange Server (with the same level of service packs/patches installed as in the original system) back to your computer

ii. Restore Windows Active Directory (if required)

If you have re-installed Windows, please download the Windows System State backup file, named [SystemState.bkf], from the Data Vaulting Center or decrypt the file from a local copy. Use [NTBackup.exe] to restore your Windows System State from the backup file by following the instructions below:

a. Run [NTBackup.exe] from [Start] -> [Run]

b. Press the [Restore Wizard] button and then press the [Next] button

c. Press the [Import] button and use the [Browse] button to select the backup file [SystemState.bkf]

d. Select the checkbox next to the description that matches your backup file

e. Press the [Next] button and then the [Finish] button

iii. Install StorState Pro Backup Manager (if required)

iv. Startup the [Microsoft Information Store] service from Windows Services

v. Restore Exchange database(s) from backup:

a. Download the database backup files to be restored from the Data Vaulting Center to a temporary folder, or decrypt backup files from a local copy (or copy from the temporary directory defined in your backup set). Please make sure the restored backup directory structure is similar to below:

->[C:]
-->[backup]
---->[ABC]
------>[Microsoft Information Store]
-------->[First Storage Group]
---------->[Mailbox Store(ABC)]
---------->Priv1.edb
---------->Priv1.stm
---------->[Public Folder Store(ABC)]
---------->Pub1.edb
---------->Pub1.stm
---------->E0000001.log

b. If the database to be restored exists on the server already, please dismount it from the Exchange System Manager using [Start] -> [Program] -> [Microsoft Exchange] -> [System Manager]

c. Use [ExchangeRestore.exe] (use [ExRestore2k7.exe] for MS Exchange 2007) from the [bin] directory under the installation directory of StorState Pro Backup Manager (ex. C:\Program Files\StorState Pro\bin\ExchangeRestore.exe) to restore the Exchange database(s).

Run [ExchangeRestore.exe] to print the usage

ExchangeRestore.exe Usage:

```
C:\Program Files\StorState Pro\bin> ExchangeRestore.exe

Microsoft Exchange Server 2000/2003 Backup Recovery Utility

Usage:
ExchangeRestore DIR=path SERVER=server TEMP=tempDir [SERVICE=service [STORAGE=st
orage [DATABASE=database]]]

  DIR       Directory containing all backup files
  SERVER    Name of Exchange Server to be restored
  TEMP      Temporary directory to be used during restore
            Please specific a path with plenty of free space
  SERVICE   Name of Exchange Service to be restored. It must be either
            "Microsoft Information Store", "Microsoft Key Management Service"
            or "Microsoft Site Replication Service"
```

```
  STORAGE   Name of storage group to be restored
  DATABASE  Name of database to be restored

Examples:
1. To restore an exchange server:
   ExchangeRestore DIR="C:\Backup" SERVER="ExchangeServer" TEMP="C:\Temp"

2. To restore the information store:
   ExchangeRestore DIR="C:\Backup" SERVER="ExchangeServer" TEMP="C:\Temp"
      SERVICE="Microsoft Information Store"

3. To restore an exchange storage group:
   ExchangeRestore DIR="C:\Backup" SERVER="ExchangeServer" TEMP="C:\Temp"
      SERVICE="Microsoft Information Store" STORAGE="StorageGroup1"

4. To restore an exchange database:
   ExchangeRestore DIR="C:\Backup" SERVER="ExchangeServer" TEMP="C:\Temp"
      SERVICE="Microsoft Information Store" STORAGE="StorageGroup1"
      DATABASE="Database1"
where
  "C:\Backup"       is the directory containing all backup files
  "ExchangeServer"   is the server name of an exchange server
  "C:\Temp"         is the temporary directory to be used
  "StorageGroup1"   is the name of a storage group
  "Database1"       is the name of a database
```

d. (Example 1) To restore all databases from backup available in [F:\Backup] to an Exchange Server named [WIN2000SVR] using the temporary directory [F:\Temp], you can use this command:

C:\Program Files\StorState Pro\bin> ExchangeRestore DIR="F:\Backup" TEMP="F:\Temp" SERVER="WIN2000SVR"

Exchange Server Recovery Example:

```
C:\Program Files\StorState Pro\bin> ExchangeRestore DIR="F:\Backup" TEMP="F:\Temp"
SERVER="WIN2000SVR"

Microsoft Exchange Server 2000/2003 Backup Recovery Utility

 [Start] Exchange Server - 'WIN2000SVR'
  [Start] Service - 'Microsoft Information Store'
   [Start] Storage Group - 'First Storage Group'
    [Start] Database - 'Mailbox Store (WIN2000SVR)'
     Restoring file 'E:\Program Files\Exchsrvr\mdbdata\priv1.edb' ...
     Restoring file 'E:\Program Files\Exchsrvr\mdbdata\priv1.stm' ...
    [End] Database - 'Mailbox Store (WIN2000SVR)'
    [Start] Database - 'Public Folder Store (WIN2000SVR)'
     Restoring file 'E:\Program Files\Exchsrvr\mdbdata\pub1.edb' ...
     Restoring file 'E:\Program Files\Exchsrvr\mdbdata\pub1.stm' ...
    [End] Database - 'Public Folder Store (WIN2000SVR)'
    [Start] Restoring transaction log - 'First Storage Group'
     Restoring Log File 'F:\Temp\restore.tmp\First Storage Group\E00000B3.log' ...
     Restoring Log File 'F:\Temp\restore.tmp\First Storage Group\E00000B4.log' ...
    [End] Restoring transaction log - 'First Storage Group'
    [Start] Applying transaction log ...
    [End] Applying transaction log
   [End] Storage Group - 'First Storage Group'
.....
   [Start] Storage Group - 'SG2'
    [Start] Database - 'acct'
     Restoring file 'E:\Program Files\Exchsrvr\SG2\acct.edb' ...
     Restoring file 'E:\Program Files\Exchsrvr\SG2\acct.stm' ...
    [End] Database - 'acct'
    [Start] Restoring transaction log - 'SG2'
     Restoring Log File 'F:\Temp\restore.tmp\SG2\E0100072.log' ...
     Restoring Log File 'F:\Temp\restore.tmp\SG2\E0100073.log' ...
    [End] Restoring transaction log - 'SG2'
    [Start] Applying transaction log ...
    [End] Applying transaction log
   [End] Storage Group - 'SG2'
[End] Exchange Server - 'WIN2000SVR'

C:\Program Files\StorState Pro\bin>
```

e. (Example 2) To restore the database named [mail] in storage group [SG5] from backup available in [F:\Backup] to an Exchange Server named [WIN2000SVR] using the temporary directory [F:\Temp], you can use this command:

C:\Program Files\StorState Pro\bin> ExchangeRestore DIR="F:\Backup" TEMP="F:\Temp" SERVER="WIN2000SVR" SERVICE="Microsoft Information Store" STORAGE="SG5" DATABASE="mail1"

Exchange Server Recovery Example:

```
C:\Program Files\StorState Pro\bin> ExchangeRestore DIR="F:\Backup" TEMP="F:\Temp"
SERVER="WIN2000SVR" SERVICE="Microsoft Information Store" STORAGE="SG5"
DATABASE="mail"

Microsoft Exchange Server 2000/2003 Backup Recovery Utility

  [Start] Storage Group - 'SG5'
   [Start] Database - 'mail'
    Restoring file 'E:\Program Files\Exchsrvr\SG5\mail.edb' ...
    Restoring file 'E:\Program Files\Exchsrvr\SG5\mail.stm' ...
   [End] Database - 'mail'
   [Start] Restoring transaction log - 'SG5'
    Restoring Log File 'F:\Temp\restore.tmp\SG5\E0300012.log' ...
    Restoring Log File 'F:\Temp\restore.tmp\SG5\E0300013.log' ...
   [End] Restoring transaction log - 'SG5'
   [Start] Applying transaction log ...
   [End] Applying transaction log
  [End] Storage Group - 'SG5'

C:\Program Files\StorState Pro\bin>
```

f. Repeat the same procedure for each database to be restored to the Exchange Server.

g. You can use [Start] -> [Programs] -> [Administrative Tools] -> [Event Viewer] to check if there are any errors generated from the Exchange databases during restore activities.

vi. If ExchangeRestore.exe cannot mount the restored files and returns errors, ex. bad signature, or null errors, the Exchange Server might have incorrectly spooled the backup files. Please try to mount the restored database and log files manually by following these instructions:

a. In MS Exchange System Manager, dismount both the Mailbox Store and Public Folder Store from the server.

b. Copy all restored database files to the MDBDATA folder (By default, the MDBDATA folder is located under C:\Program Files\Exchsrvr\)

Mailbox Store:
- priv1.edb
- priv1.stm

Public Folder Store:
- pub1.edb
- pub1.stm

c. Run "eseutil /r" to apply the transaction log files to bring the database to a consistent state, ex.:

```
C:\Program Files\Exchsrvr\MDBDATA> ..\bin\eseutil /r e00
```

The above command will try to bring all databases handled by the transaction log files starting with “e00” located in “C:\Program Files\Exchsrvr\MDBDATA” into a clean shutdown state.

d. Run "eseutil /p" to repair the database files, ex.:

```
C:\Program Files\Exchsrvr\MDBDATA> ..\bin\eseutil /p priv1.edb
C:\Program Files\Exchsrvr\MDBDATA> ..\bin\eseutil /p pub1.edb
```

e. Mount both the Mailbox Store and Public Folder Store using the MS Exchange System Manager.

vii. Restoration completed

13 Backup/Restore Windows System State

This chapter will describe in detail how to use StorState Pro Backup Manager to backup the Windows System State and how you can restore the System State from backup.

13.1 Requirements

i. Microsoft Windows 2000 / XP Professional / 2003

ii. StorState Pro Backup Manager must be installed on the computer containing the System State you want to backup

iii. Windows System State will be backed up to a temporary file before it is sent to the Data Vaulting Center. Please make sure you have sufficient space on your computer to store the temporary file when you run the backup job.

13.2 Overview

StorState Pro Backup Manager will backup your Windows System State by taking the following steps:

i. Run all Pre-Commands of this backup set

ii. Windows System State will be backed up to the temporary directory specified in the backup set using NTBackup.

iii. Run all Post-Commands of this backup set

iv. Upload the Windows System State backup file from the temporary directory to the Data Vaulting Center.

v. Remove the Windows System State temporary backup file from the temporary directory if [Setting] -> [Temporary Directory for storing backup files] is enabled

13.3 How to backup Windows System State

Please follow the instructions below to backup the Windows System State:

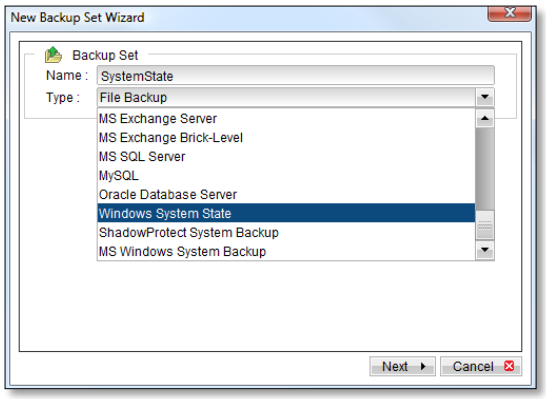
i. Open StorState Pro Backup Manager

ii. Create a new backup set:

a. To setup backup sets, click the  button to open the [Backup Setting] page.

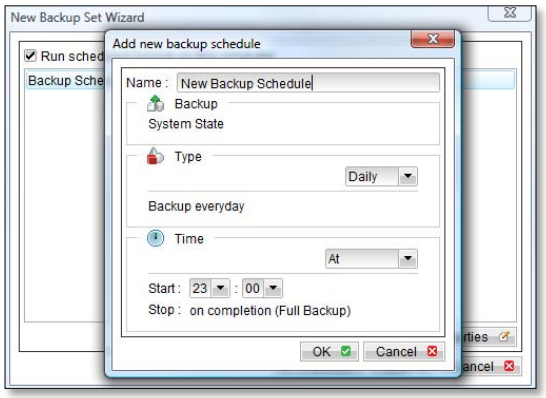
b. On the left panel, press the  button to create a new backup set.

c. On the dialog, choose [Windows System State] as the [Type].



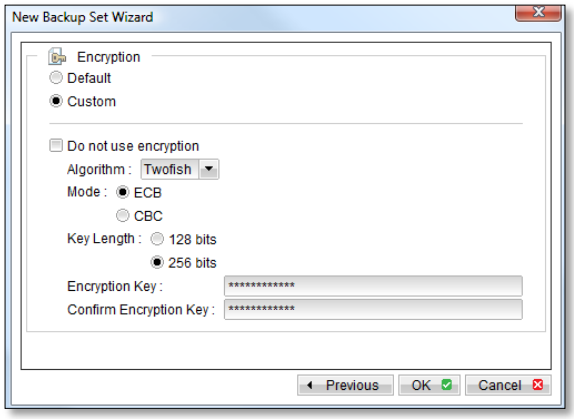
d. Enter a name for your backup set

e. Setup the backup schedule for this backup set. You can have multiple schedules in a backup set.



f. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave the default setting.

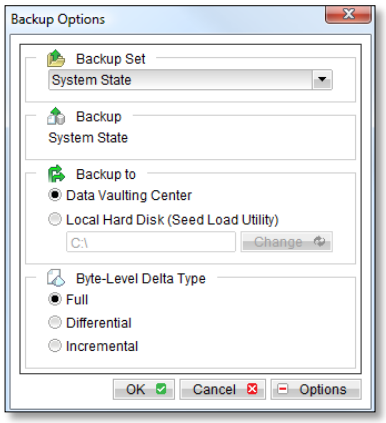
IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!



iii. Run Backup

g. Press the [Backup] button on the main screen of StorState Pro Backup Manager.

h. Select your Windows System State backup set from the [Backup Set] list. If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



i. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

13.4 How to restore Windows System State

Please follow the instructions below to restore the Windows System State.

i. Download the System State backup from the Data Vaulting Center to a temporary folder, or decrypt the backup file from a local copy.

ii. Use [NTBackup.exe] to restore your Windows System State by following the instructions below:

a. Run [NTBackup.exe] from [Start] -> [Run]

b. Press the [Restore Wizard] button and then press the [Next] button

c. Press the [Import] button and use the [Browse] button to select the backup file [SystemState.bkf] restored

d. Select the checkbox next to the description that matches your backup file

e. Press the [Next] button and then the [Finish] button

iii. Restore Completed

14 Backup/Restore Brick-Level Backup for Microsoft Exchange Server

14.1 Requirements

i. Microsoft Exchange Server 2000 with Services Pack 3 and post-SP3 update rollup installed.
Or
Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007.

ii. StorState Pro Backup Manager must be installed on the computer running Microsoft Exchange Server.

14.2 Overview

Brick-Level Backup for Microsoft Exchange Server is not designed to fully protect an Exchange server, but to facilitate easy backup, fast restore, and archive of individual emails, contacts, calendars, tasks etc. A Brick-Level restore cannot fully recover an Information Store after a disaster. A Brick-Level Backup must be utilized in conjunction with a full Information Store Backup (see section above), in order to fully protect the Exchange Server. Brick-Level backup on mailboxes with large folders (10k+ items) can be time consuming. Limiting backup to important mailboxes/folders, and/or adjusting the backup schedule can help minimize the impact of the backup.

14.3 Granting Privileges

Brick-Level Backup requires "Full Mailbox Access" permission for the user running StorState Pro Backup Manager. Normally, StorState Pro can acquire the permission on its own but if you encounter 'Access Denied' errors you need to manually grant access privileges to the user running StorState Pro using one of the following instructions below:

For one specific mailbox

Use the following procedure to grant access to an Exchange mailbox:

1 Start Active Directory Users and Computers.

2 On the View menu, ensure that the Advanced Features check box is selected.

3 Right-click the user whose mailbox you want to give permissions to and choose Properties.

4 On the Exchange Advanced tab, click Mailbox Rights.

5 Notice that the Domain Admins and Enterprise Admins have both been given Deny access to Full Mailbox access.

6 Click Add, click the user or group who you want to give access to this mailbox, and then click OK.

7 Check that the user or group is added in the Name box.

8 In the Permissions list, click Allow next to Full Mailbox Access, and then click OK.

9 Click Ok on all open windows.

10 Restart the Microsoft Exchange Information Store service.

For mailboxes located within a specific mailbox store

Use the following procedure to grant access to an Exchange mailbox found on a specific mailbox store:

1 Start Exchange System Manager.

2 Drill down to your server object within the appropriate Administrative Group. Expand the server object and find the required mailbox store within the appropriate Storage Group. Right-click it and choose Properties.

3 In the Properties window click to the Security tab.

4 Click Add, click the user or group who you want to give access to the mailboxes, and then click OK.

5 Check that the user or group is added in the Name box.

6 In the Permissions list, click Allow next to Full Control, and then click OK.

7 Click 'Apply' and 'OK'

8 Restart the Microsoft Exchange Information Store service.

For mailboxes located within a specific server

1 Start Exchange System Manager.

2 Drill down to your server object within the appropriate Administrative Group. Right-click it and choose Properties.

3 In the Properties window go to the Security tab.

4 Click Add, click the user or group who you want to give access to the mailboxes, and then click OK.

5 Be sure that the user or group is selected in the Name box.

6 In the Permissions list, click Allow next to Full Control, and then click OK.

7 Click Ok on all open windows.

8 Restart the Microsoft Exchange Information Store service.

14.4 How to backup Individual Brick-Level Backup

Please follow the instructions below to backup all individual items within your Microsoft Exchange Server using StorState Pro Backup Manager:

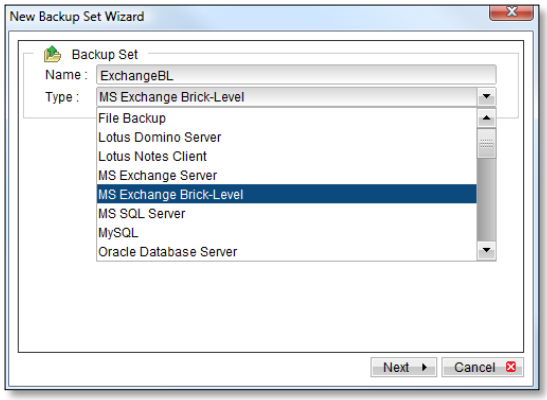
i. Open StorState Pro Backup Manager

ii. Create a new backup set:

a. To setup backup sets, click the button to open the [Backup Setting] page.

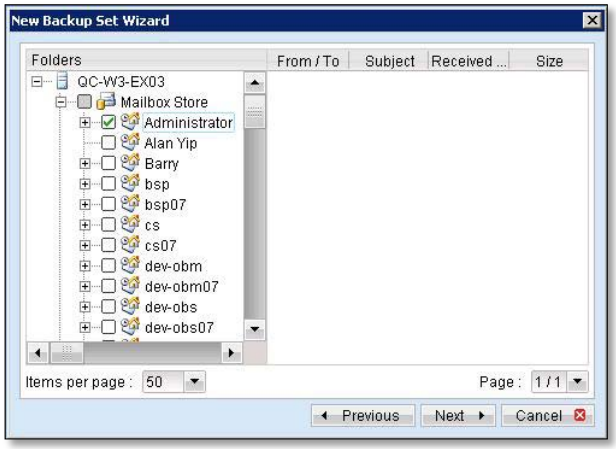
b. On the left panel, press the  button to create a new backup set.

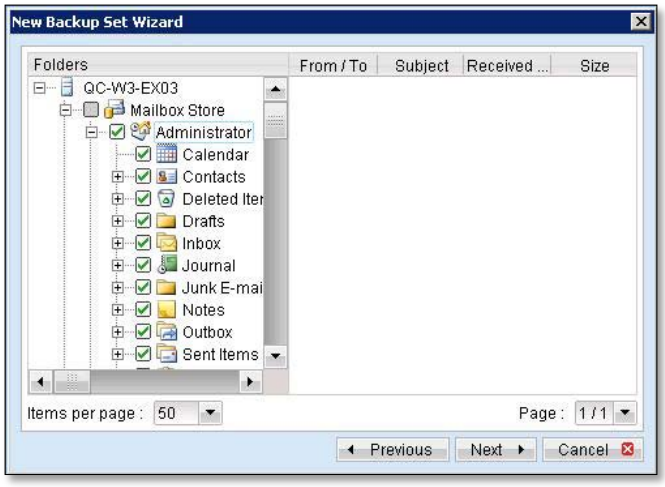
c. On the dialog, choose [MS Exchange Brick-Level] as the [Type].



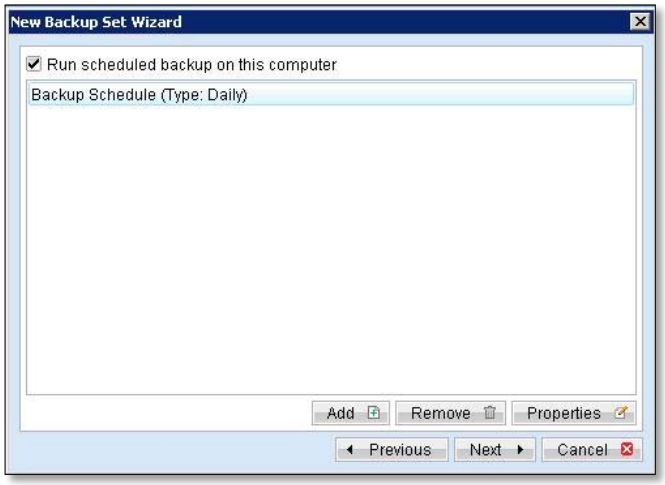
d. Enter a name for your backup set.

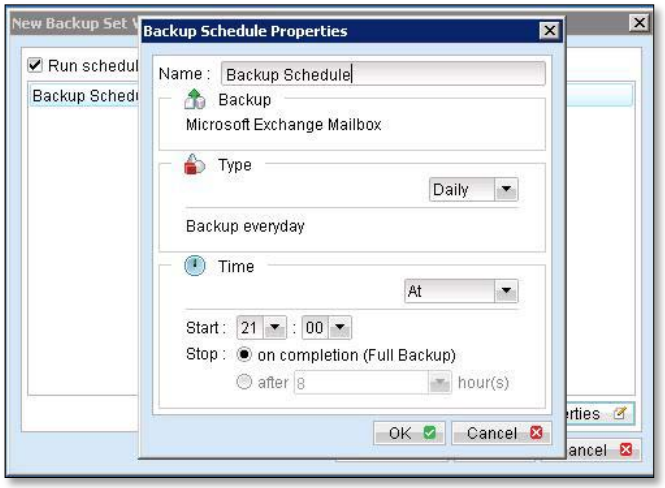
e. Select/deselect the mailboxes/folders to backup. Drill down to select/deselect individual items.





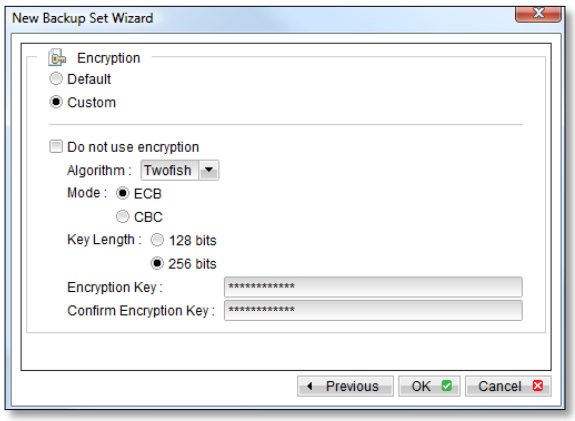
f. Setup the backup schedule.





g. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave the default setting.

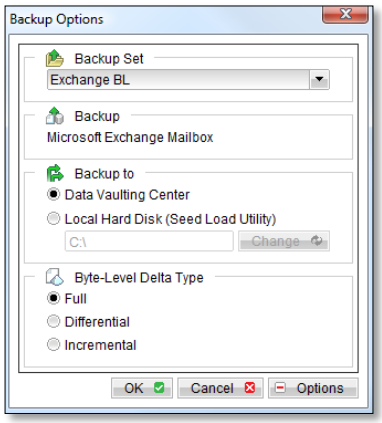
IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!



iii. Run Backup

a. Press the [Backup] button on the main screen of StorState Pro Backup Manager.

b. Select your Exchange Brick-Level backup set from the [Backup Set] list. If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

14.5 How to restore Individual Brick-Level Backup

Please follow the instructions below to restore individual emails, contacts, calendars, tasks etc. from StorState Pro Backup Manager directly into your Exchange Server. The StorState Pro Backup Manager client application must be used for Brick-Level restoration. Web-based restoration is not possible.

i. Open StorState Pro Backup Manager

ii. Select the [Restore] button on the left of the main page of StorState Pro Backup Manager.

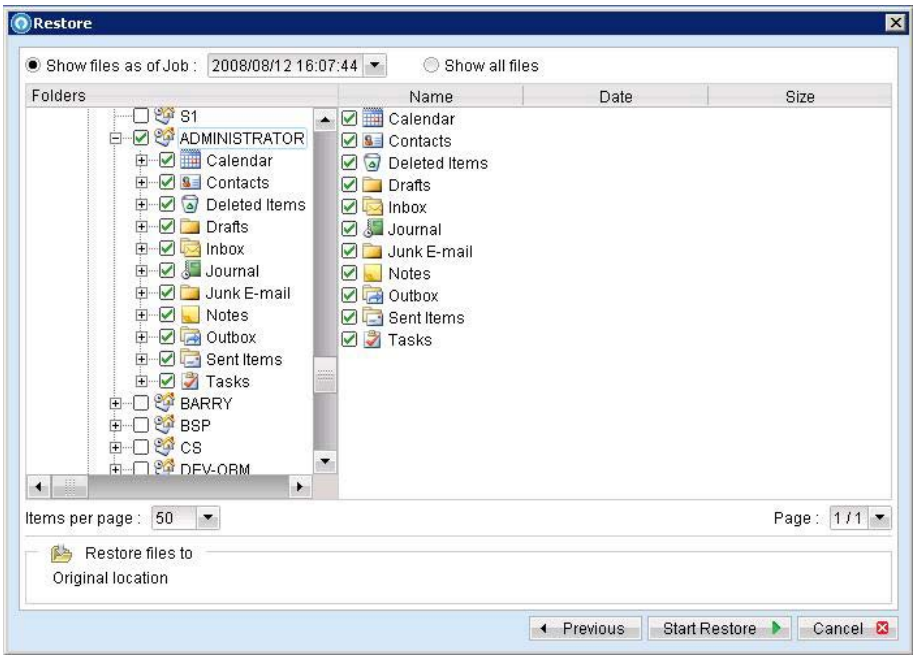
iii. Select your Exchange Brick-Level backup set from the list.

iv. Select the backup job you wish to restore from the [Show files as of Job] drop-down box, or leave on "Latest" to restore from the latest backup. Select [Show all files] to view all snapshots of objects stored in your data vault.

v. Optional - Click the Filter button on the top right corner to filter objects/folders based on your criteria.

vi. Optional - Click the Search button on the bottom left corner to search for objects/folders based on your criteria.

vii. Select the objects you want to restore. Drill down to select/deselect folders/items.



viii. Click [Start Restore] to start the restore operation. A dialog will display the progress and alert you when completed.

15 Backup/Restore Full System with Microsoft Windows System Backup

This chapter will describe in detail how to use StorState Pro Backup Manager to make a full-system backup of a Microsoft Windows Server 2008 or Vista system and how you can restore the complete system from the backup files. This feature is only available on Windows Vista Business/Enterprise/Ultimate Edition and Windows Server 2008.

15.1 Requirements

i. The OS must be Windows Vista Business/Enterprise/Ultimate Edition or Windows Server 2008.

ii. StorState Pro Backup Manager must be installed on the computer.

iii. You must install the Windows Server Backup, Command-line Tools, and Windows PowerShell items that are available in the Add Features Wizard in Server Manager (if not installed). This installs the following tools:

- Windows Server Backup Microsoft Management Console (MMC) snap-in
- Wbadmin command-line tool
- Windows Server Backup cmdlets (Windows PowerShell commands)

iv. System images generated by Windows Server Backup will be backed up to a temporary directory before they are sent to the Data Vaulting Center. Please make sure you have sufficient space on your computer to store this data when you run the backup job.

15.2 Overview

StorState Pro Backup Manager will backup your system by taking the following steps:

i. Before running any backup activities, StorState Pro will run all Pre-Commands in the backup set.

ii. StorState Pro will issue a system backup command to backup the volume(s) selected in the backup source to a set of files, and save it in the [WindowsImageBackup] directory under the temporary directory specified in the backup set settings.

iii. After all files have been spooled to the [WindowsImageBackup] directories, StorState Pro will run all Post-Commands in the backup set.

iv. All files copied to the temporary directory are uploaded to the Data Vaulting Center.

15.3 How to backup a system with Microsoft Windows System Backup

Please follow the instructions below to backup your Microsoft Windows Server 2008 or Windows Vista Business /Enterprise/Ultimate Edition using StorState Pro.

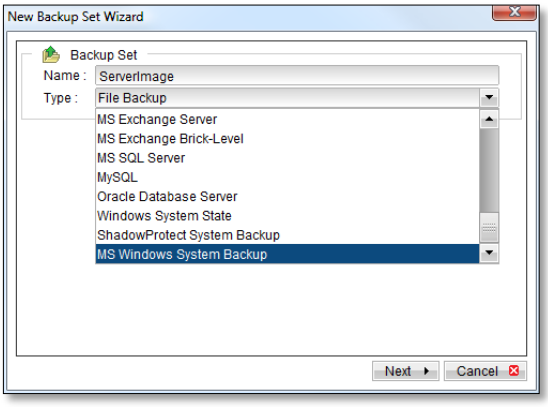
i. Open StorState Pro Backup Manager

ii. Create a new backup set:

a. To setup backup sets, click the  button to open the [Backup Setting] page.

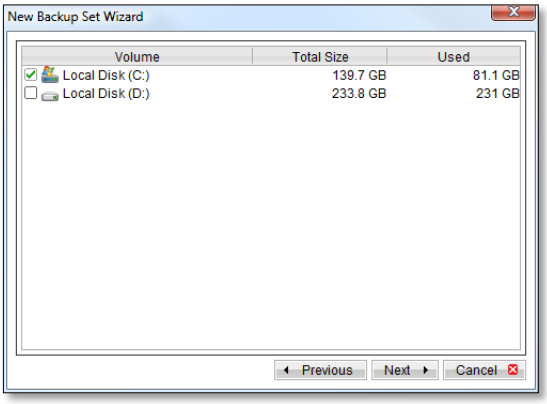
b. On the left panel, press the button to create a new backup set.

c. On the dialog, choose [MS Windows System Backup] as the [Type].



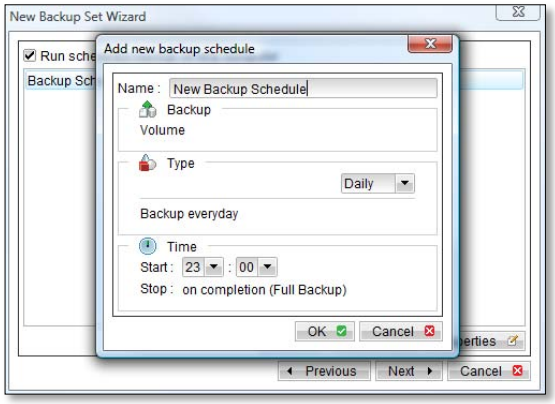
d. Enter a name for your backup set.

e. Select the volume(s) you want to backup.



Note: For Windows Vista, C: will be selected as default and cannot be deselected.

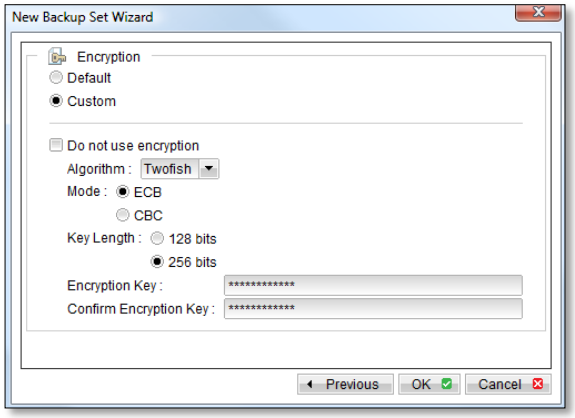
f. Setup the backup schedule.



g. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave the default setting.

IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new

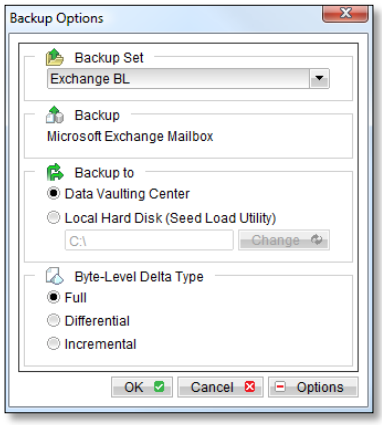
encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!



iii. Run Backup

a. Press the [Backup] button on the main screen of StorState Pro Backup Manager.

b. Select your Microsoft Windows System Backup backup set from the [Backup Set] list. If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

15.4 How to restore a system with Microsoft Windows System Backup

Please follow the instructions below to restore a Microsoft Windows Server 2008 or Windows Vista Business/Enterprise/Ultimate Edition system with StorState Pro Backup Manager.

Begin by downloading the Windows System Backup from the Data Vaulting Center, or decrypt the backup file from a local copy.

Windows Server 2008 – Restore from within OS

Please follow the instructions below to recover volumes from within Windows using the Windows Recovery Wizard:

a. From the [Start] menu, click [Administrative Tools], and then click [Windows Server Backup].

b. In the [Actions] panel of the snap-in default page, under [Windows Server Backup], click [Recover]. This opens the Recovery Wizard.

c. On the [Getting started] page, specify whether you will recover volumes from backups stored on this computer or another computer, and then click [Next].

d. If you are recovering volumes from backups stored on another computer, do the following, and then click [Next]:

- On the [Specify location type] page, specify you want to restore from a local drive.
- On the [Select backup location] page, select the location of the backup from the drop-down list.

e. Click [Next] to continue.

f. For a recovery either from the local computer or another computer, from the [Select backup date] page, select the date from the calendar and the time from the drop-down list of backup you want to restore from.

g. On the [Select recovery type] page, click [Volumes], and then click [Next].

h. On the [Select volumes] page, select the check boxes for the volumes in the [Source Volume] column that you want to recover. Then, from the associated drop-down list in the [Destination Volume] column, select the location that you want to recover the volume to. Click [Next].

Note: You will receive a message that any data on the destination volume will be lost when you perform the recovery. Make sure that the destination volume is empty or does not contain information that you will need later.

i. On the [Confirmation] page, review the details, and then click [Recover] to restore the specified volumes.

j. On the [Recovery progress] page, you can view the status of the recovery.

Note: To recover volumes from a backup using Windows Server Backup, you must be a member of the Backup Operators or Administrators group, or you must have been delegated the appropriate authority. As a security best practice, consider using [Run as] to perform this procedure.

Windows Server 2008 – Restore full server or OS

Please follow the instructions below to recover the operating system or a full server with the Install Windows Wizard:

a. Insert the Windows Setup disc into the CD or DVD drive and turn on the computer. If needed, press the required key to boot from the disc. The Install Windows Wizard should appear.

b. Specify language settings, and then click [Next].

c. Click [Repair your computer].

d. Setup searches the hard disk drives for an existing Windows installation and then displays the results in [System Recovery Options]. If you are recovering the operating system to fresh hardware, the list should be empty (there should be no operating system on the computer). Click [Next].

e. On the [System Recovery Options] page, click [Windows Complete PC Restore]. This opens the Windows Complete PC Restore Wizard.

f. Perform one of the following actions:

- Click [Use the latest available backup (recommended)] and then click [Next].
- Click [Restore a different backup] and then click [Next].

g. If you chose to restore a different backup, please perform one of the following actions on the [Select the location of the backup] page:

- Click the computer that contains the backup that you want to use, and then click [Next]. Then, on the [Select the backup to restore] page, click the backup that you want to use, and then click [Next].
- Click [Advanced] to browse for a backup on the network, and then click [Next].

h. On the [Choose how to restore the backup] page, do the following optional tasks, and then click [Next]:

- Select the [Format and repartition disks] check box to delete existing partitions and reformat the destination disks to be the same as the backup. This enables the [Exclude disks] button. Click this button and then select the check boxes associated with any disks that you want to exclude from being formatted and partitioned. The disk that contains the backup that you are using is automatically excluded.

  Note: Unless a disk is excluded, data on it can be lost – regardless of whether it was part of the backup or whether it has volumes that are being restored. In [Exclude disks], if you do not see all the disks that are attached to the computer, you might need to install the associated drivers for the storage device.

- Select the [Only restore system disks] check box to perform an operating system-only recovery.
- Click [Install drivers] to install device drivers for the hardware that you are recovering to.
- Click [Advanced] to specify whether the computer is restarted and the disks are checked for errors immediate after the recovery.

i. Confirm the details for the restoration, and then click [Finish].

Windows Server 2008 – Command-line restore

For Windows Server 2008, you can also recover volumes with the following sub command:

Wbadmin start recovery -version: <VersionIdentifier> -itemtypeVolume -items:<VolumesToRecover> -backupTarget: <VolumeHostingBackup> -recoveryTarget:<TargetVolumeForRecovery>

- Version Identifier: Specifies the version identifier of the backup to recover in MM/DD/YYYY-HH:MM format. If you do not know the version identifier, type [wbadmin get versions].

- VolumesToRecover: Specifies a comma-delimited list of volumes.
- VolumesHostingBackup: Specifies the storage location that contains the backup that you want to recover
- TargetVolumeForRecovery: Specifies the volume drive letter of the volume to restore to.

  For example,

  Wbadmin start recovery –version:03/31/2009-09:00 –itemType:Volume –items:D: -backupTarget:E: -recoveryTarget:F:

Windows Vista – Restore full OS

For Windows Vista, please perform a Complete PC Restore within the Windows Recovery Environment:

a. Insert the Windows Vista DVD into the DVD drive and turn on the computer. On most systems you will see that a bootable DVD is inserted.

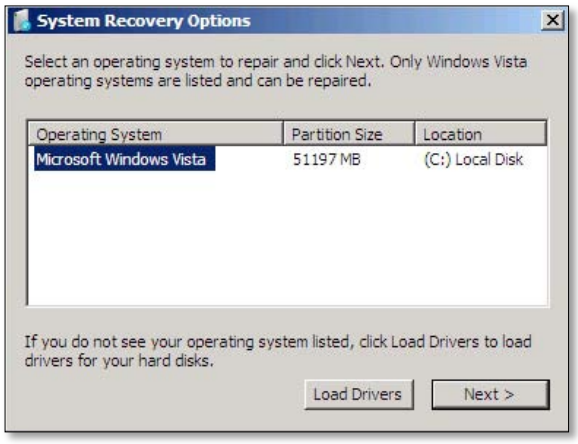
b. Press any key to boot the computer from the Windows Vista DVD. Please wait until Windows completes loading.

Note: It is possible that the DVD came with your computer does not allow you to boot from it. If this is the case, then your computer manufacturer most likely installed the Windows Recovery Environment directly to a small partition on your hard drive. To access this partition, you would slowly tap the [F8] key on your keyboard after the BIOS information clears from your screen, until you see the Windows startup menu. From this menu use your arrow keys to select the option for the Windows Recovery Environment, and press the enter key on your keyboard.

c. Configure the [Language to install], [Time and currency format], and [Keyboard or input method] options. Then, press the [Next] button.

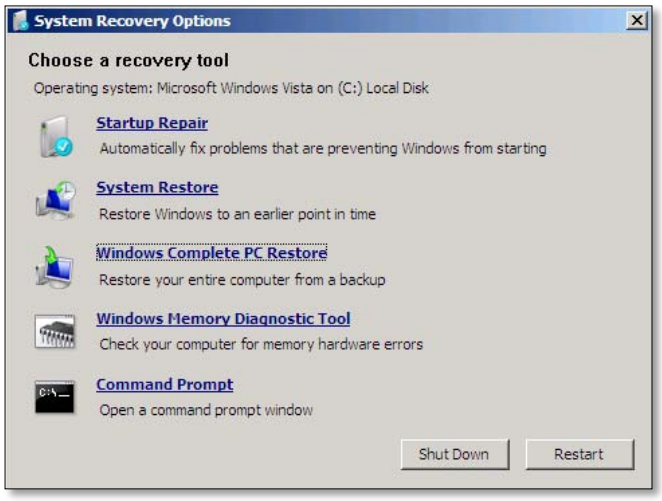
d. Click [Repair your computer].

e. The [System Recovery Options] dialog box will be shown. Select the Vista installation you would like to repair.



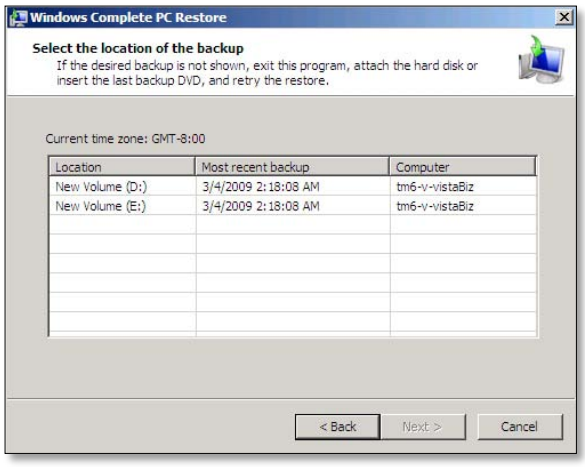
Note: If there are drivers you need to load in order for Vista to access any of your drives or other components, click on the [Load Drivers] button to load them. When ready, press the [Next] button to continue. If the repair process does not detect any problems starting Vista, it will display a list of available recovery tools. If it does detect a problem it will attempt to perform a Startup Repair to automatically fix these problems. Click on the [Cancel] button and select the [View advanced options for system recovery and support] option to see the list of recovery tools.

f. Click on the [Windows Complete PC Restore] option.

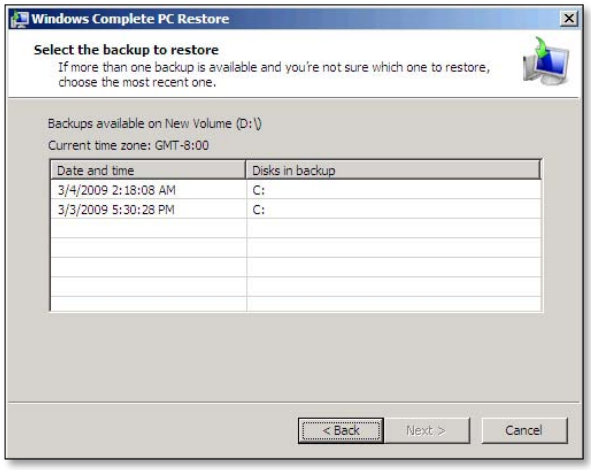


g. Complete PC Restore will search your hard drives and DVD media for any backup images. Backups found on your drives or the inserted media will be shown with the latest backup selected.

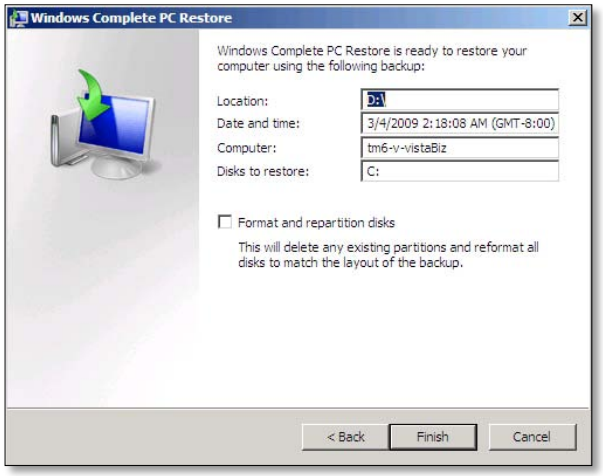
h. If the selected backup is the one you wish to restore, press the [Next] button to continue. If there is a different backup that you would like to use, select the [Restore a different backup] option and press the [Next] button. This will display a screen listing the backups you have created in the past.



i. Select the backup that you would like to restore. Then click on the [Next] button. Complete PC Restore will now examine your selected backup and see if there is more than one backup job. If you have backed up multiple times it will display an entry for each job.



j. Choose the snapshot you would like to restore (usually the most recent) and press [Next].



k. Review the backup job to be restored.

Note: if you select the [Format and repartition disks] options, Complete PC Restore will repartition and format the hard drive you are restoring to exactly as it was when you made the backup. If you do not choose this method, it will just erase the hard disk and restore the data to it. If you are using the same hard drive that you originally used to backup your computer then you may want to select the option to format and repartition disks. Alternatively, if this is a new hard drive that you have partitioned in a different manner, then you should not select this option in order to keep your current disk configuration. It is important to note that with either option, all the data on the disk you are restoring to will be erased. When you are ready to continue, click the [Finish] button.

l. A new window is opened stating that all of your data will be erased. If you want to continue with the restore then you need to check [I confirm that I want to erase all existing data and restore the backup] and then press the [OK] button. Complete PC Restore will now restore the backup.

m. When the restore is completed, you will see a message stating that it is complete and your computer will be rebooted.

n. All volume(s) are restored.

16 Backup/Restore Windows System with StorageCraft ShadowProtect

This chapter will describe in detail how to use StorState Pro Backup Manager and StorageCraft ShadowProtect to make a bare-metal backup of a Microsoft Windows XP / Vista / 2003 / 2008 system and how you can restore the system from the backup files.

16.1 Requirements

i. StorState Pro Backup Manager and StorageCraft ShadowProtect must be installed on the computer. ShadowProtect is purchased separately and is available from storagecraft.com.

ii. System images generated by ShadowProtect will be backed up to a temporary directory before they are sent to the Data Vaulting Center. Please make sure you have sufficient space on your computer to store this data when you run the backup job.

16.2 Overview

StorState Pro Backup Manager will backup your system by taking the following steps:

i. Before running any backup activities, all Pre-Commands of the backup set are run.

ii. For each volume that is to be backed up, StorState Pro will issue a system backup command to backup each volume to a ShadowProtect backup image file (*.spf and *.spi file) and save them in the temporary directory you specified.

iii. After all image files have been spooled to the temporary directory, all Post-Commands of the backup set are run.

iv. All files copied to the temporary directory are uploaded to the Data Vaulting Center.

16.3 How to backup a system with ShadowProtect

Please follow the instructions below to backup a system with ShadowProtect using StorState Pro Backup Manager.

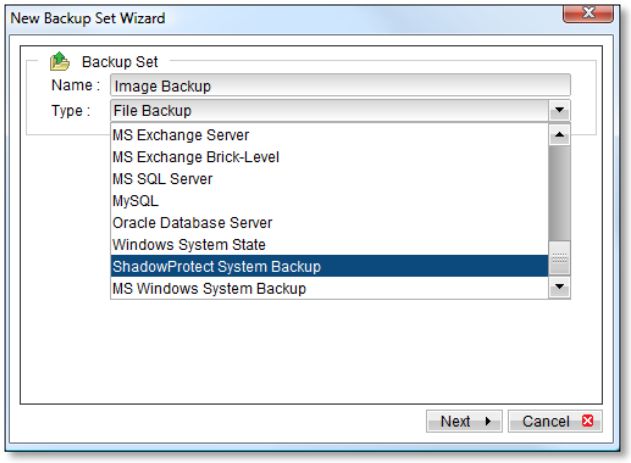
i. Open StorState Pro Backup Manager

ii. Create a new backup set:

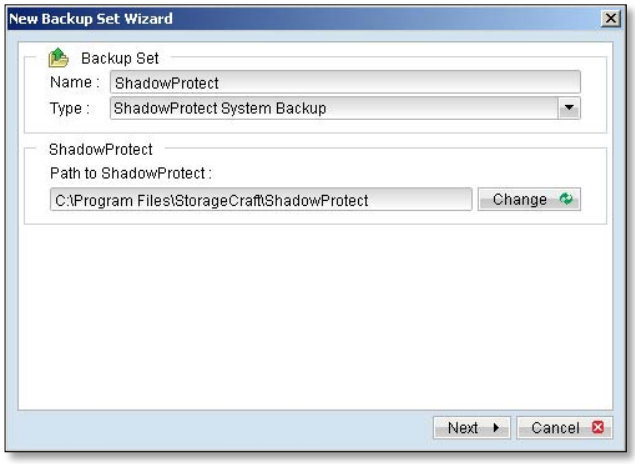
a. To setup backup sets, click the  button to open the [Backup Setting] page.

b. On the left panel, press the  button to create a new backup set.

c. On the dialog, choose [ShadowProtect System Backup] as the [Type].

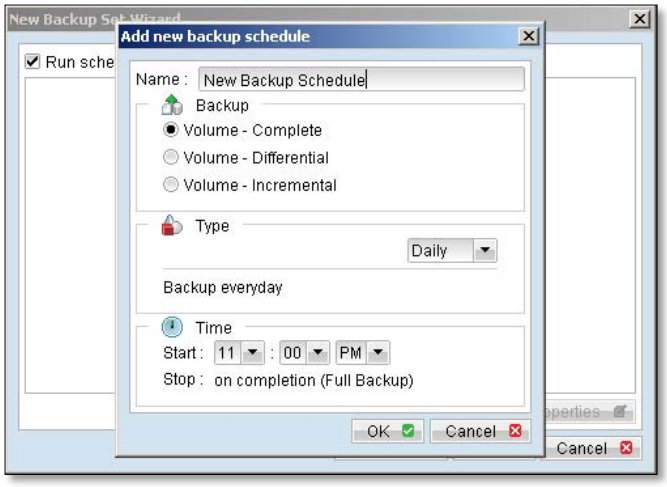


d. Enter a name for your backup set, then select the installation path of ShadowProtect by clicking the [Change] button.



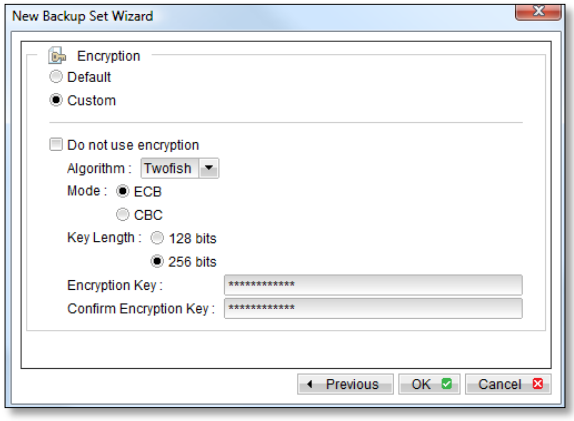
e. Select the volume(s) you want to backup.

f. Setup the backup schedule.



g. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave the default setting.

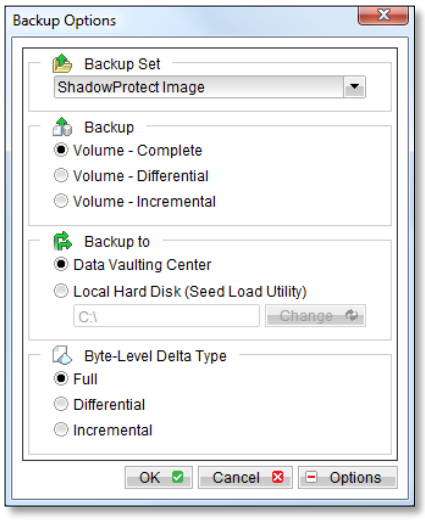
IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!



iii. Run Backup

a. Press the [Backup] button on the main screen of StorState Pro Backup Manager.

b. Select your ShadowProtect System Backup backup set from the [Backup Set] list. Select the [Backup] type (Complete, Differential, Incremental) you would like to perform. If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

16.4 How to restore a system with ShadowProtect

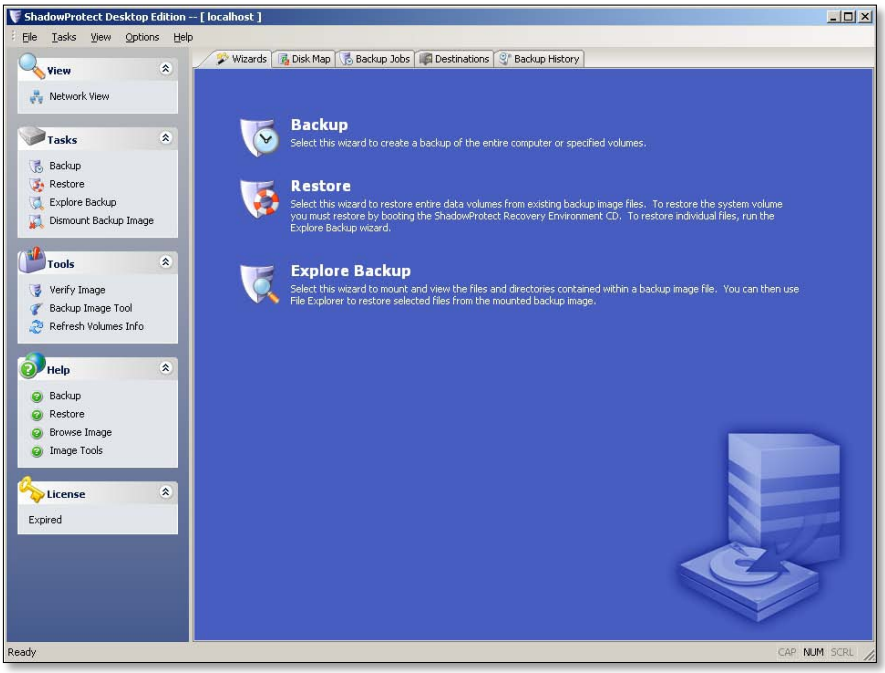
Please follow the instructions below to restore a ShadowProtect backup.

i. Download the backup files (.spf, .spi) from the Data Vaulting Center, or decrypt backup files from a local copy.

ii. There are two methods you can use to restore volumes. The first method is to boot to the StorageCraft Recovery Environment and perform the restore. This option must be used when restoring a system volume where the operating system resides. The second method, for restoring a volume other than the system volume, runs inside of Windows using the Restore Volume Wizard. This method does not require the machine to be rebooted.

To restore a volume, please do the following:

a. Start ShadowProtect from within Windows (non-system volume restore) or boot to the StorageCraft Recovery Environment (system volume restore).

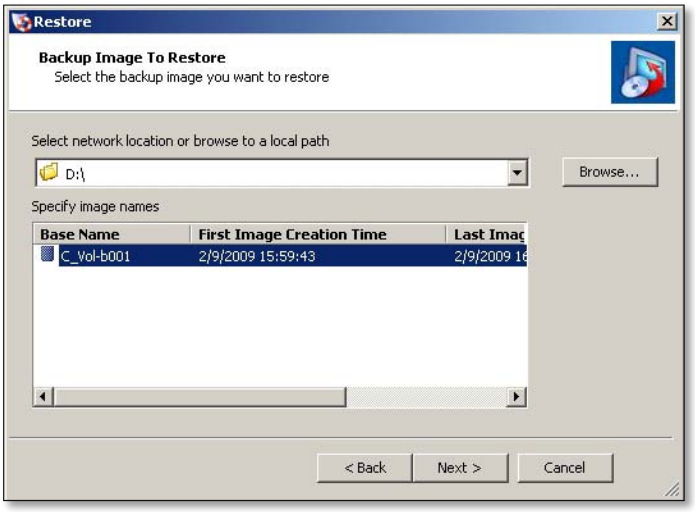


b. Start the Restore Wizard by clicking the [Restore] button in the left panel of the main screen or clicking on the Restore Wizard button from the center panel of the main screen.

c. Click [Next] to continue.

d. From the Backup Image to Restore dialog screen, you must locate the image file you wish to restore. Locations for the backup image can be a local directory or a network share. Click the [Browse] button to navigate to the location of your image backup files. Click [Next] to continue.

Note: To restore a backup image that is stored on a network share, you must have the proper credentials to access the file.

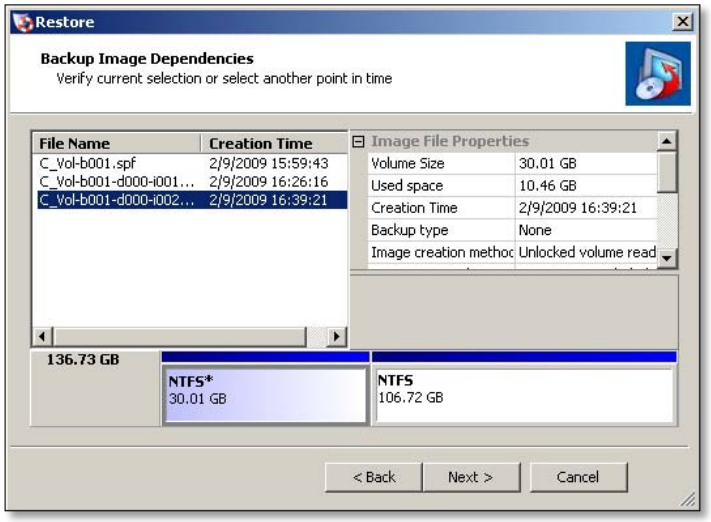


e. The Backup Image Dependencies dialog screen will load. Here you can navigate the incremental backup image files associated with the full backup image file you selected. Select an image file to view its properties in the right side of the dialog. Image file properties include:

- Image File Properties: volume size, creation time, compression, password protection, comment.
- Original Partition Information: style, number, type, bootable option, starting offset and length.
- Disk Information: disk geometry, disk size and number of the first track sectors. You can also view the disk layout graphically at the bottom of the screen. This represents what the disk looked like at the time of backup.
- Originating machine: the operating system version, the machine name, MAC address and the engine version of ShadowProtect used to create the image file.

By viewing the properties, particularly the information in the image file properties, you can best select the backup image file you wish to restore.

Click [Next] to continue.



f. The Restore Destination dialog screen will load. Select the location where you want to restore the backup image. You may also right click on a volume for the following options:

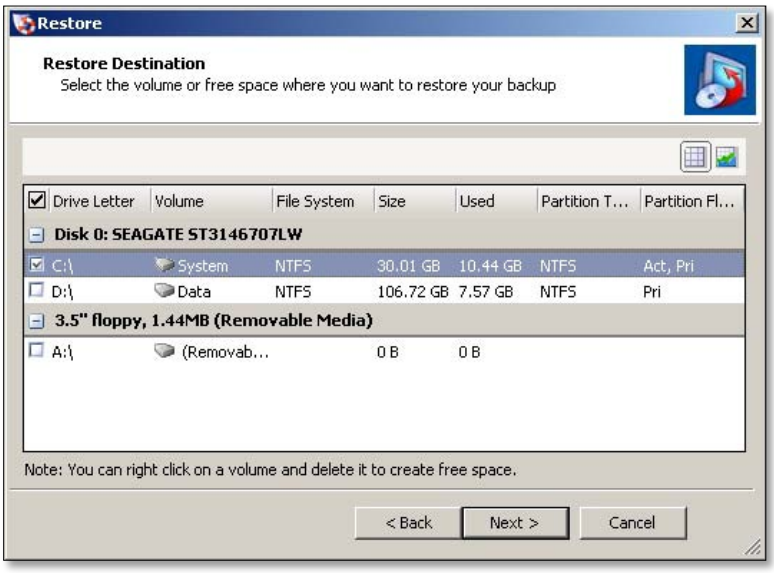
- Delete Volume: This will delete a volume. The deleted volume will become unassigned space on the disk that can be repartitioned.
- Set Active: This will set the volume as active. Only one partition may be designated as active.

By setting a volume active, the computer will boot to the volume.
- Create an exact primary partition: Allows you to define and create a primary partition on the disk. You cannot create more than four (4) primary partitions on a disk.
- Create extended partition: Allows you to extend a partition and then subdivide this partition in to one or more logical partitions.

Notes:
Restoring a backup image to a volume overwrites all data currently on the volume.

You must have enough hard disk space to restore the backup image. For example, you cannot restore a 40GB image backup to a 30GB disk.

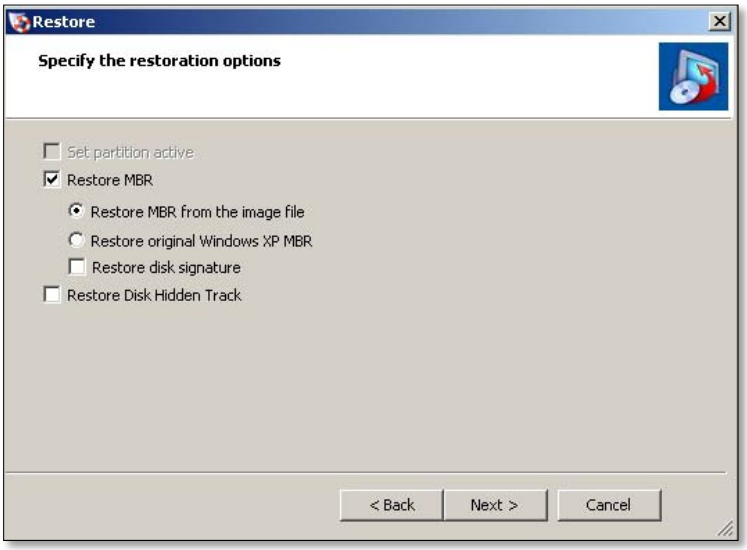
Click [Next] to continue.



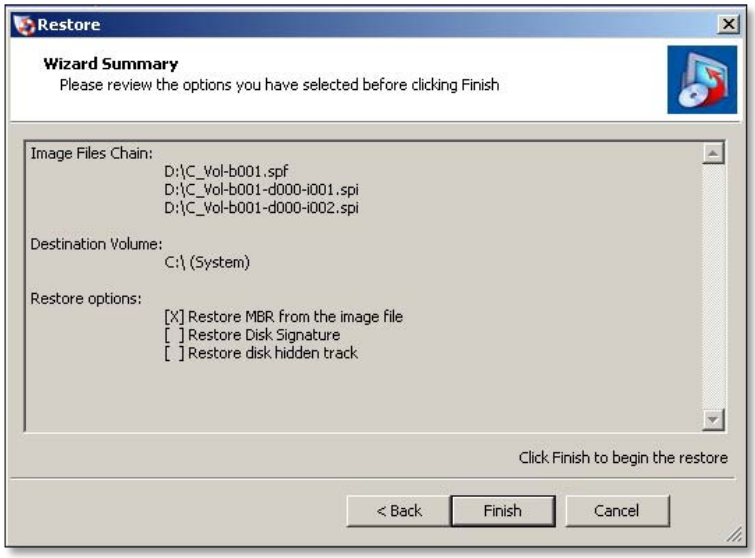
g. The “Specify the Restoration Options” dialog screen will load. All of these options are important when restoring the system volume of a computer.

- Set Partition Active: This will make the restored partition the active partition (the location that the machine boots from).
- Restore MBR: Restore the master boot record. The master boot record is contained in the first sector of the first physical hard drive. The MBR consists of a master boot program and a partition table that describes the disk partitions. The master boot program looks at the partition table to see which primary partition is active. It then starts the boot program from the boot sector of the active partition. You can restore the MBR from the image file that was saved with the backup image or you can restore an original Windows MBR.
- Restore disk signature: Restores the original physical disk signature of the hard drive. Disk signatures are part of Windows Server 2003, Windows 2000 Advanced Server, and Windows NT Server 4.0 Enterprise Edition (SP3 and later) and are necessary before the hard drive can be used.
- Restore Disk Hidden Track: This will restore the first 63 sectors of a drive. Some boot loader applications require this for the system to boot.

Click [Next] to continue.



h. The Wizard Summary dialog window will load. Review the Restore Wizard Summary and click [Finish] to start the restoration.



i. You can review the progress of the restoration by clicking on the [Volume Restore] tab associated with the restore job.

iii. Volume restoration completed.

17 Backup/Restore MySQL Server

This chapter will describe in detail how to use StorState Pro Backup Manager to backup your MySQL Database Server and how you can restore your MySQL Server from the database backup files.

17.1 Requirements

i. StorState Pro Backup Manager must be installed on the computer running MySQL.

ii. Data from the MySQL server will be backed up to a temporary directory before being sent to the Data Vaulting Center. Please make sure you have sufficient space to store this data when you run the backup job.

iii. A MySQL superuser account with sufficient rights to connect from localhost.

17.2 Overview

StorState Pro Backup Manager will backup your MySQL Server by taking the following steps:

i. Run all Pre-Commands of the backup set

ii. All database(s) (either local or external) selected are backed up to a temporary directory specified in the backup set

iii. Run all Post-Commands of the backup set

iv. Upload all backup files from the temporary directory to the Data Vaulting Center

v. Remove temporary files from the temporary directory if enabled in the backup set

17.3 How to backup MySQL Server on Windows

Please follow the instructions below to backup your MySQL server using StorState Pro Backup Manager:

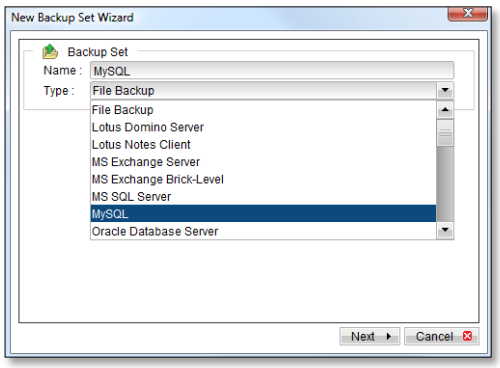
i. Open StorState Pro Backup Manager

ii. Create a new backup set:

a. To setup backup sets, click the button to open the [Backup Setting] page.

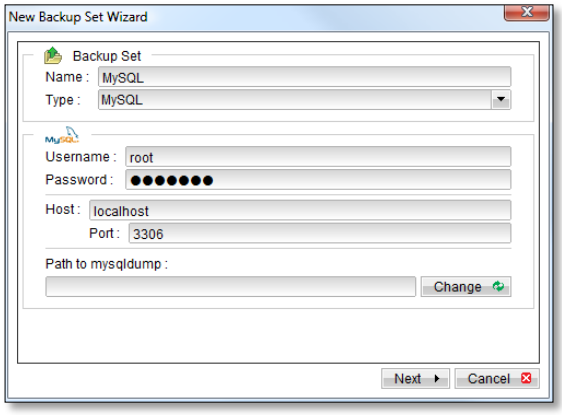
b. On the left panel, press the button to create a new backup set.

c. On the dialog, choose [MySQL] as the [Type].

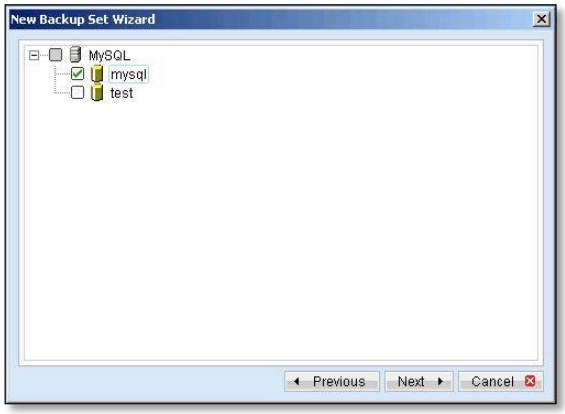


d. Enter a name for your backup set

e. Enter the username, password, the MySQL Server host address and TCP/IP port number, and the path to MySQL backup utility (mysqldump)

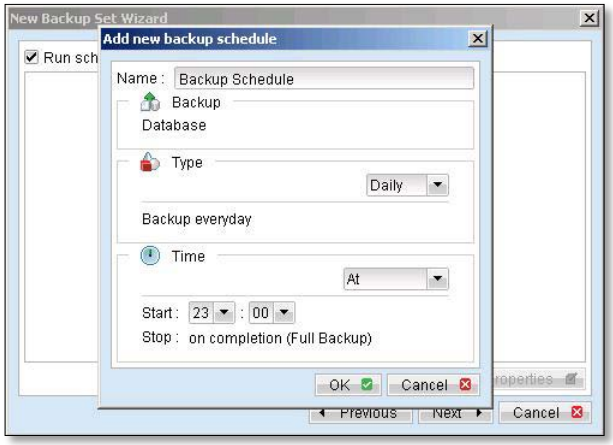


f. Select the database(s) to be backed up



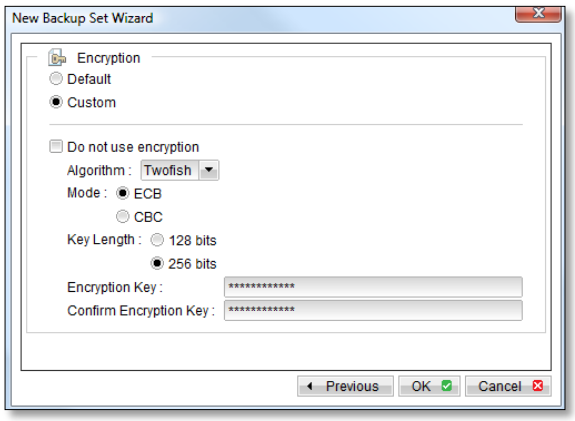
g. Enter a temporary directory for storing the backup files before they are sent to the Data Vaulting Center, ex. C:\Backup\MySQL

h. Setup the backup schedule



i. Set the encryption algorithm, encryption mode, key length and encryption key for this backup set, or leave the default setting.

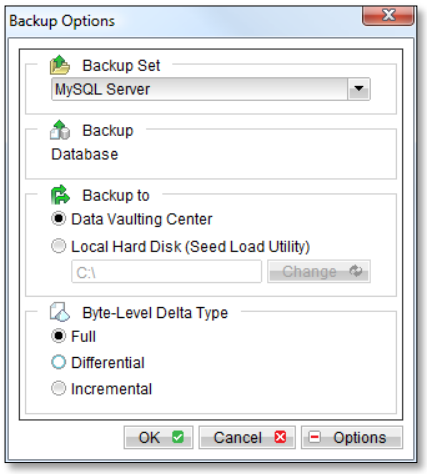
IMPORTANT: The default setting uses your account login password as your encryption key. THE ENCRYPTION KEY CANNOT BE CHANGED AFTER A BACKUP SET IS CREATED. If you change your account password in the future, this has no effect on your encryption key. To start using a new encryption key, you must delete the backup set and create a new one. This will delete all data backed up in the vaulting center for that backup set. You may retain your data by leaving the backup set and simply deleting any backup schedules for the set. YOU MUST HAVE THE ENCRYPTION KEY USED WHEN THE BACKUP SET WAS CREATED IN ORDER TO RESTORE DATA!



iii. Run Backup

a. Press the [Backup] button on the main screen of StorState Pro Backup Manager.

b. Select your MySQL Server backup set from the [Backup Set] list. If applicable, change the [Backup to] setting to Local Hard Disk for seed loading, or modify the Byte-Level Delta Type.



c. Click [OK] to start the backup. A dialog will display the progress and alert you when completed.

17.4 How to backup MySQL Server on Linux (command line mode)

If you want to setup StorState Pro Backup Manager to backup MySQL Server running on Linux using command line mode, please do the followings:

i. Create a new backup set by logging in to your Web Management Console: https://www.storstate.com/login/

ii. Click the [Backup Set] button on the top menu, then click the [Add] button next to the [Backup Set] field.

iii. Enter a name for the new backup set in the [Name] field, then select the [MySQL Database Server] radio button in the [Type] section. Press the [Update] button at the bottom of the page to continue configuring the backup set.

iv. Setup the [Database Backup Setting] fields:

Settings	Descriptions
MySQL Username	A MySQL user account that has localhost backup access to the databases to be backed up, ex: "root"
MySQL Password	Password of the MySQL user account being used
Host	IP address / Hostname of the MySQL Server, ex: "localhost"
MySQL Connection TCP/IP Port	TCP/IP port used to access the MySQL Server (default: 3306)
Path to MySQL backup utility (mysqldump)	Full path to where mysqldump can be found, ex: /usr/bin/mysqldump

v. Setup the [Backup Source] fields:

- Add a "MySQL" entry to the [Backup Source] to backup all databases under this MySQL Server
- Add "MySQL/database1" to the [Backup Source] to backup individual databases, with "database1" being the name of the database to backup

  (Please use "\" instead of "/" if the MySQL Server is running on Windows instead of Linux)

vi. Setup the [Backup Schedule] by pressing the [Add] link next the "Backup Schedule" sub-title

vii. Setup the [Temporary Directory] section with a directory to be used to store all MySQL database dump files before they are uploaded to the Data Vaulting Center. Select "Enable Delete Temp. File" to delete the temporary MySQL database dump files after they are uploaded to the Data Vaulting Center.

viii. Configure additional settings as needed, and click the [Update] button on the bottom of the page

ix. Install StorState Pro Backup Manager on the Linux server running MySQL Server (Please refer to the [2.3 Installing StorState Backup Manager for Linux/Unix/Solaris] section for details)

x. Scheduled backups will run automatically if you have started the StorState Pro backup scheduler while installing StorState Pro Backup Manager.

17.5 How to restore MySQL Server

Please follow the instructions below to restore MySQL Server.

i. Download the database backup files from the Data Vaulting Center, or decrypt backup files from a local copy

ii. Restore a database [ex: db_name] from the database backup file [ex: db_name.sql]:

   a. Connect to the MySQL server

      (Windows) C:\> mysql
      (Linux) [root@server ~]# mysql

   b. Create the database to be restored

      mysql> CREATE DATABASE IF NOT EXISTS db_name

   c. Restore the database backup file to the MySQL server

      mysql> use db_name ;
      mysql> source db_name.sql ;

      If db_name.sql is not located in the current directory, please specify the full path to the db_name.sql file in the command above.

iii. Repeat the above procedure for each database to be restored to the MySQL Server.

iv. Restoration completed.

18 Email Reporting

The StorState Data Vaulting System uses email reports to keep you informed of the status of your backup activities. Please make sure the contact information in your profile is kept up-to-date to receive the reports described in this chapter.

18.1 Account Created

When your backup account is created in the Data Vaulting Center, an Account Created email will be delivered to the contact email addresses associated with the new account. A sample Account Created email is below:

Sample Account Created Email

STORSTATE ONLINE BACKUP & RECOVERY.

Welcome to the StorState Data Vaulting System

Generated at: Wed Aug 12 02:23:11 PDT 2009

Getting started:
Please follow the instructions available in the Installation Guide to download and install StorState Pro. Please add "storstate.com" to your spam filter whitelist.

Further Information:
User Guide
FAQs
Support Info
Management Console

Account Info		
Login Name	:	demo
Alias	:	StorState Demo
Language	:	English
Contact	:	demo@storstate.com
Backup Quota	:	50G

18.2 Forgotten Password Request

If you have forgotten your account password, you can use the [Forgotten Password] link on the Web Management Console login page: https://www.storstate.com/login/

All contacts on the account will receive an email with the encrypted account password. Use this password to login to your account using StorState Backup Manager, and promptly change your password. Change your account password by clicking the [User Profile] button on the bottom left corner, and clicking [Change] next to the [Password] field. Keep in mind, changing your account password does not change the encryption key used for any backup sets, which is needed for recovery.

A sample Forgotten Password Request email is below:

Sample Forgotten Password Request Email

STORSTATE ONLINE BACKUP & RECOVERY.

Request for forgotten password

Generated at: Wed Aug 12 02:28:20 PDT 2009

Why are you receiving this email?
Someone has visited the forgotten password page and requested the password for this backup account. All registered contacts for this account will receive an email with the encrypted password.

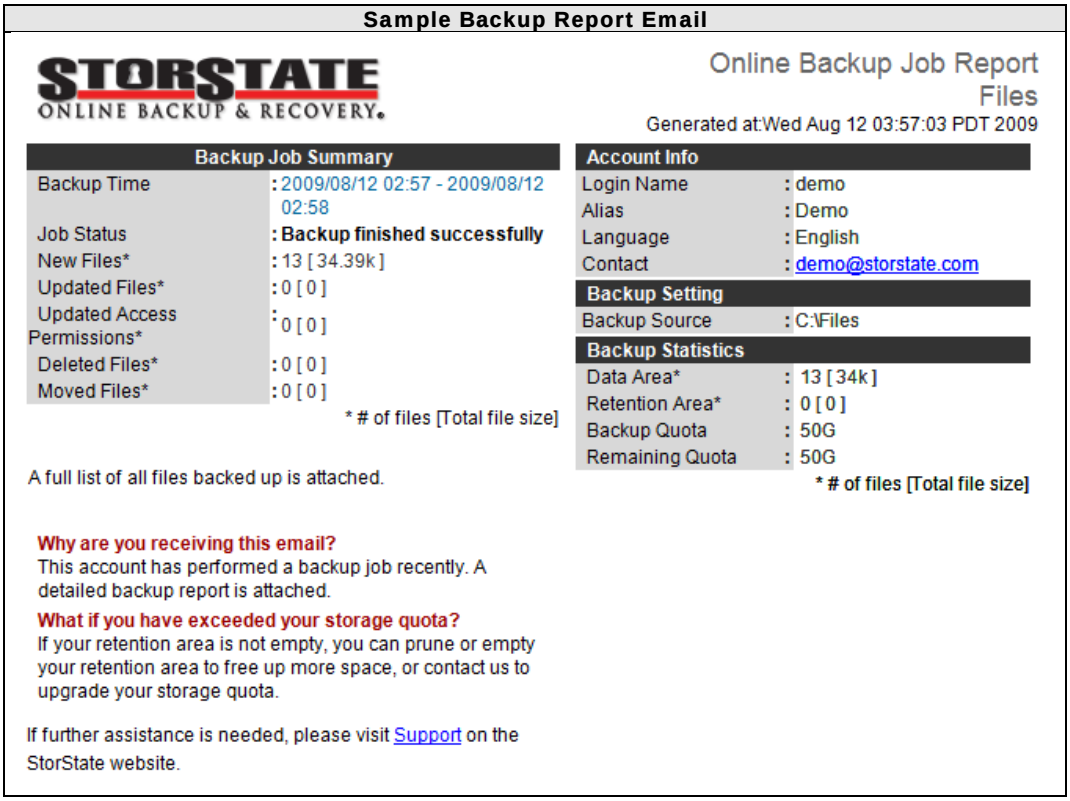
What should you do after reading this email ?
Your current password is shown under the Account Info, in an encrypted state. We recommend changing your password to a new password and deleting this email to avoid any third party gaining your password.

Account Info		
Login Name	:	demo
Password	:	**ShjlWmLjLpZxoOsKUxQJGg==**
Alias	:	StorState Demo
Language	:	English
Contact	:	demo@storstate.com

18.3 Backup Report

For each backup job, a Backup Report will be sent to each contact by email. This email contains a summary of the backup job that was run, and an attachment with a full listing of all backup activity during the backup job. A sample Backup Report email is below:

Sample Backup Report Email



STORSTATE ONLINE BACKUP & RECOVERY.

Online Backup Job Report
Files
Generated at:Wed Aug 12 03:57:03 PDT 2009

Backup Job Summary

Backup Time	: 2009/08/12 02:57 - 2009/08/12 02:58
Job Status	: **Backup finished successfully**
New Files*	: 13 [34.39k]
Updated Files*	: 0 [0]
Updated Access Permissions*	: 0 [0]
Deleted Files*	: 0 [0]
Moved Files*	: 0 [0]

* # of files [Total file size]

Account Info

Login Name	: demo
Alias	: Demo
Language	: English
Contact	: demo@storstate.com

Backup Setting

Backup Source	: C:\Files

Backup Statistics

Data Area*	: 13 [34k]
Retention Area*	: 0 [0]
Backup Quota	: 50G
Remaining Quota	: 50G

* # of files [Total file size]

A full list of all files backed up is attached.

Why are you receiving this email?
This account has performed a backup job recently. A detailed backup report is attached.

What if you have exceeded your storage quota?
If your retention area is not empty, you can prune or empty your retention area to free up more space, or contact us to upgrade your storage quota.

If further assistance is needed, please visit Support on the StorState website.

Key	Description
Backup Time	The time when the backup job ran
Job Status	The overall status of the backup job. Normally, you should see “Backup finished successfully” in this field. If you receive another message, please review the attached Full Backup Report for more information.
New Files	Total number and size of backup files added to your backup set
Updated Files	Total number and size of backup files updated in your backup set
Updated Access Permissions	Total number and size of backup files with updated access permissions in your backup set
Deleted Files	Total number and size of backup files deleted from your backup set
Moved Files	Total number and size of backup files relocated in your backup set
Backup Source	All sources to be backed up in this backup set
Data Area	The total backup data stored in the Data Area of your vault. The current copies of files in your backup set are stored in the Data Area.
Retention Area	The total backup data stored in the Retention Area of your vault. Copies of updated or deleted backup files are retained in the Retention Area for the length of time specified by the retention policy of the backup set before they are removed from the vaulting center.
Backup Quota	The storage limit of your backup account
Remaining Quota	The remaining storage in your backup account

The Full Backup Report, which contains a full listing of all backup activity during the backup job, is attached to the Backup Report email as an html file compressed with zip. You must unzip the file before you can read the Full Backup Report.

Sample Full Backup Report

Full Backup Report

Generated at: Wed Aug 12 03:57:03 PDT 2009

Backup Job Summary	
Login Name	demo
Backup Set	Files (1249783137880)
Backup Job	2009-08-12 (02:57)
Job Status	Backup finished successfully
Backup Time	2009/08/12 02:57 - 2009/08/12 02:58 (PDT)

Backup Job Statistics	
New Files*	13 [34.4k / 2.3M (99%)]
Updated Files*	0 [0 / 0 (0%)]
Permission Updated Files*	0 [0 / 0 (0%)]
Deleted Files*	0 [0 / 0 (0%)]
Moved Files*	0 [0 / 0 (0%)]

*# of files [Total zipped file size / Total file size (ratio)]

Backup Logs

No.	Type	Timestamp	Backup Logs
1	Info	2009/08/12 02:57	Start [Windows Vista (Vista), StorState Pro 5.5.3.2]
2	Info	2009/08/12 02:57	Start running pre-commands
3	Info	2009/08/12 02:57	Finished running pre-commands
4	Info	2009/08/12 02:57	Start Creating Shadow Copy Set ...
5	Info	2009/08/12 02:58	Shadow Copy Set successfully created
6	Info	2009/08/12 02:58	Start running local backup
7	Info	2009/08/12 02:58	Reading local backup files from hard disk
8	Info	2009/08/12 02:58	Reading local backup files from hard disk ... Completed
9	Info	2009/08/12 02:58	Finish running local backup
10	Info	2009/08/12 02:58	Deleting Shadow Copy Volume for "C:\"
11	Info	2009/08/12 02:58	Start running post-commands
12	Info	2009/08/12 02:58	Finished running post-commands

New Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
1	C:\	1.5k / 0 [0%]	-
2	C:\Files	1.5k / 0 [0%]	-
3	C:\Files\Excel doc 1.xls	3.3k / 301.8k [99%]	2009/08/08 19:12
4	C:\Files\Excel doc 2.xls	3.3k / 301.8k [99%]	2009/08/08 19:12
5	C:\Files\Excel doc 3.xls	3.3k / 301.8k [99%]	2009/08/08 19:12
6	C:\Files\Important File 1.txt	2k / 35.7k [95%]	2009/08/07 00:37
7	C:\Files\Important File 2.txt	2k / 35.7k [95%]	2009/08/07 00:37
8	C:\Files\Important File 3.txt	2.3k / 107.1k [98%]	2009/08/08 19:15
9	C:\Files\Important File 4.txt	2k / 35.7k [95%]	2009/08/07 00:37
10	C:\Files\Important File 5.txt	2k / 35.7k [95%]	2009/08/05 23:52
11	C:\Files\Word doc 1.doc	4.7k / 553.5k [99%]	2009/08/08 19:15
12	C:\Files\Word doc 2.doc	3.3k / 301.8k [99%]	2009/08/08 19:12
13	C:\Files\Word doc 3.doc	3.3k / 301.8k [99%]	2009/08/08 19:12

Updated Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been updated.			

Permission Updated Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No Permissions have been updated.			

Deleted Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No files have been deleted.			

Moved Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been moved.			

Key	Description
Backup Set	The name of the backup set
Backup Job	The name of the backup job (which is the start time of the backup job)
Job Status	The overall status of the backup job. Normally, you should see “Backup finished successfully” in this field. If you receive another message, please review the Full Backup Report for more information.
Backup Time	The time when the backup job started and completed
New Files	Total number and size of backup files added to your backup set
Updated Files	Total number and size of backup files updated in your backup set
Permission Updated Files	Total number and size of backup files with updated access permissions in your backup set
Deleted Files	Total number and size of backup files deleted from your backup set
Moved Files	Total number and size of backup files relocated in your backup set
Backup Logs	All messages logged while running this backup job
New Files List	Full list of all new files backed up during the backup job
Updated Files List	Full list of all updated files backed up during the backup job
Permission Updated Files List	Full list of all files with updated access permissions backed up during the backup job
Deleted Files List	Full list of all deleted files detected during the backup job
Moved Files List	Full list of all relocated files detected during the backup job

18.4 Restore Report

For each restoration job, a Restore Report will be sent to each contact by email. This email contains a summary of the restore job that was run, and an attachment with a full listing of all restoration activity during the restore job. A sample Restore Report email is below:

Sample Restore Report

STORSTATE ONLINE BACKUP & RECOVERY.

File Download Report
Files
Generated at: Wed Aug 12 03:58:00 PDT 2009

Why are you receiving this email?
Backup files have recently been downloaded from the vaulting center. Please see the attached report for a list of files downloaded.

Account Info		
Login Name	:	demo
Alias	:	Demo
Language	:	English
Contact	:	demo@storstate.com

File Download Summary		
Download Time	:	2009-08-12 02:58 - 2009-08-12 02:58
Total files	:	11
Total file size	:	14k

Key	Description
Download Time	The time when the restore job ran
Total files	Total number of files restored during the restore job
Total file size	Total amount of data restored during the restore job

The File Download Report, which contains a full listing of all restoration activity during the restore job, is attached to the Restore Report email as an html file compressed with zip. You must unzip the file before you can read the File Download Report.

Sample File Download Report

File Download Report

Generated at: Wed Aug 12 03:58:00 PDT 2009

Account Info		
Login Name	:	demo
Alias	:	Demo
Language	:	English
Contact	:	demo@storstate.com

File Download Summary		
Download Time	:	2009-08-12 02:58 - 2009-08-12 02:58
Total files	:	11
Total file size	:	14k

Downloaded Files List

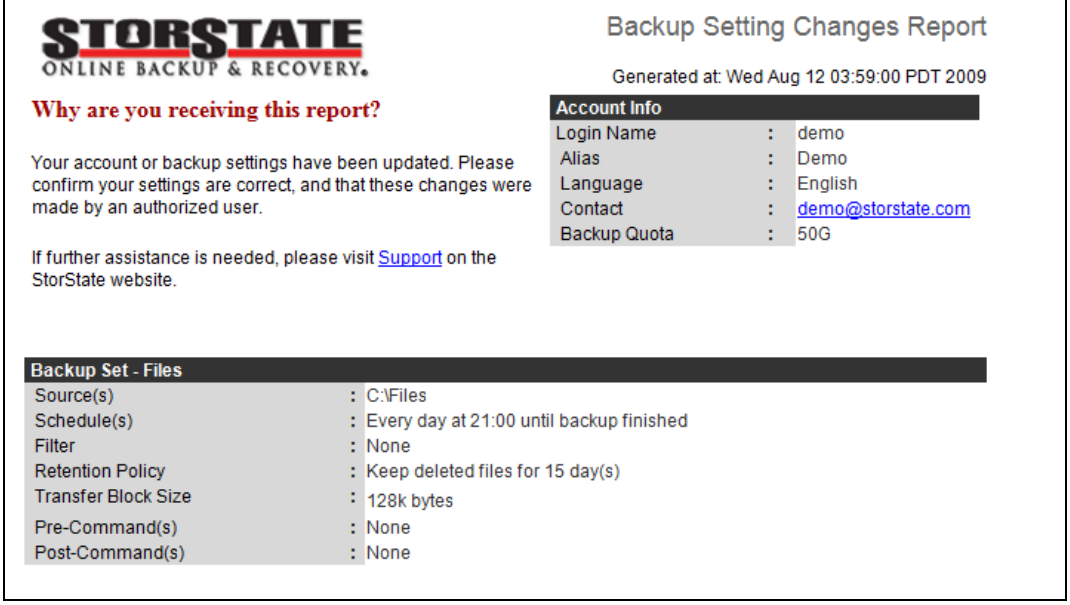
	Download Time	Filename	Size	Last Modified	IP
1	2009-08-12 02:58	C:\Files\Excel doc 1.xls	1k	2009-08-08 19:12	98.246.38.150
2	2009-08-12 02:58	C:\Files\Excel doc 2.xls	1k	2009-08-08 19:12	98.246.38.150
3	2009-08-12 02:58	C:\Files\Excel doc 3.xls	1k	2009-08-08 19:12	98.246.38.150
4	2009-08-12 02:58	C:\Files\Important File 1.txt	464	2009-08-07 00:37	98.246.38.150
5	2009-08-12 02:58	C:\Files\Important File 2.txt	464	2009-08-07 00:37	98.246.38.150
6	2009-08-12 02:58	C:\Files\Important File 3.txt	864	2009-08-08 19:15	98.246.38.150
7	2009-08-12 02:58	C:\Files\Important File 4.txt	464	2009-08-07 00:37	98.246.38.150
8	2009-08-12 02:58	C:\Files\Important File 5.txt	464	2009-08-05 23:52	98.246.38.150
9	2009-08-12 02:58	C:\Files\Word doc 1.doc	3k	2009-08-08 19:15	98.246.38.150
10	2009-08-12 02:58	C:\Files\Word doc 2.doc	1k	2009-08-08 19:12	98.246.38.150
11	2009-08-12 02:58	C:\Files\Word doc 3.doc	1k	2009-08-08 19:12	98.246.38.150

Key	Description
Backup Set	The name of the backup set
Backup Job	The name of the backup job (which is the start time of the backup job)
Job Status	The overall status of the backup job. Normally, you should see "Backup finished successfully" in this field. If you receive another message, please review the Full Backup Report for more information.
Backup Time	The time when the backup job started and completed
New Files	Total number and size of backup files added to your backup set
Updated Files	Total number and size of backup files updated in your backup set
Permission Updated Files	Total number and size of backup files with updated access permissions in your backup set
Deleted Files	Total number and size of backup files deleted from your backup set
Moved Files	Total number and size of backup files relocated in your backup set
Backup Logs	All messages logged while running this backup job
New Files List	Full list of all new files backed up during the backup job
Updated Files List	Full list of all updated files backed up during the backup job
Permission Updated Files List	Full list of all files with updated access permissions backed up during the backup job
Deleted Files List	Full list of all deleted files detected during the backup job
Moved Files List	Full list of all relocated files detected during the backup job

18.5 Setting Change

After any user profile or backup setting changes are made, a Setting Change email report will be sent to all account contacts. This report allows you to track changes that have been made to your backup account.

Sample Report



STORSTATE ONLINE BACKUP & RECOVERY.

Backup Setting Changes Report

Generated at: Wed Aug 12 03:59:00 PDT 2009

Why are you receiving this report?

Your account or backup settings have been updated. Please confirm your settings are correct, and that these changes were made by an authorized user.

If further assistance is needed, please visit Support on the StorState website.

Account Info		
Login Name	:	demo
Alias	:	Demo
Language	:	English
Contact	:	demo@storstate.com
Backup Quota	:	50G

Backup Set - Files		
Source(s)	:	C:\Files
Schedule(s)	:	Every day at 21:00 until backup finished
Filter	:	None
Retention Policy	:	Keep deleted files for 15 day(s)
Transfer Block Size	:	128k bytes
Pre-Command(s)	:	None
Post-Command(s)	:	None

Key	Description
Source(s)	All sources to be backed up in the backup set
Schedule(s)	All backup schedules for the backup set
Filter	All filters applied to the backup set
Retention Policy	The retention policy of the backup set
Transfer Block Size	The transfer block size of the backup set
Pre-Command(s)	All Pre-Commands run before the backup
Post-Command(s)	All Post-Commands run after the backup

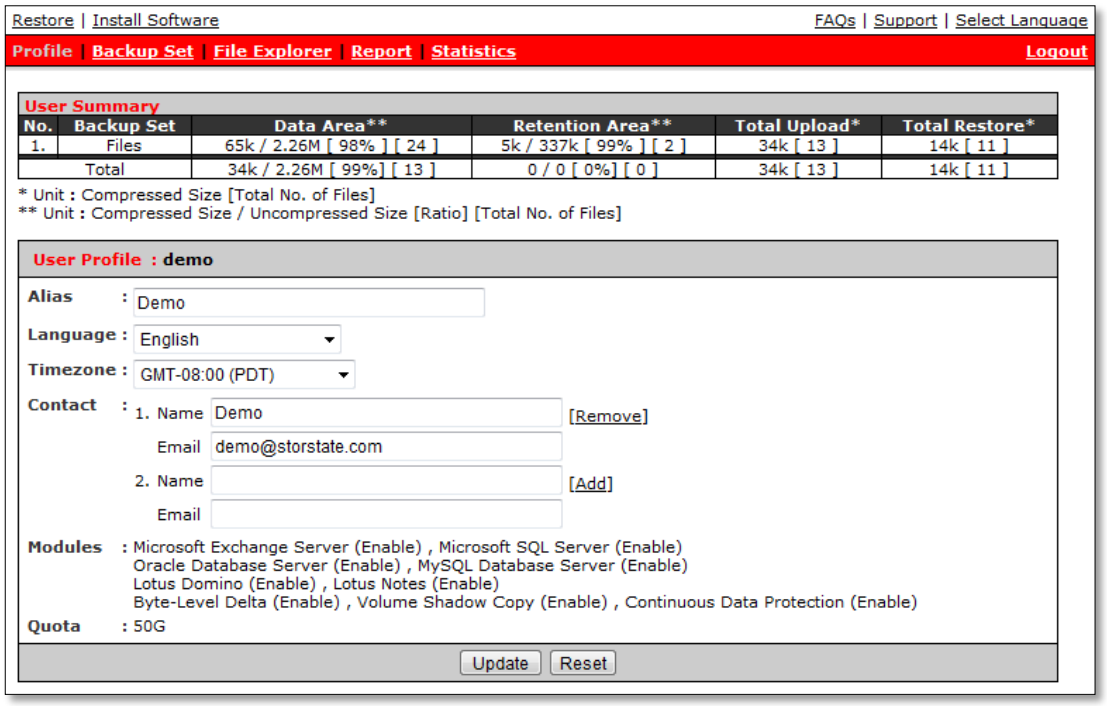
19 Web Management Console

The StorState Data Vaulting System Management Console can be used to:

- Request a forgotten account password
- Download the StorState Backup Manager software and access installation instructions
- Update user profile settings
- Review, restore and delete backup files
- Add, change and remove backup sets
- Review backup job reports
- Review storage statistics

Login to the Web Management Console:
https://www.storstate.com/login/

Request a forgotten account password by clicking the link on the login page



Key	Description
Quota	Total storage limit of your backup account
Data Area	The total backup data stored in the Data Area of your vault. The current copies of files in your backup set are stored in the Data Area.
Retention Area	The total backup data stored in the Retention Area of your vault. Copies of updated or deleted backup files are retained in the Retention Area for the length of time specified by the retention policy of the backup set before they are removed from the vaulting center.
Total Upload	Total size and number of backup files uploaded to the Data Vaulting Center
Total Restore	Total size and number of backup files restored from the Data Vaulting Center

19.1 Download and Install StorState Backup Manager

Before you can run a backup you must install StorState Backup Manager. You can download the installer and access the installation guide from the [Install Software] link on the top-left menu.

19.2 Update User Profile

Update your user profile by clicking the [Profile] link from the top-left menu. Make any changes to your profile and press the [Update] button.

19.3 Review, Restore, and Delete Backup Files

Review Backup Data

Click the [File Explorer] link to browse through the backup data in your vault.

Delete Backup Files

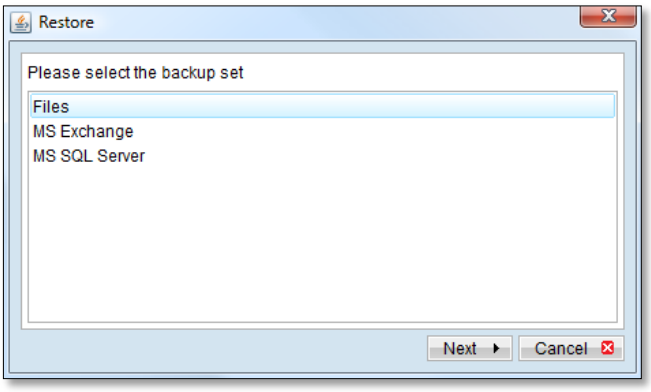
To delete backup files from your data vault, select the checkbox next to the file to remove and click [Delete].

Restore Backup Files

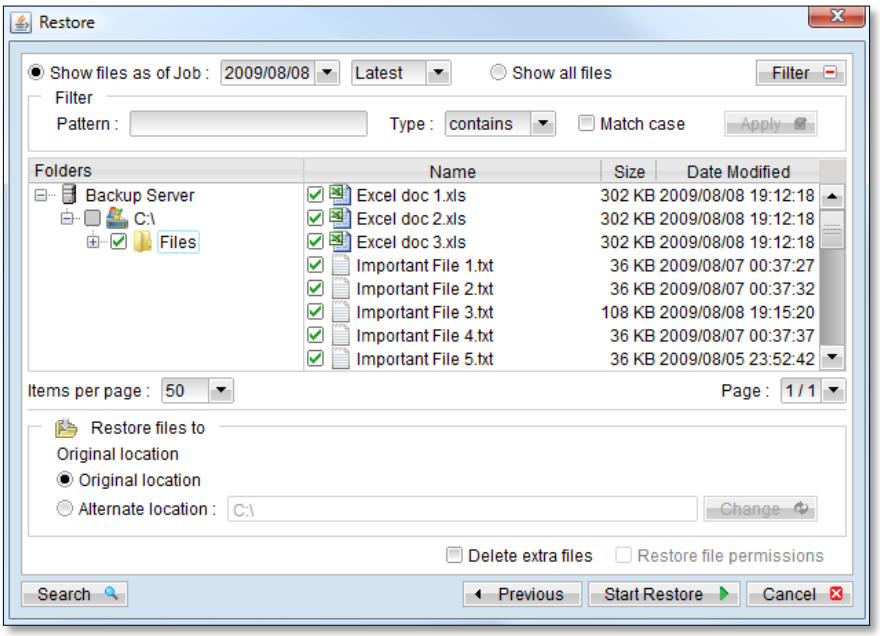
You can restore data from the Web Management Console by following the instructions below:

i. Click [Restore] on far right side of the [File Explorer] page to open the Java Restoration Applet.

ii. Select the required [Backup Set] from the list and press [Next] to proceed.



iii. Select the backup job you wish to restore from the [Show files as of Job] drop-down box, or leave on "Latest" to restore from the latest backup. Select [Show all files] to view all snapshots of files stored in your data vault.



iv. Optional - Click the Filter button on the top right corner to filter the files/folders view based on your criteria.

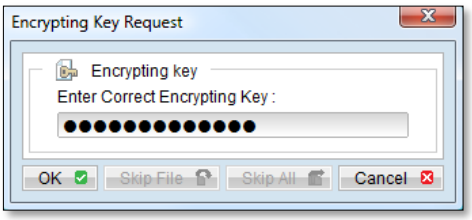
v. Optional - Click the Search button on the bottom left corner to search for files/folders based on your criteria.

vi. Select the files/folders you would like to restore. A file won't be downloaded from your data vault if an identical file exists in the restore path already.

vii. In the "Restore files to" section, leave the setting to "Original location" to restore files and folders to the same location as when backed up. Select "Alternative location" to specify a different folder to restore to.

viii. Select the "Delete extra files" checkbox to synchronize the restore location with the backup files/folders being restored. This setting will delete existing files/folders from the restore location that were not part of the backup.

ix. Click [Start Restore] to start the restore operation. The Encrypting Key Request window will open.



x. Enter the Encryption Key used when the backup set was created and click [OK].

xi. The Restore Progress window will display the restoration progress and alert you when completed.

19.4 Add, Change and Remove Backup Sets

Click the [Backup Set] link to work with backup sets. From here you can use the [Backup Set] drop-down list to review existing backup sets. StorState Xpress is limited to one file backup set.

Make changes to an existing backup set

To make changes, edit the settings as needed and click the [Update] button at the bottom of the page.

Remove a backup set

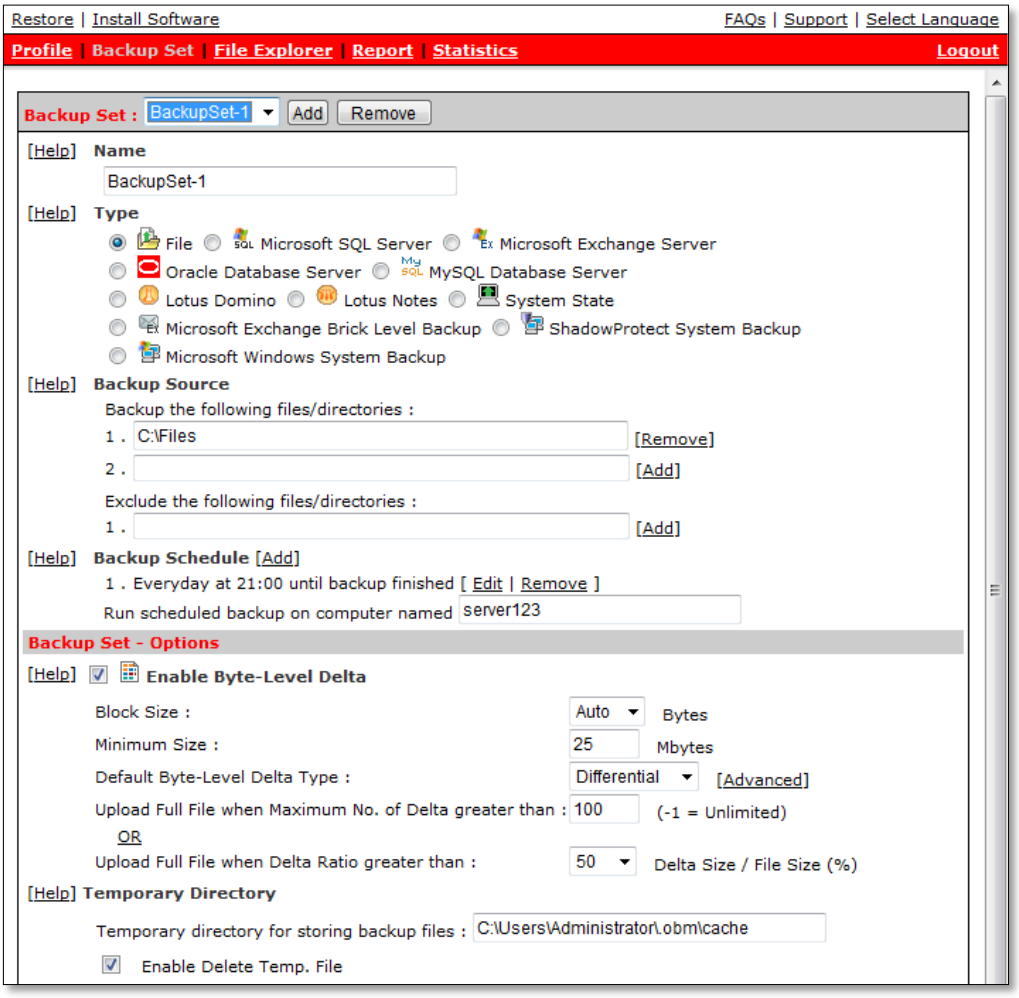
To remove a backup set, select the set to be removed from the [Backup Set] drop-down list, and click the [Remove] button.

Add a new backup set

To add a new backup set, follow the instructions below:

i. Click the [Backup Set] button on the top menu, then click the [Add] button next to the [Backup Set] field.

ii. Enter a name for the new backup set in the [Name] field.



iii. Select the appropriate backup set [Type] from the radio button list. Click the [Update] button at the bottom of the page before continuing to configure the backup set.

iv. Setup the [Backup Source] fields, and any applicable database fields for backup types other than "File". Please reference the appropriate sections in this guide for more information on each backup type.

File Backup Source Setup

a. In the [Backup the following files/directories] field, enter a path to be backed up on the computer running StorState Backup Manager. Click [Add] to include the path in the backup set.

b. (optional) In the [Exclude the following files/directories] field, enter any file path within a path entered above to exclude it from the backup set.

c. Click the [Remove] link next to any path to remove it from the backup set.

v. Setup the [Backup Schedule] by pressing the [Add] link next the "Backup Schedule" sub-title. StorState Pro may have multiple backup schedules.

vi. In the [Run scheduled backup on computer named] field, enter the computer name/hostname of the computer on which this backup set should run. The computer name can be found on a Windows system in [Control Panel]-[System].

vii. Setup the [Temporary Directory] section with a directory to be used to store all files before they are uploaded to the Data Vaulting Center. Be sure there is enough space in the temporary folder before the backup is run. Select "Enable Delete Temp. File" to delete the temporary files after they are uploaded to the Data Vaulting Center.

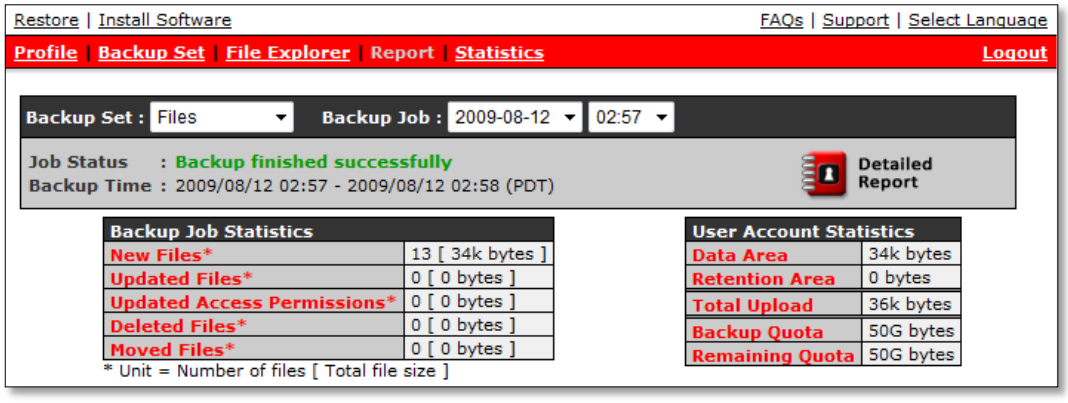
viii. Configure additional settings as needed, and click the [Update] button on the bottom of the page to save your settings. Reference the appropriate sections of this guide for more information on specific settings.

ix. Scheduled backups will run automatically if you have started the StorState backup scheduler while installing StorState Backup Manager on the computer to be backed up.

19.5 Review Backup Jobs

In addition to reviewing your backup activities from the email reports and from within StorState Backup Manager, you can also review any of your backup job reports by using the Report section on the Web Management Console. To review a backup job, click the [Report] menu link, then select the [Backup Set], and then the [Backup Job] required from the drop-down lists.

You can open the [Full Backup Report] to review all information logged during a backup job by clicking the [Detailed Report] button on the [Report] page.



Full Backup Report Example

Full Backup Report

Generated at: Thu Aug 13 01:33:24 PDT 2009

Backup Job Summary	
Login Name	demo
Backup Set	Files (1249783137880)
Backup Job	2009-08-12 (02:57)
Job Status	**Backup finished successfully**
Backup Time	2009/08/12 02:57 - 2009/08/12 02:58 (PDT)

Backup Job Statistics	
New Files*	13 [34.4k / 2.3M (99%)]
Updated Files*	0 [0 / 0 (0%)]
Permission Updated Files*	0 [0 / 0 (0%)]
Deleted Files*	0 [0 / 0 (0%)]
Moved Files*	0 [0 / 0 (0%)]

* # of files [Total zipped file size / Total file size (ratio)]

Backup Logs

No.	Type	Timestamp	Backup Logs
1	Info	2009/08/12 02:57	Start [Windows Vista (reb1), StorState Pro 5.5.3.2]
2	Info	2009/08/12 02:57	Start running pre-commands
3	Info	2009/08/12 02:57	Finished running pre-commands
4	Info	2009/08/12 02:57	Start Creating Shadow Copy Set ...
5	Info	2009/08/12 02:58	Shadow Copy Set successfully created
6	Info	2009/08/12 02:58	Start running local backup
7	Info	2009/08/12 02:58	Reading local backup files from hard disk
8	Info	2009/08/12 02:58	Reading local backup files from hard disk ... Completed
9	Info	2009/08/12 02:58	Finish running local backup
10	Info	2009/08/12 02:58	Deleting Shadow Copy Volume for "C:\"
11	Info	2009/08/12 02:58	Start running post-commands
12	Info	2009/08/12 02:58	Finished running post-commands

New Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
1	C:\	1.5k / 0 [0%]	-
2	C:\Files	1.5k / 0 [0%]	-
3	C:\Files\Excel doc 1.xls	3.3k / 301.8k [99%]	2009/08/08 19:12
4	C:\Files\Excel doc 2.xls	3.3k / 301.8k [99%]	2009/08/08 19:12
5	C:\Files\Excel doc 3.xls	3.3k / 301.8k [99%]	2009/08/08 19:12
6	C:\Files\Important File 1.txt	2k / 35.7k [95%]	2009/08/07 00:37
7	C:\Files\Important File 2.txt	2k / 35.7k [95%]	2009/08/07 00:37
8	C:\Files\Important File 3.txt	2.3k / 107.1k [98%]	2009/08/08 19:15
9	C:\Files\Important File 4.txt	2k / 35.7k [95%]	2009/08/07 00:37
10	C:\Files\Important File 5.txt	2k / 35.7k [95%]	2009/08/05 23:52
11	C:\Files\Word doc 1.doc	4.7k / 553.5k [99%]	2009/08/08 19:15
12	C:\Files\Word doc 2.doc	3.3k / 301.8k [99%]	2009/08/08 19:12
13	C:\Files\Word doc 3.doc	3.3k / 301.8k [99%]	2009/08/08 19:12

Updated Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been updated.			

Permission Updated Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No Permissions have been updated.			

Deleted Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No files have been deleted.			

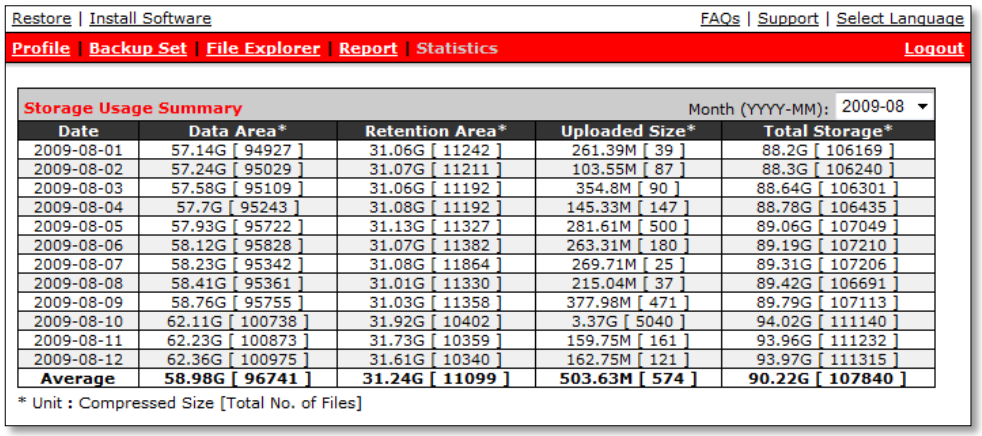
Moved Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been moved.			

Key	Description
Job Status	The overall status of the backup job. Normally, you should see “Backup finished successfully” in this field. If you receive another message, please click the [Detailed Report] button.
Backup Time	The time when the backup job started and completed
New Files	Total number and size of backup files added to your backup set
Updated Files	Total number and size of backup files updated in your backup set
Updated Access Permissions	Total number and size of backup files with updated access permissions in your backup set
Deleted Files	Total number and size of backup files deleted from your backup set
Moved Files	Total number and size of backup files relocated in your backup set
Data Area	The total backup data stored in the Data Area of your vault. The current copies of files in your backup set are stored in the Data Area.
Retention Area	The total backup data stored in the Retention Area of your vault. Copies of updated or deleted backup files are retained in the Retention Area for the length of time specified by the retention policy of the backup set before they are removed from the vaulting center.
Total Upload	Total number and size of backup files uploaded to the Data Vaulting Center
Backup Quota	The storage limit of your backup account
Remaining Quota	The remaining storage in your backup account

19.6 Review Storage Statistics

You can review the amount of data you have stored in the Data Vaulting Center and access statistics on your storage and upload usage by clicking the [Statistics] link. To review your storage statistics for a different month, select the month required from the [Month] drop-down list.



Key	Description
Data Area	The total backup data stored in the Data Area of your vault on the particular date. The current copies of files in your backup set are stored in the Data Area.
Retention Area	The total backup data stored in the Retention Area of your vault on the particular date. Copies of updated or deleted backup files are retained in the Retention Area for the length of time specified by the retention policy of the backup set before they are removed from the vaulting center.
Uploaded Size	Total size and number of backup files uploaded to the Data Vaulting Center on the particular date
Total Storage	Total size and number of backup files stored in your backup account on the particular date

20 Further Information

20.1 FAQ

Please review our constantly updated FAQ for answers to many questions not covered in this guide:

http://www.storstate.com/docs/storstate-faq.pdf

20.2 Support Information

StorState Online Backup & Recovery is committed to excellent customer support.

Please review this User Guide and the FAQ for setup and troubleshooting, as nearly all issues are covered in detail and they are frequently updated.

For the fastest assistance, please submit a support ticket on our website:

https://www.storstate.com/tts/

Email Tech Support

support@storstate.com

Telephone Support

800.979.0224