Gigasoft Data Protection Ltd

GIGASOFT BACKUP MANAGER

User Guide

Version: 22.11.x

06/12/2022

Gigasoft Backup

User's Guide

Trademarks

Disclaimer

Gigasoft Data Protection Limited will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by Gigasoft Data Protection Limited without prior notice to you.

Table of Contents

Contents

1 Overview

1.1 Conventions

Convention	Descriptions	Example
Bold	**Important information**	**Important: The encrypting key is independent from a backup account's password.**
Italic	**Folder path or file path**	***C:\Program Files\Gigasoft Backup***
[]	**Graphical Interface Elements**	**[Backup]**
Italic	**Command**	***sudo ./uninstall.sh***

1.2 System requirements

- x86_32+SSE2 or x86_64 CPU architecture
- Minimum 1024x600 screen resolution
- Windows 7, 8, 8.1, 10, or newer
- Windows Server 2008 R2, 2012, 2012 R2, 2016, or newer

Microsoft ended Extended support for Windows 7, Server 2008, and Server 2008 R2 on January 14th 2020. Future versions of GBM may drop support for older versions of Windows no longer under active security support from Microsoft.

Not compatible with Windows XP & Server 2003

At the time of writing, there is no version of GBM available for Windows XP / Server 2003. All versions of GBM rely heavily on features that were only introduced in Windows Vista / Server 2008.

Windows XP / Server 2003 no longer receives security patches from Microsoft. *It is **unsafe** to connect such a machine to the internet.* If you are attempting to supply backup services to a customer in this situation, you should arrange to first upgrade their operating system *with urgency*.

You can work around this issue by

- installing GBM on another machine, and then backup the XP machine over the network; or
- virtualizing the XP machine, and backing up the VM guest from the VM host. This also allows you to remove internet access from the XP machine.

Workarounds

You can work around this issue by

- installing GBM on another machine, and then backup the XP machine over the network; or
- virtualizing the XP machine, and backing up the VM guest from the VM host. This also allows you to remove internet access from the XP machine.

1.3 Important notes

Images, workflow or description in this document may be different from your installation. If you are uncertain about any of the instructions provided, please contact us for advice.

1.4 Application structure

The client software is split into two components; backup-tool is a command-line tool which implements all the software functionality. The graphical user interface is backup-interface, which wraps this command-line tool. Backup schedules will still run even if logged out of the GUI, as the background service will still be logged in.

Additionally, clients can remotely control their installed software by logging in to the GBM Server web interface as a user.

On platforms without a desktop interface available (e.g. Linux server), only the backup-tool part is used, and you should control the application via the web interface.

1.5 Windows: running as administrator, elevator, and VSS snapshots

One of Gigasoft Backup's features is the ability to take a filesystem snapshot on Windows, to back up files that are currently in use. Taking a filesystem snapshot requires parts of Gigasoft Backup to run as Administrator. But in general, it's best to minimize Administrator surface for defence-in-depth security principles - and furthermore, Administrator has a different set of mounted network shares versus the regular non-elevated user, so it can be confusing for users if Administrator is used any more often than necessary.

Gigasoft Backup works around this issue with an Elevator service, that is pre-authorized to run ***backup-tool*** as administrator.

- If VSS is not enabled, then ***backup-interface*** communicates with ***backup-tool*** to perform the backup job.
- However, if VSS was required for a Protected Item, ***backup-tool*** instead transmits a message to the Elevator service, to re-run itself as Administrator.

1.6 Protected items and storage vaults

The user's configuration is broadly separated into Protected Items and Storage Vaults.

A Protected Item is a description of the set of data that should be backed up.

A Storage Vault is a location where the backed-up data can be stored. In most common configurations, this would be a Gigasoft Backup Server with the Storage Role enabled; but it's possible for the client software to back up to a local / removable disk or network location.

All data within a Storage Vault is compressed, encrypted, and deduplicated. A Storage Vault is the unit of deduplication; data is not deduplicated between multiple Storage Vaults.

1.7 Devices

Multiple devices (e.g. different computers, servers or laptops) can log in to the same Gigasoft Backup user account with a shared password. Each device has its own private set of Protected Items but shares access to the same Storage Vaults. This allows you to deduplicate data between multiple devices.

Each device can also restore and delete each other’s backed-up data, so it is important that multi-device accounts are only used in trusted contexts.

1.8 Device registration

Each Gigasoft Backup account can be used by multiple devices. This allows you to deduplicate backups from multiple accounts, since backups can be targeted to the same Storage Vault.

When you log in to the same Gigasoft Backup account from another device, such as a laptop or tablet, you will see a private view of Protected Items but a public view of Storage Vaults.

- You can view, edit, and use Storage Vaults configured by other devices

- You cannot view, edit, nor use Protected Items configured by other devices
- You can restore data from any device's Protected Item (hidden by default)
- You can view job logs from any device (hidden by default)

1.9 Encryption

We strongly recommend that users use strong passwords. Even the best security is foiled by a user choosing a weak or commonly-used password, such as 123456 or letmein.

Gigasoft Backup always encrypts all user data before storing it, using strong AES-256-CTR with Poly1305 in AEAD mode with high-entropy random keys. For more technical details about the encryption formats and key management.

The user's password is used to derive two 192-bit keys (the "L" and "R" keys) via PBKDF2-SHA512, with hard-coded parameters for repeatable output.

- The L-key is used to log in to the Auth Role server in place of the real password; the server stores only a bcrypt(sha512) hash of this L-key.
- The R-key never leaves the client and is used to encrypt secret keys stored within the user's profile on the server.

This means that one password can be used for all client-side account operations, while preventing servers from uncovering client-only secrets.

When Gigasoft Backup sets up a Storage Vault for the first time, it generates two high-entropy random keys (the 256-bit "A" and 128-bit "E" keys). All user data in the Storage Vault is stored encrypted with the A-key using AES-256 in CTR mode and authenticated using Poly1305 in AEAD (encrypt-then-MAC) mode.

The permanent A-key is stored inside the Storage Vault, encrypted with the E-key. The E-key is then encrypted with the R-key and stored in the user's profile on the Authorisation server. When a backup is performed, the client uses its password to derive the private R-key, to decrypt the E-key from the vault, to decrypt the A-key for data storage. This extra level of indirection enables some key rotation scenarios, as a new E-key can be generated without needing to re-encrypt all the data in the Storage Vault.

If the Storage Vault is for a Storage Role bucket, a high-entropy random 128-bit PSK is used to gate access to the bucket. The Storage Role server stores only a bcrypt(sha512) hash of this PSK. The client encrypts this PSK with the R-key and stores it in the user's profile on the Authorisation server.

1.10 Commands

You can register additional commands to run before- or after any backup job. For maximum flexibility, commands can be registered

- for a Protected Item (e.g. to dump a database), or
- for a Storage Vault (e.g. to perform custom network authentication), or
- for a Schedule (e.g. to shut down the computer afterward).

During a backup job, the commands are run in this order: Schedule Before, Protected Item Before, Storage Vault Before, Backup, Storage Vault After, Protected Item After, Schedule After.

Shell built-ins can be used as part of the command execution - the specified command is passed to either ***cmd.exe*** or ***/bin/sh*** as appropriate for your operating system.

1.11 Backup algorithm

Gigasoft Backup backs up data by first splitting it into variable-sized chunks, which are individually compressed, encrypted, and uploaded. Gigasoft Backup uses data-dependent chunking, efficiently splitting a file into consistent chunks even in the face of random inserts.

A backup job consists of a list of files and which chunks would be needed to reconstruct them. Any successive incremental backup jobs simply realize that chunks already exist on the server and do not need to be re-uploaded.

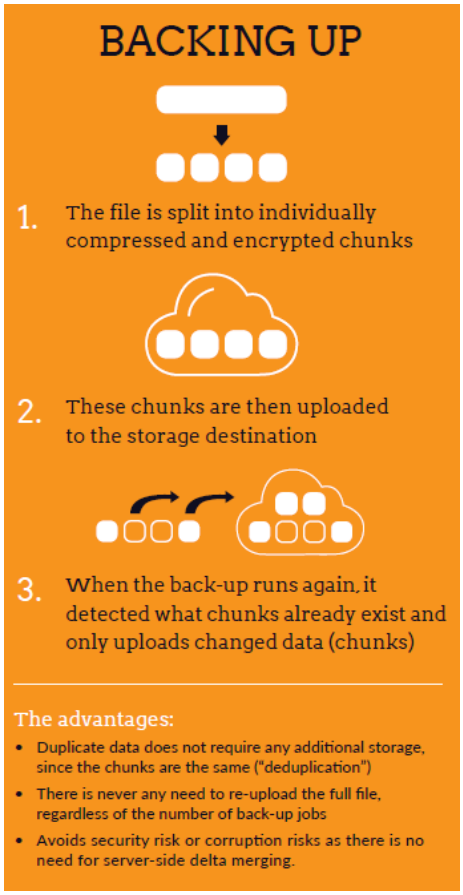
This chunking technique has the following properties:

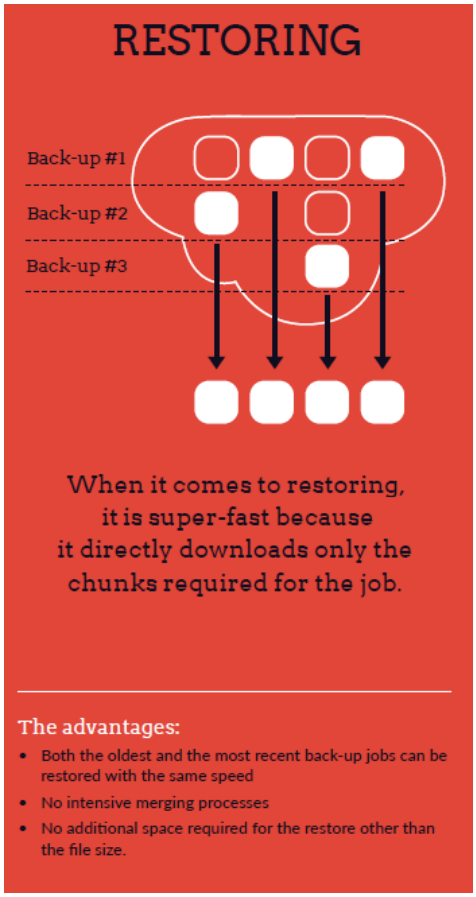
- Both the oldest and the most recent backup jobs can be restored with the same speed
- Duplicate data does not require any additional storage, since the chunks are the same ("deduplication")
- There is never any need to re-upload the full file, regardless of the number of backup jobs
- There is no need for the server to be trusted to decrypt data

1.12 Gigasoft Backup chunking overview

At the core of Gigasoft Backup is our technology that allows us to back-up and restore faster than the competition, this is called Chunking. Gigasoft Backup backs up data by first splitting it into variable-sized chunks, which are individually compressed, encrypted, and uploaded. Gigasoft Backup uses data-dependent chunking, efficiently splitting a file into consistent chunks even in the face of random inserts.

Further incremental back-up jobs simply realize that chunks already exist on the server and do not need to be re-uploaded. When it comes to restoring, Gigasoft Backup is just as fast. Gigasoft Backup directly downloads only the chunks it needs for the file and requires no additional space other than the size of the file and has no CPU intensive merging processes.





2 Creating & logging in to your backup account

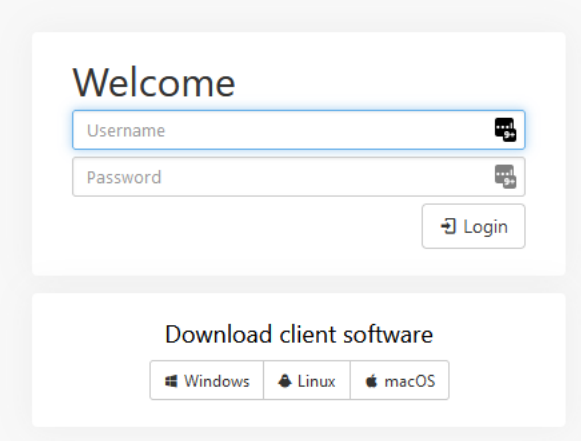
2.1 Creating your Gigasoft Backup account

During the first stages of release Gigasoft will create your account for you, you will then be asked to login to the client and change the password to one that only you know, this is not the encryption key, the encryption key is generated by the system and only the system knows what this is.
Soon there will be a facility for you to create your own accounts.

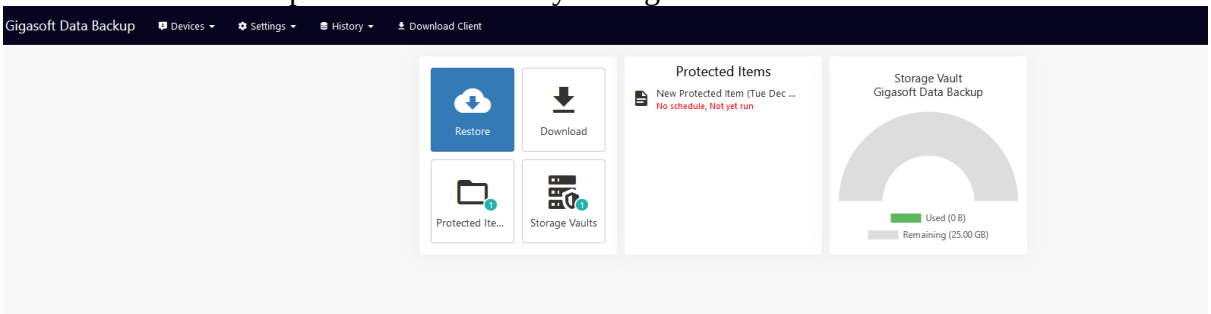
2.2 Logging into your Gigasoft Backup account

Once your account has been created you can download and install the client to configure your backups, you also have a web console that you can log into to get an overview of your account and make changes to your protected items

To login to your customer portal please navigate to https://stratus.gigasoftdatabackup.org



Now select the **User** option and then enter your login details



Once logged in you will see a screen like this, as this is a new account there isn't much to look at but as you add protected items and devices this page will populate with more information as well as backup reports.
From the main page you can perform a restore to one of your devices, there is a direct download page, so you can easily get the installer should you wish to add further devices.
The protected items button shows you all the protected items you have configured across all your devices and allows you to create new protected items for your devices, this is where you would configure your protected items for command line Linux installs.
The Storage vault button gives you an overview of all the storage vaults you have (local and offsite) it also shows how much space you are using.

3 Downloading Gigasoft Backup

Please navigate to the user portal https://stratus.gigasoftdatabackup.org and select the appropriate download option.

4 Gigasoft Backup installation

4.1 Windows

4.1.1 System requirements

- ***x86_32+SSE2*** or ***x86_64*** CPU architecture
- Minimum 1024x600 screen resolution
- We recommend using any version of Windows still under active security support from Microsoft (e.g. Windows 7, Windows 10, Windows Server 2008 or newer). Older versions of Windows might work but are not supported by Gigasoft.

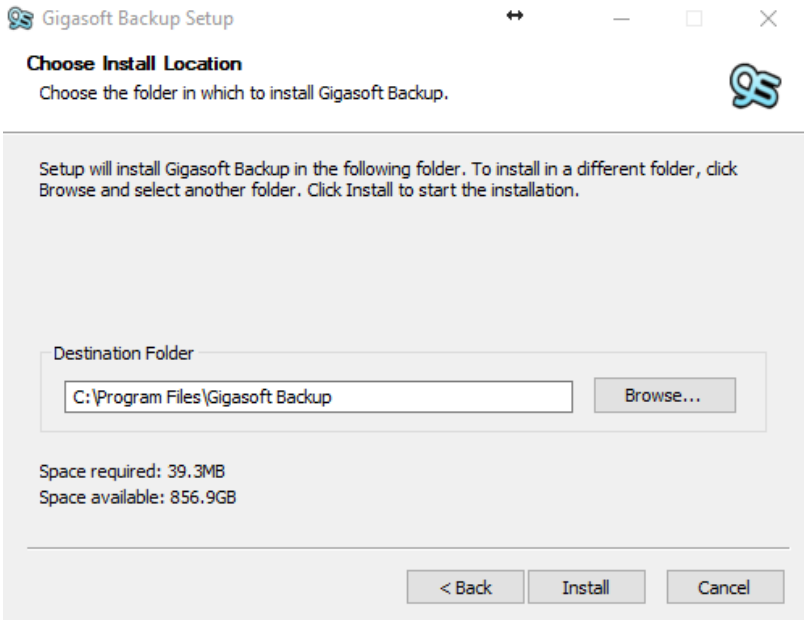
Not compatible with Windows XP (released 2001)

At the time of writing, there is no version of Gigasoft Backup available for Windows XP / Server 2003. All versions of Gigasoft Backup rely heavily on features that were only introduced in Windows Vista / Server 2008.

Windows XP / Server 2003 no longer receives security patches from Microsoft. *It is unsafe to connect such a machine to the internet*.

4.1.2 Install

Extract the ***Gigasoft Backup x.x.x.zip*** file and then run the ***Gigasoft Backup x.x.x.exe*** file and follow the prompts.



Once installed, the client software prompts for account details to log in.

4.1.3 Silent install (advanced)

Gigasoft Backup 17.12.0 or later allow you to install and configure the software silently, by running ***Gigasoft Backup x.x.x.exe /CONFIGURE=user:password*** via your remote management software.

4.1.4 Upgrading / Downgrading

The installer will safely remove and upgrade / downgrade any prior version of Gigasoft Backup, Upgrades / downgrades are usually done automatically but there may be occasions where we may ask you to manually upgrade or downgrade your client to resolve a problem.

4.1.5 Uninstall

The software can be uninstalled via the "Programs and Features" section in the Windows Control Panel.
Uninstalling the software preserves any username/password credentials saved on this computer. To remove the saved credentials, delete the ***AppData/Roaming/backup-interface/config.sys file***.

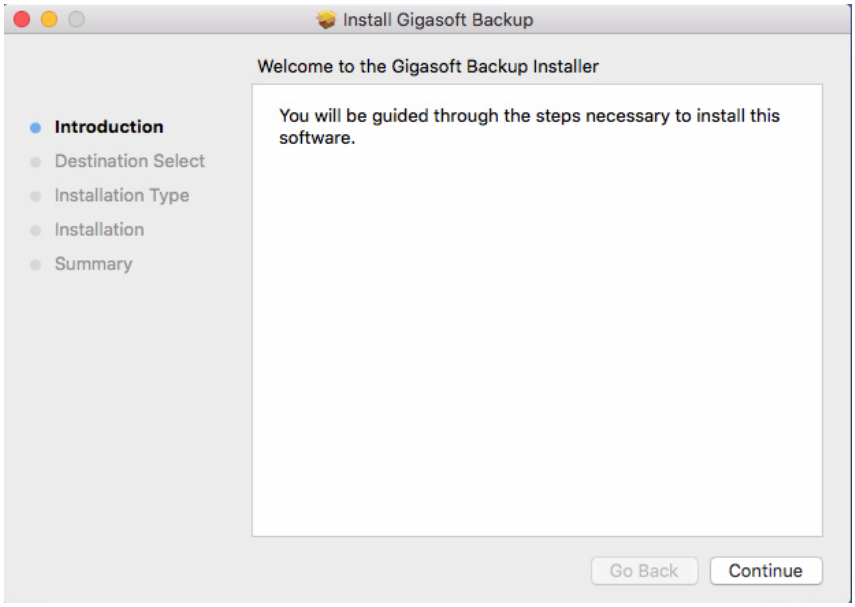
4.2 MacOS

4.2.1 System requirements

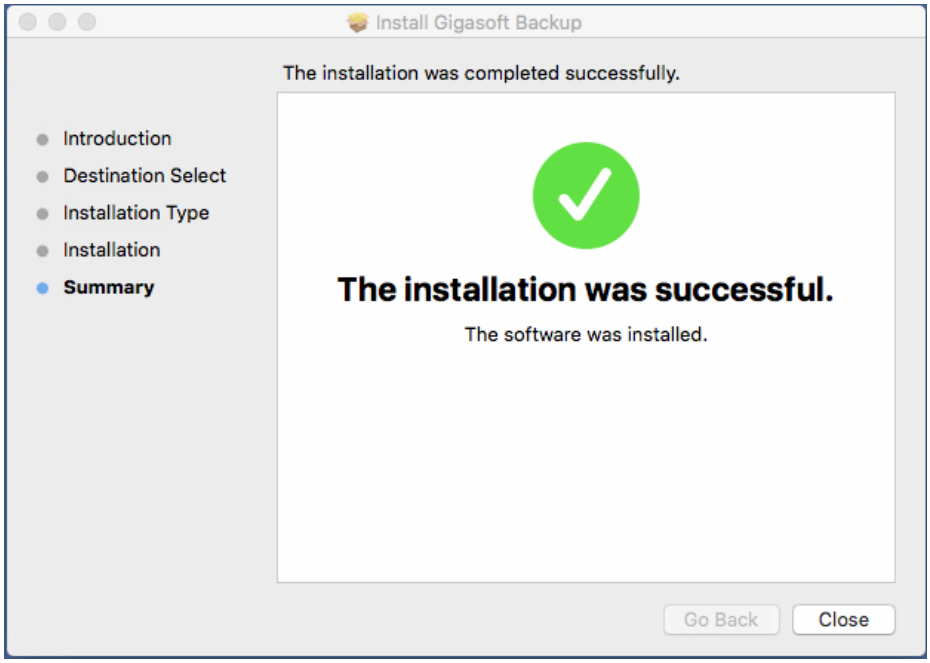
- `x86_64` or Apple silicon CPU
  - `x86_64h` is supported
- macOS 10.11 "El Capitan" or later
  - We recommend using a version of macOS that receives ongoing security support from Apple (usually the last 3 versions)
  - macOS 10.12.1 is required for Let's Encrypt's ISRG Root X1
  - macOS 11.0 is required for Apple silicon

4.2.2 Install

After downloading the ***Gigasoft Backup x.x.x.pkg*** file, right click on it and choose **Open** to start the install.



Click ***Continue*** to move on with the installation.



Click on the ***Close*** button and you should see a login screen.
Please refer to the section Getting started with Gigasoft Backup for the next steps.

4.2.3 Uninstall

MacOS does not have a standard system for uninstalling programs. However, you can still uninstall Gigasoft Backup by running the following command from a terminal window:
sudo -u root "/Applications/Gigasoft Backup.app/Contents/Resources/uninstall"

This will automatically stop all running GBM processes, unregister GBM's launchd services, and remove all application files from the disk.

Uninstalling the software preserves any username/password credentials saved on this computer. If you also want to remove the saved username/password credentials, add this command-line:

sudo -u root "/Applications/Gigasoft Backup.app/Contents/Resources/uninstall" --also-remove-saved-passwords

4.3 Linux (Debian, Ubuntu)

4.3.1 Not currently released

Future versions of Gigasoft Backup will provide *.deb* packages for Debian, Ubuntu, and compatible distributions. In the meantime, you can install Gigasoft Backup using the "Other Distribution" package.

4.4 Linux (Red Hat Enterprise Linux (RHEL), CentOS)

4.4.1 Not currently released

Future versions of Gigasoft Backup will provide *.rpm* packages for RHEL, CentOS, and compatible distributions. In the meantime, you can install Gigasoft Backup using the "Other distribution" package.

4.5 Linux NAS (Synology)

Since GBM 21.12.6, branded Synology SPKs can be generated and downloaded from the GBM Server web interface. The web interface offers two downloads for Synology: one for DSM 6 and one for DSM 7. Due to Synology packaging rules, these SPKs are not interchangeable.

SPKs are available for Synology NAS' which meet the following requirements:

- CPU: x86_64, i686, ARMv7, or ARMv8
- DSM version: 6 or 7

The Synology SPK does not include a graphical client. Instead, creating Protected Items and running backups and restores can be done from your GBM Server.

4.5.1 Installation

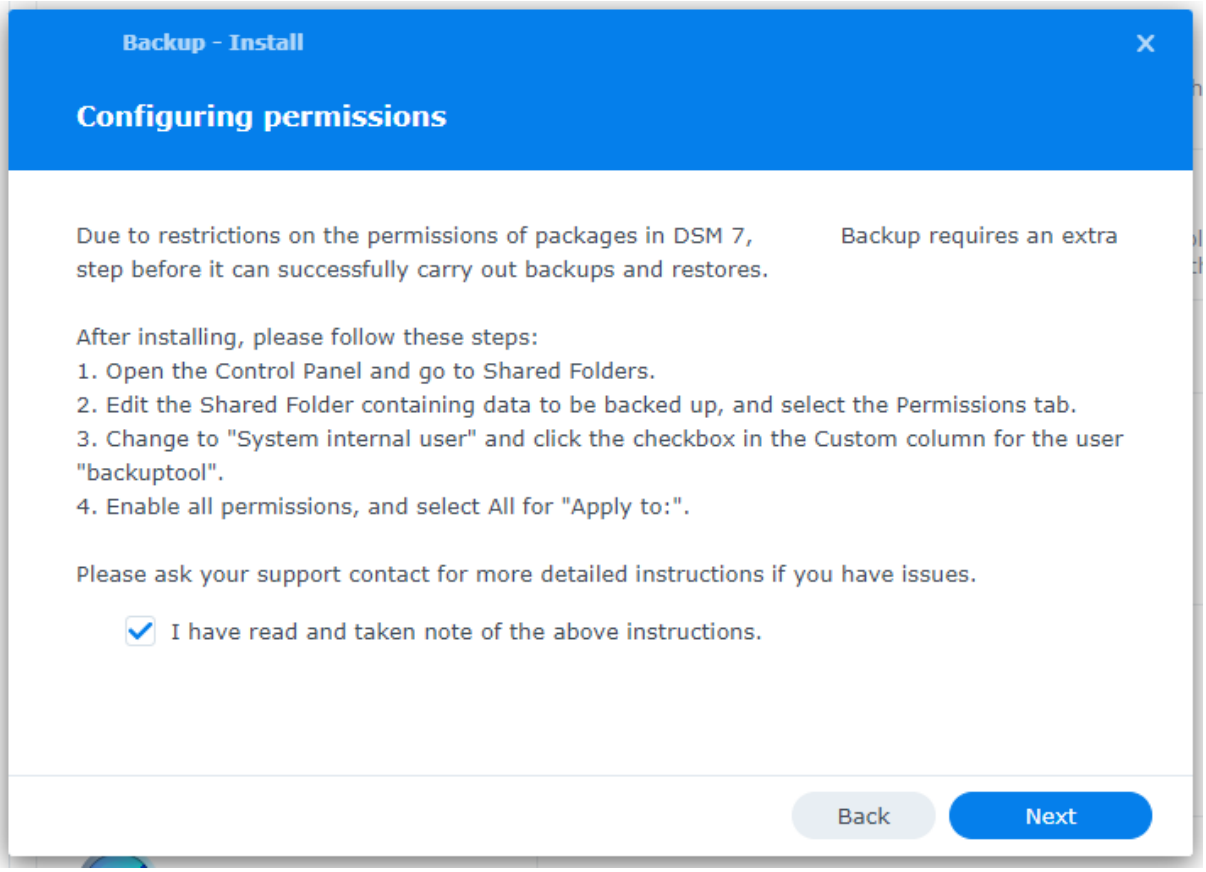
DSM 6 only: Installation of packages published by any publisher must be allowed before GBM can be installed. This setting can be enabled from the Package Center; in `Settings > General > Trust Level`, select the "Any publisher" radio button and accept the settings.

Installation of GBM on a Synology NAS follows the same process as installing any other SPK:

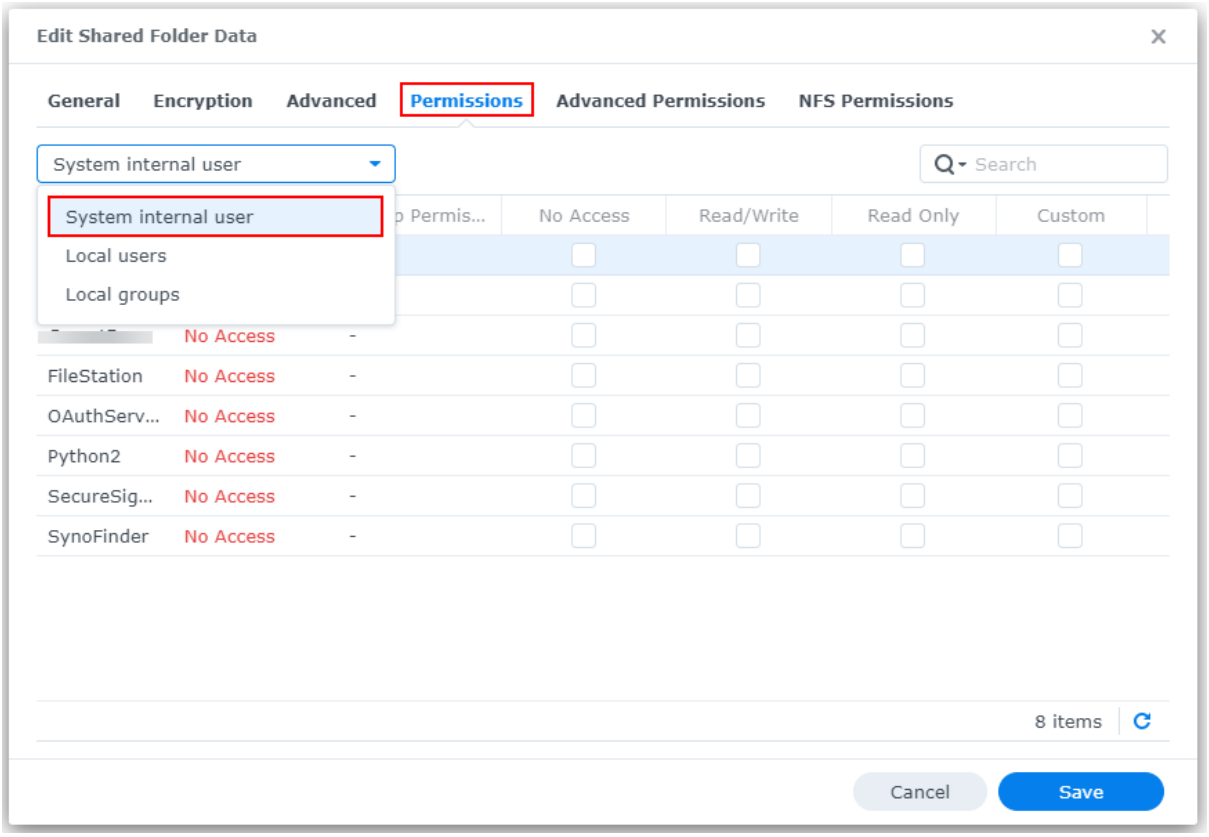
1. Open the Package Center
    - If on DSM 6, ensure the settings noted above have been applied.
2. Click "Manual Install" in the top right
3. Upload the `.spk` file downloaded from GBM Server
    - If on DSM 7, accept the prompt to allow the installation of a third-party package.
4. Accept the license agreement
5. Enter credentials the appropriate GBM Server and user
    - If a previous version of GBM has been installed on the NAS and its settings were not removed when it was uninstalled, the installer will automatically detect the credentials. Leaving all fields blank will reuse the existing credentials; new credentials can also be entered as usual and will take precedence.

4.5.2 Permissions

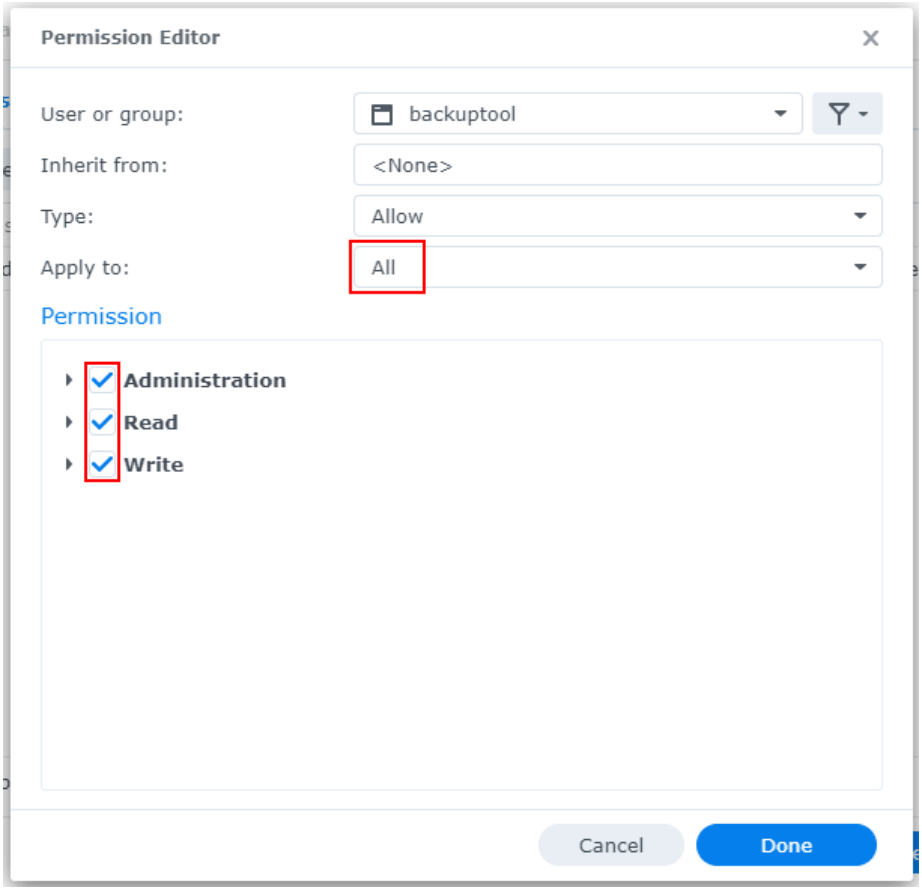
On DSM 7, GBM runs a special package-specific user named `backuptool`. In order to perform backups and restores, this user must be granted permissions to access the appropriate Shared Folders. *This does not apply to DSM 6*.



1. Log in to the Synology NAS
2. Open the Control Panel and go to Shared Folders
3. Select the Shared Folder containing the data to be backed up and click Edit
4. In the Permissions tab, select "System internal user" from the dropdown menu on the left



5. For the user `backuptool`, click the checkbox in the Custom column
6. In the dialog that appears, ensure the following:
    1. "Apply to:" is set to "All"
    2. All permissions are checked



4.5.3 Limitations

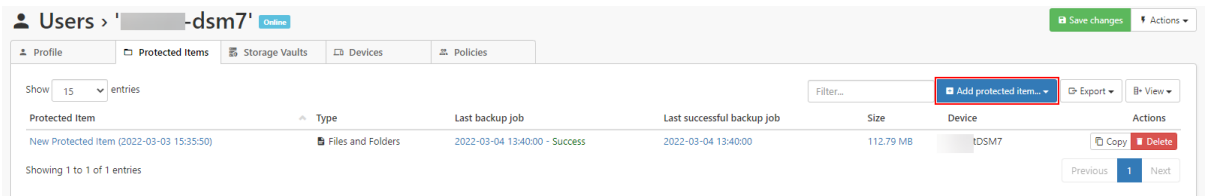
Due to restrictions placed on packages by Synology for DSM 7, GBM runs as a special package-specific user, which results in some limitations:

- Remote upgrade/uninstall is not supported. This is because third-party SPKs are no longer allowed to run as root, which means GBM cannot initiate a package upgrade/uninstall from within a package itself.
- When performing a restore to a Synology NAS, permissions/ownership may not be restored correctly. This is because a package user is not allowed to `chown` to a user other than themselves.

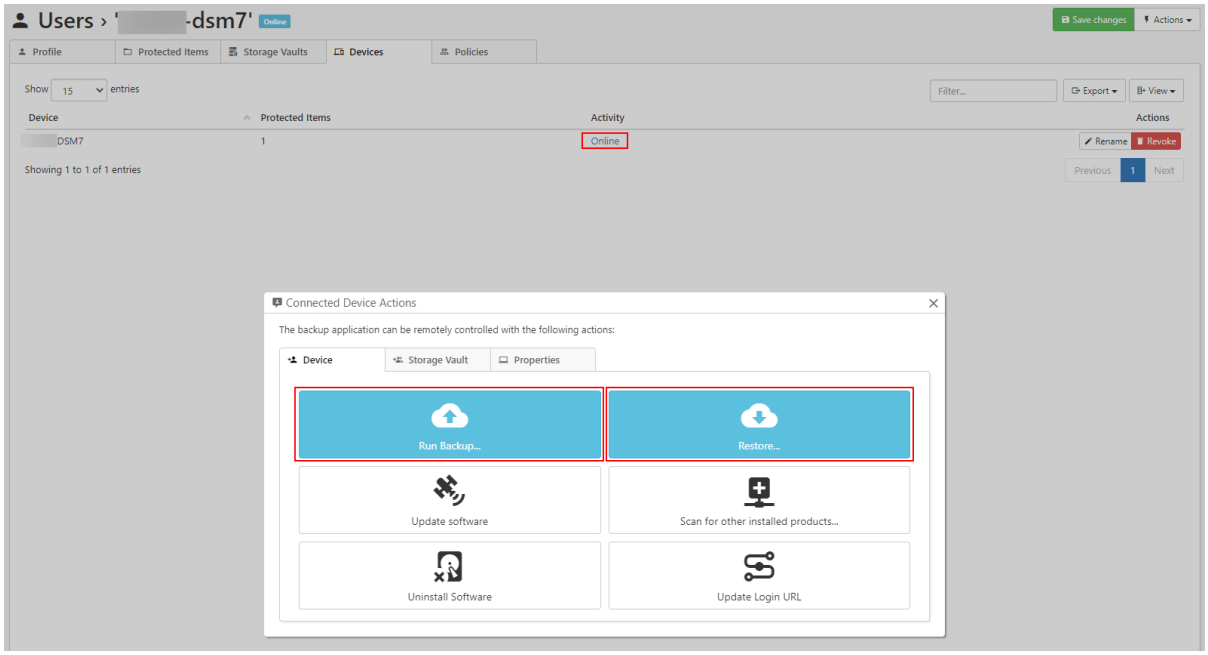
4.5.4 After installation

The Synology SPK does not provide a graphical client for GBM. Creating Protected Items and manually running backups or restores is done from the GBM Server web interface.

Creating a Protected Item can be done from the Protected Items tab on the user's page:



Backups and restores can be run by selecting the connection to the online Synology device from the Devices tab on the user's page:



4.6 Linux (Other Distribution)

This is a distribution-agnostic package that can be used if Gigasoft does not have a more specific package available for your Linux distribution.

Please note that in order to avoid distribution-specific differences, the package does not automatically start on boot. You should configure your system to run the launch script in ***/opt/*** on boot (e.g. via a systemd unit, upstart script, ***/etc/init.d/*** script, or a line in ***init.rc***).

4.6.1 System requirements

- CPU: x86_64, or x86_32 with SSE2, or ARM (see below)
- Kernel 2.6.23 or later
- Support for ISRG root X1 certificates for Let's Encrypt requirements
- Unique SSH host keys (this can be an issue with cloned VMs)
- Dependencies
    - bash, xz, GNU awk, and standard GNU/Linux system utilities
    - ca-certificates and tzdata (see below)

ARM CPU support

Gigasoft Backup is available for multiple ARM platform variants. The Gigasoft Backup installer will select the best available binary for your hardware at install-time.

The following platform variants are supported:

Platform	Description
ARMv8l	ARM 64-bit (Aarch64), no glibc required
ARMv7l	ARM 32-bit with vfp, and a glibc-based OS with the "hard-float" ABI (gnueabihf)
ARMv6kl	ARM 32-bit with vfp, no glibc required

Timezone database dependency

Gigasoft Backup on Linux requires the OS to provide an up-to-date timezone database, to perform timezone calculations

- On many Linux distributions, installing the tzdata or timezone package should be sufficient
- Otherwise, GBM will look for a timezone database in all of the following locations;
  - /usr/share/zoneinfo
  - /usr/share/lib/zoneinfo
  - /usr/lib/locale/TZ

CA certificate database dependency

Gigasoft Backup on Linux requires the OS to provide an up-to-date set of root certificate authorities, to validate HTTPS / SSL connections.

- On many Linux distributions, installing the ca-certificates package should be sufficient
- Otherwise, GBM will look for a certificate bundle in all of the following locations;
  - /etc/ssl/certs/ca-certificates.crt (used by Debian/Ubuntu/Gentoo etc.)
  - /etc/pki/tls/certs/ca-bundle.crt (used by Fedora/RHEL 6)
  - /etc/ssl/ca-bundle.pem (used by OpenSUSE)
  - /etc/pki/tls/cacert.pem (used by OpenELEC)
  - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem (used by CentOS/RHEL 7)

4.6.2 Install

Run the .run file. This is a self-extracting archive.

The installer will

1. install the software into a branded /opt/BRANDNAME/ subdirectory
2. prompt you for an initial username and password
3. register the current Linux device into that GBM account
4. start running Gigasoft Backup in the background.

If you make a mistake with the username/password prompt, you should follow the instructions below to completely remove the software, and then start the installation again.

Linux Installation options

You can control the installer by setting environment variables in your shell before running the .run file.

The following options are available:

- WRITE_INSTALL_LOG. Set this to a file path, to record details of the installation.
- OVERRIDE_INSTALL_SERVER. Set this to a URL (including http/https and trailing slash) to override the GBM Server URL used by Gigasoft Backup.

You can set an environment variable in bash either on the same line (e.g. WRITE_INSTALL_LOG=install.log ./install.run) or as a separate export command (e.g. export WRITE_INSTALL_LOG=install.log followed by ./install.run).

Silent installation (Linux advanced)

GBM allows you to install and configure the software silently by running (echo $username ; echo $password ;) | ./install.run via your remote management software.

4.6.3 Restarting at boot

The installer creates a backup-daemon-start.sh script that can start the service. The Gigasoft Backup agent on "Other Distribution" Linux can be restarted by running the backup-daemon-start.sh script.

In order for Gigasoft Backup to start after a system reboot, you must configure this script to be run on system boot. Different Linux distributions support different methods for running commands on system boot: choose the most appropriate method for your Linux distribution. Some common choices are documented below.

Preserve HOME environment variable

GBM uses the $HOME environment variable to find its saved credentials. When configuring GBM to start at system boot, ensure that the $HOME environment variable is set (i.e. to /root/), to ensure that GBM can find its saved credentials. If GBM is unable to log in, it's possible that your Linux distribution does not set $HOME at this early-boot stage. In that case, you should try running HOME=/root/ /opt/GigasoftBackup/backup-daemon-start.sh & instead. GBM 19.8.0 and later will automatically try to use /root/ as the $HOME directory if $HOME is not already set or if it is set to a blank path.

Note: If you execute the .run installation script as root, this may have different results than if you execute the .run script using an elevated terminal session with 'sudo'. The 'sudo' command preserves the $HOME variable on Ubuntu; whilst on Debian the $HOME variable is erased, and sudo then sets it to the home directory of the originating user.

Start in the background

If you are running commands over SSH, please be aware that the backup-daemon-start.sh script runs in the foreground and will die when the SSH session is closed. You can avoid this by running the script in the background.

You can run the script in the background (daemonize) by using the backup-daemon-start-background.sh file instead.

Prior to GBM 19.5.0, the backup-daemon-start-background.sh file is not available, and you must daemonize it yourself via nohup / disown / double-fork (e.g. (cd /opt/GigasoftBackup ; ./backup-daemon-start.sh >/dev/null 2>/dev/null &) &).

4.6.4 Run at start up

The installer includes a ***backup-daemon-start.sh*** script that can start the service. It is recommended that you configure this script to be demonised on system boot, by writing either an ***init.d*** script, ***systemd*** unit, or ***rc.local*** entry, depending on your specific Linux distribution.

4.6.5 Start-up via *rc.local*

You can make Gigasoft Backup start at system boot by adding an entry to the ***rc.local*** file.

First, find the ***rc.local*** file on your system:

- ***/etc/rc.local*** (Debian/Ubuntu)
- ***/etc/rc.d/rc.local*** (CentOS/RHEL)

Add the following content to the ***rc.local*** file:

/opt/GigasoftBackup/backup-daemon-start.sh &

If the ***rc.local*** file contains an ***exit 0*** statement, the additional command should be added ***before*** such a statement.

If you are using CentOS 7, rc.local is no longer executed by default due to systemd changes, to make this work please use the following command

Chmod -x /etc/rc.d/rc.local

With Debian add ***sleep 1m*** to give a bit of time for the system to start before trying to run Gigasoft Backup Manager.

Now Gigasoft Backup Manager will start automatically when the system restarts.

4.6.6 Start-up via *rc.d*

You can make Gigasoft Backup start at system boot by adding a file to the rc.d directory.

First, find the rc.d directory on your system:

- /usr/local/etc/rc.d (Synology DSM 6.1+)

Add a new file to the rc.d directory with the following contents:

#!/bin/bash
/opt/GigasoftBackup/backup-daemon-start-background.sh

Mark the file as executable: chmod +x /usr/local/etc/rc.d/my-Gigasoft-startup-script.sh

4.6.7 Start-up via *cron*

You can make Gigasoft Backup start at system boot by adding an entry to ***root's*** crontab.

1. Run ***crontab -e -u root*** to launch a crontab editor
2. Add the line ***@reboot /opt/GigasoftBackup/backup-daemon-start.sh***

4.6.8 Start-up via *init.d*

No further documentation is available for this topic.

4.6.9 Start-up via systemd

You can use the following unit as an basic example:

```
[Unit]
Description=Gigasoft Backup Client
After=network-online.target

[Service]
Type=simple
RemainAfterExit=true
User=root
ExecStart=/opt/GigasoftBackup/backup-daemon-start.sh

[Install]
WantedBy=multi-user.target
```

This unit file correctly starts the Gigasoft Backup service at system boot.

However, the process management in systemd is not fully compatible with the way GBM's multi-process model works. In particular, there are compatibility issues with the software updater. As a result, the above unit is (A) unable to take advantage of process group cleanup; (B) unable to auto-restart the Gigasoft Backup agent service; and (C) after a software upgrade, GBM will keep running but the unit will remain in "exited" state.

A future version of Gigasoft Backup for Linux may change the updater system to work more seamlessly with systemd unit files.

4.6.10 Upgrading / Downgrading

The "Other Distribution" version of GBM supports upgrading the software, with some caveats:

- The .run file will automatically upgrade the existing version
- The software can be remotely upgraded via the GBM Server web interface.

Note: If you delete the GBM directory and all its contents in /opt/, this will trigger a full-reinstallation of the client software, requiring the username and password.

4.6.11 Uninstall

To uninstall "Other Distribution" versions of Gigasoft Backup, you should

1. Stop all Gigasoft Backup processes

2. Remove the relevant subdirectory under ***/opt/ i.e rm -r GigasoftBackup***
3. Remove any custom start up scripts

4.6.12 Change password on Linux Client

Use the 'Change Password' function in the client web interface, or change the password in the admin web interface.

Then fully uninstall and reinstall the client, using the new credential. Your device settings and Protected Items will be preserved.

5 Getting started with Gigasoft Backup

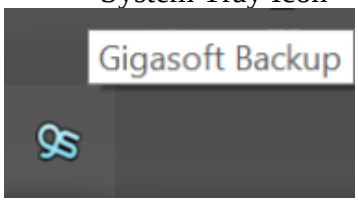
This chapter describes the various features available in the backup client application.

5.1 System tray and desktop icon

5.1.1 System tray and desktop icon (Windows)

After a successful installation of Gigasoft Backup, a system tray and desktop icon will be installed, the tray icon will be displayed under the Windows system tray area.

System Tray Icon



Desktop Icon

5.1.2 System tray and desktop icon (Mac)

Dock Icon

Menu Bar Icon

5.2 Login dialog

5.2.1 Windows

To open double-click on the Gigasoft Backup desktop icon or right-click on the system tray icon and select the **[Show Interface]** option

5.2.2 MacOS

To open click on the Gigasoft Backup icon located in the menu bar and select the **[Show Interface]** option, you can also click on the docked icon if the interface is already open and minimised.

5.2.3 Linux (Command Line)

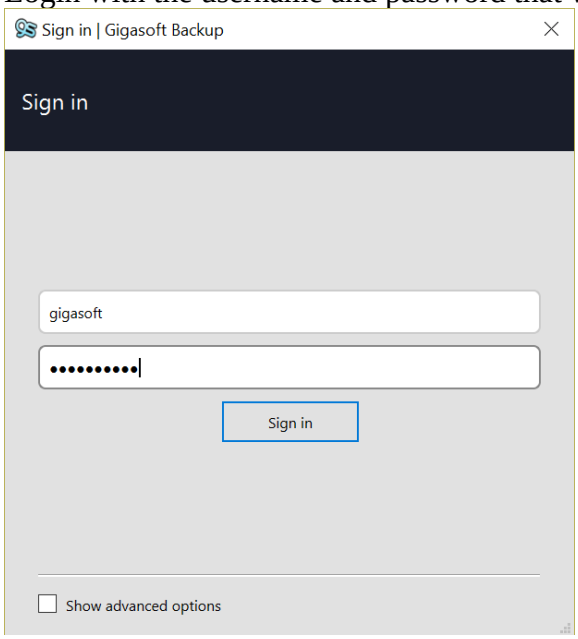
Currently the Linux version is command line only, once you have installed and set the options to start after reboot there is nothing else that needs to be done, the client will stay logged in automatically.

5.3 Gigasoft Backup 1st time use & device registration

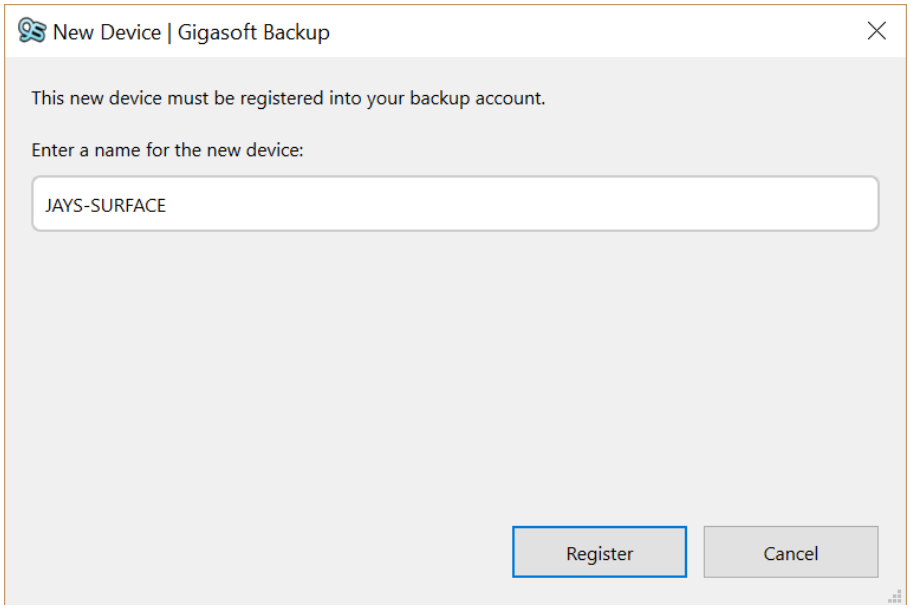
Gigasoft Backup can be used on multiple devices on a single account, each device needs to be registered the first time it is installed, once registered to an account you are able to configure protected items and view / restore protected items from other devices on your account.

5.3.1 Gigasoft Backup 1st time use & device registration (windows)

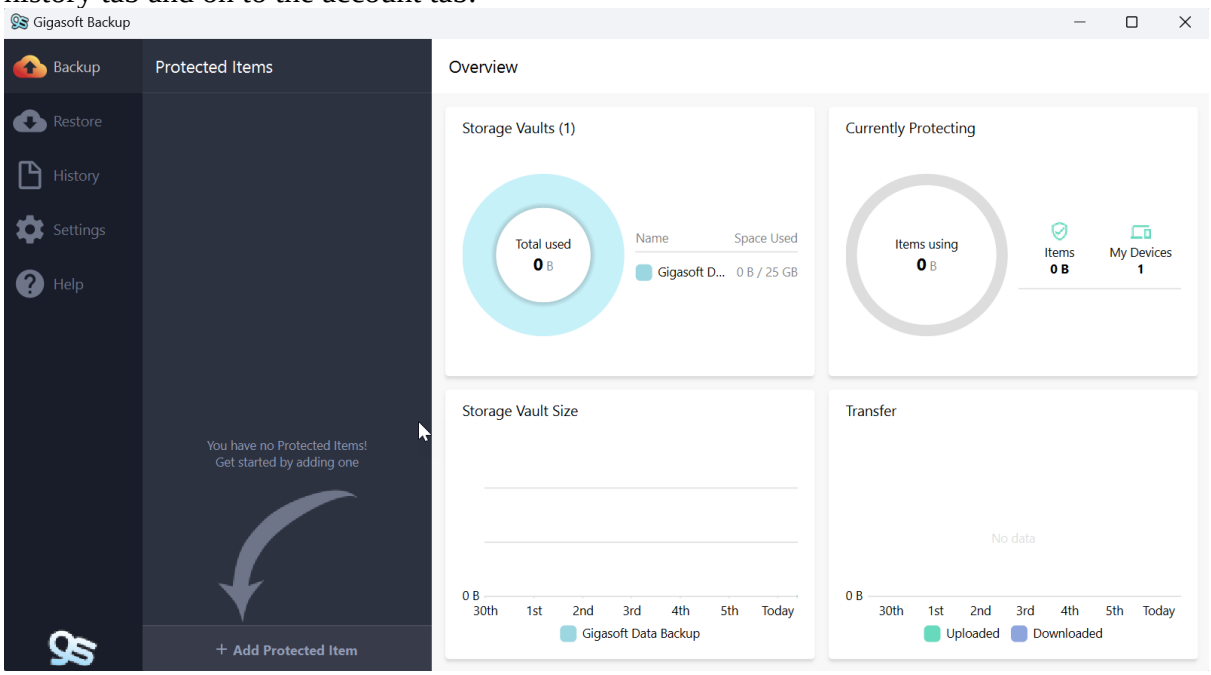
In this section we will cover the first steps needed to open Gigasoft Backup and register the device ready for use using the Windows client.
Open the client using either the desktop icon or the system tray icon, you will be presented with a login screen.
Login with the username and password that was setup from the portal.



Once you have logged in for the first time you will be presented with a register device screen, Gigasoft Backup picks up the name of the device you are using and displays it within the new device screen, simply click the **[Register]** button and the device will be registered to your account

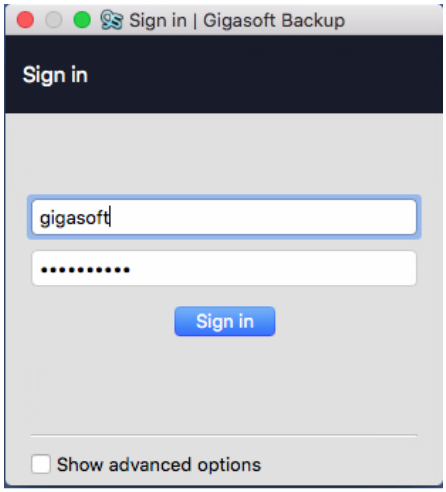


Now you have registered your device you will be asked to change the password from the one that was created for you to one that only you know, this will only happen on the first device that's installed, once the password has been changed you will see the main dashboard which has some options down the left-hand side of the screen, the following sections in this guide will guide you through setting up a protected item to restoring items and then through the history tab and on to the account tab.



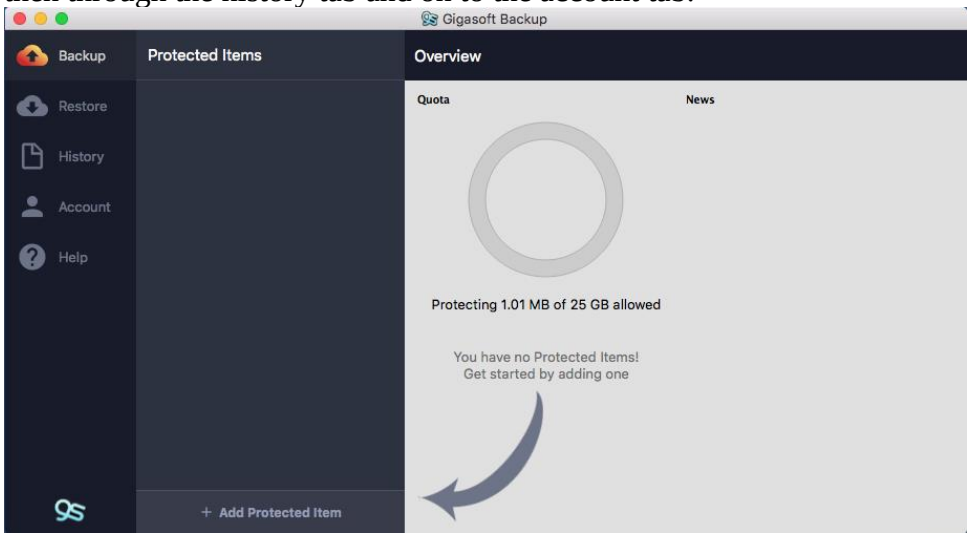
5.3.2 Gigasoft Backup 1st time use & device registration (MacOS)

In this section we will cover the first steps needed to open Gigasoft Backup and register the device ready for use using the Mac client.
Open the client using either the icon in the dock or the system tray icon, you will be presented with a login screen.
Login with the username and password that was setup from the portal.



Once you have logged in for the first time you will be presented with a register device screen, Gigasoft Backup picks up the name of the device you are using and displays it within the new device screen, simply click the **[Register]** button and the device will be registered to your account

Now you have registered your device you will be prompted to change the password from the one that was generated for you to one that only you know, this will only happen on the first device that is added to the account, once you have changed the password you will see the main dashboard which has some options down the left-hand side of the screen, the following sections in this guide will guide you through setting up a protected item to restoring items and then through the history tab and on to the account tab.



5.3.3 Gigasoft Backup 1st time use & device registration (Linux)

With the command line version there is no 1st time use or device registration steps as this is all done as part of the installer.

5.3.4 Two-factor authentication for end-users

Two-factor authentication is available for end-users. TOTP is supported.

You can set up a TOTP code in the Gigasoft Server web interface. If so, the TOTP code will also be required when using the Gigasoft Backup desktop app.

WARNING: This is a limited-security feature only, protecting only (A) registering new devices; (B) opening the desktop app; and (C) logging in to the Gigasoft Server web interface as an end user. Because backup jobs need to run unattended without 2FA prompting, this feature does not provide full 2FA protection in all cases.

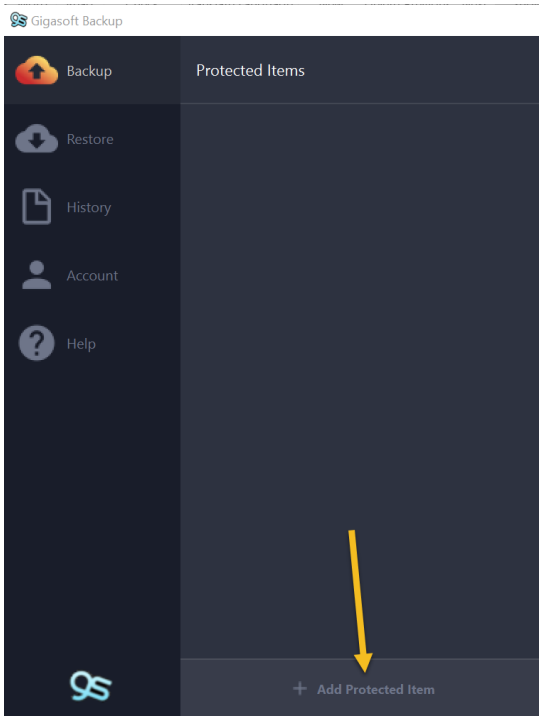
6 Creating protected items

In this section we will guide you through the process of creating the various types of protected item, the idea is to provide a simple step by step walk through of the main steps needed to create a protected item that anyone can easily follow.

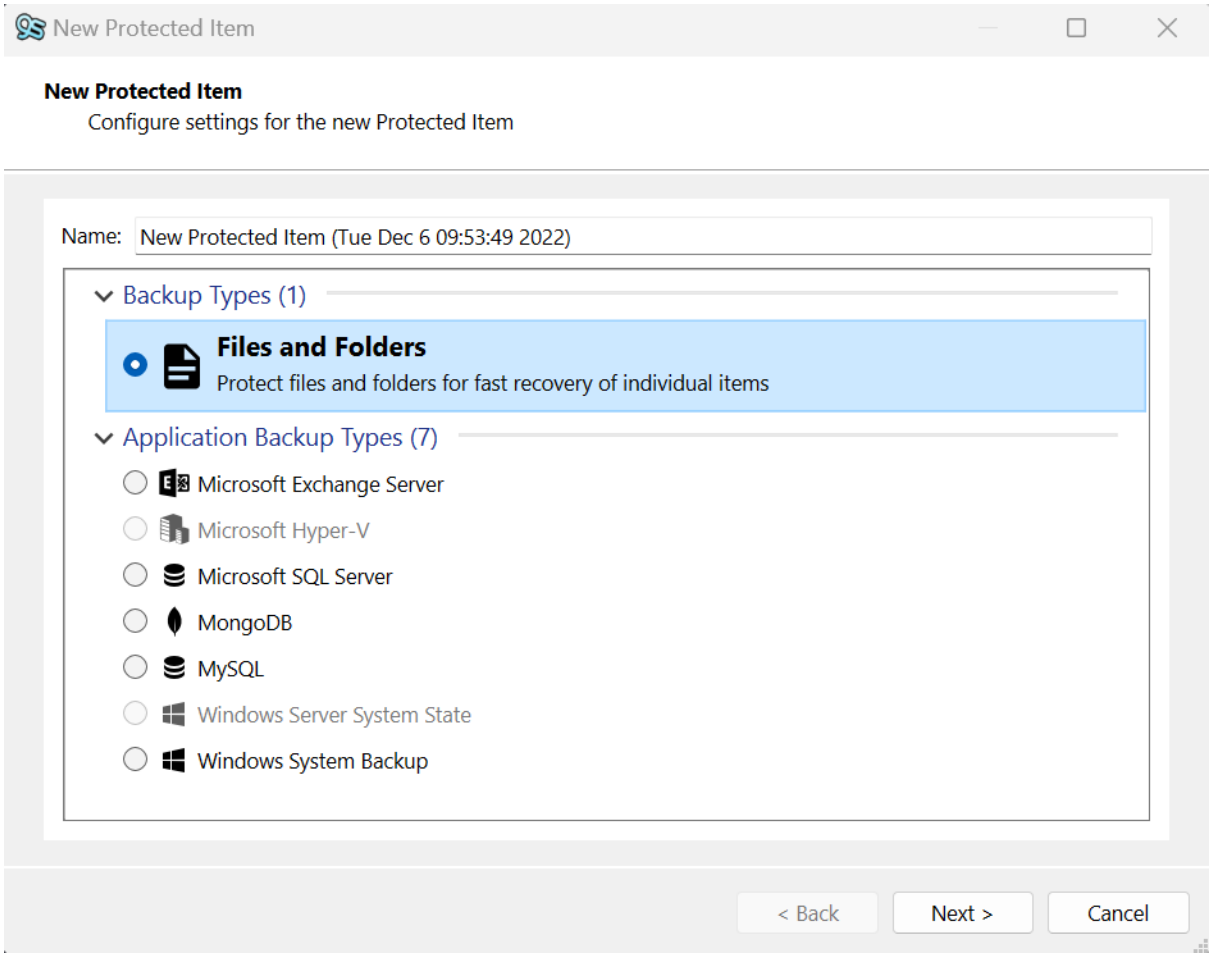
6.1 file protected items

6.1.1 Creating a file protected item (windows)

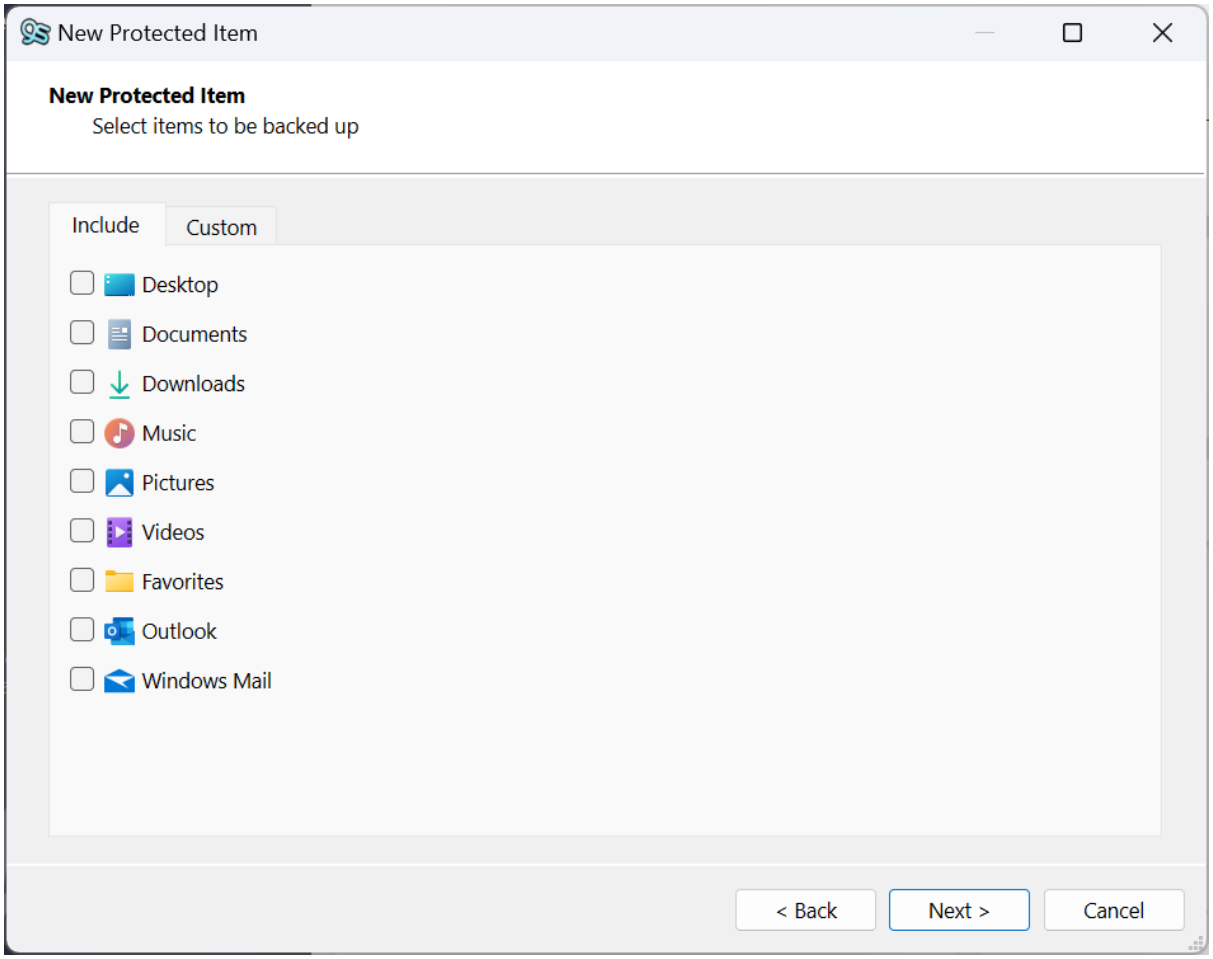
In this section we will go through the steps to create a file protected item.
Once logged in to Gigasoft Backup from the main dashboard click the **[Add Protected Item]** button



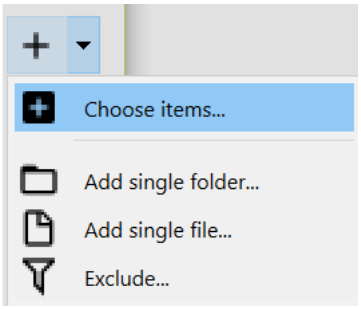
You will then be presented with the new Protected Item screen



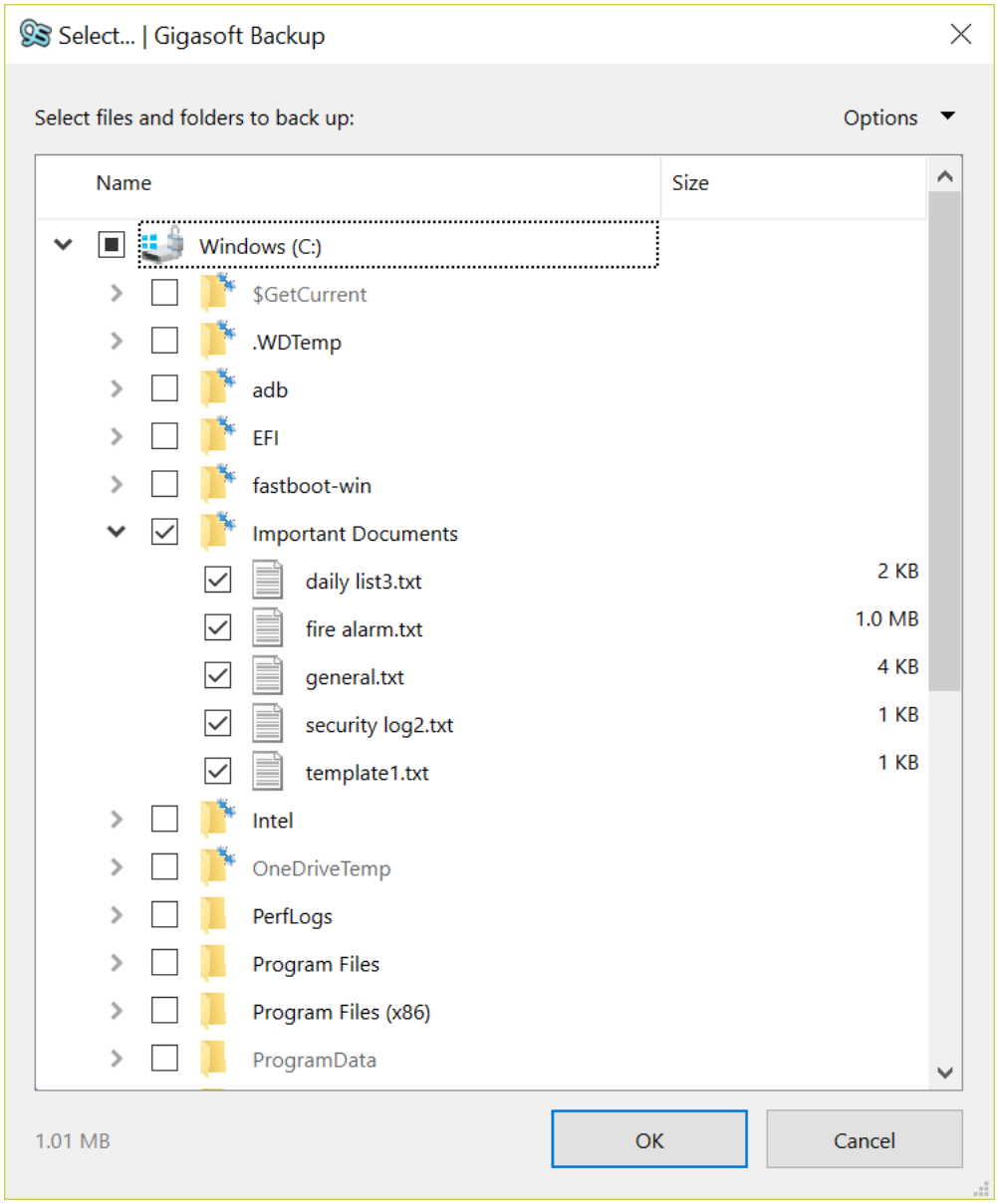
Change the name of the Protected Item to something meaningful so it's easy to identify at a later date and click **Next**



This gives you the basic selection screen where you can select common items, in order to setup a more granular backup click on the Custom tab and click the "+" icon

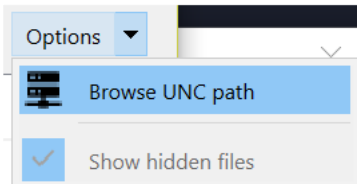


Select the **[Choose items]** option

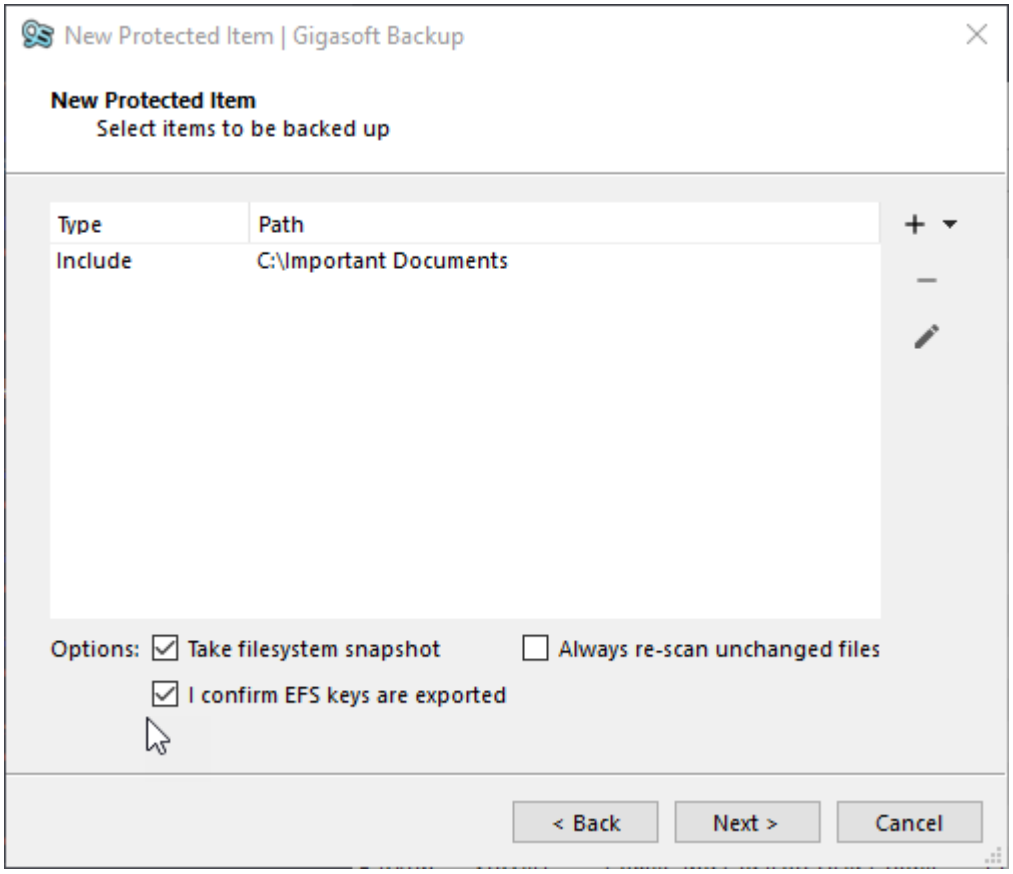


Now you can drill down through the local drives to select the files and folders you wish to backup.

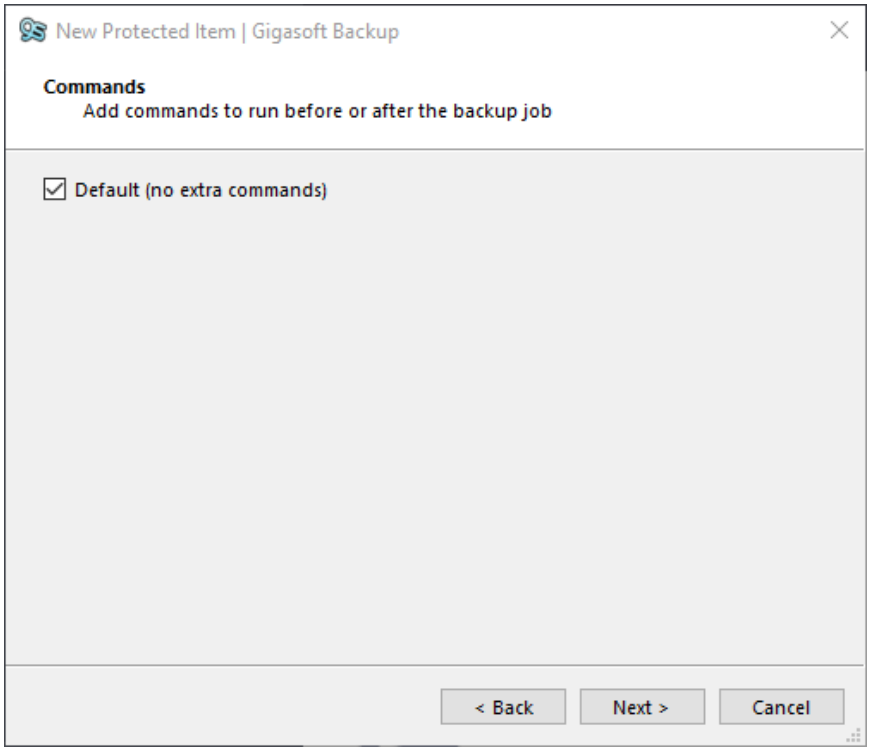
In this example we are just selecting all the files under the folder “Important Documents” notice how in the bottom left of the window the client can detect how much data will be backed up.



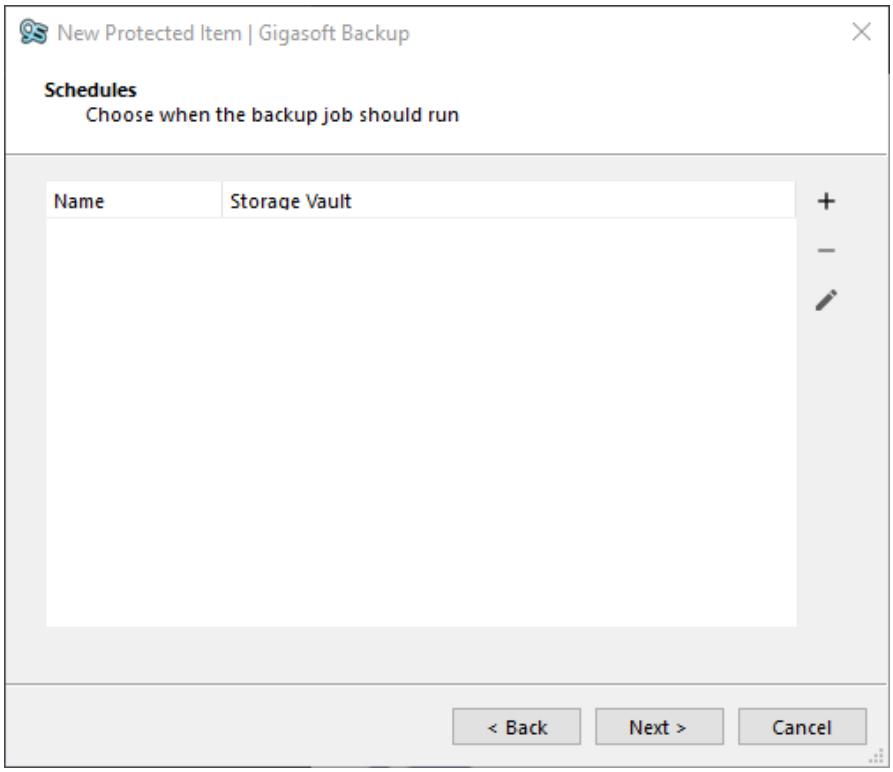
If you need to back up from a network share click on the **[Options]** drop down from the top left and enter the path details.



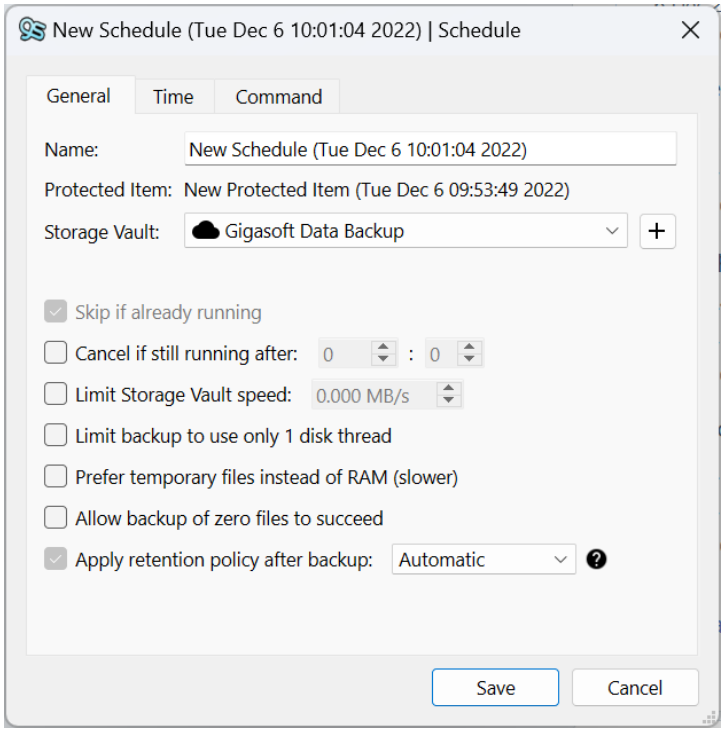
You can select **[Take filesystem snapshot]** if you have problems backing up open or access denied files.
The **[Always re-scan unchanged files]** is useful if you have software that modifies files and does not change the file attributes, this option will scan all files selected even if they have not changed to compare them to what is currently held on the backup server.
If you have encrypted files on your machine the software will attempt to back them up using the same method as a file backup, if the files were encrypted elsewhere then this is not possible so the system will back up the entire file without being able to access it, if this is a case you will receive an error in the backup report advising you about this and to make sure the EFS keys are backed up, you can silence this warning by ticking the **[I confirm EFS keys are exported]** if the keys are not exported you will still be able to restore the files in their encrypted state but you will be unable to access the contents.
Click **Next** to move on to the next stage.



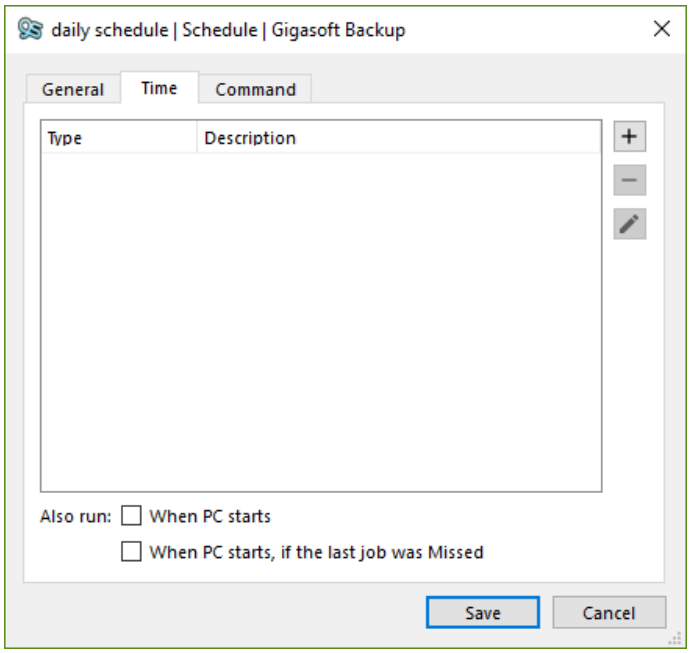
If you need to add any pre backup commands untick the tick box and add any commands you need else you can leave this ticked and click **Next**



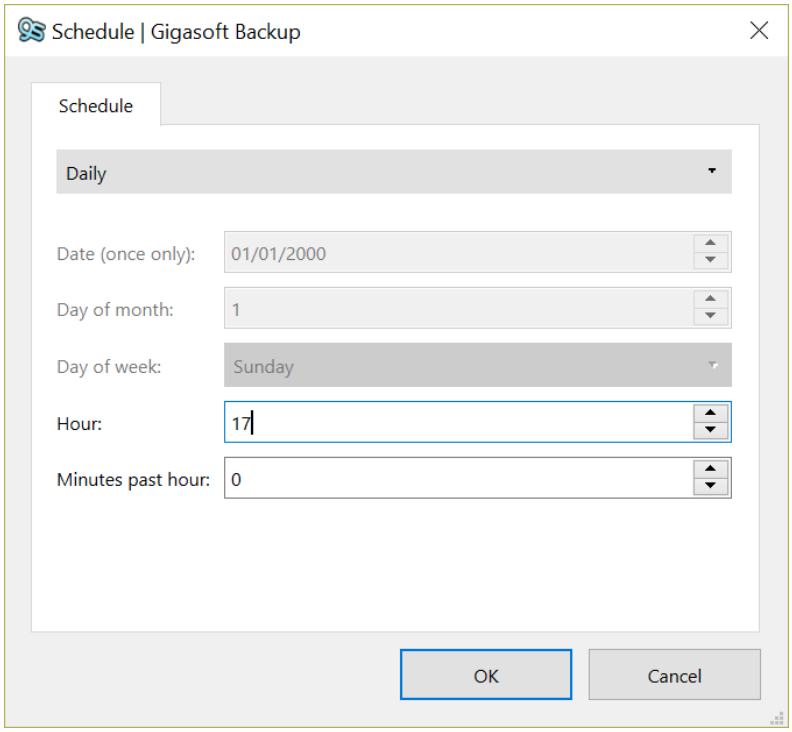
Selecting the **[+]** icon allows you to add a schedule.



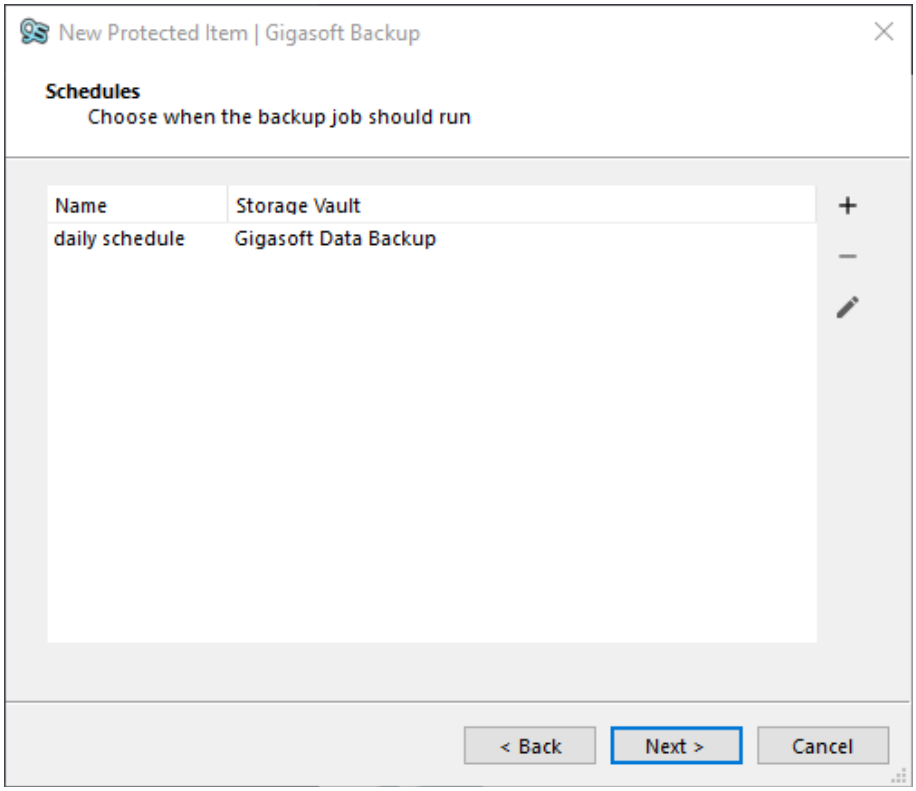
Name the schedule to something meaningful and then decide if you wish the schedule to be skipped if a backup is already running or you can choose to cancel the backup if it runs longer then a pre-determined amount of time, you can also limit the bandwidth available to this protected item, this is especially useful if you have a large amount of data and you don't want it to use all of the available upload bandwidth.
On older machines or machines that are busy we can now request that GBM uses a single disk thread, this causes the backup to take a bit longer but uses less resources, this is useful if you find your machine is running slower than normal when the backup is running.



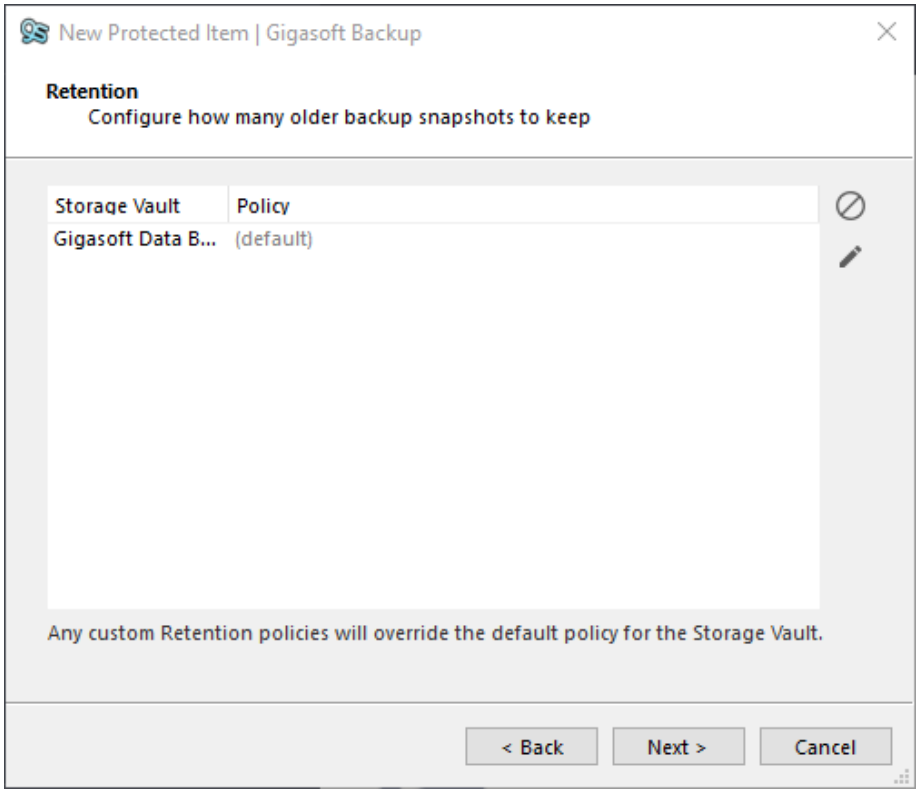
Click on the Time tab and then the **[+]** icon to set the schedule start time.
From here you can also specify that the backup runs when the machine is turned on or run if the machine was turned off and the last scheduled backup was missed.



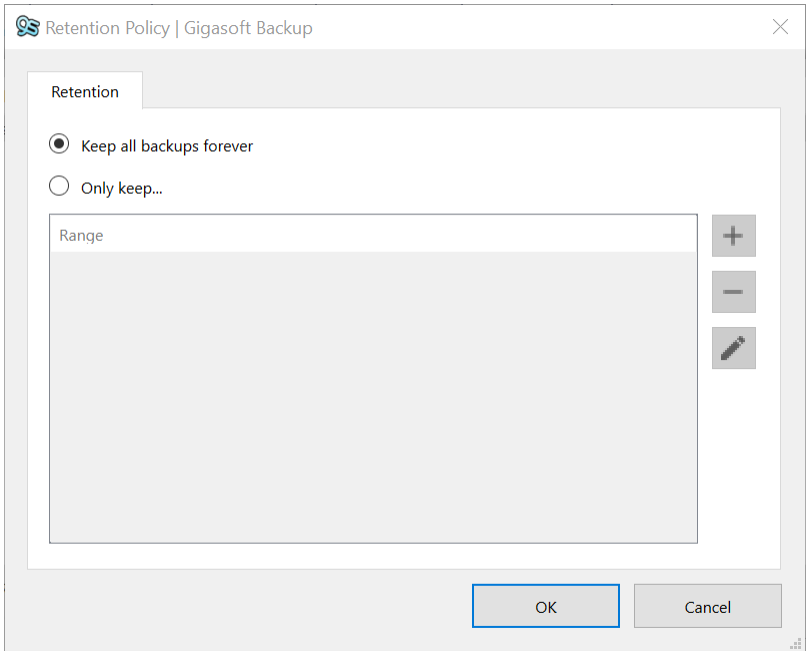
In this example we will choose the Daily schedule and set it to run at 17:00, now click **[OK]**, the Command tab can be used if you want to run pre- or post-commands at the schedule level. Clicking **[Save]** will return you back to the Schedule tab



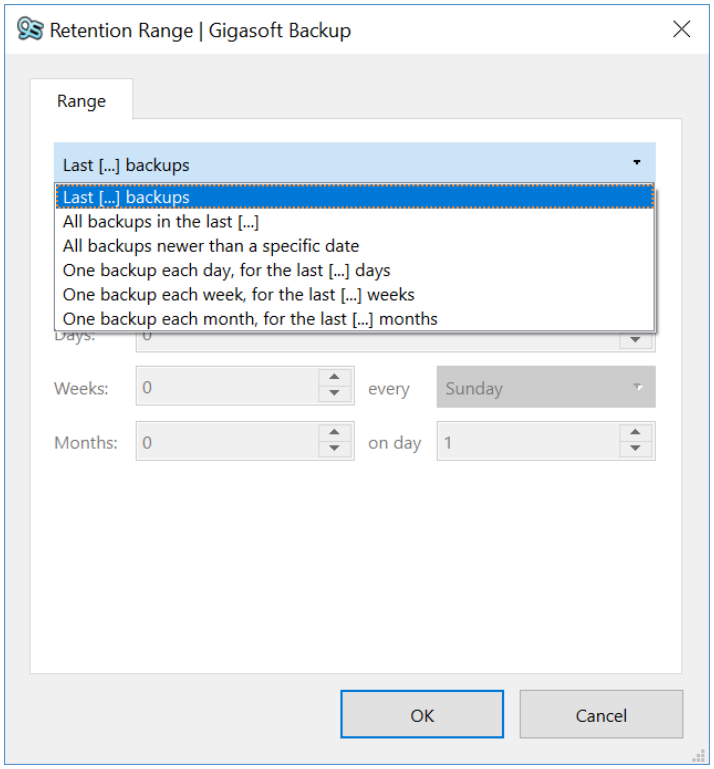
Click **Next** to move on to the retention settings..



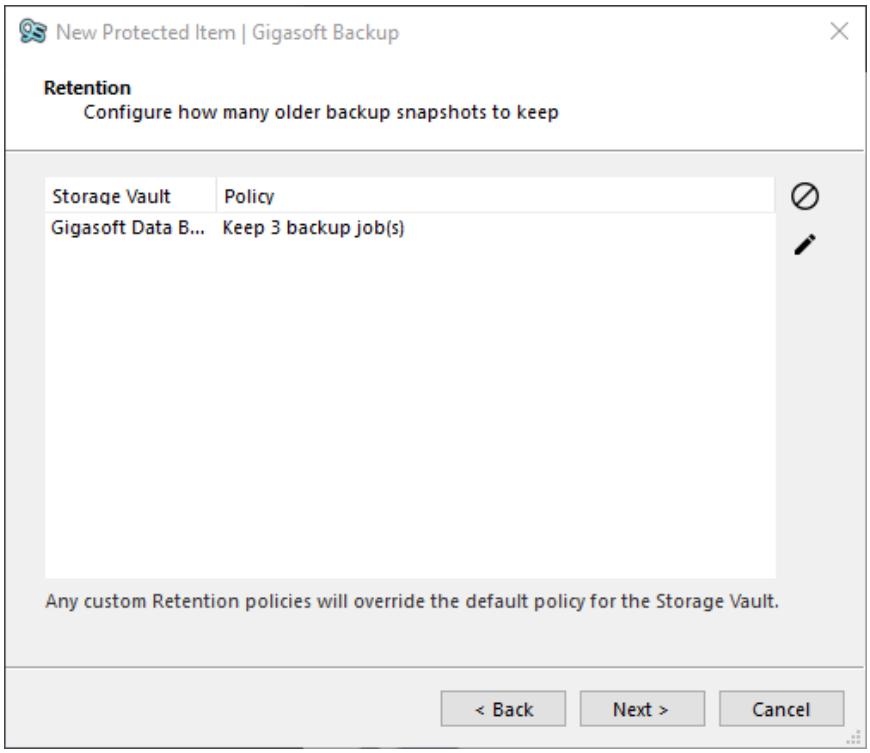
By default, the policy is to keep all data forever, but you can change this to a retention period that suits you by clicking on the current policy and then clicking the **[pencil]** icon.



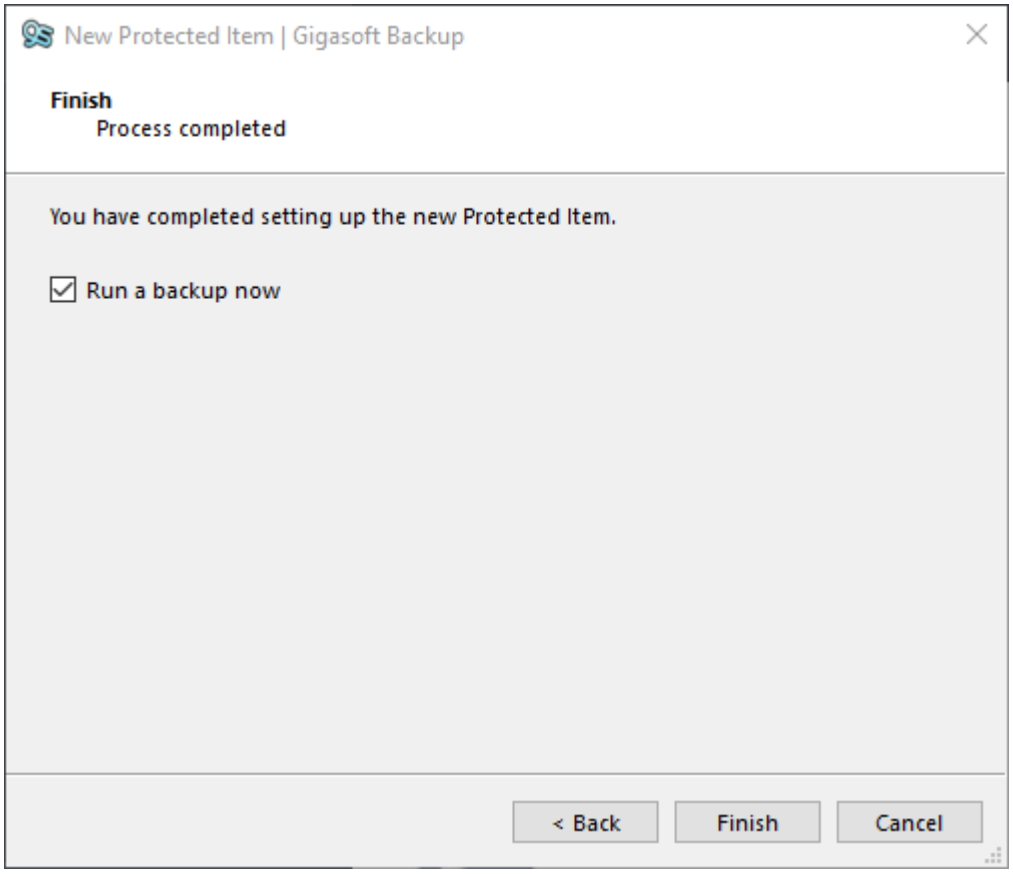
To change the retention policy, click on the **[Only keep…]** radio button and then click on the **[+]** icon.



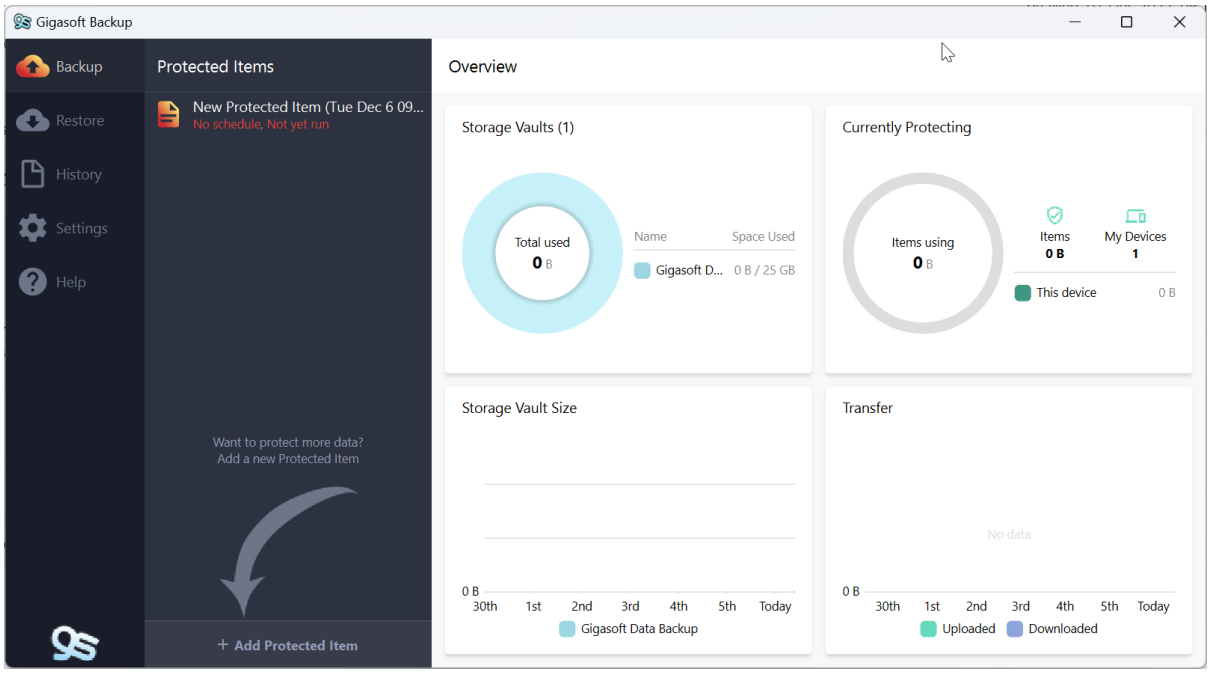
Use the drop-down menus to select a setting that suits you. In this example we will set the retention to **[keep the last 3 jobs]**, now click **OK**



Now click the **[Next]** button and the settings will be saved, and you will be asked if you would like to run the backup now.



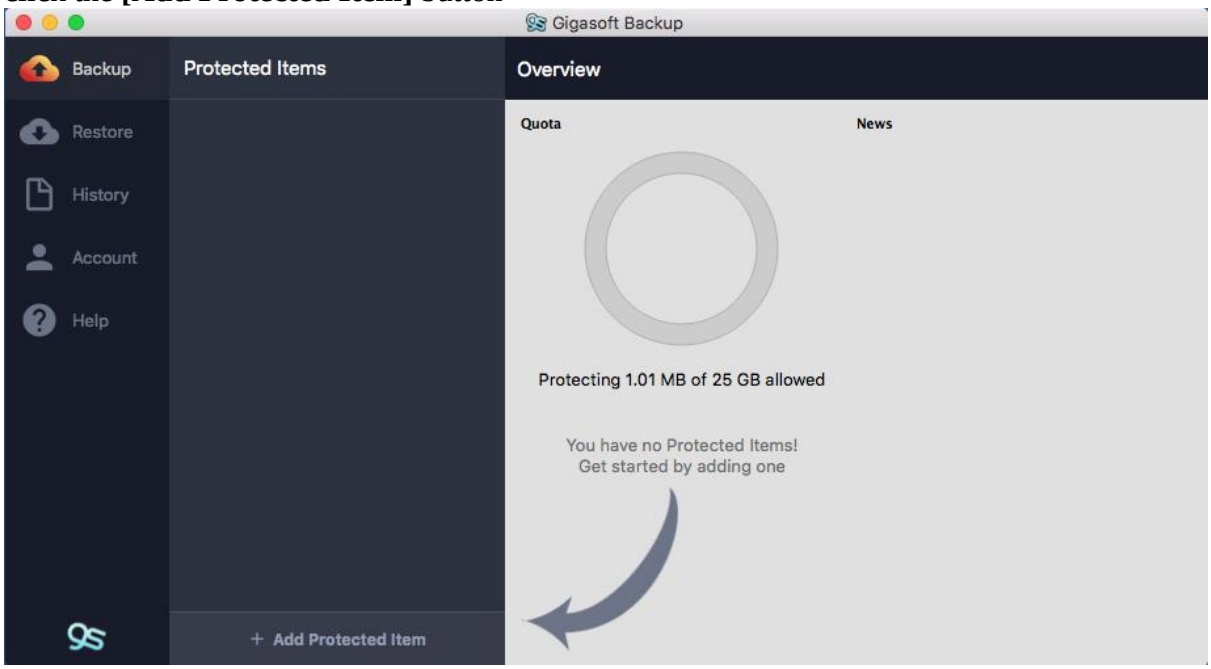
If you click the **Finish** button you will be taken into the run backup menu, if you do not wish to run the backup now untick the radio button before clicking **Finish** and you will be returned to the main dashboard.



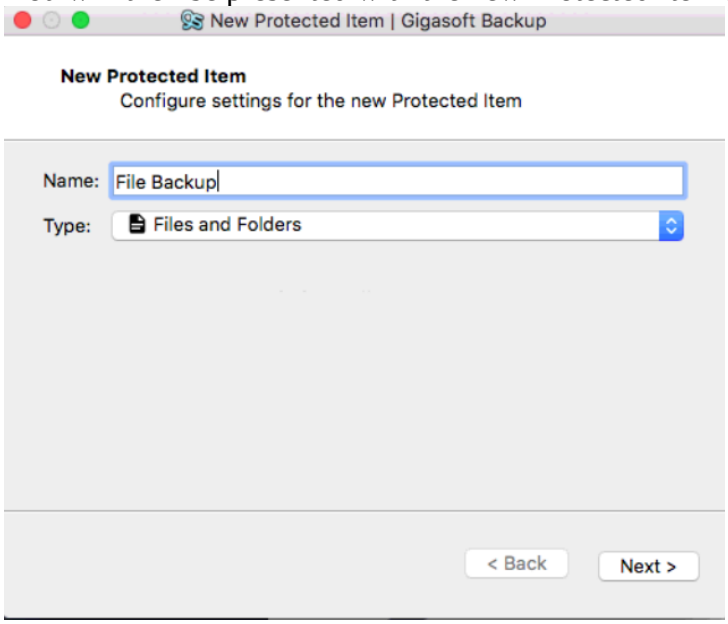
Here you can see your protected item has been created but has not been run yet, this can be left, and the backup will run at the scheduled time or you can run a manual backup, please refer to the section on running a manual backup for further details.

6.1.2 Creating a file protected item (MacOS)

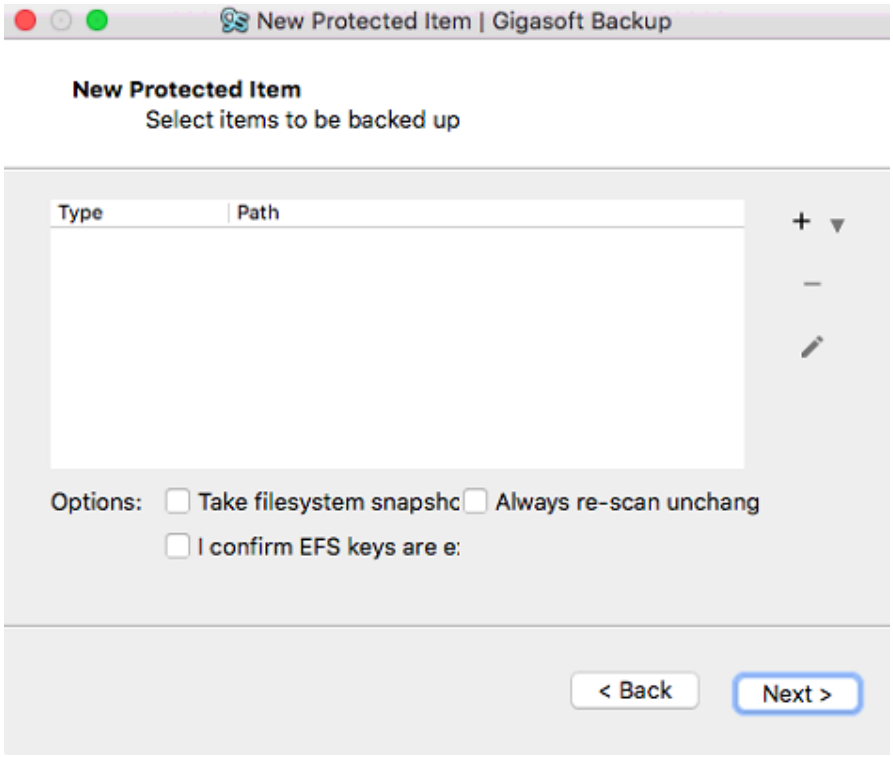
In this section we will go through the steps to create a file protected item using the MacOS Client.
Once you have logged in to Gigasoft Backup you will be presented with the main dashboard click the **[Add Protected Item]** button



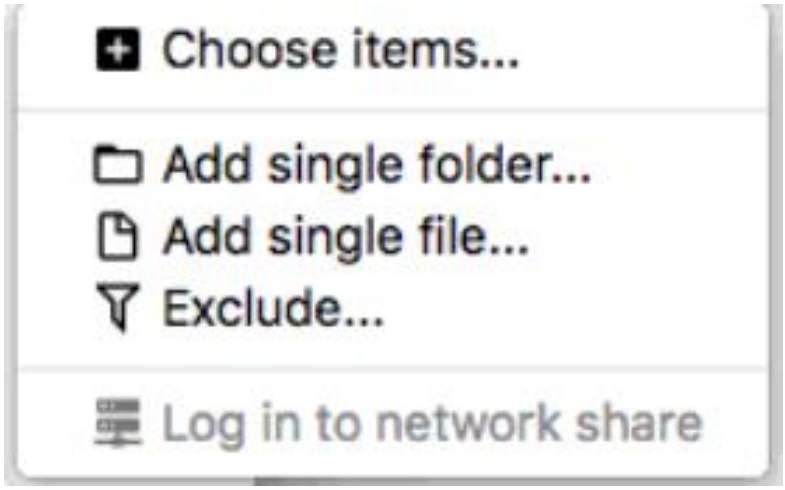
You will then be presented with the new Protected Item screen



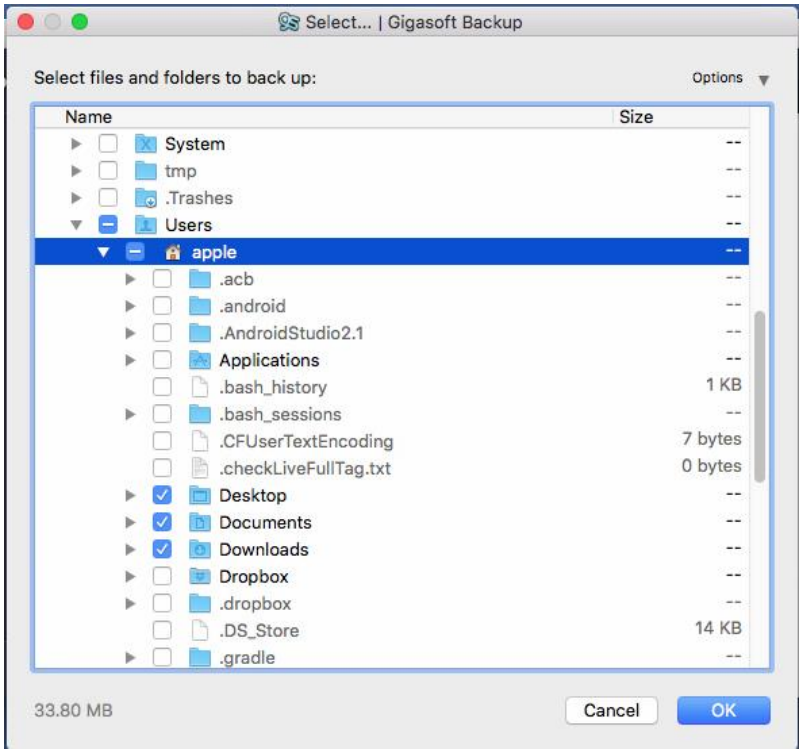
Change the name of the Protected Item to something meaningful so it's easy to identify at a later date, in this case I have called it "File Backup", now click the **[Next]** button



Now click on the down arrow next to **[+]**



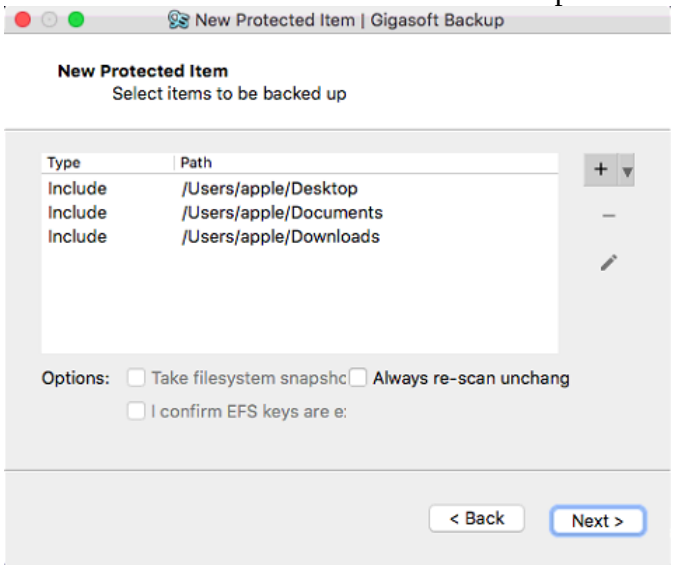
Select the **[Choose items]** option



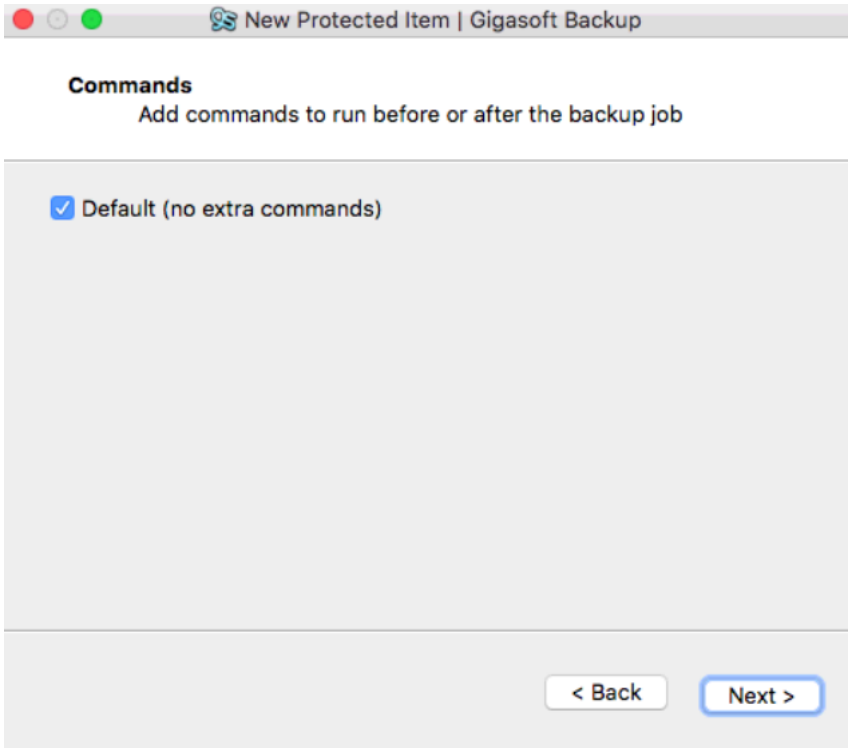
Now you can drill down through the local drives to select the files and folders you wish to backup.

If you need to back up from a network share click on the **[Options]** drop down from the top left and enter the path details.

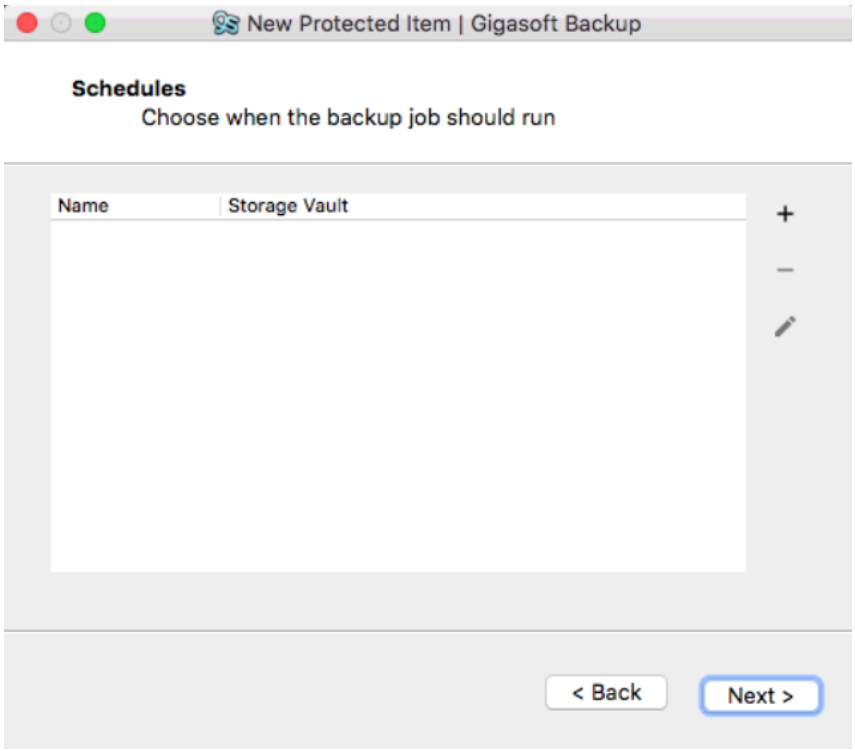
In this example we are just selecting all the files under the folders Desktop, Documents, Downloads from the User apple folder notice how in the bottom left of the window the client can detect how much data will be backed up.



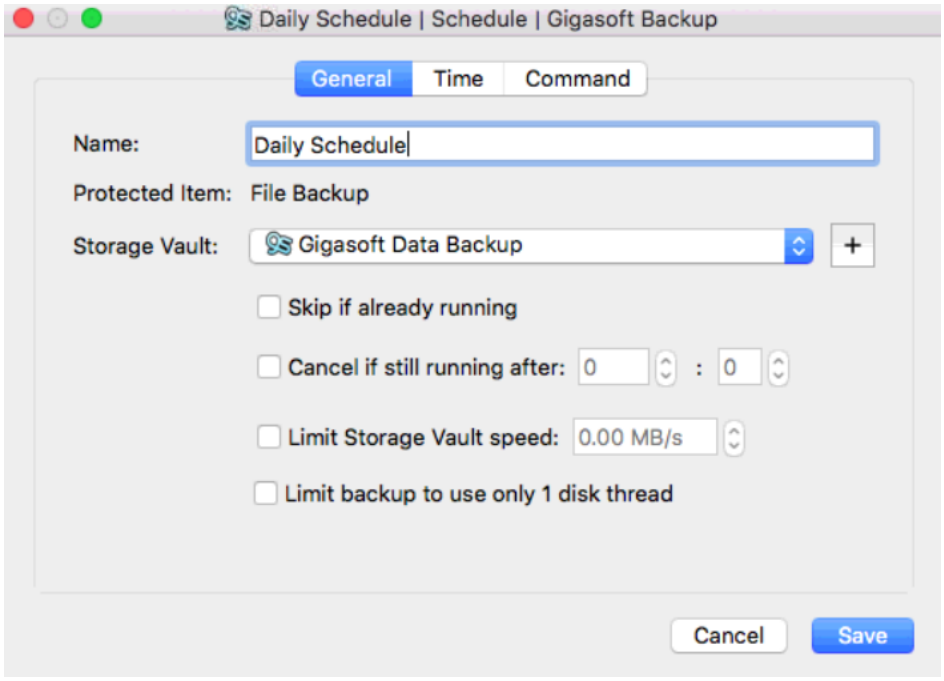
The **[Always re-scan unchanged files]** is useful if you have software that modifies files and does not change the file attributes, this option will scan all files selected even if they have not changed to compare them to what is currently held on the backup server, click **[Next]** to continue.



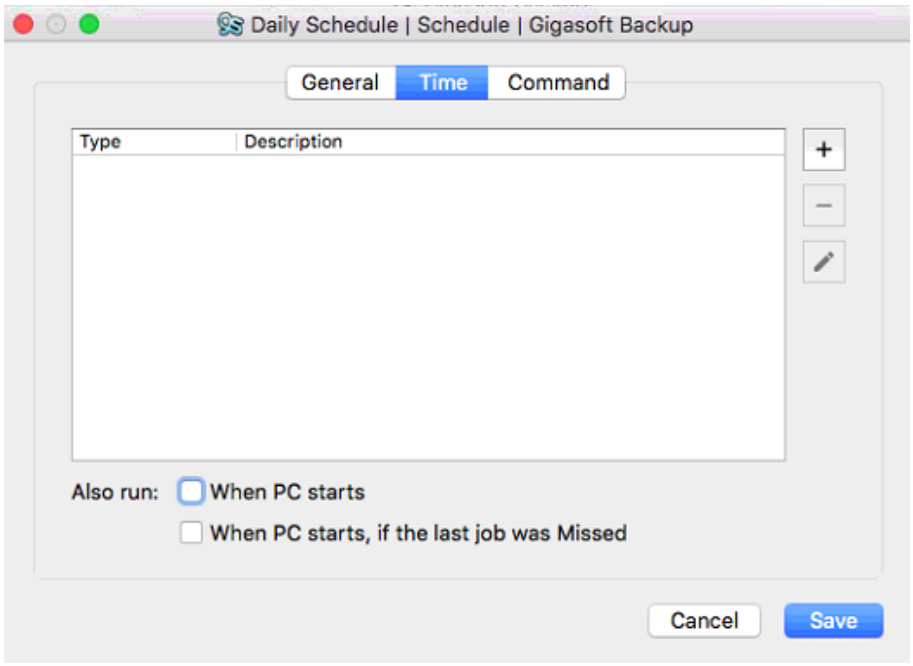
Un checking the Commands option allows you to add any pre or post commands you may need, if you don't need any leave this ticked and click **[Next]**



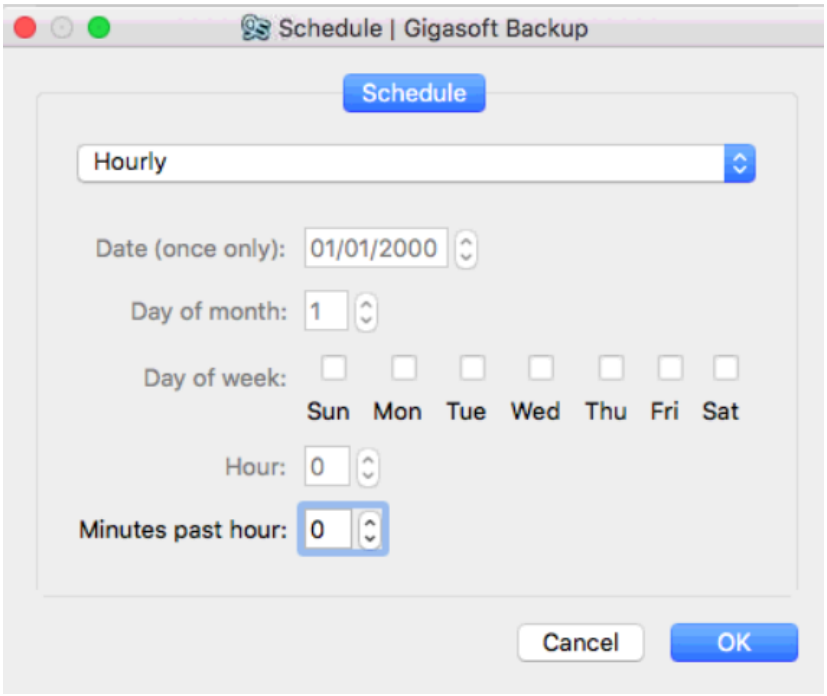
Here you can set the schedule for this protected item, Select the **[+]** icon to add a schedule.



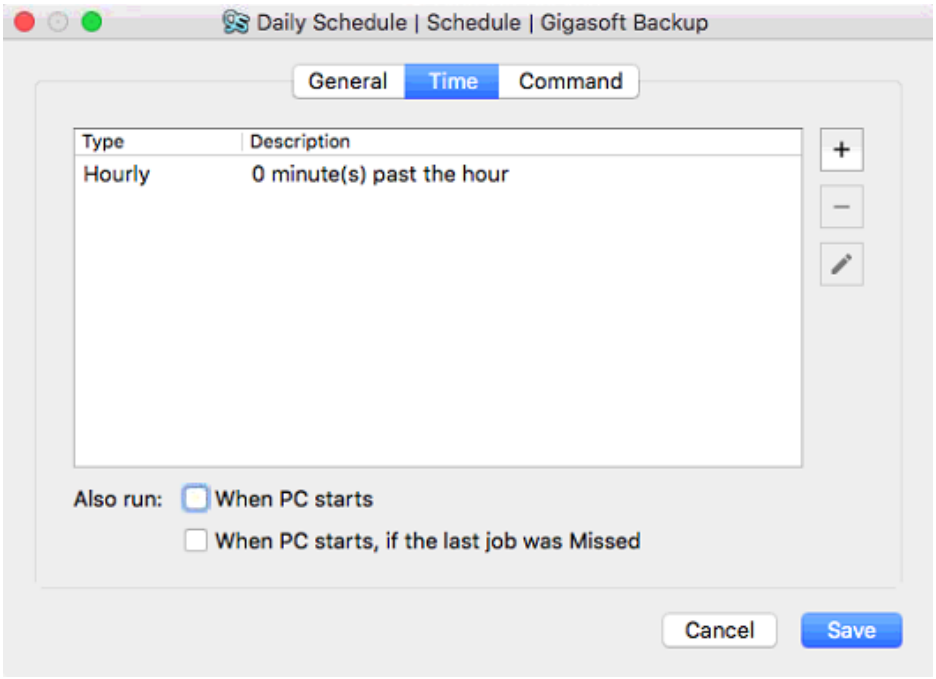
Name the schedule to something meaningful and then decide if you wish the schedule to be skipped if a backup is already running or you can choose to cancel the backup if it runs longer then a pre-determined amount of time, in this example I have named it “Daily Schedule”



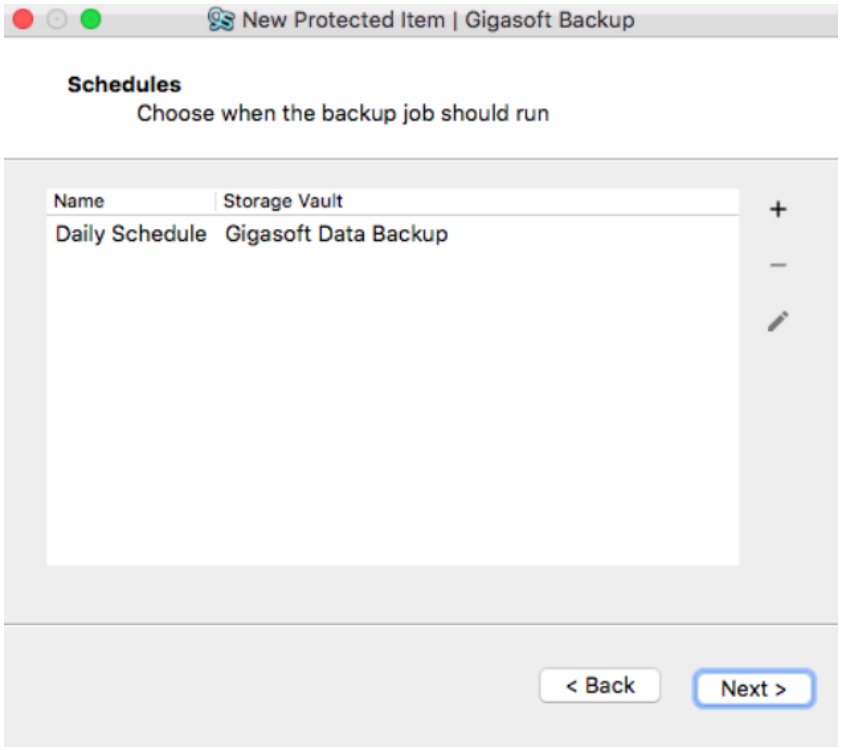
Click on the Time tab and then the **[+]** icon to set the schedule start time.



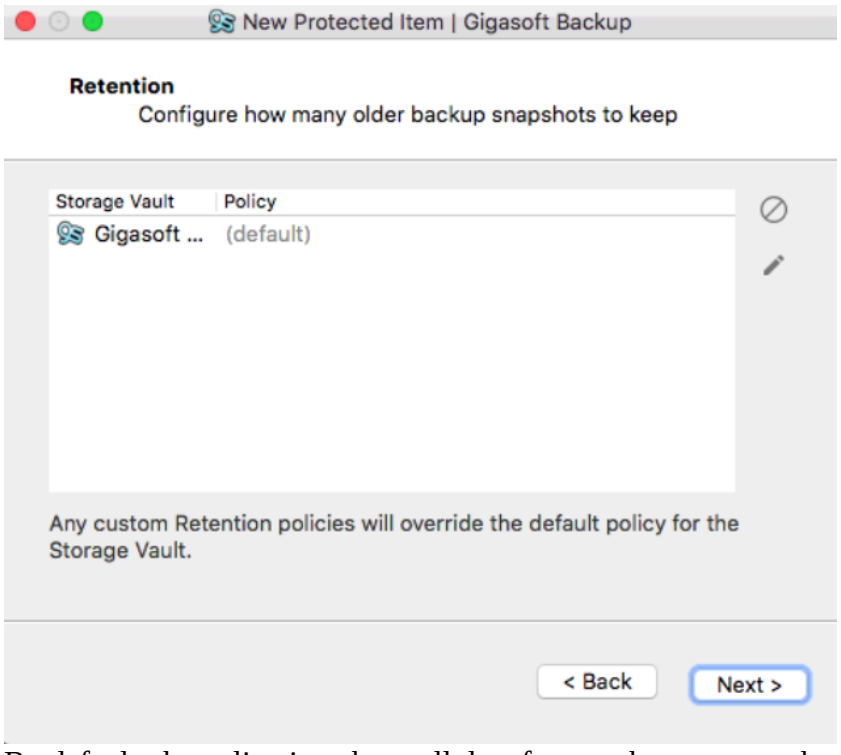
In this example we will choose the Hourly schedule and set it to run at 0 Minutes past each hour, now click **[OK]**, the Command tab can be used if you want to run pre- or post-commands at the schedule level.



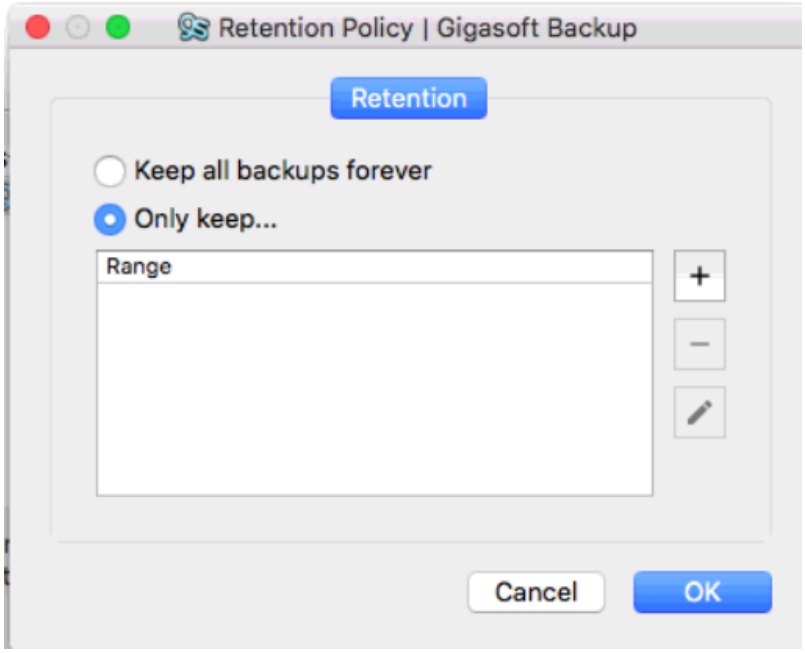
From here you can also specify that the backup runs when the machine is turned on or run if the machine was turned off and the last scheduled backup was missed.
Clicking **[Save]** will return you back to the Schedule tab



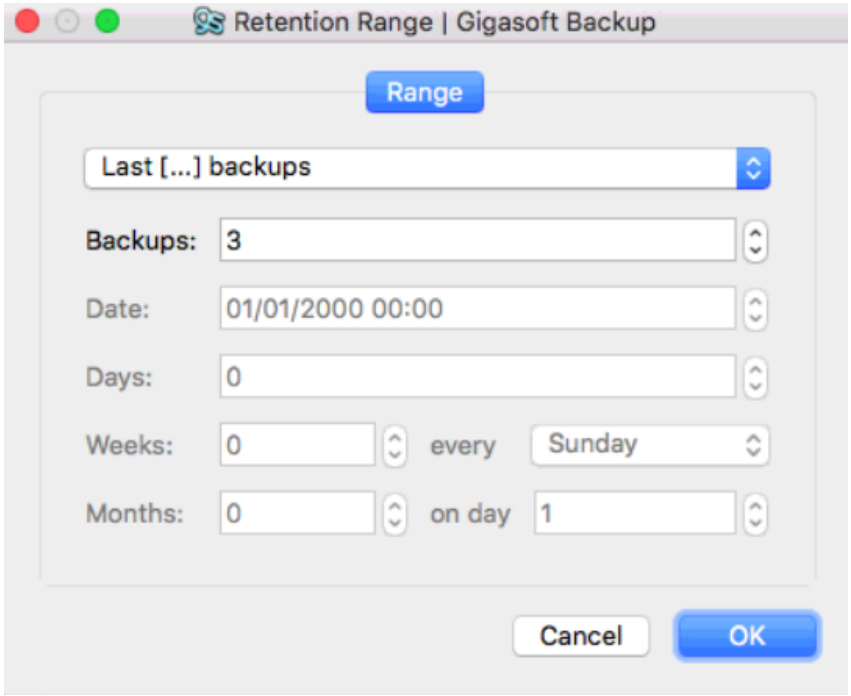
Finally click **[Next]** to set the Retention.



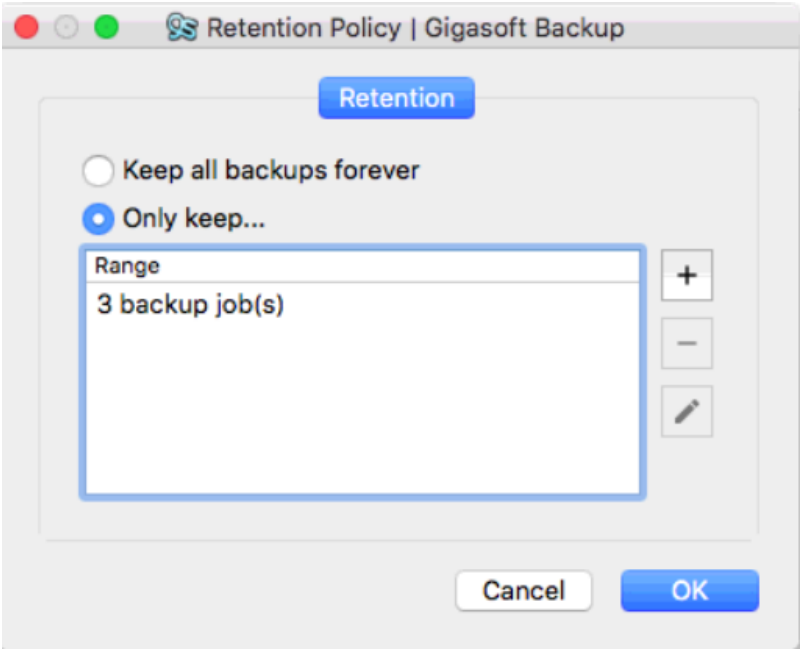
By default, the policy is to keep all data forever, but you can change this to a retention period that suits you. Click on the current policy and then click the **[pencil]** icon.



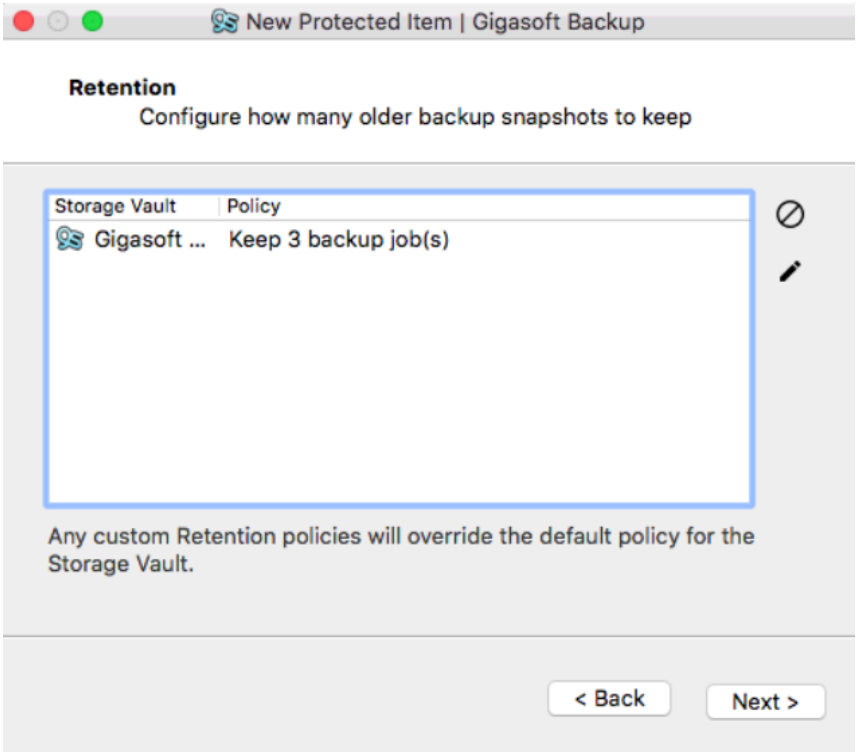
To change the retention policy, click on the **[Only keep…]** radio button and then click on the **[+]** icon.



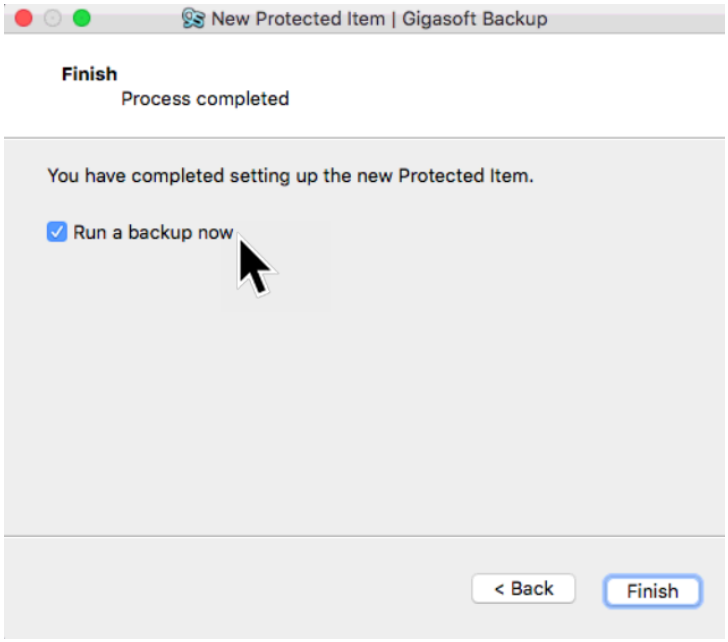
Use the drop-down menus to select a setting that suits you. In this example we will set the retention to **[keep the last 3 jobs],** click the **[OK]** to accept the changes.



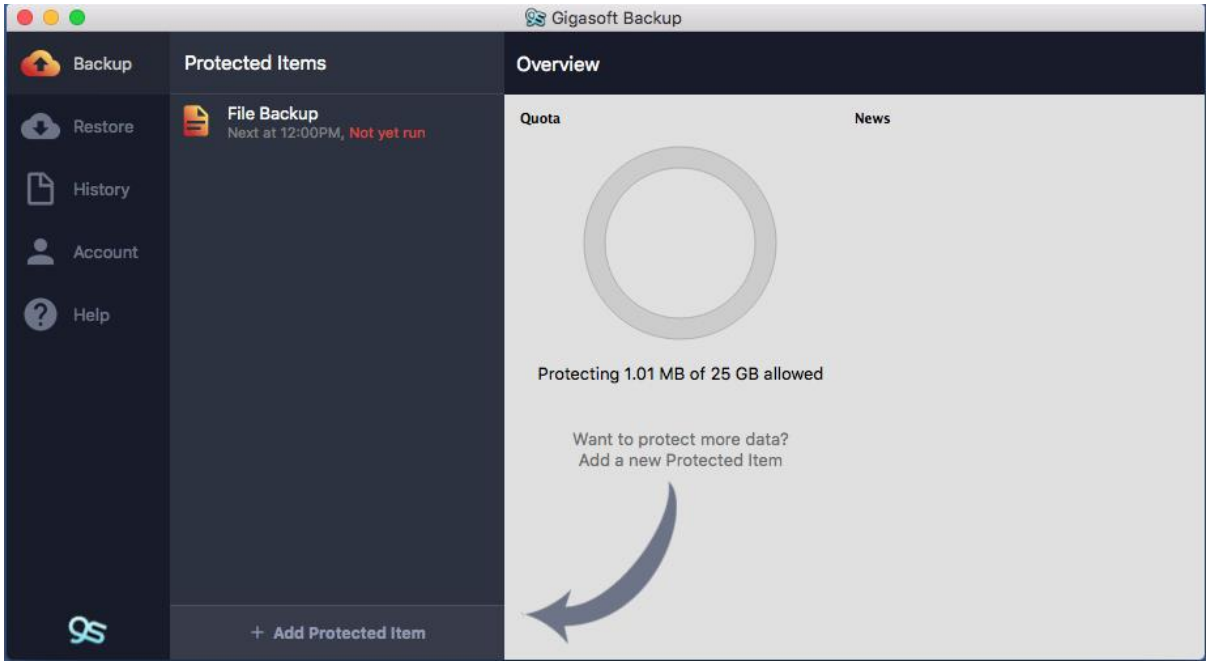
You will now be taken to the retention overview page, here you can set additional retention policies for a more advanced setup. Click **[OK]** to accept the changes.



Now click the **[Next]** button and you will now be asked if you want to run a backup now.



Untick the check box if you do not want to run a manual backup now and then click **[Finish]** to be returned to the main dashboard.



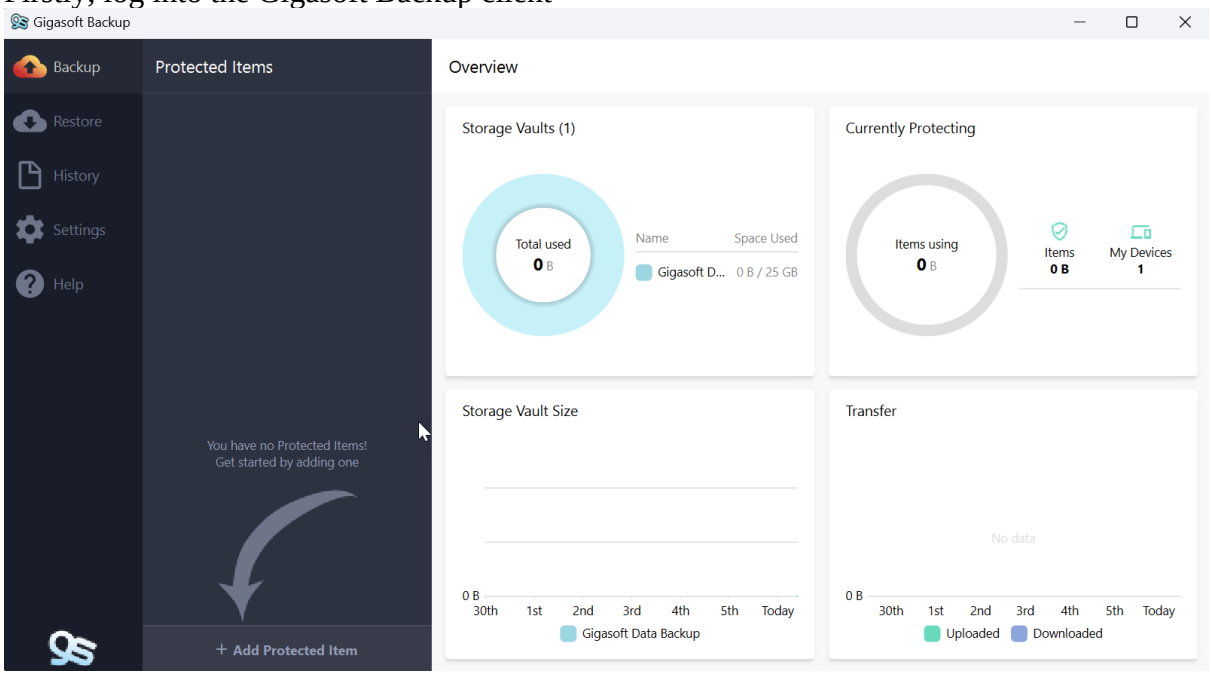
Here you can see your protected item has been created but has not been run yet, this can be left, and the backup will run at the scheduled time or you can run a manual backup, please refer to the section on running a manual backup for further details.

6.1.3 Creating a file protected item (Linux)

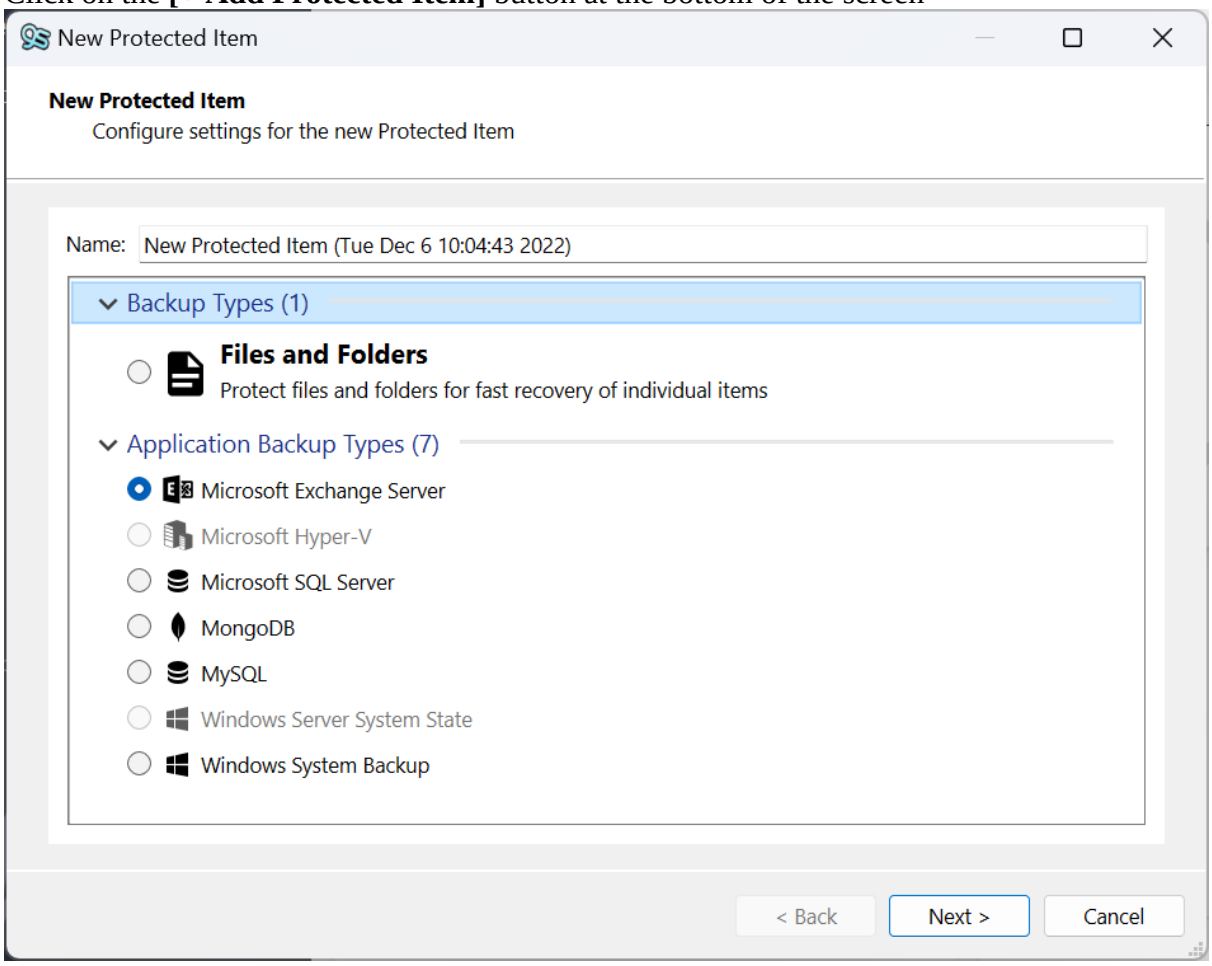
Currently the Linux version is command line only, any changes to the protected items need to be performed via the customer web portal.

6.2 Exchange protected item

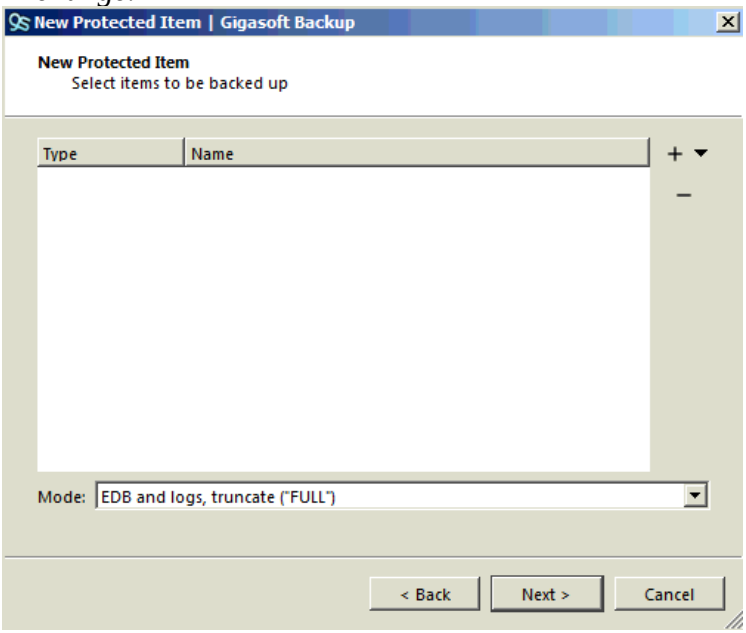
In this section we will guide you through the process of creating an exchange protected Item, we will use an example to demonstrate the steps involved.
Firstly, log into the Gigasoft Backup client



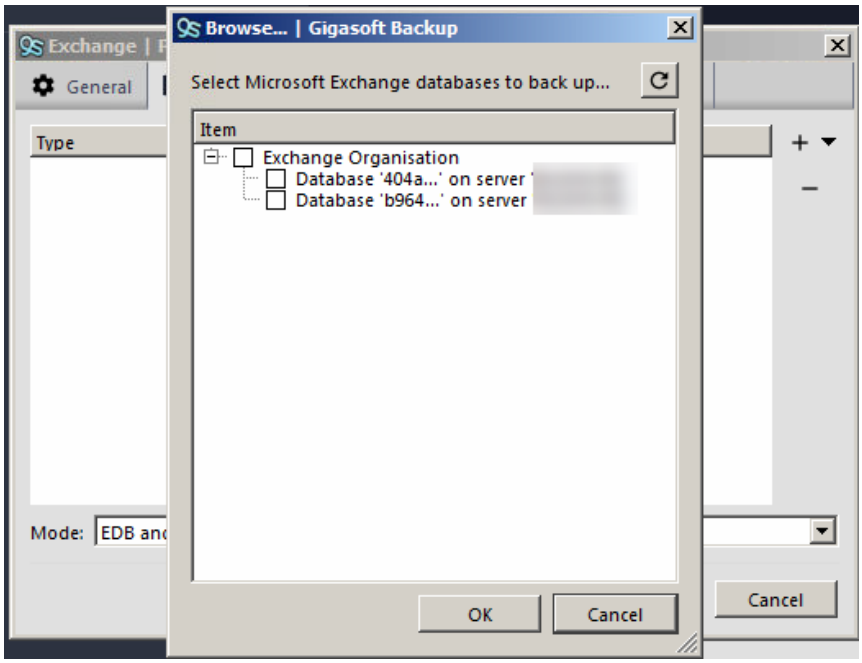
Click on the **[+ Add Protected Item]** button at the bottom of the screen



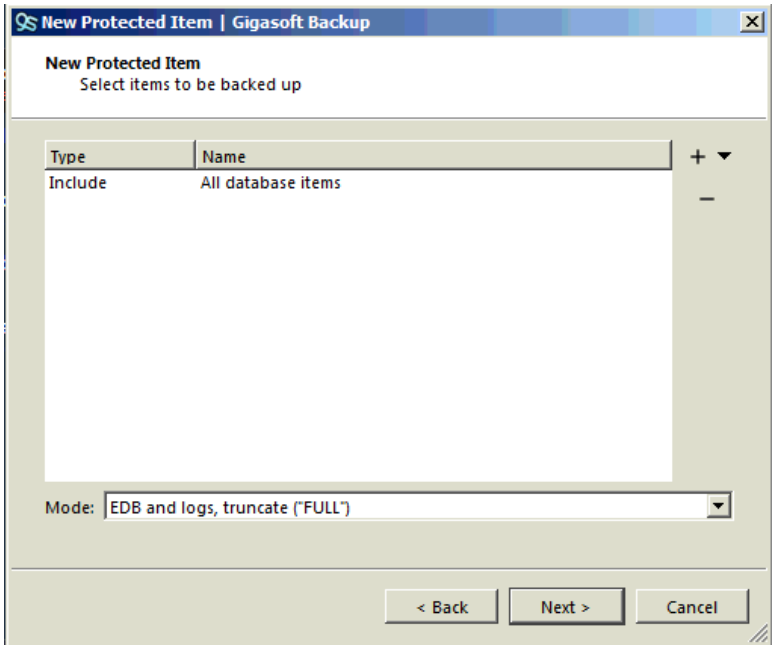
Select the **[Microsoft Exchange Server]** from the drop-down list and change the Name to something more meaningful and click on the **[Next]** button, in this example we will use *Exchange*.



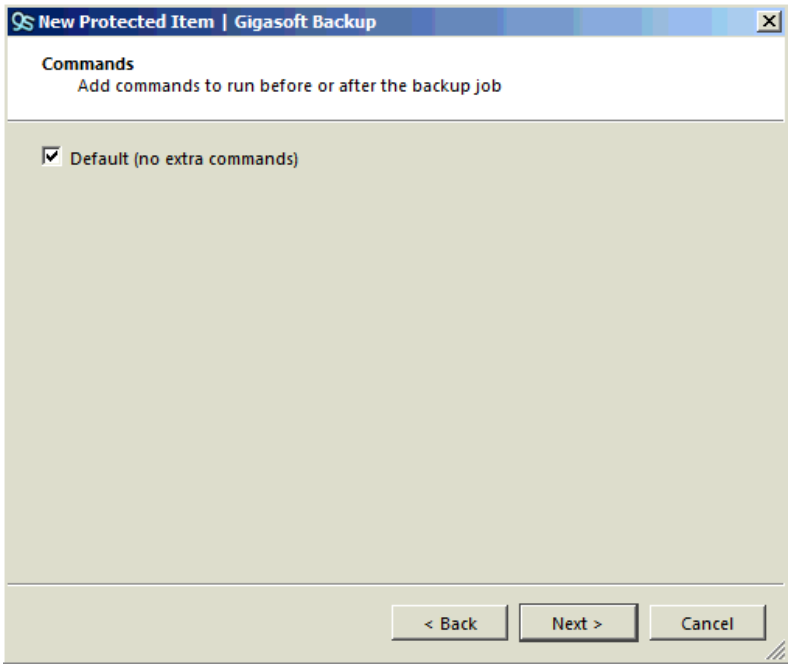
On the next screen click on the **[+]** button and select **[Choose tables]** the following screen will appear.



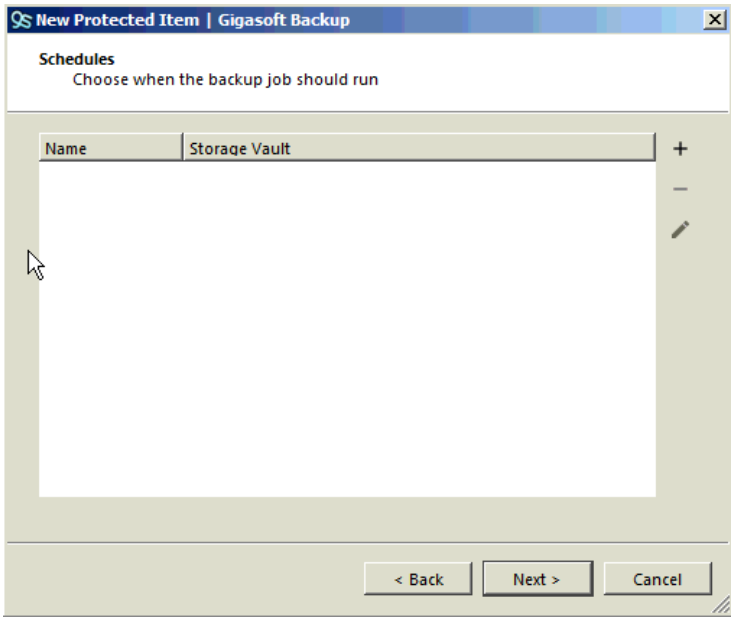
Tick the Databases you wish to backup and click **[OK]**



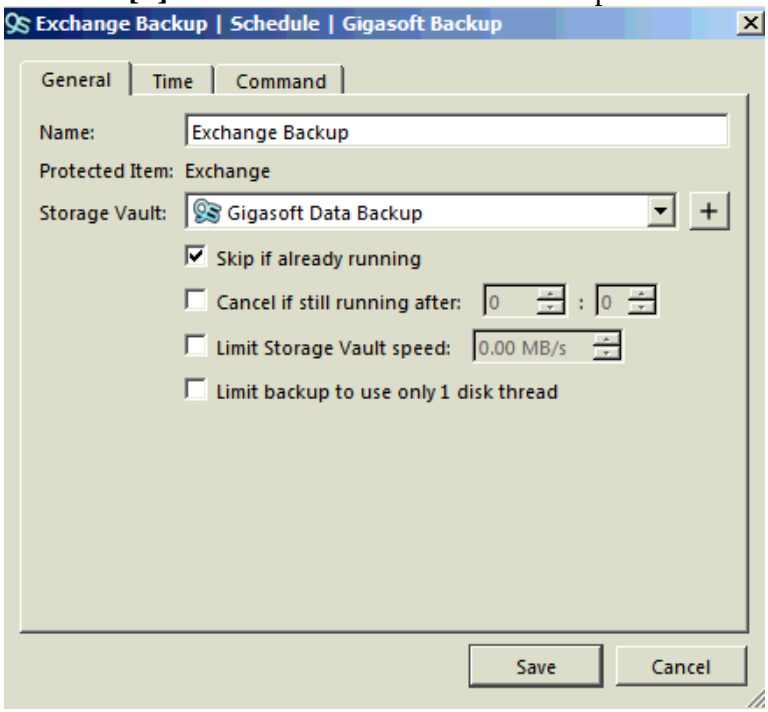
In this example we are going to select all the Databases and we want to back up a full database each time, now click **[Next]**.



Unless you need to add any pre or post commands leave the radio button checked and click the **[Next]** button.

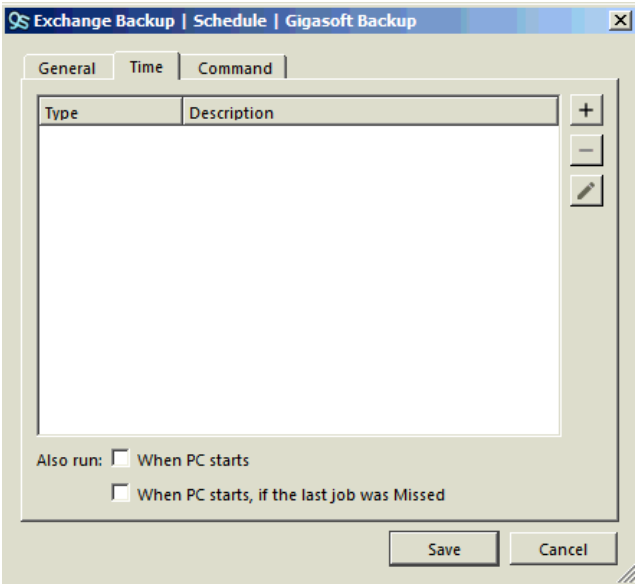


Click the **[+]** button to add a schedule for this protected item.

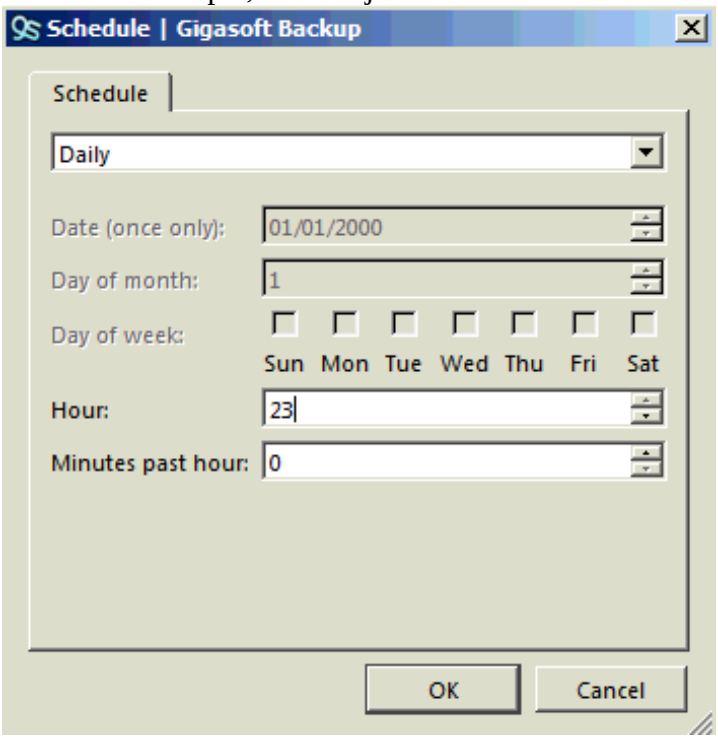


Enter a meaningful name into the Name box, we have used *Exchange backup*, select which vault this backup will go to. In this example we will use the default offsite storage vault. Change the options if you want the job to stop after a certain amount of time or to skip another backup if there is one already running, you can also limit the bandwidth available to this protected item, this is especially useful if you have a large amount of data and you don't want it to use all of the available upload bandwidth, It is advisable to tick the **Skip if already running** check box to prevent multiple jobs trying to backup exchange, especially on the initial upload.

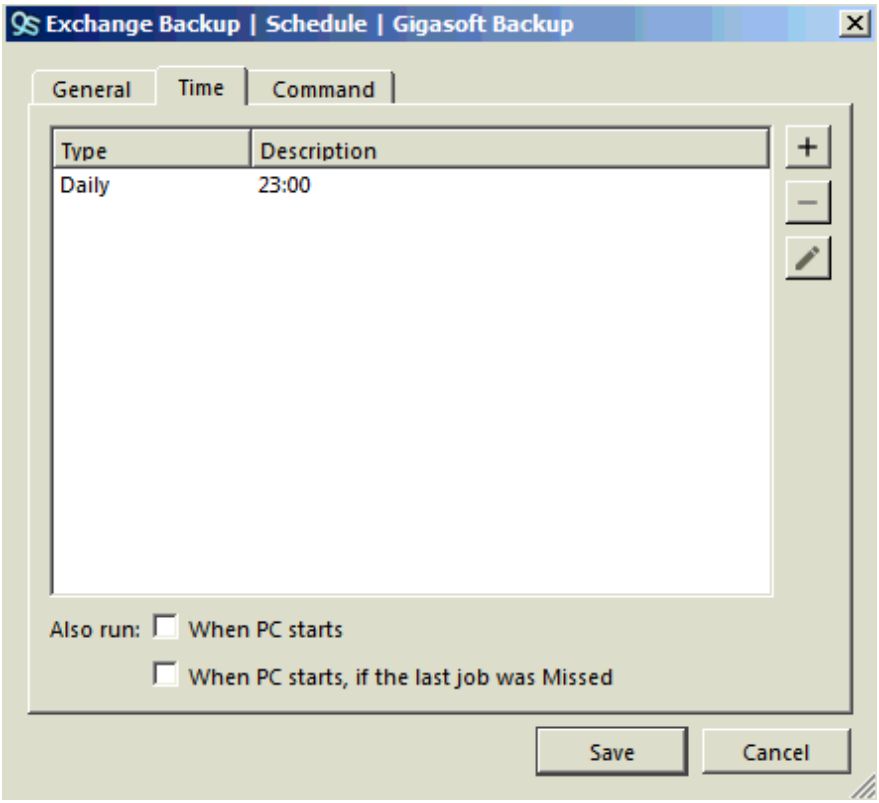
On older machines or machines that are busy we can now request that GBM uses a single disk thread, this causes the backup to take a bit longer but uses less resources, this is useful if you find your machine is running slower than normal when the backup is running, now click on the **[Time]** tab.



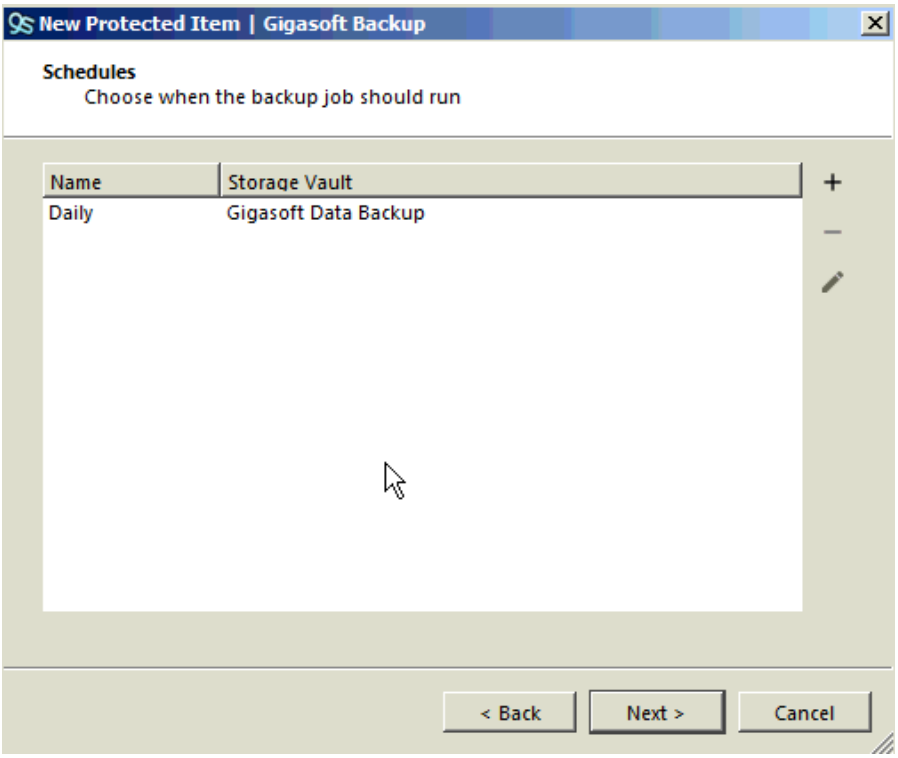
Here we can set a schedule for this protected item, we can create multiple schedules if needed but in this example, we will just create the one. Click on the **[+]** button to add a schedule



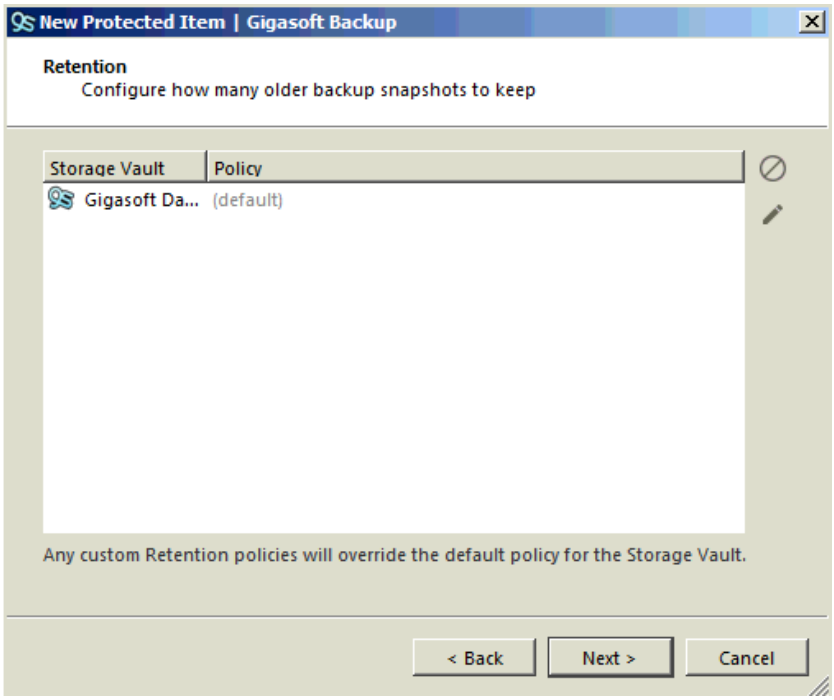
Use the drop down to select the desired type of schedule, in this example we will set the schedule to run daily at 23:00, click **[OK]** once you are done.



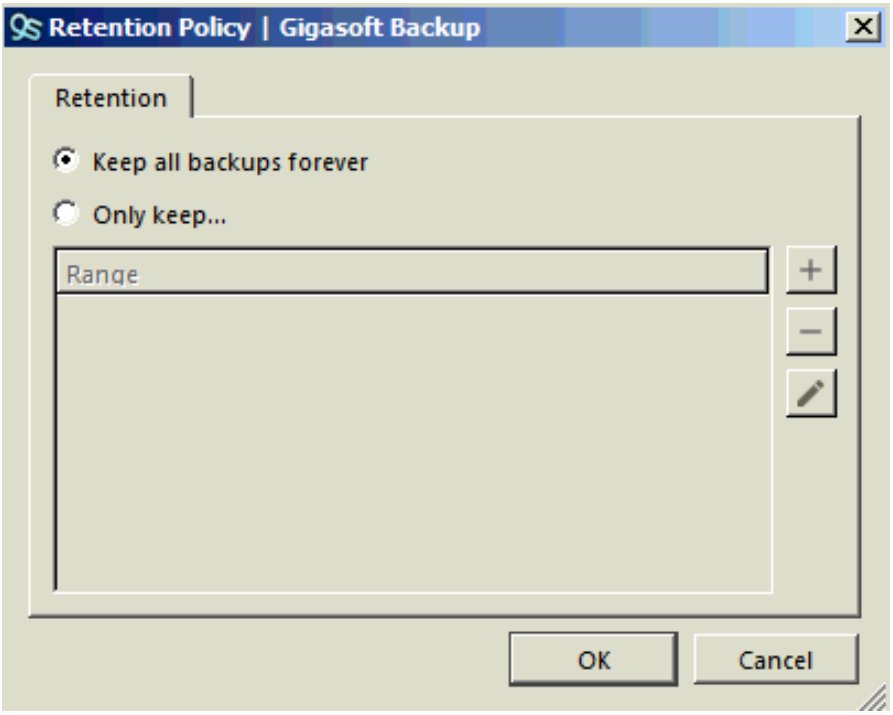
We are taken back to the schedule overview page, here you can add more schedules if needed, you can also set any pre or post commands if needed else click the **[Save]** button to move on.



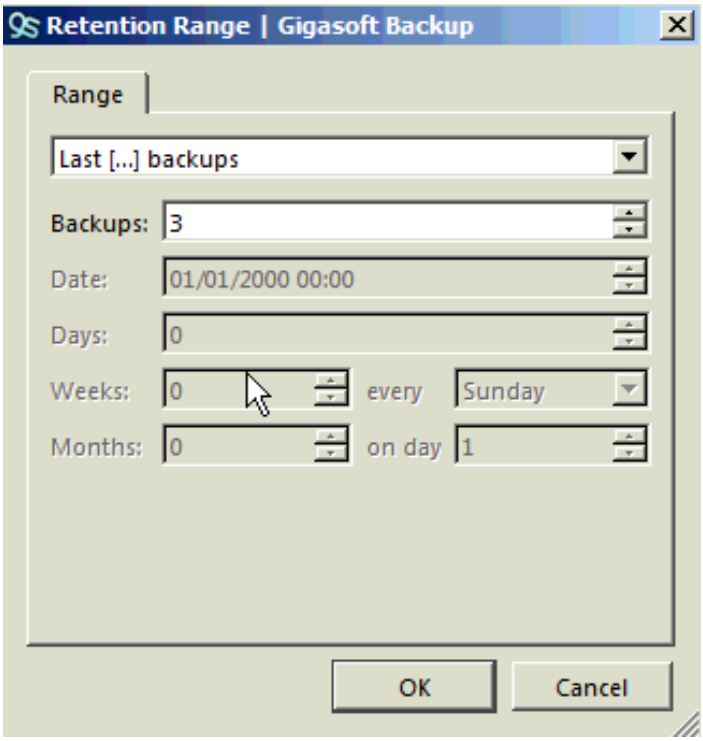
We are now back to the Schedule item overview page, we now need to set the retention policy for this set. Click on the **[Next]** button.



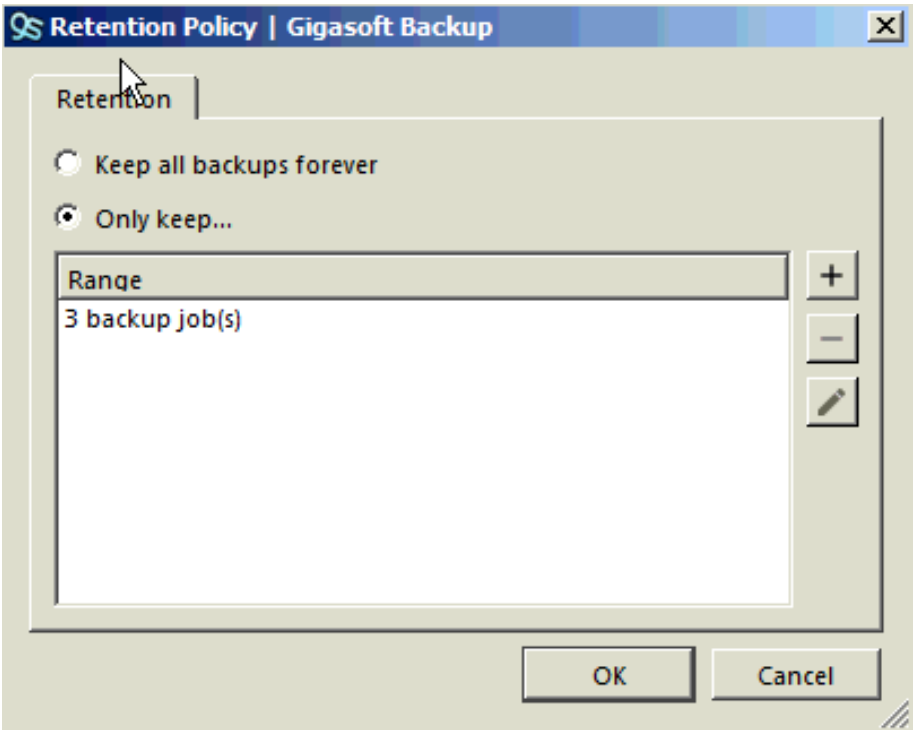
Here you can see there is a default retention policy set, this is to keep all the data forever, to change this to one that suits your needs, click on the current policy to highlight it and then click the **[pencil]** button.



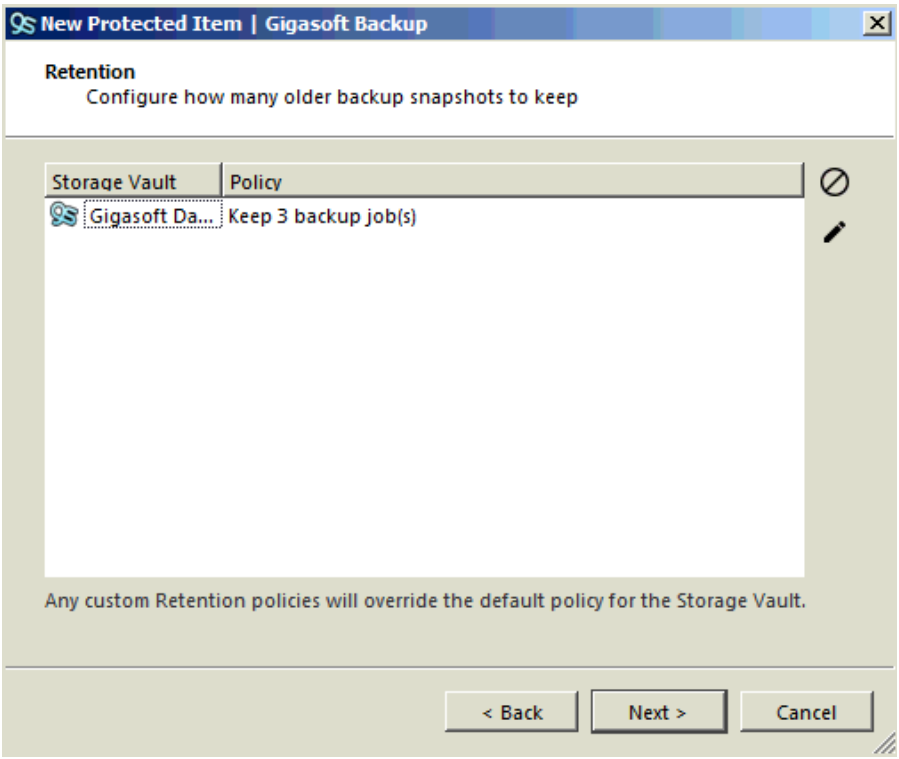
Here you can see the retention will be kept forever, change the radio button to **[Only keep…]** and then click on the **[+]** button.



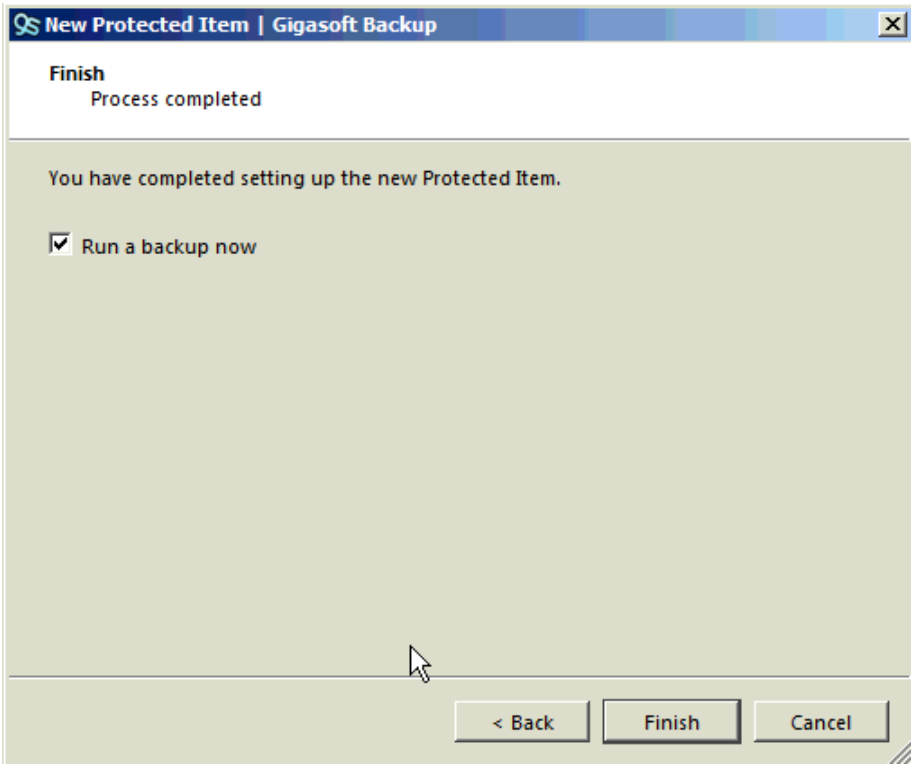
Use the drop-down selection box to choose a retention schedule that suits you, in this example we will select *Last […] backups*. In the next box we will select *3* this will allow us to keep the last 3 backups, this can be changed to anything you require. Once you have completed your selection click the **[OK]** button.



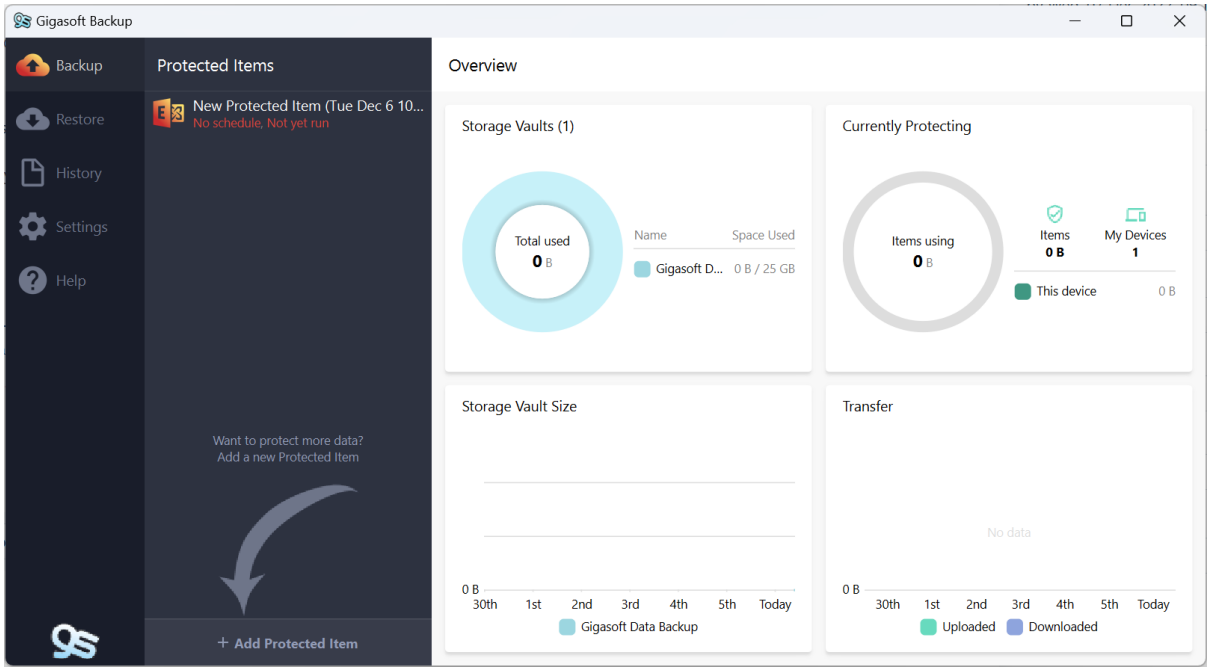
You will now be taken back to the overview page, you can set other schedules for this same protected item if you wish else please click the **[OK]** button.



Now we are back to the retention overview page, once you are happy you have all the settings you need click the **[Next]** button.



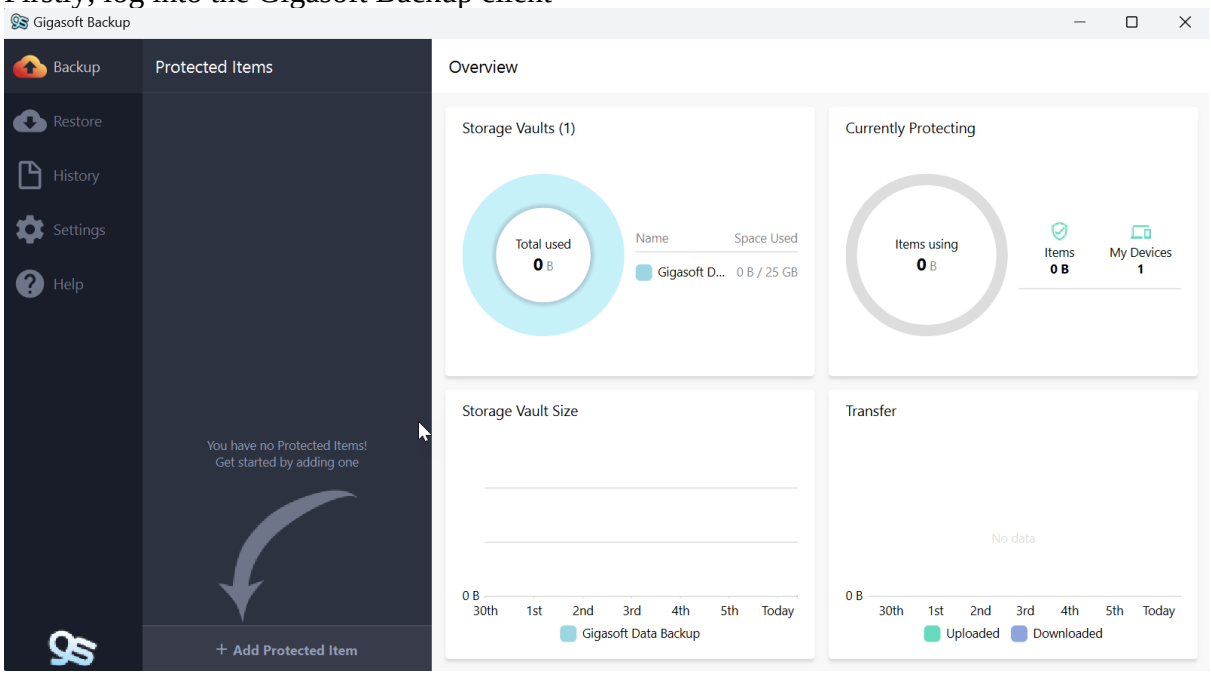
If you wish to run the backup now click the **[Finish]** button or if you wish to run the backup later un tick the **run a backup now** box and then click on the **[Finish]** button



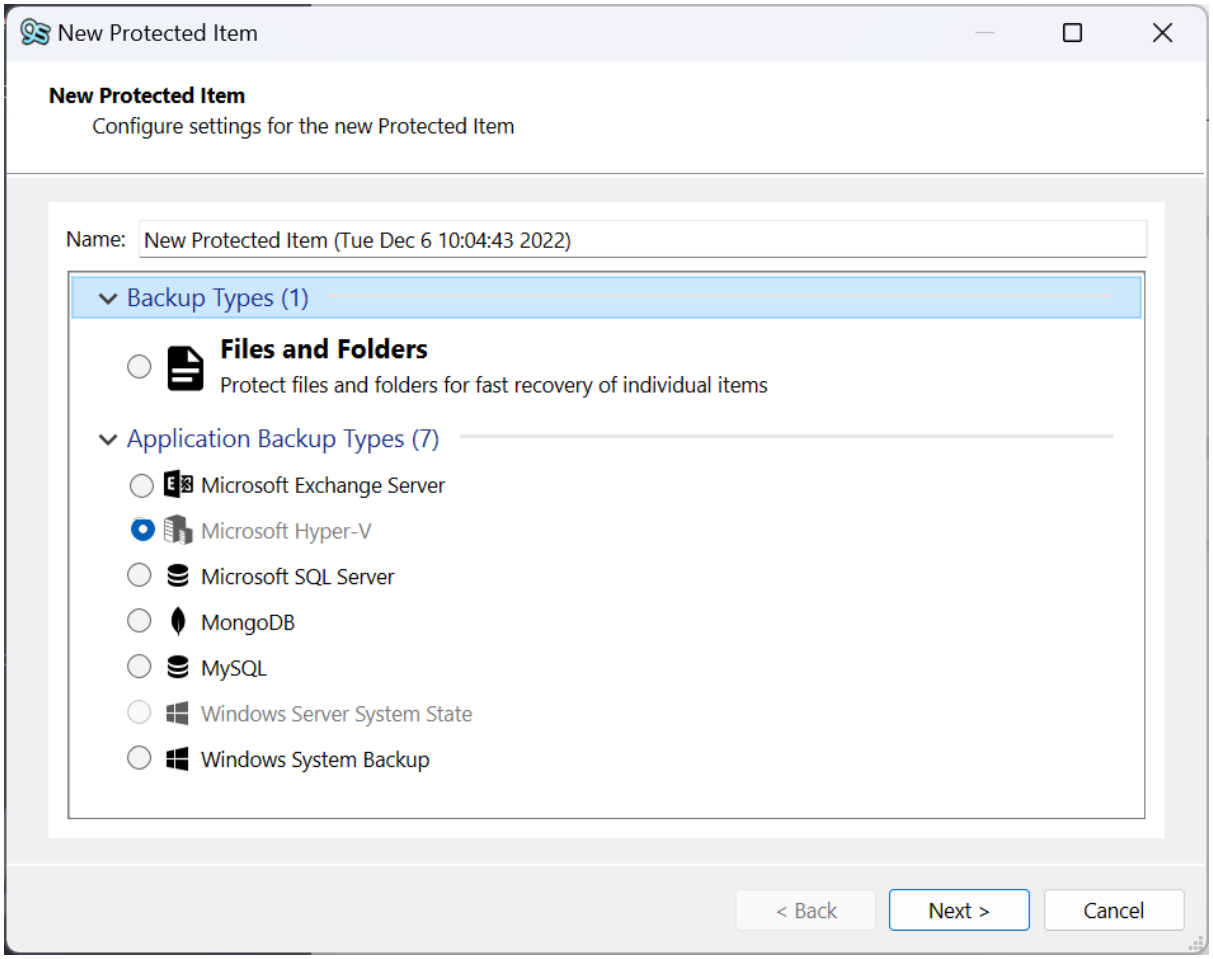
After clicking finish you are taken back to the main dashboard, from here you can create further protected items if you need to.

6.3 Hyper V Protected item

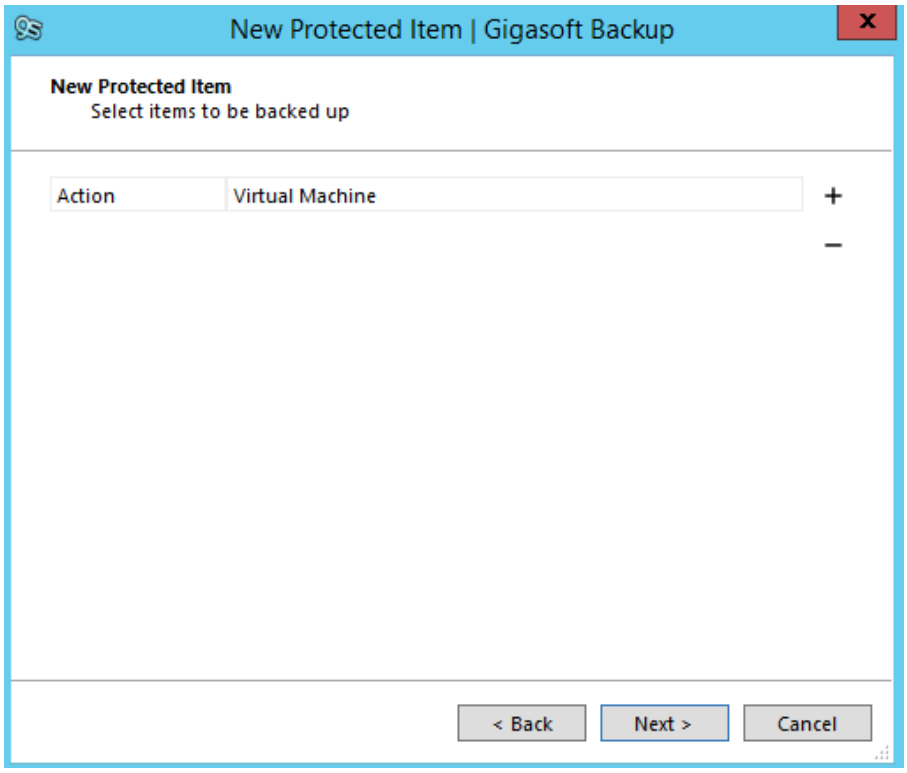
In this section we will guide you through the process of creating a Hyper-V protected Item, we will use an example of a webserver, but you would obviously select your own machines. To be able to back up a Hyper-V machine you need to make sure the service is running on this machine and the virtual machines are visible in the Hyper-V manager, Hyper V backups can only be performed by a server operating system.
Firstly, log into the Gigasoft Backup client



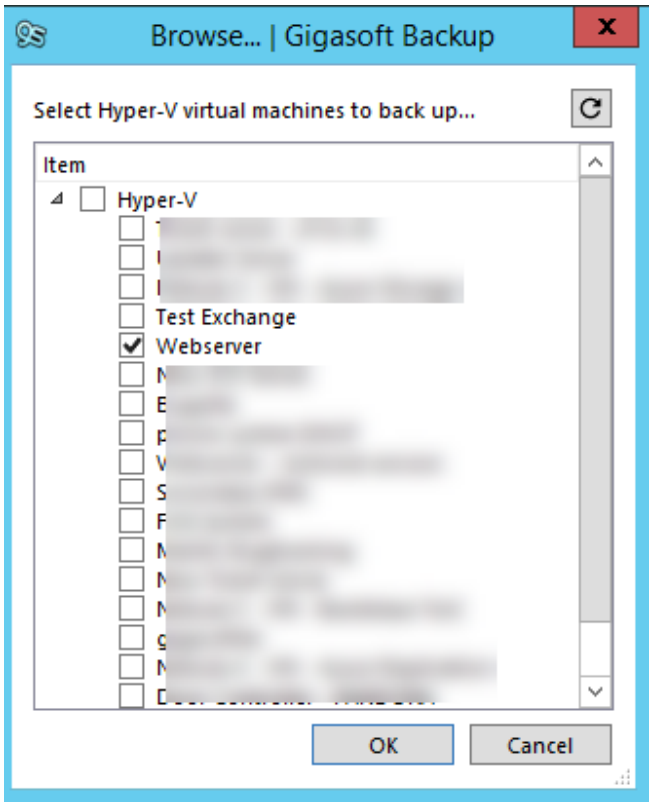
Click on the **[+ Add Protected Item]** button at the bottom of the screen



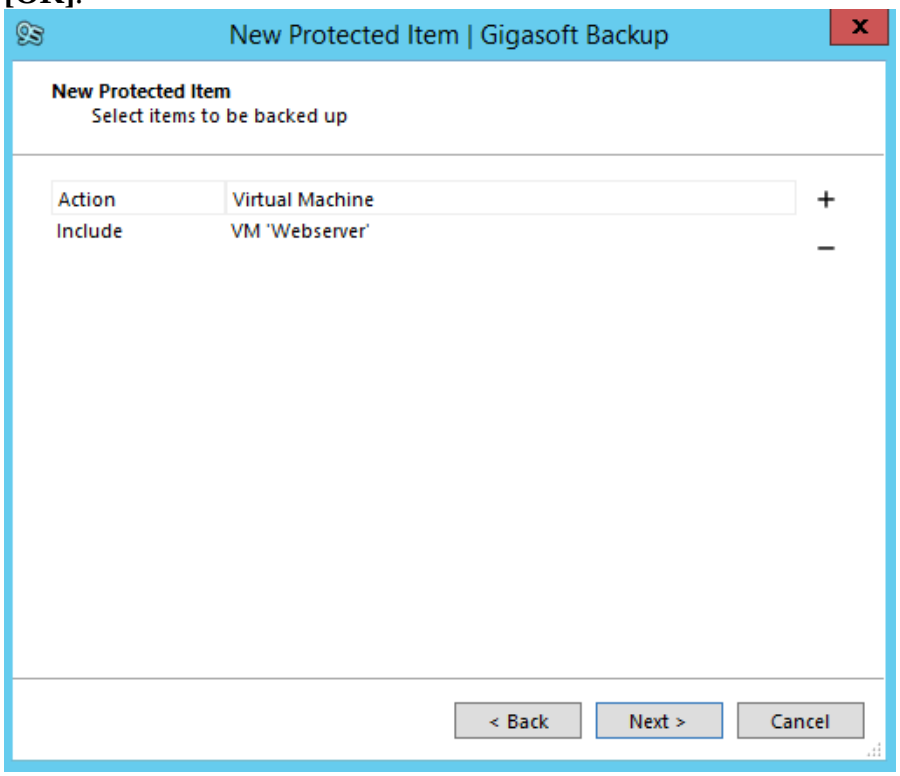
Select the **[Microsoft Hyper-V]** from the drop-down list and change the Name to something more meaningful and click on the **[Items]** tab, in this example we will use *Hyper V Backup.*



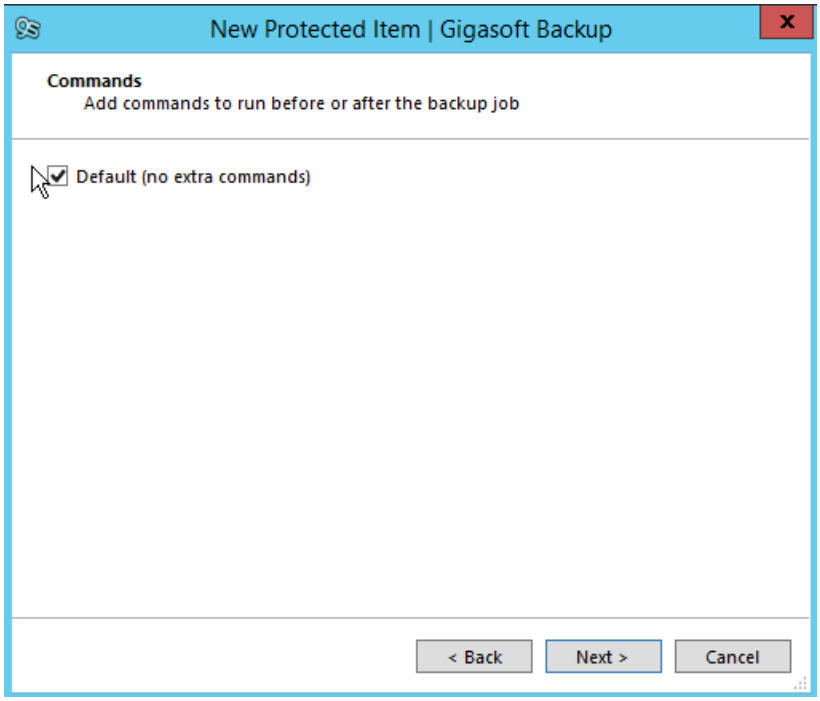
On the Items screen click on the **[+]** button and the following screen will appear.



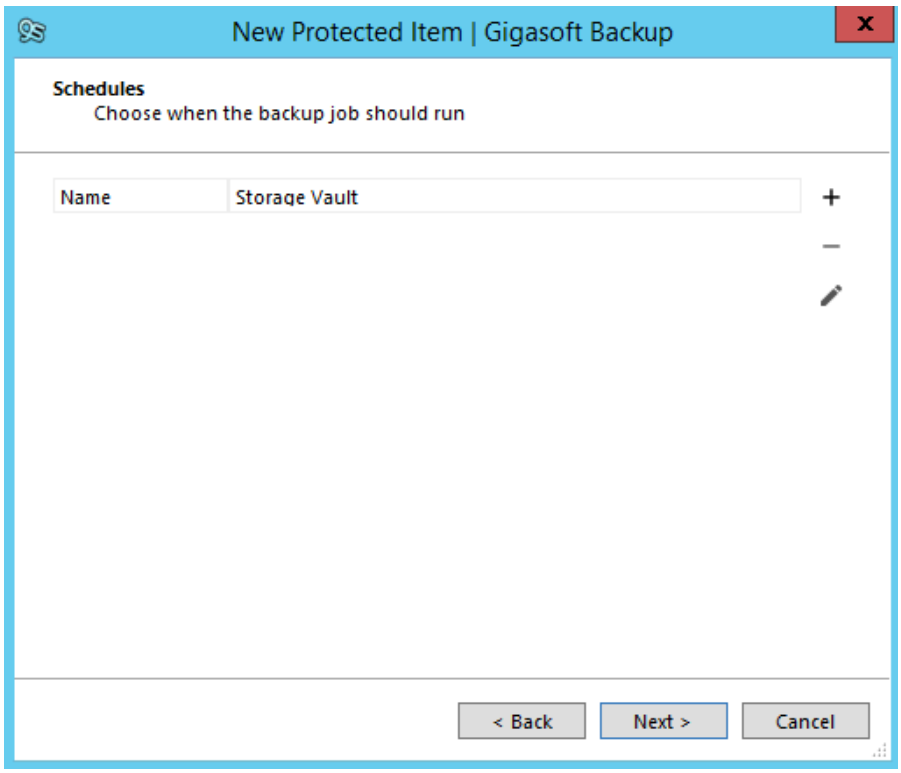
Here we can select the virtual machines you want to backup, in our example we will select the *Webserver*, to do this put a tick next to the machine(s) you want to protect and click **[OK]**.



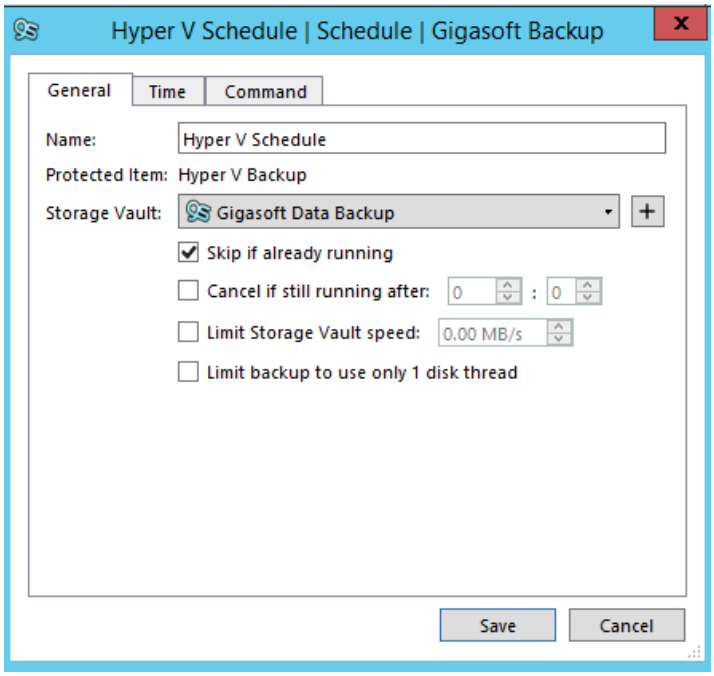
You will return back to the Items overview page and you can now see the machines that are selected to be backed up, click on to the **[Next]** button.



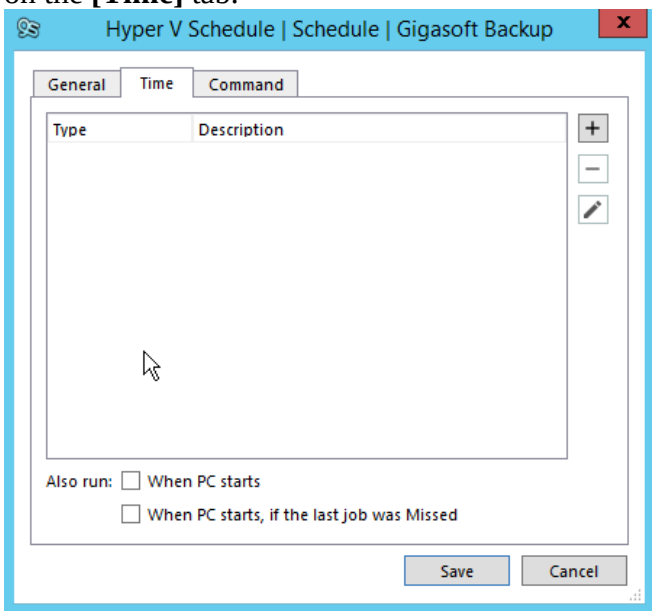
If you need to run any pre or post commands untick the radio button else, click on the **[Next]** button to continue.



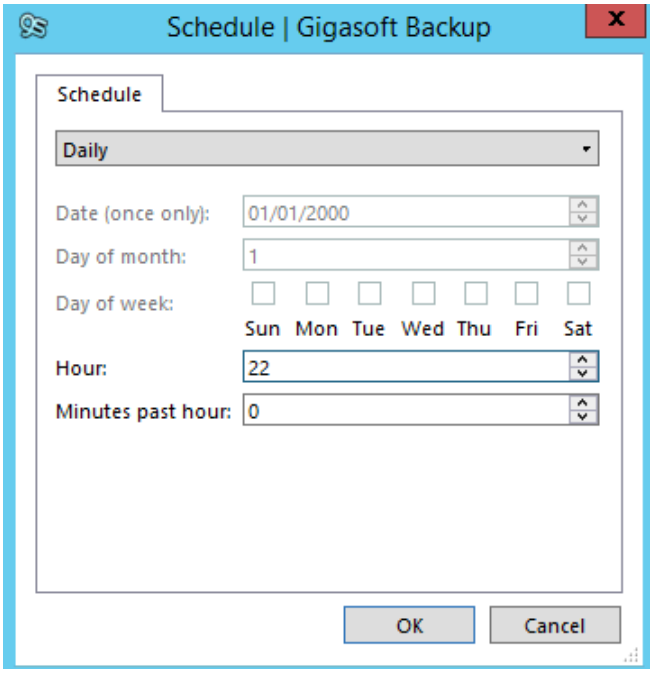
On this page you can see there is no schedules setup, to add a schedule click on the **[+]** button.



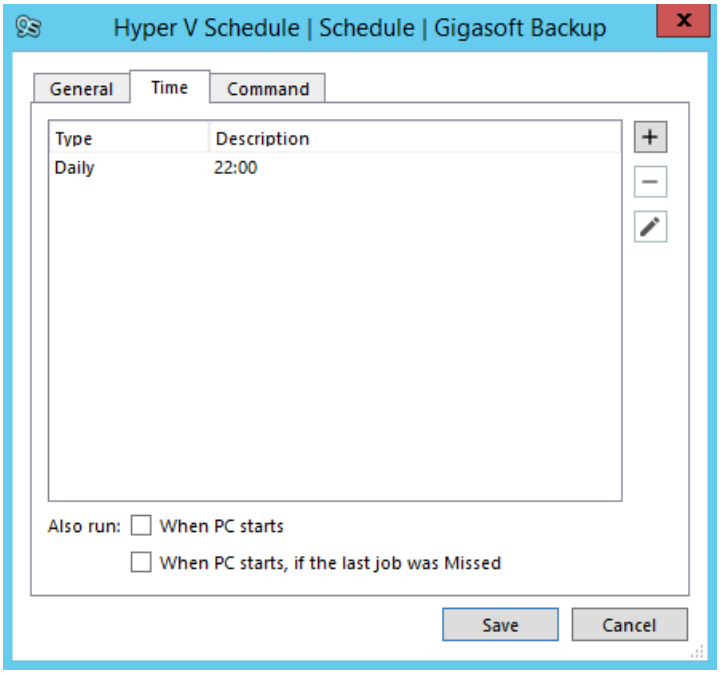
Here we can set the name of the backup schedule and select which vault this backup will go to. In this example we will name the schedule *Hyper V Schedule* and use the default offsite storage vault. Change the options if you want the job to stop after a certain amount of time or to skip another backup if there is one already running, you can also limit the bandwidth available to this protected item, this is especially useful if you have a large amount of data and you don't want it to use all of the available upload bandwidth.
On older machines or machines that are busy we can now request that GBM uses a single disk thread, this causes the backup to take a bit longer but uses less resources, this is useful if you find your machine is running slower than normal when the backup is running, now click on the **[Time]** tab.



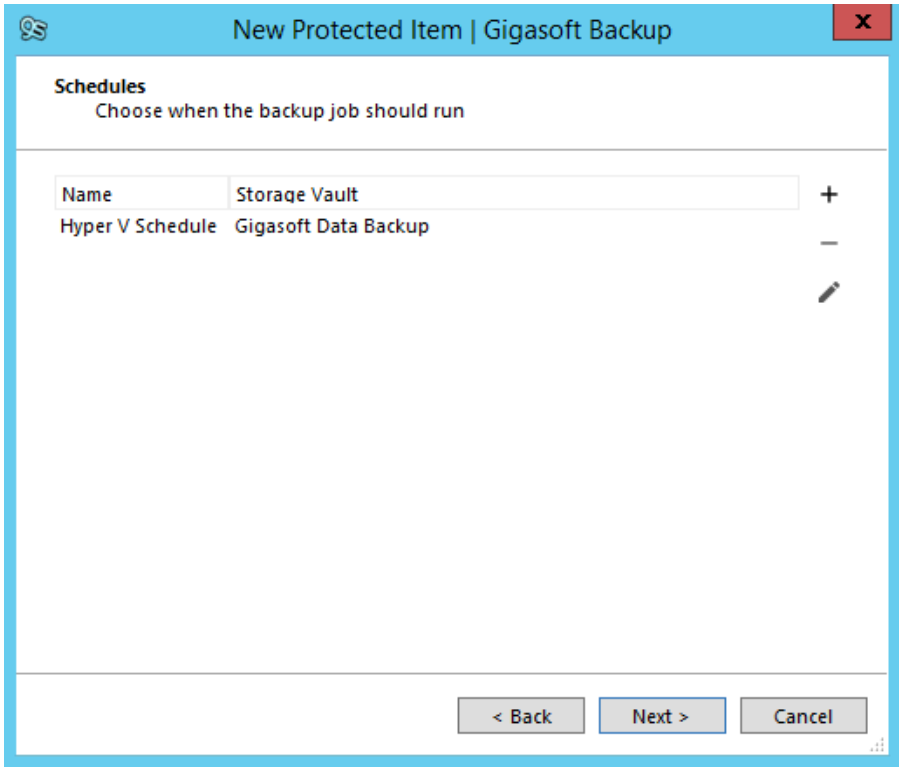
On this page we can set a schedule for this protected item to run, we can create multiple schedules if needed but, in this example, we will just create the one. Click on the **[+]** button to add a schedule



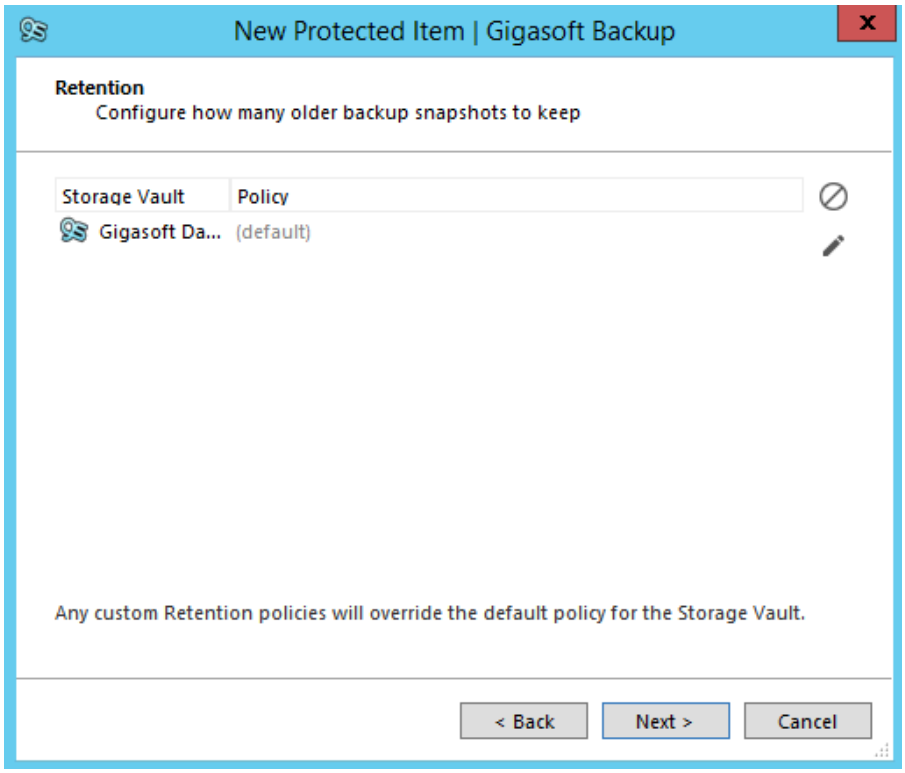
Use the drop down to select the desired type of schedule, in this example we will set the schedule to run daily at 22:00, click **[OK]** once you are done.



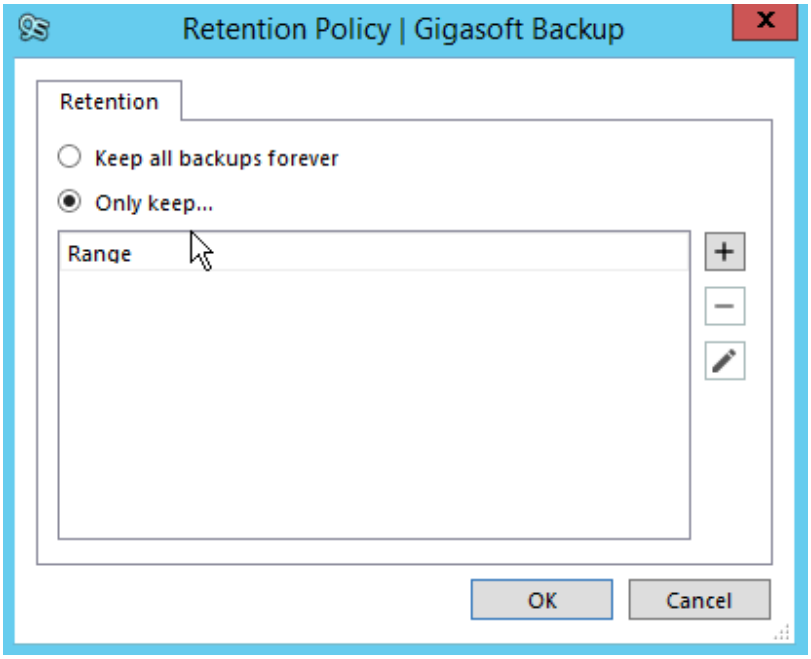
You are now taken back to the schedule overview page, from here you can add more schedules if you need to, you can set any pre or post commands to run at the schedule from the Command tab if needed else click the **[Save]** button to move on.



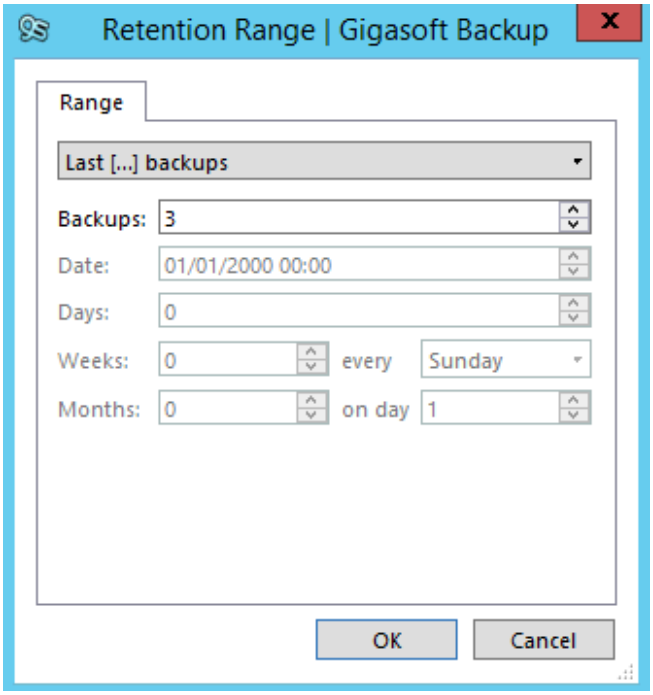
We are now back to the schedule overview page, we now need to set the retention policy for this set. Click on the **[Next]** button.



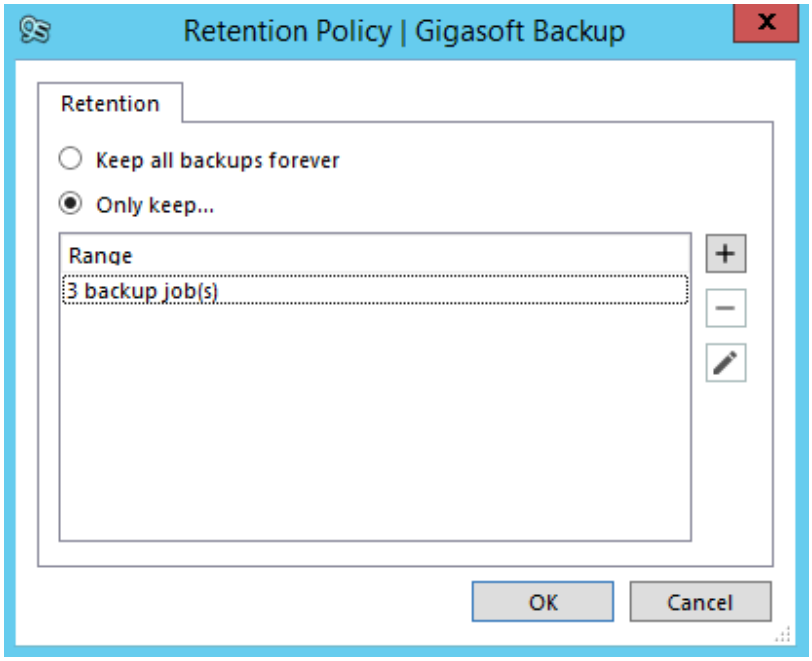
Here you can see there is a default retention policy set, this is to keep all the data forever, to change this to one that suits your needs click on the current policy to highlight it and then click the **[pencil]** button.



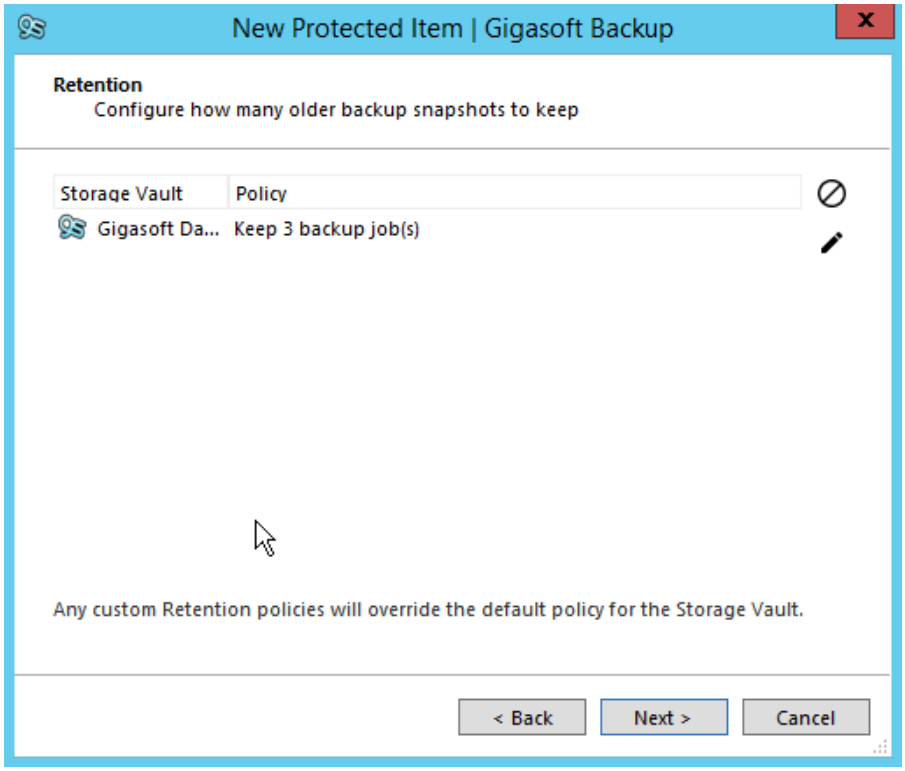
Here you can see the retention will be kept forever, change the radio button to **[Only keep…]** and then click on the **[+]** button.



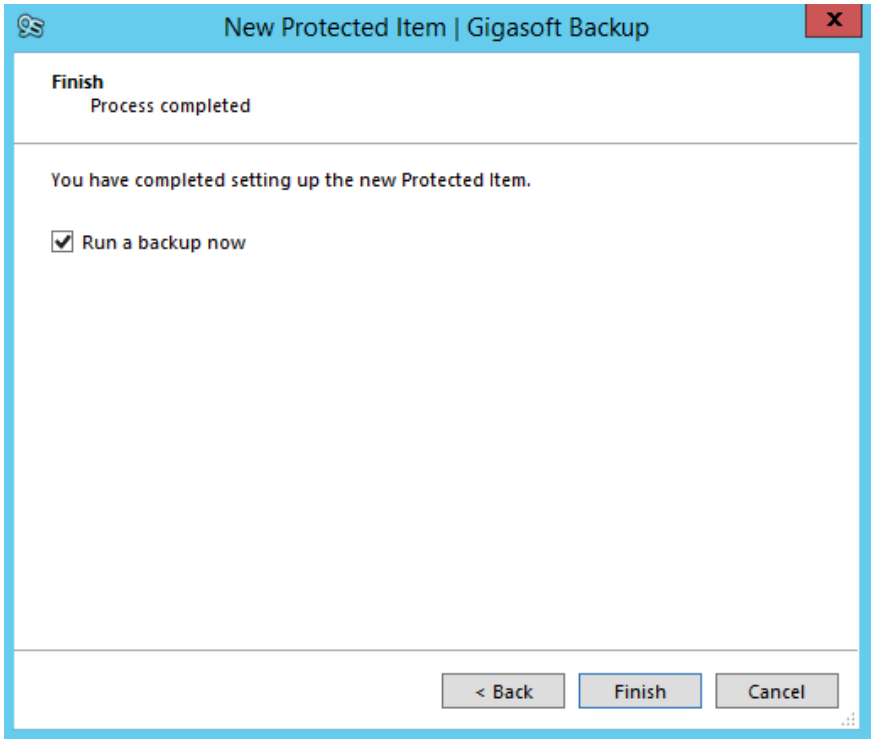
Use the drop-down selection box to choose a retention schedule that suits you, in this example we will select *Last […] backups*. In the next box we will select *3* this will allow us to keep the last 3 backups, this can be changed to anything you require. Once you have completed your selection click the **[OK]** button.



You will now be taken back to the overview page, you can set other retention policies if needed else please click the **[OK]** button.



Now we are back to the retention overview page, once you are happy you have all the settings you need click the **[Next]** button.

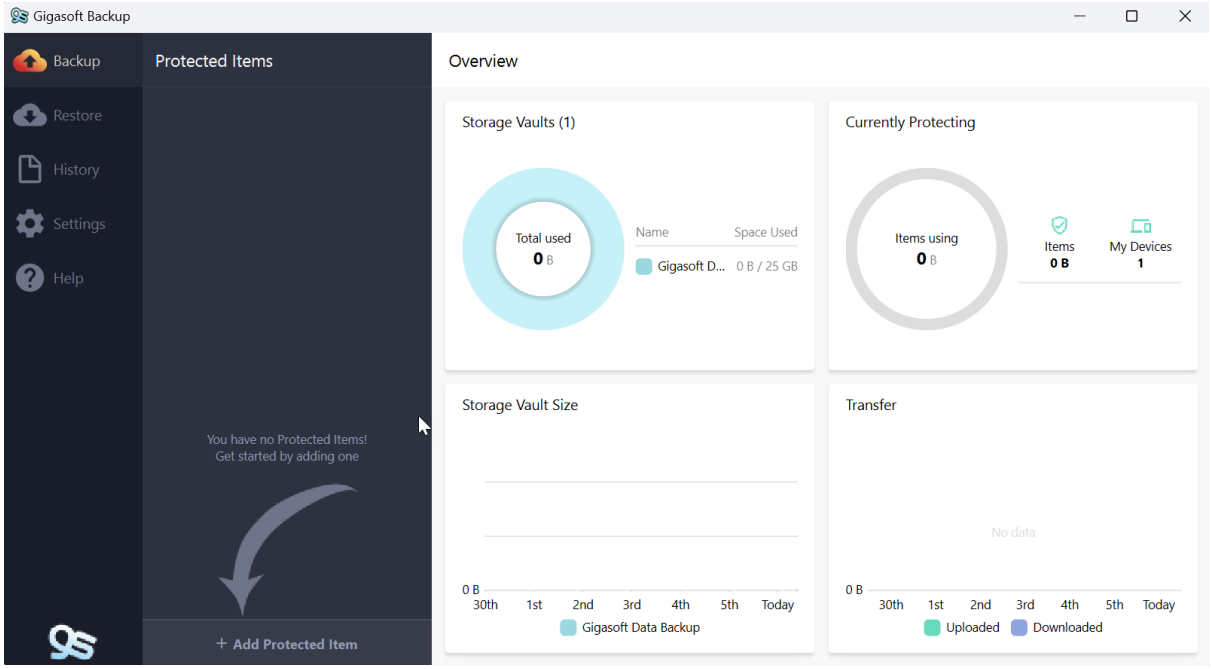


Now you are given the option to run a backup now by just clicking **[Finish]** but if you do not wish to run the backup now untick the radio button **Run a backup now** and then click the **[Finish]** button to finish the wizard.

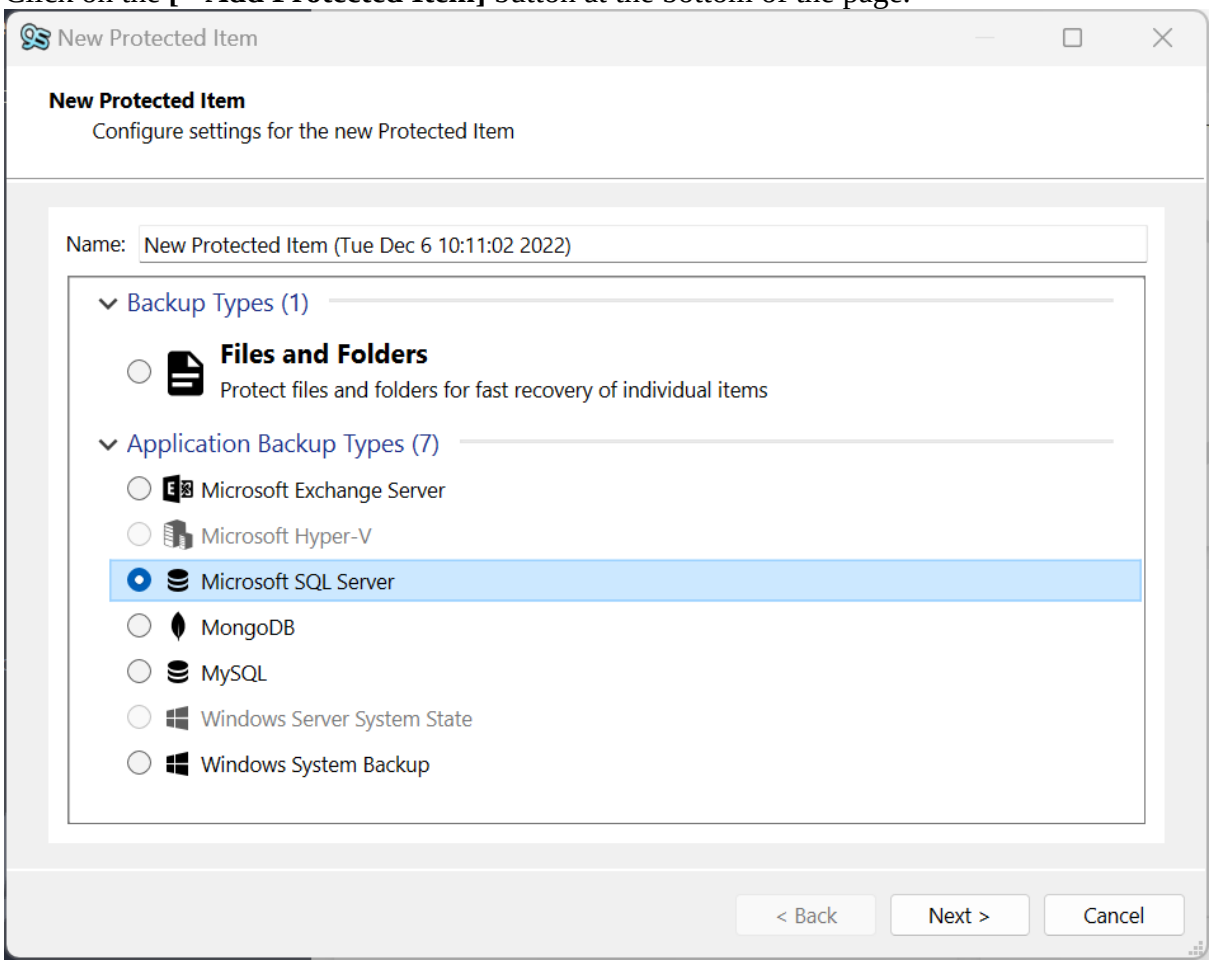
After clicking finish you are taken back to the main dashboard, from here you can create further protected items if you need to.

6.4 SQL protected item

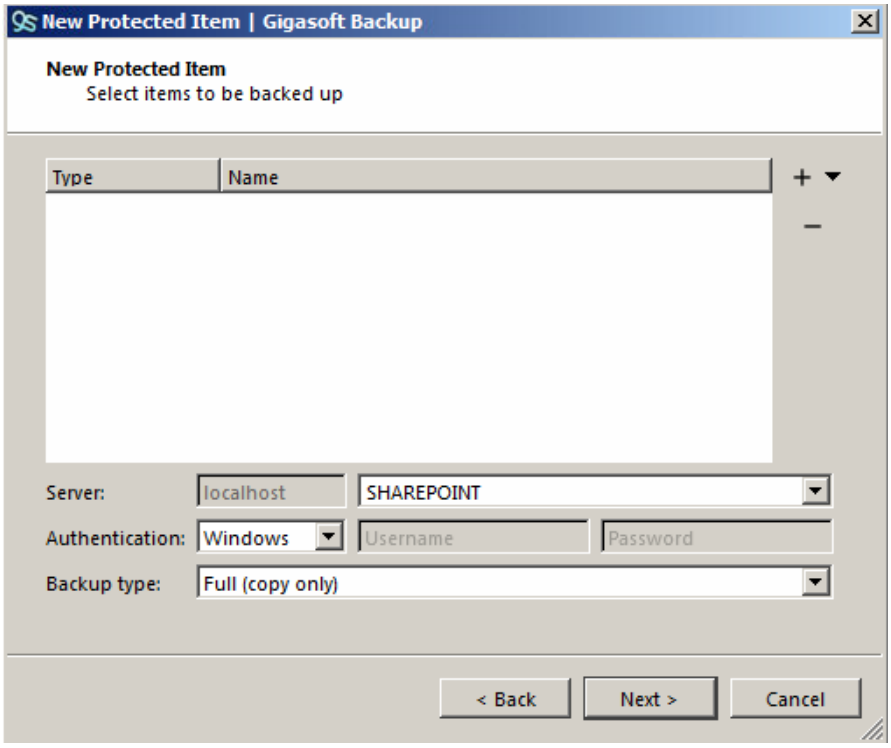
In this section we will guide you through the process of creating a SQL Server protected Item. To be able to back up SQL you need to make sure the SQL services are running on this machine.
Firstly, log into the Gigasoft Backup client



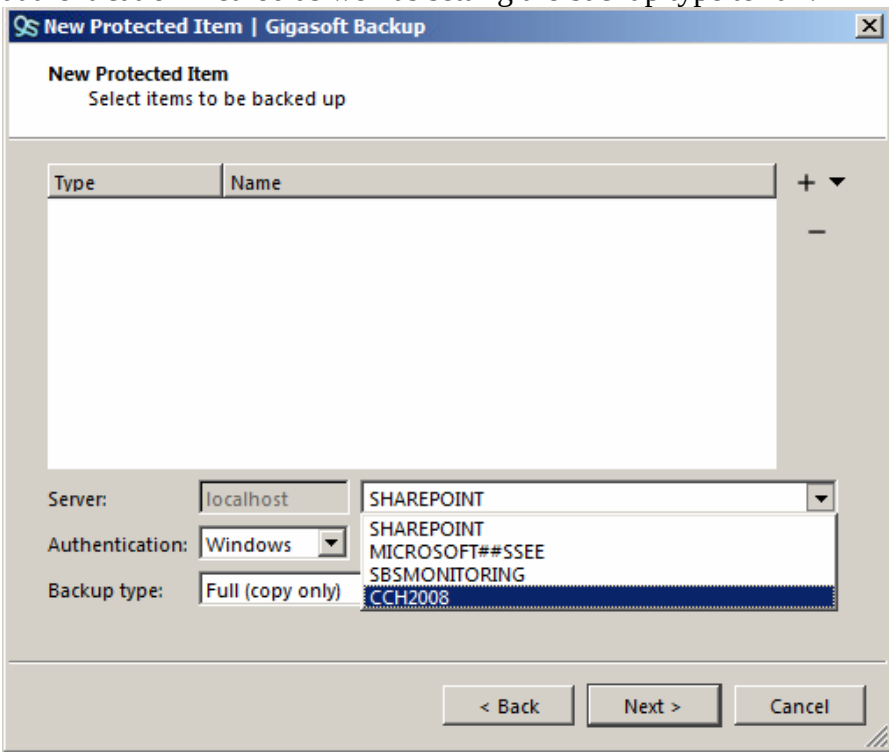
Click on the **[+ Add Protected Item]** button at the bottom of the page.



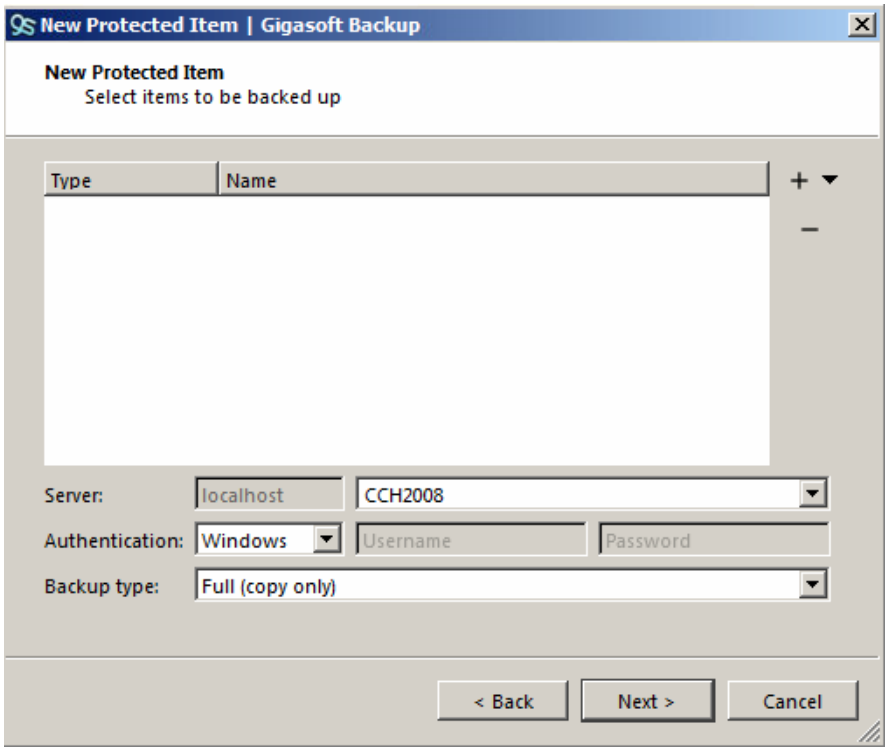
From the drop-down menu select the **[Microsoft SQL Server]** option and then change the name to a more meaningful protected item name, in our example we will use *SQL Backup*, now click on the **[Next]** button to add the items to the protected item.



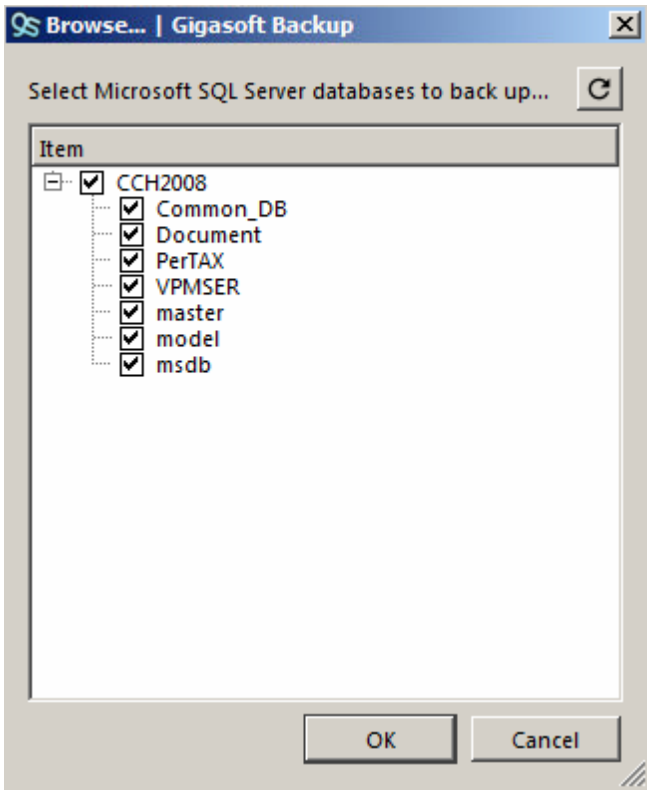
By default, the system will select the first Database it finds and will use the windows authentication method as well as setting the backup type to full.



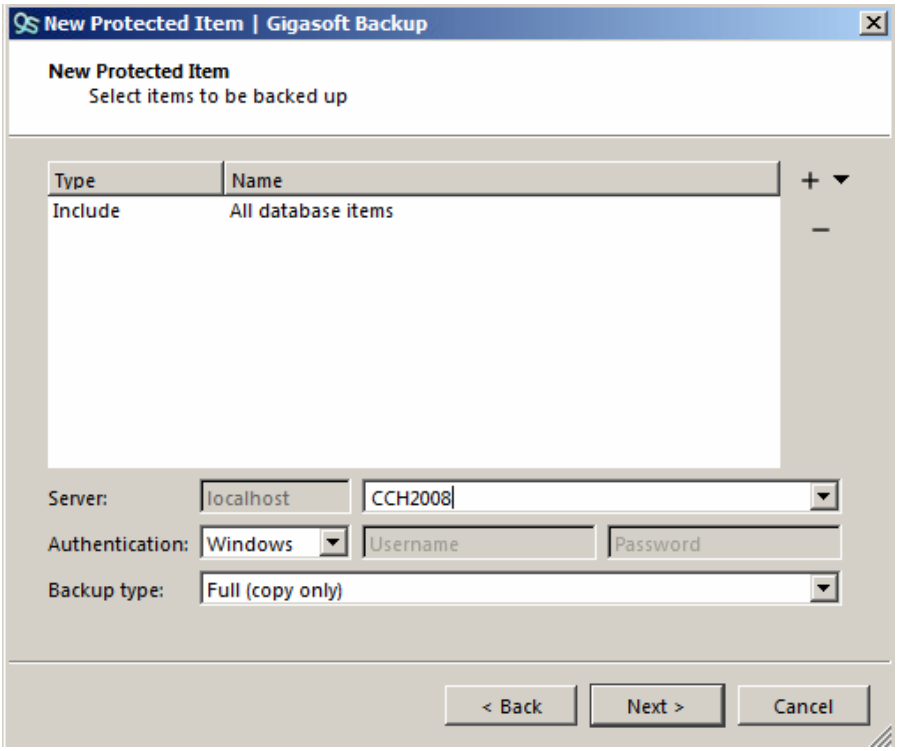
Use the drop down to select the database you wish to backup, in our example we will back up a database called *CCH2008*



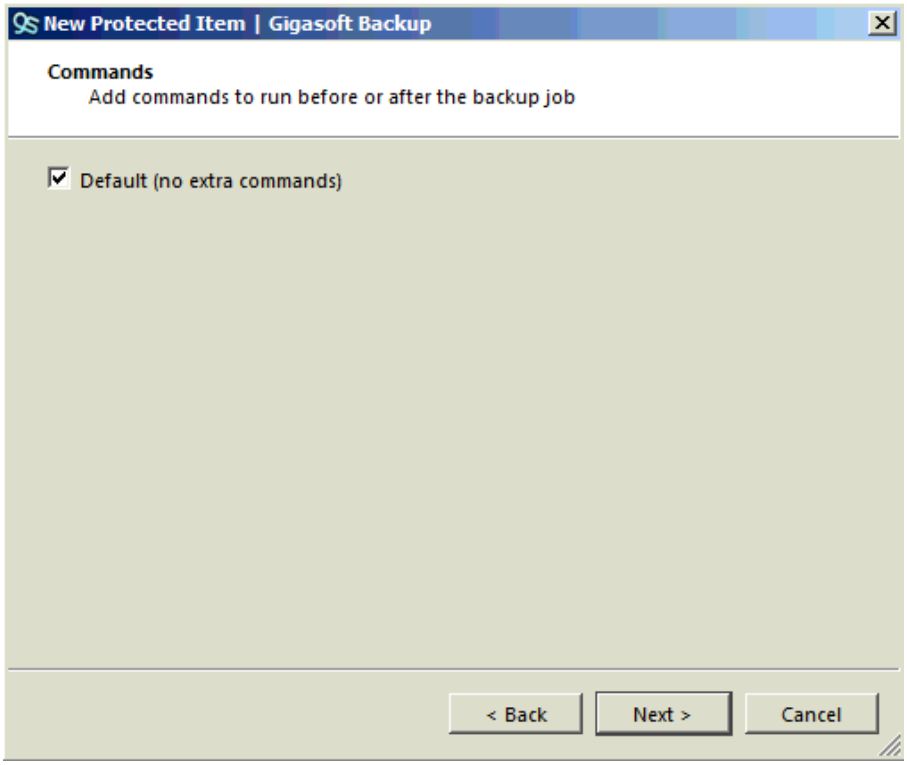
Now we need to choose the tables that are backed up under this database, Click on the **[+]** icon.



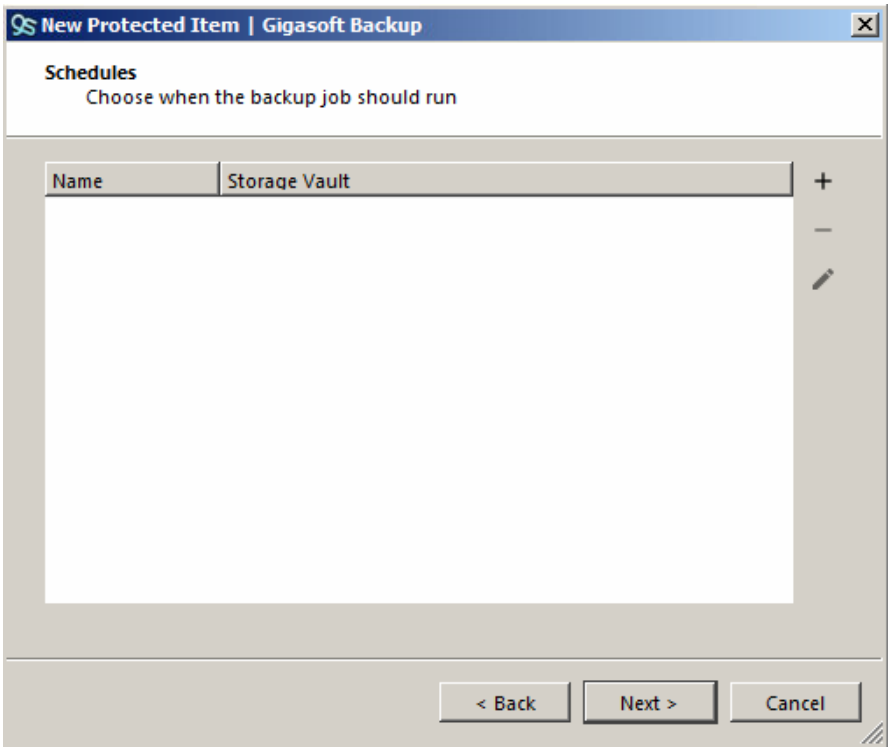
In this example we will select all the tables under this database but you can select only the tables you need if needed. Now click **[OK]** to proceed.



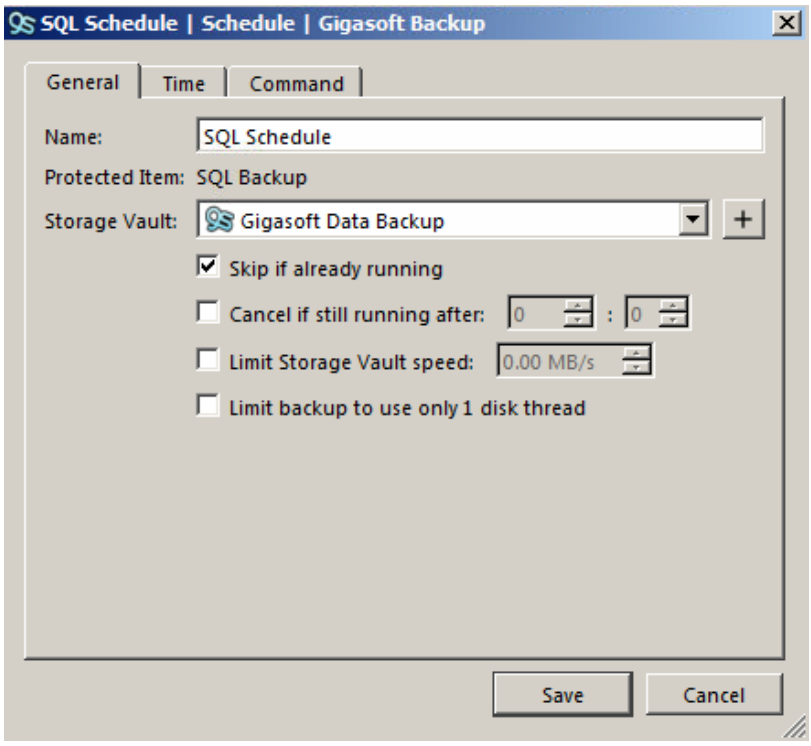
Here is the items overview page showing that we will be backing up all the database items of the database selected, we will be using the Windows Authentication and performing a full backup, click on **[Next]** to continue



If you need to run any pre or post commands for this protected item untick the **Default (no extra commands)** option and follow the prompts else leave this checked and click on **[Next]** button to set a schedule.

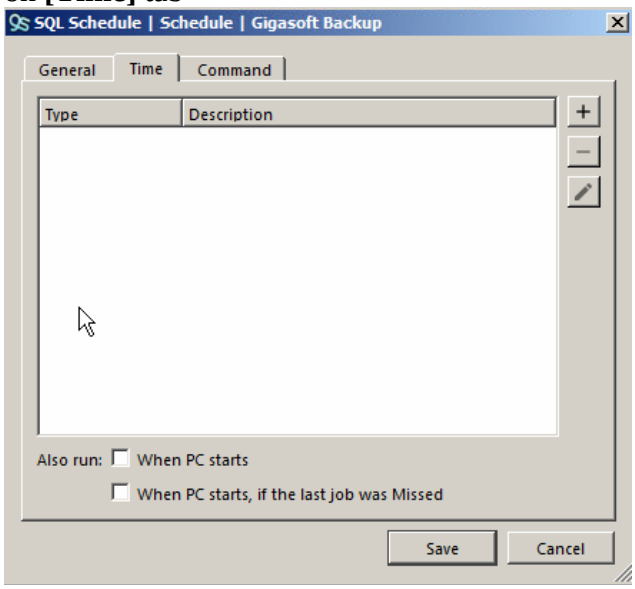


Click on the **[+]** button to add a schedule

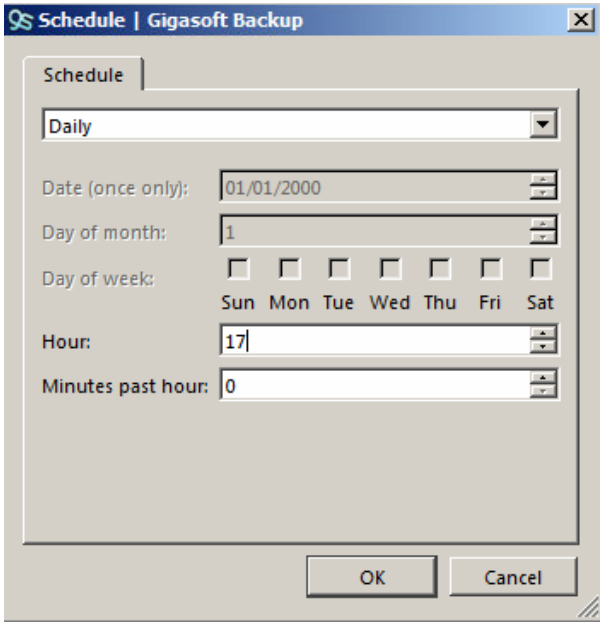


Change the name to a more meaningful name so that you can easily identify this schedule at a later date. You can also specify if the backup should skip running if it is already running from a previous schedule or you can cancel the job after a specified amount of time, you can also limit the bandwidth available to this protected item, this is especially useful if you have a large amount of data and you don't want it to use all of the available upload bandwidth.
On older machines or machines that are busy we can now request that GBM uses a single disk thread, this causes the backup to take a bit longer but uses less resources, this is useful if

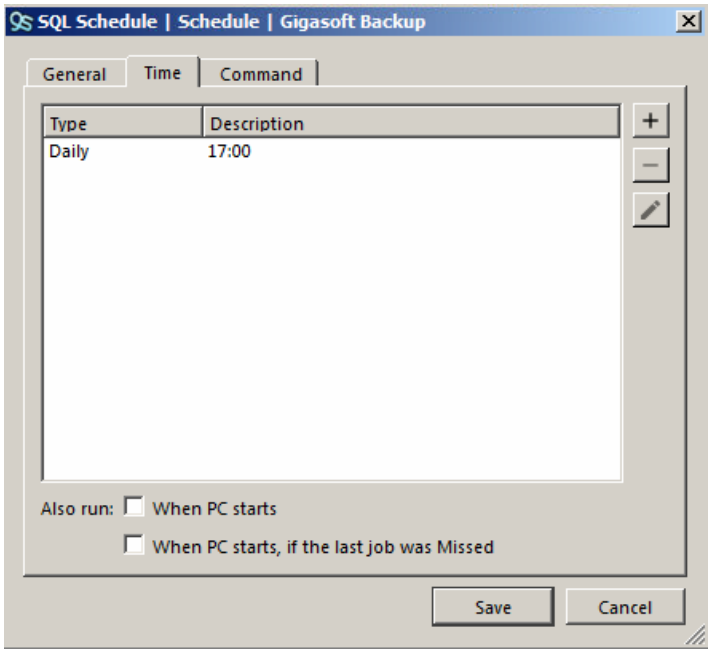
you find your machine is running slower than normal when the backup is running, now click on **[Time]** tab



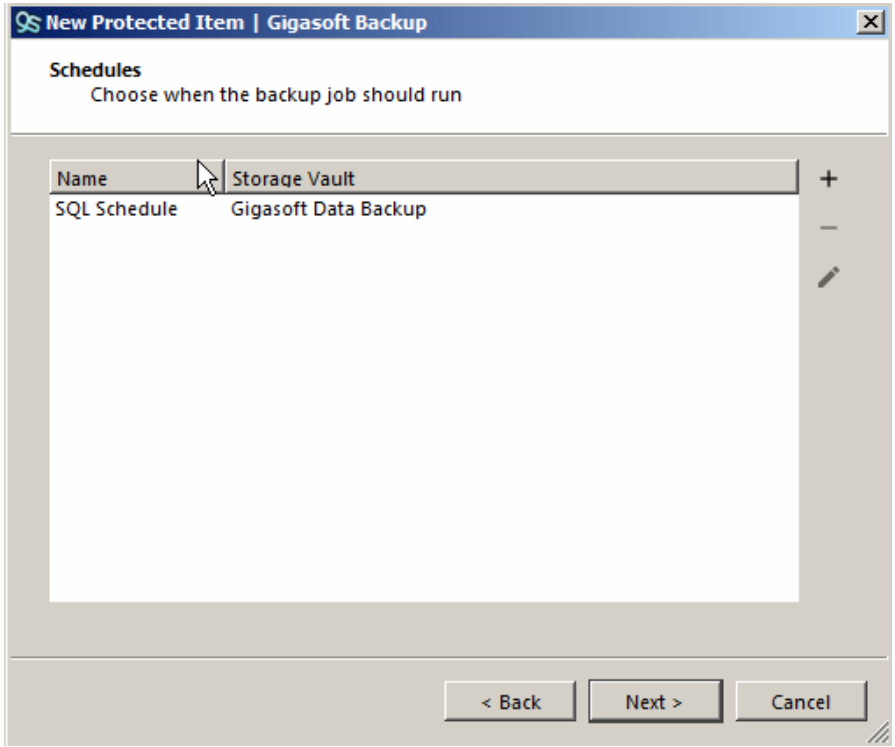
Click on the **[+]** button to add a time to run the schedule.



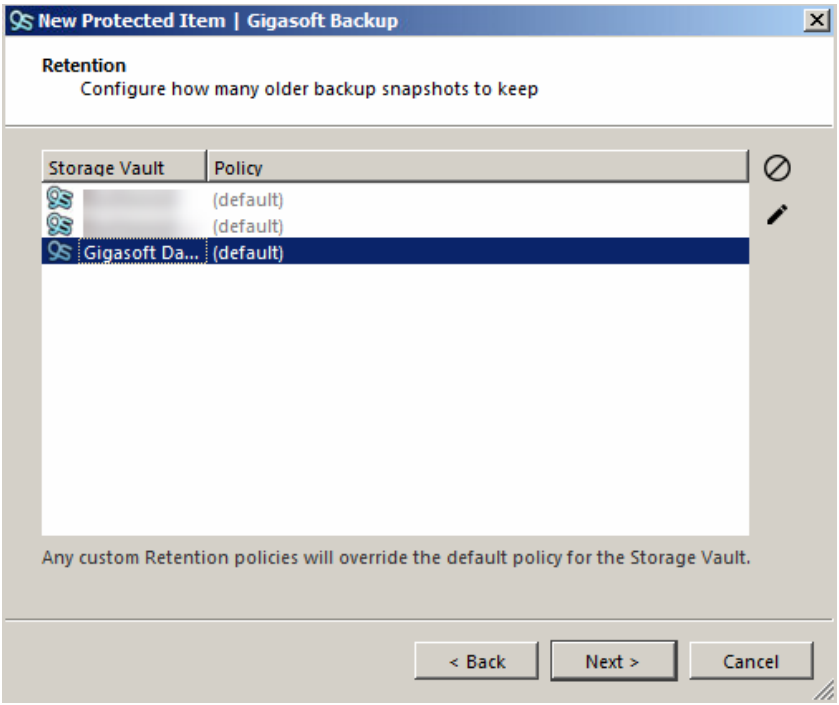
From the drop down select the type of schedule you want to run and then set the time / date. In our example we will select the daily option and run the schedule at 17:00, once you are done click **[OK]**.



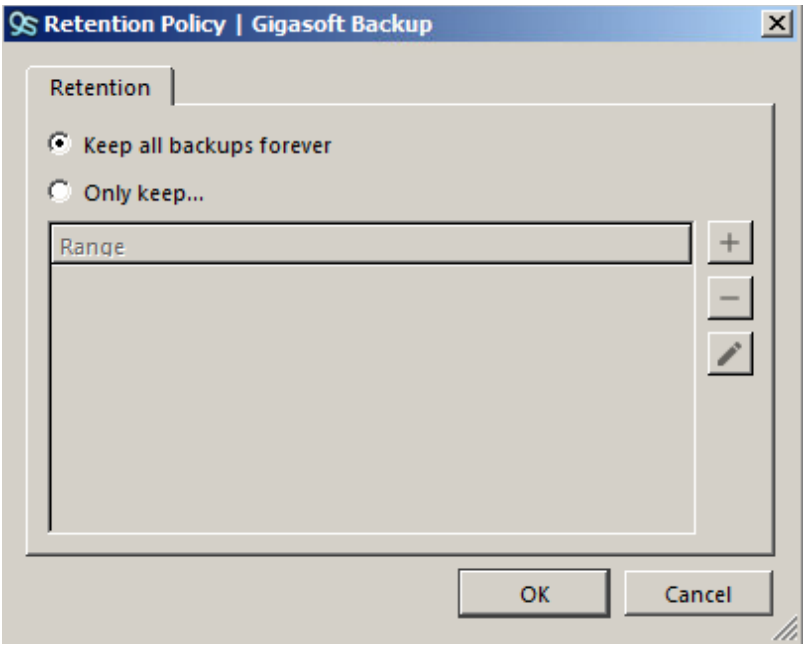
From here we can set additional schedules if we wanted to have the protected item run more than once a day, click the **[Command]** tab if you need to add any commands to the schedule else click the **[Save]** button to continue.



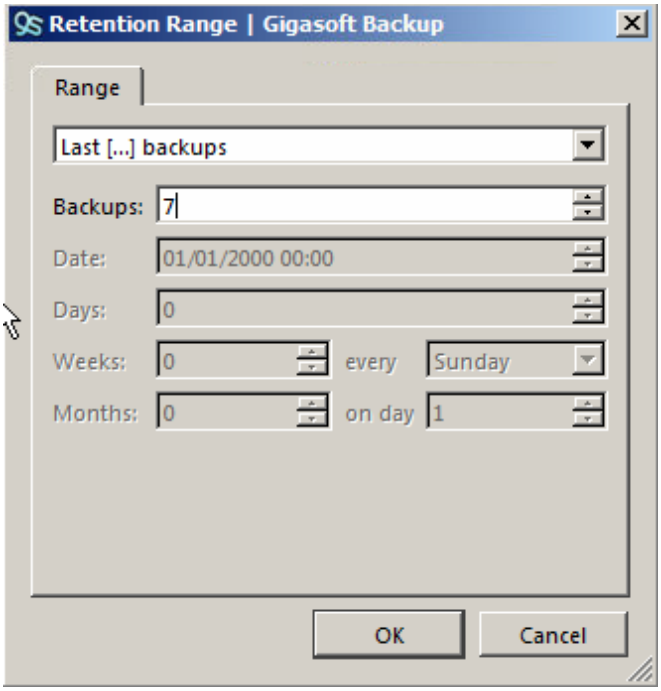
Here we are taken back to the schedule overview page, from here we can set schedules to go to other vaults if needed, click **[Next]** to continue



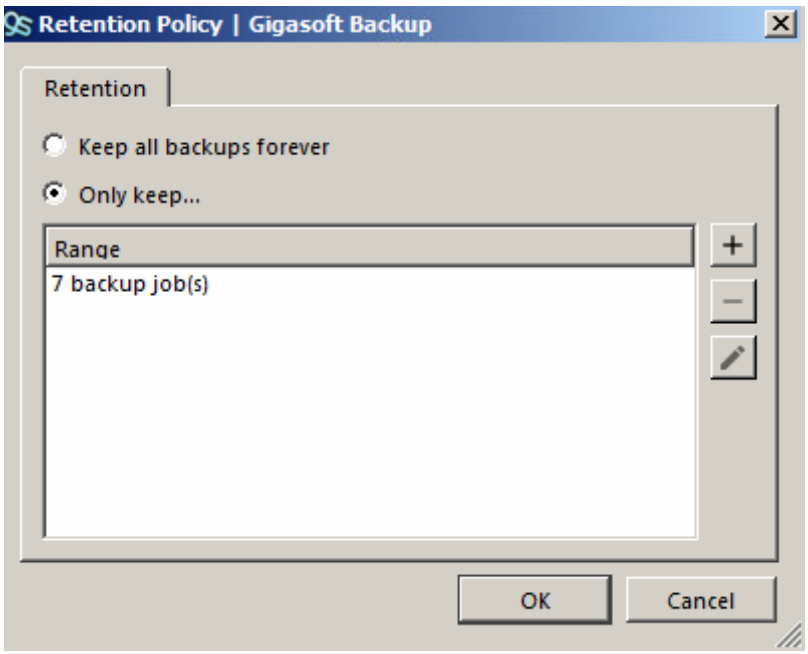
Now we need to set a retention policy for this protected item, by default it is set to keep all copies forever, to modify the existing policy click on it and click the **[pencil]** icon.



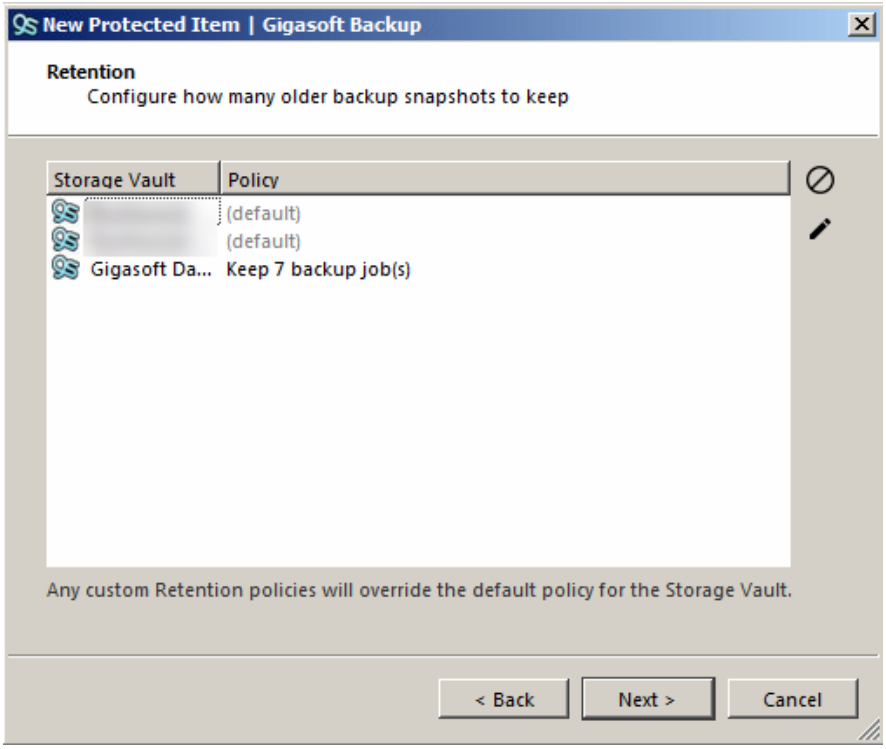
Here you can see that keep forever is selected, click on the **[Only keep…]** radio button and then click on the **[+]** button.



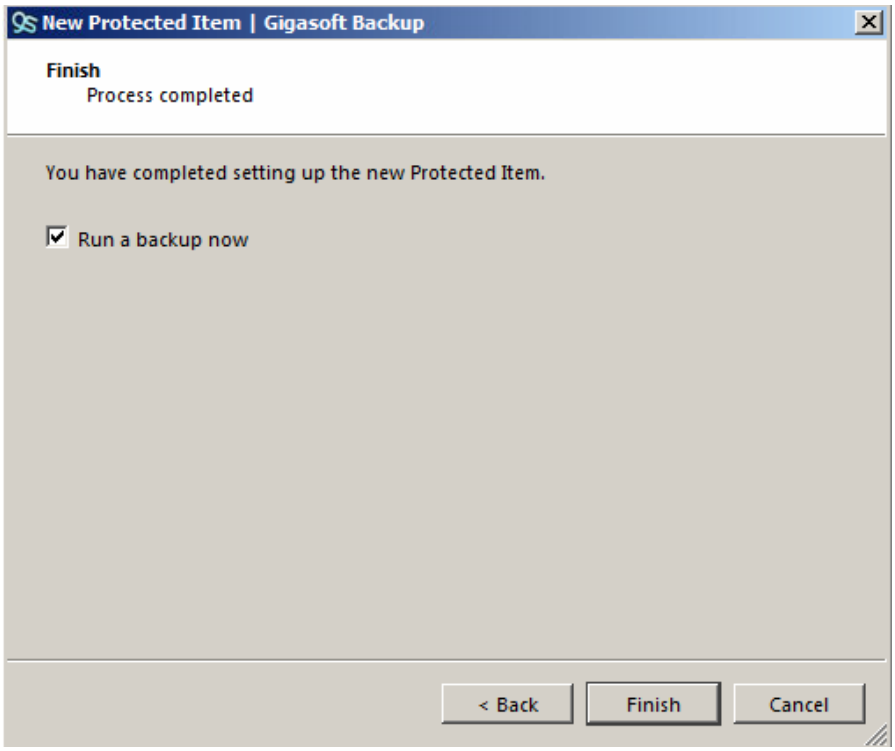
Use the drop down to select the type of retention you require, in this example we will use the *Last (...) backups* and choose 7, this will give us 7 versions of our database in case we need to go back to a previous version for some reason. Once you have selected your settings click on **[OK]** to proceed.



Here we can see the Retention policy we just created, you can add additional policies if you need to, click **[OK]** to continue.



We are now back to the overview page, check you have all the correct settings you need and then click **[Next]**.

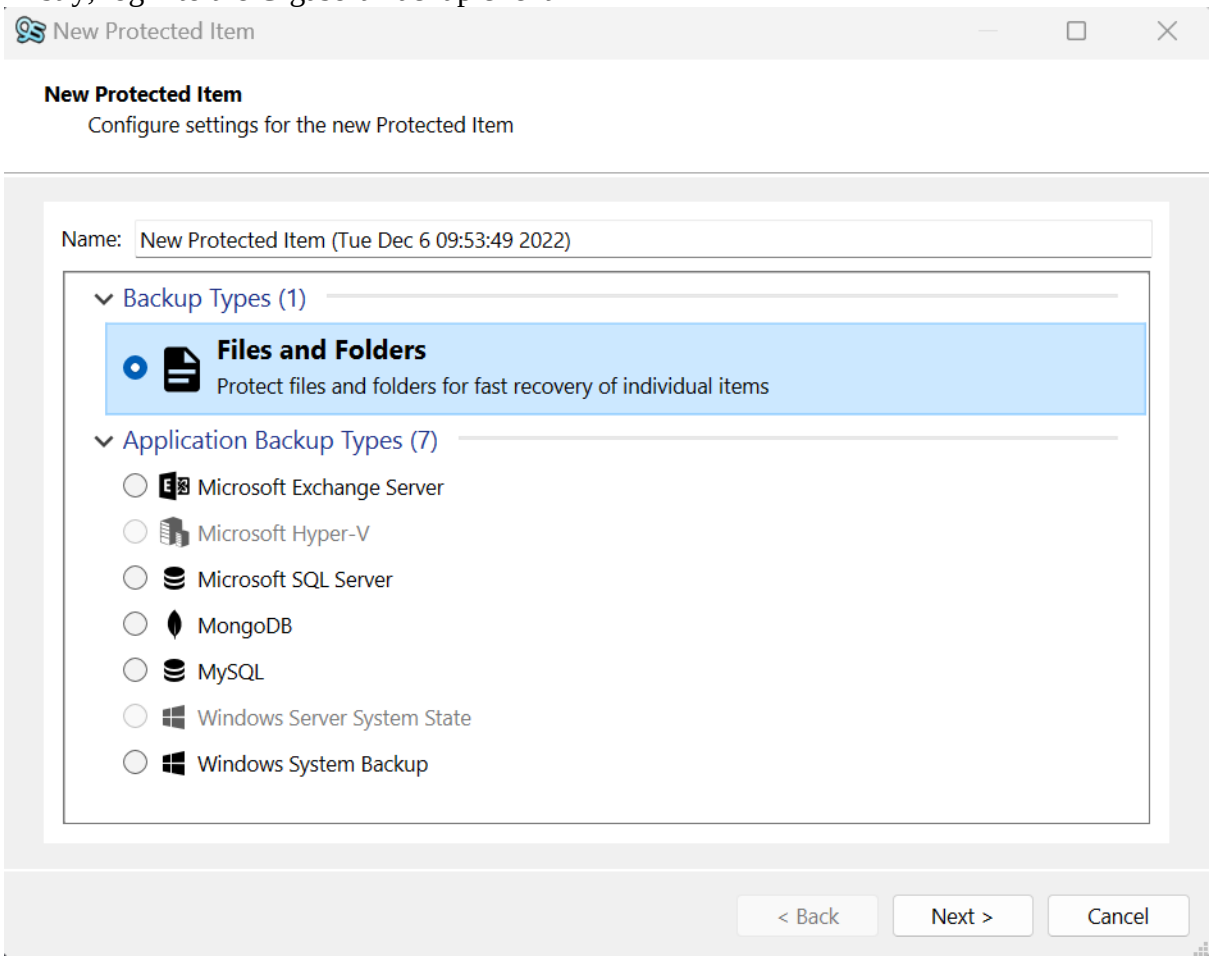


To run a backup now click **[Finish]** else uncheck the radio button **"Run a backup now"** and then click **[Finish]** to be returned to the client dashboard.

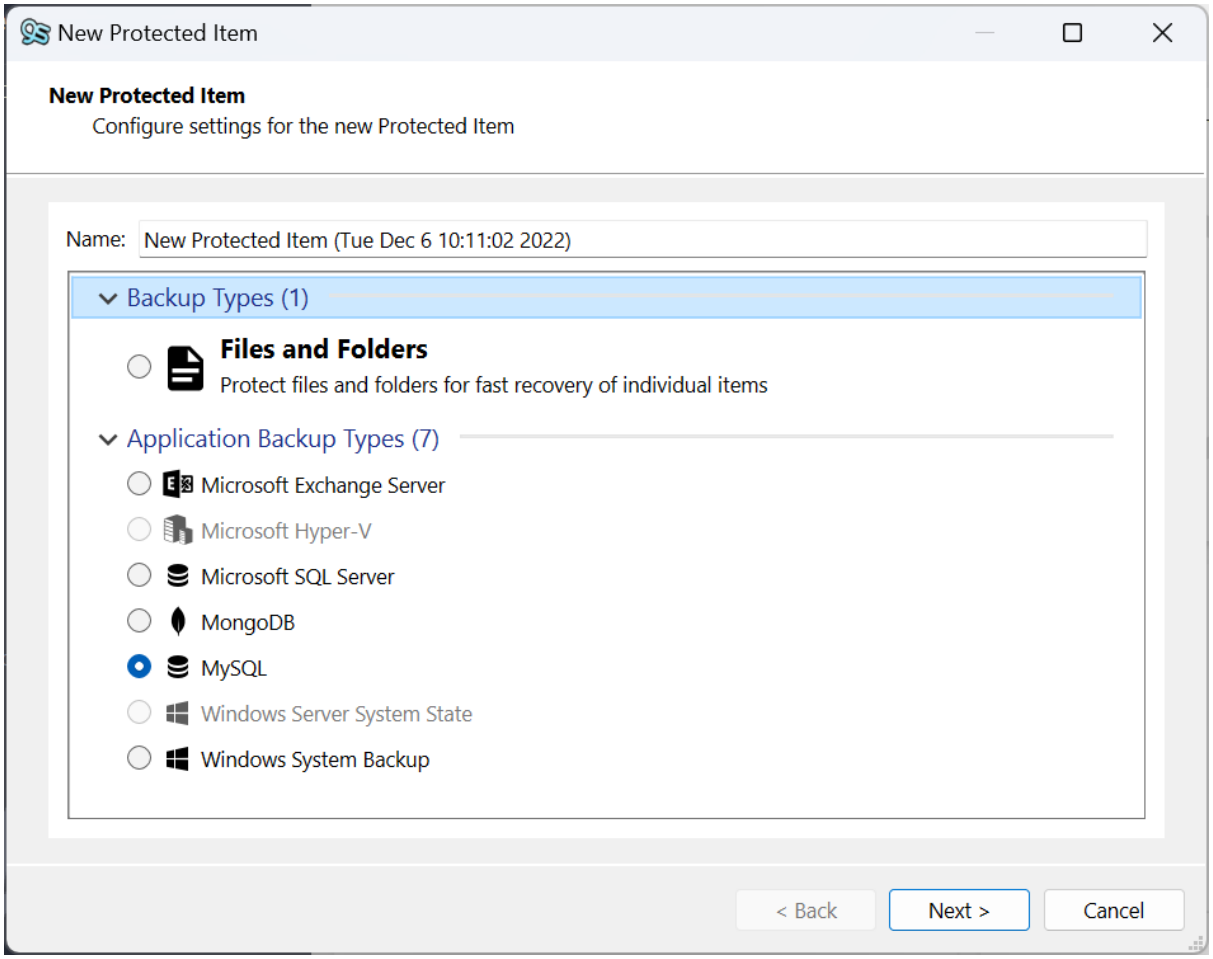
6.5 MySQL protected item

6.5.1 MySQL (Windows)

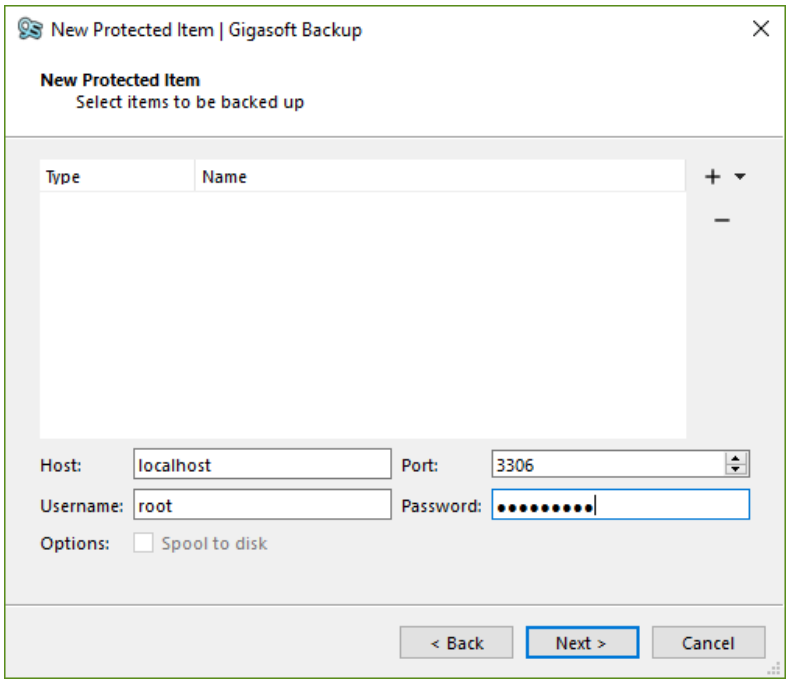
In this section we will guide you through the process of creating a MySQL protected Item. To be able to back up MySQL you need to make sure the MySQL services are installed and running on this machine. In this example we have used the supplied databases that can be installed when MySQL is first configured, your databases will obviously be different.
Firstly, log into the Gigasoft Backup client



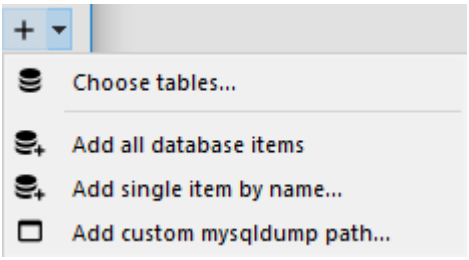
Click on the **[+ Add Protected Item]** button at the bottom of the page.



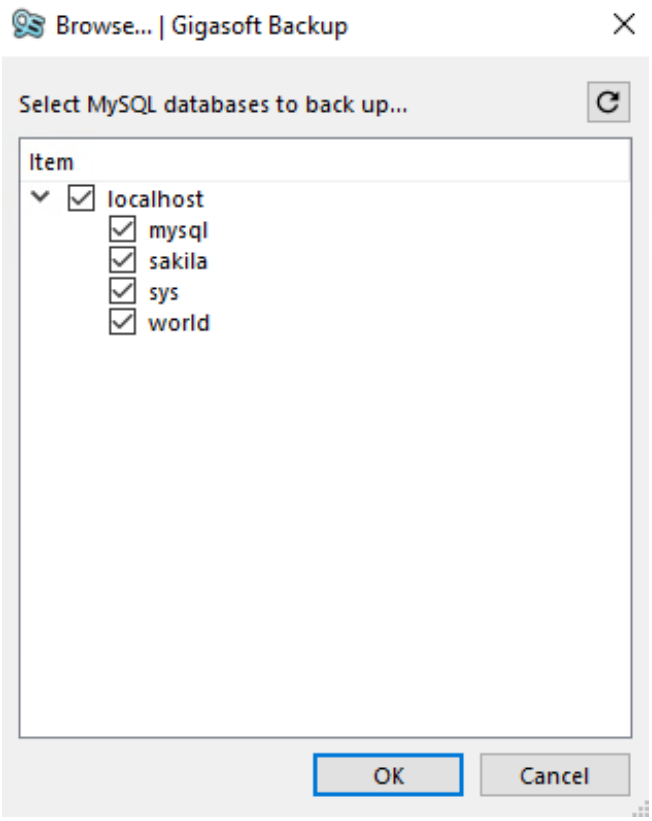
From the drop-down menu select the **[MySQL]** option and then change the name to a more meaningful protected item name, in our example we will use *MySQL Backup* click **[Next]** to continue



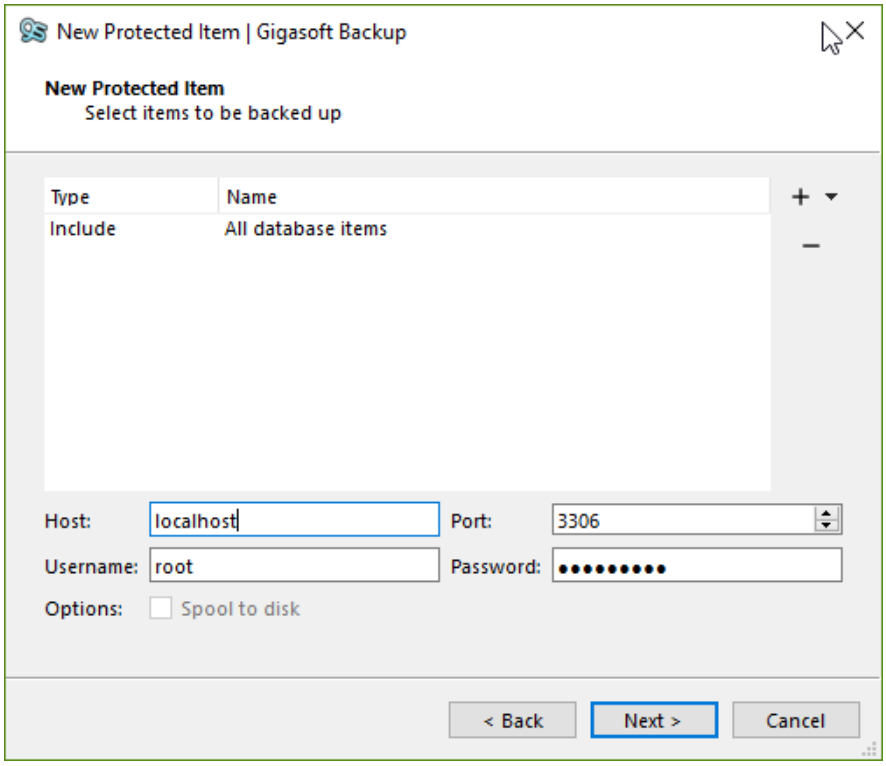
Now enter the Username and Password and verify the default port number is correct and click on the down arrow next to the **[+]** button



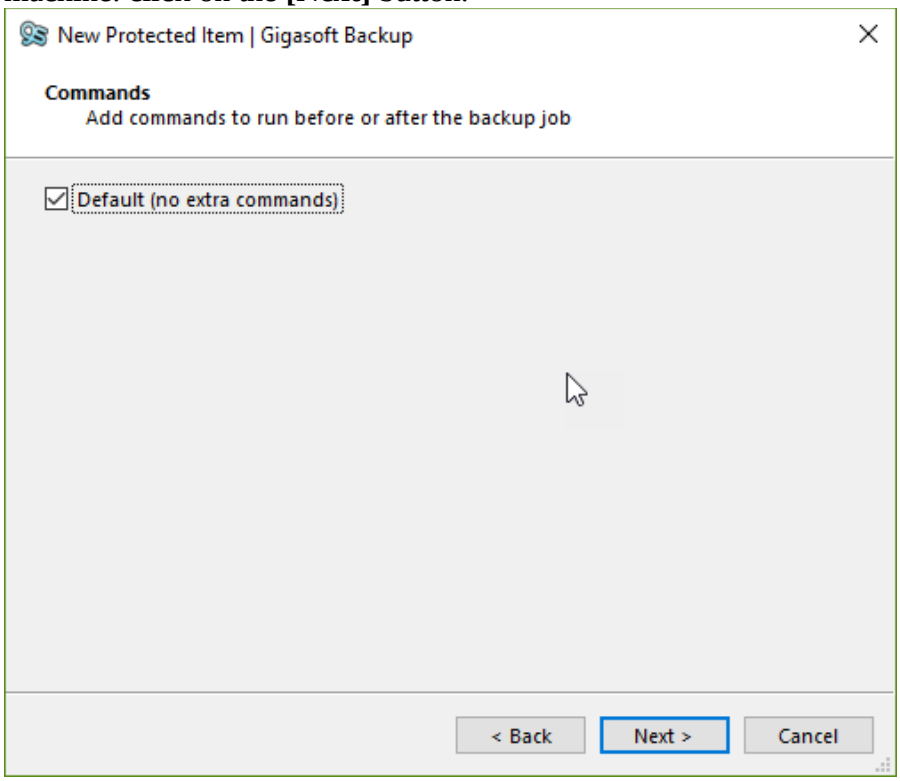
Here you will see some options on how to choose your database items, the most common and the one we will use is ***Choose tables…***



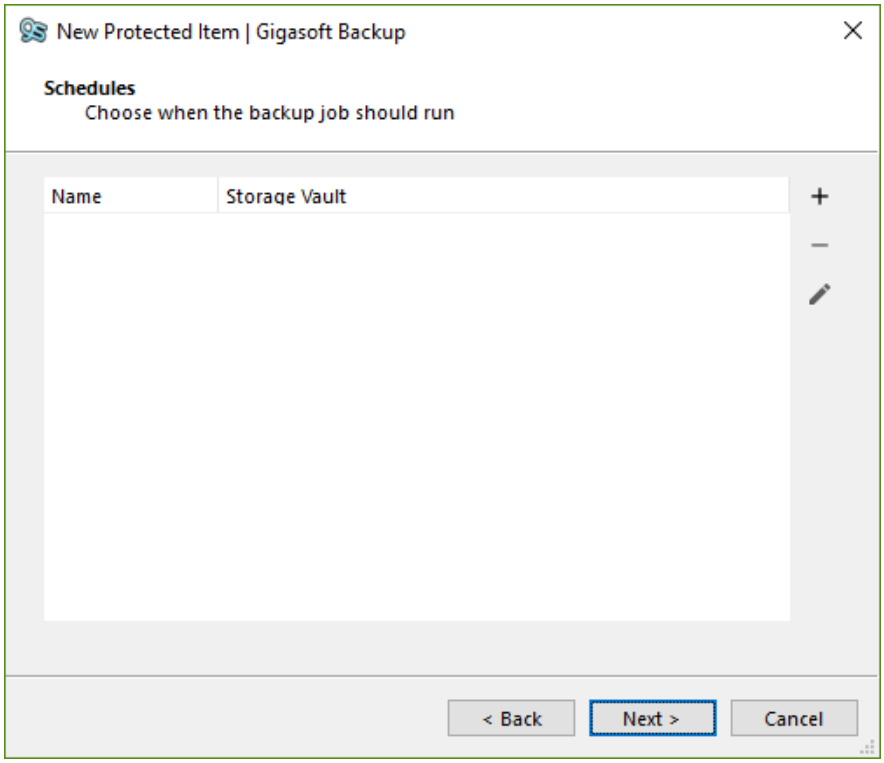
Now the client will return all the databases it has found for MySQL, simply select the ones you need or click the top box to select them all and click **[OK]**.



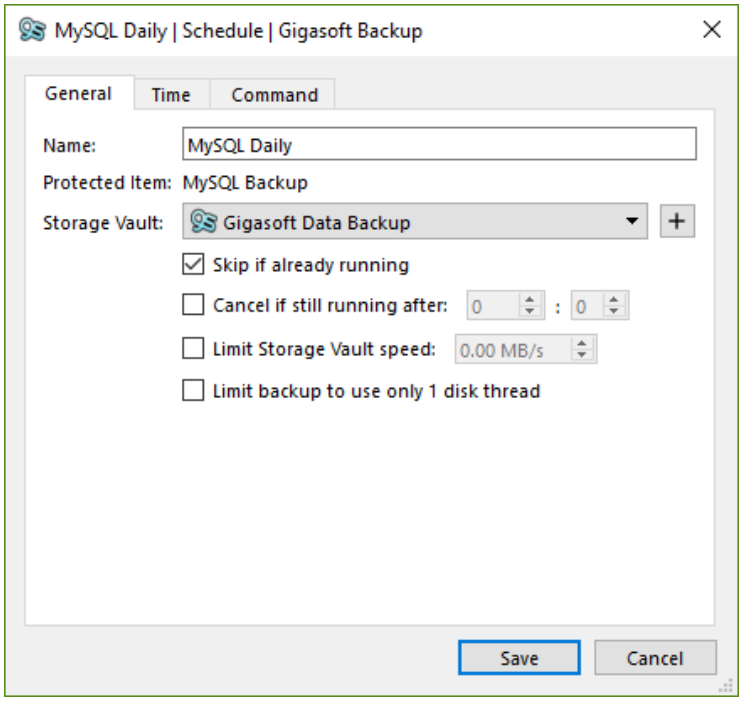
You will be taken back to the items overview page, from here you can see the databases that were selected in the previous step, in our example we have selected all the databases on this machine. click on the **[Next]** button.



If you need to run any pre or post commands please remove the tick from **Default (no extra commands)** and follow the prompts else leave this ticked and click **[Next]**.



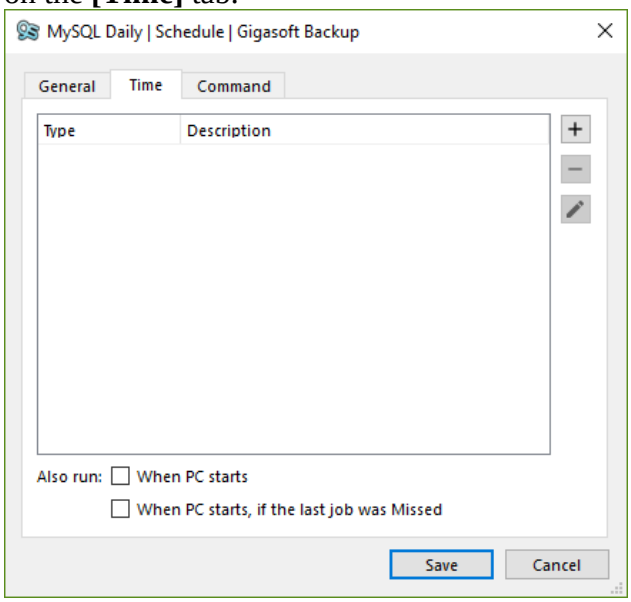
Click the **[+]** button to add a schedule for this protected item.



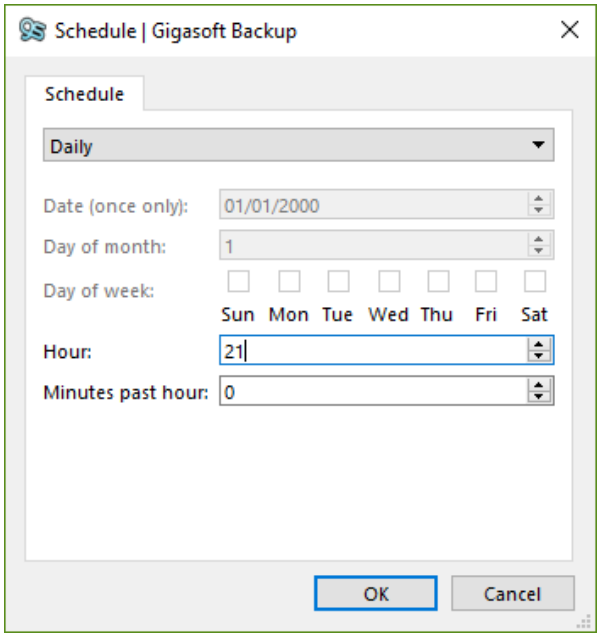
Enter a meaningful name into the Name box, we have used *MySQL Daily*, select which vault this backup will go to. In this example we will use the default *Gigasoft Data Backup storage vault*. Change the options if you want the job to stop after a certain amount of time or to skip another backup if there is one already running, you can also limit the bandwidth available to this protected item, this is especially useful if you have a large amount of data and you don't want it to use all of the available upload bandwidth.

On older machines or machines that are busy we can now request that GBM uses a single disk thread, this causes the backup to take a bit longer but uses less resources, this is useful if

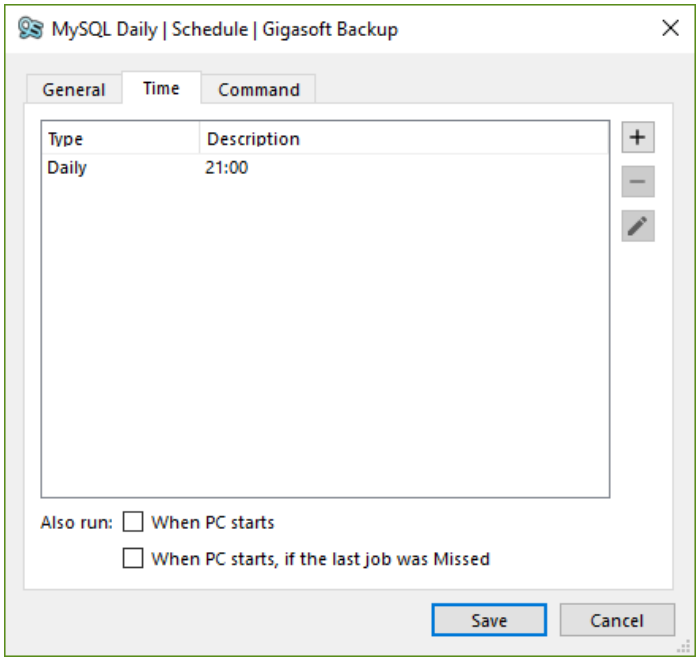
you find your machine is running slower than normal when the backup is running, now click on the **[Time]** tab.



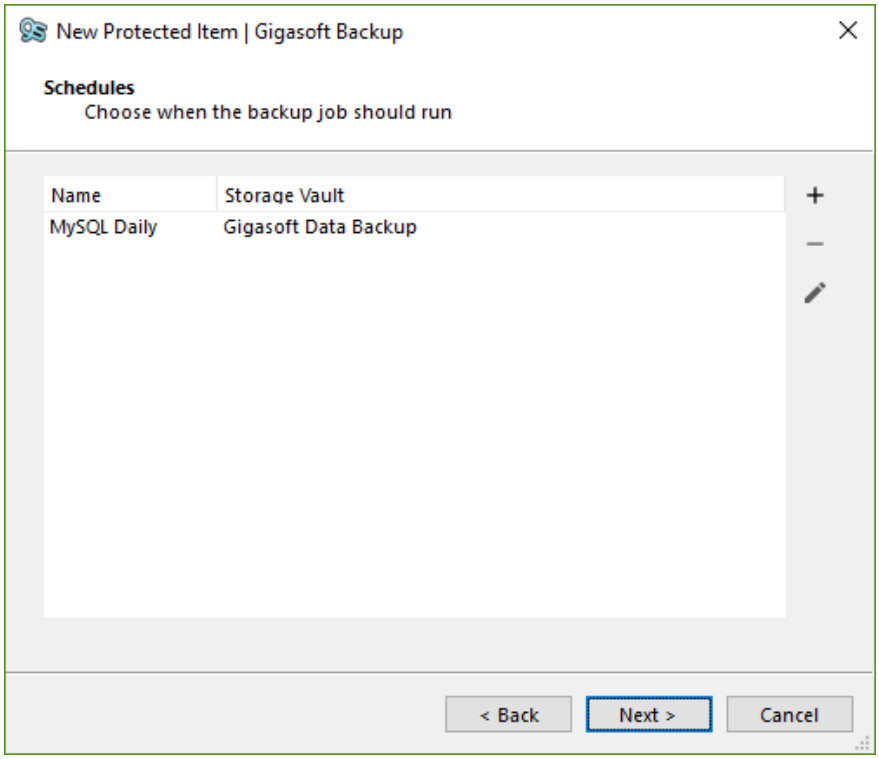
Here we can set a schedule for this protected item, we can create multiple schedules if needed but in this example, we will just create the one. Click on the **[+]** button to add a schedule



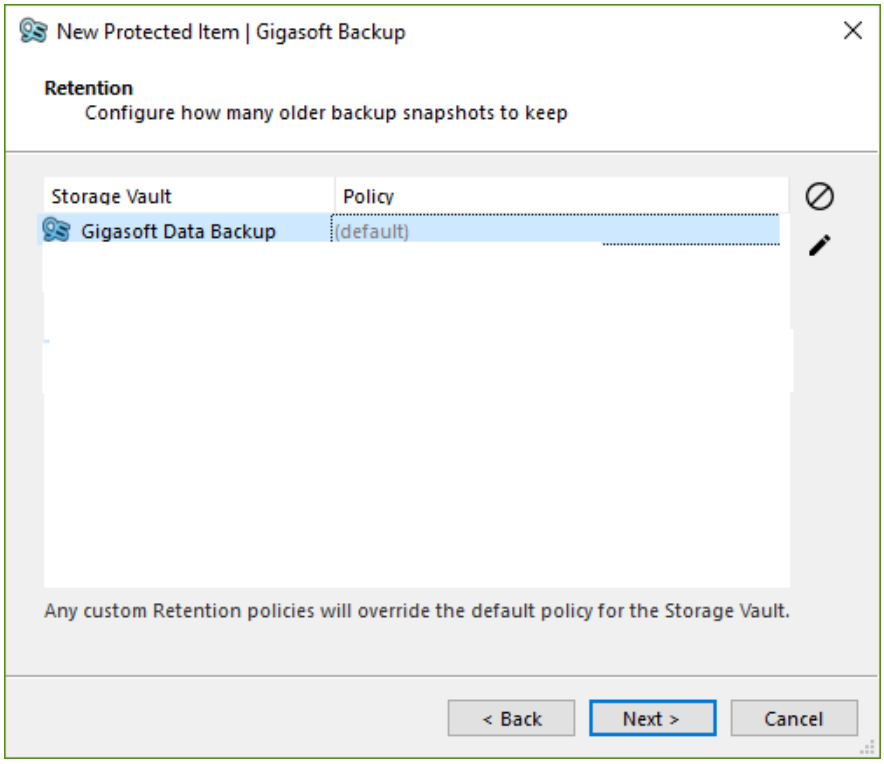
Use the drop down to select the desired type of schedule, in this example we will set the schedule to run daily at 21:00, click **[OK]** once you are done.



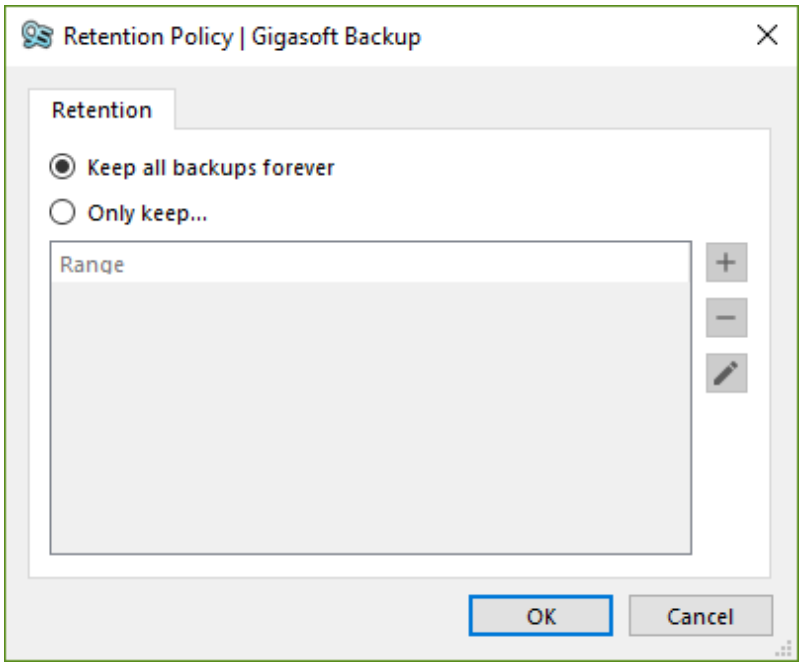
We are taken back to the schedule overview page, here you can add more schedules if needed, you can also set any pre or post commands if needed else click the **[Save]** button to move on.



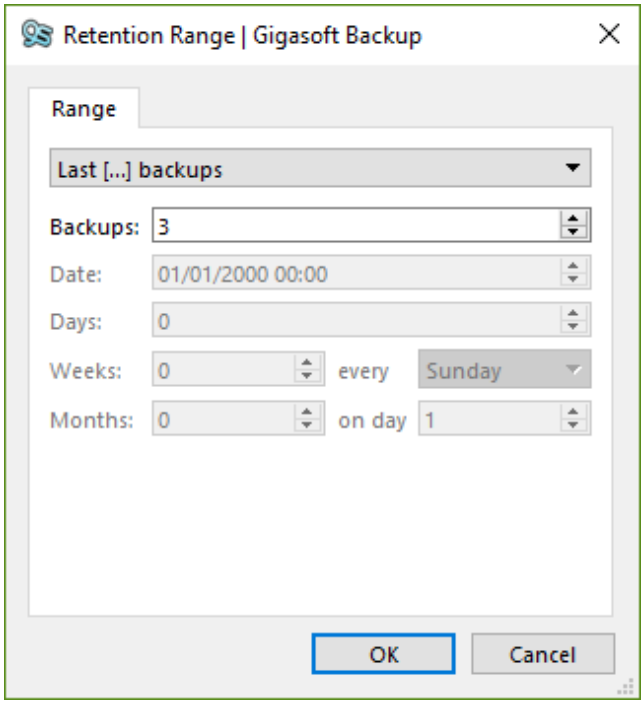
We are now back to the protected item overview page, we now need to set the retention policy for this set. Click on the **[Next]** button.



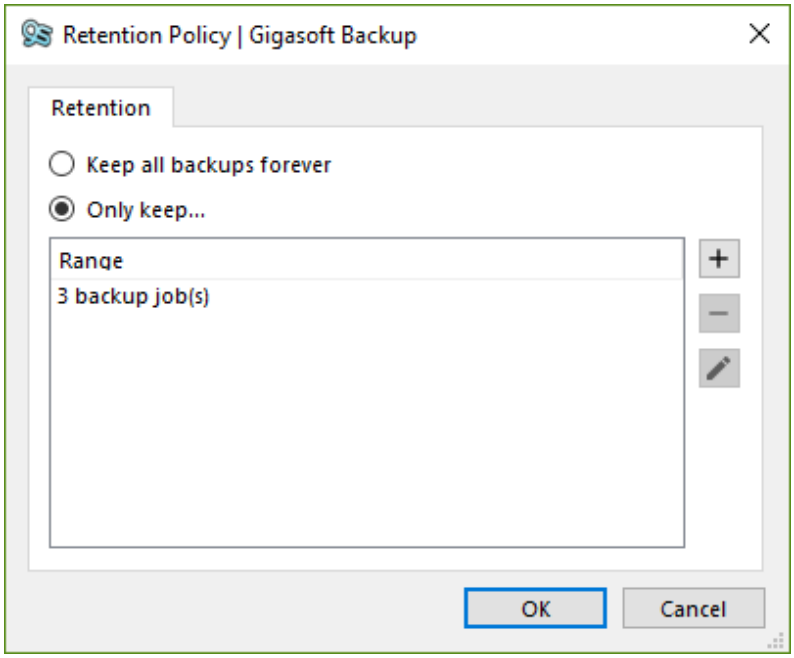
Here you can see there is a default retention policy set, this is to keep all the data forever, to change this to one that suits your needs click on the current policy to highlight it and then click the **[pencil]** button.



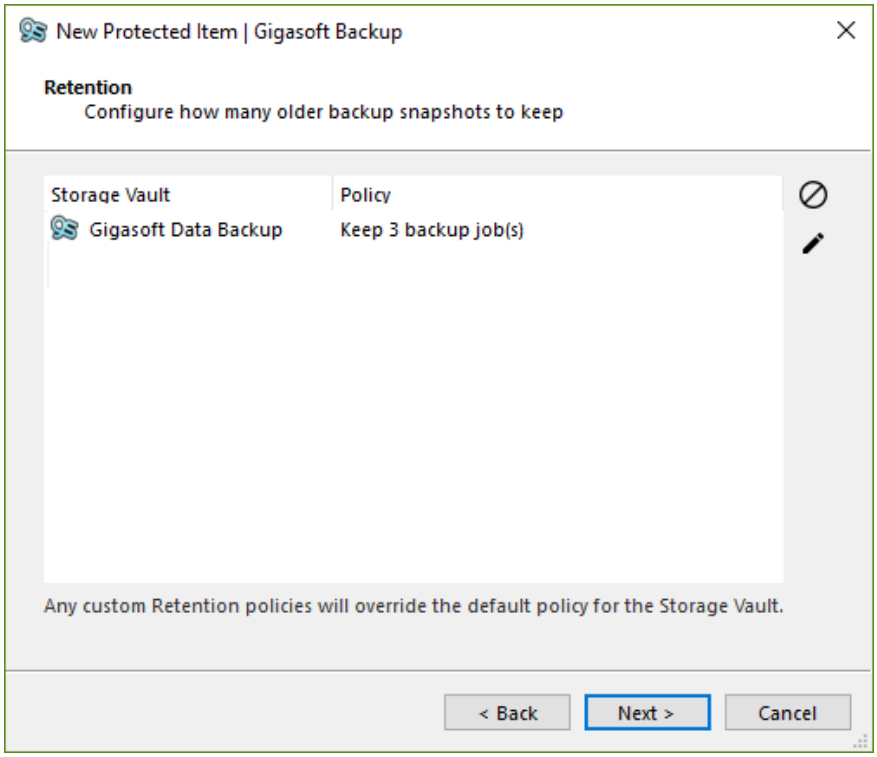
Here you can see the retention will be kept forever, change the radio button to **[Only keep…]** and then click on the **[+]** button.



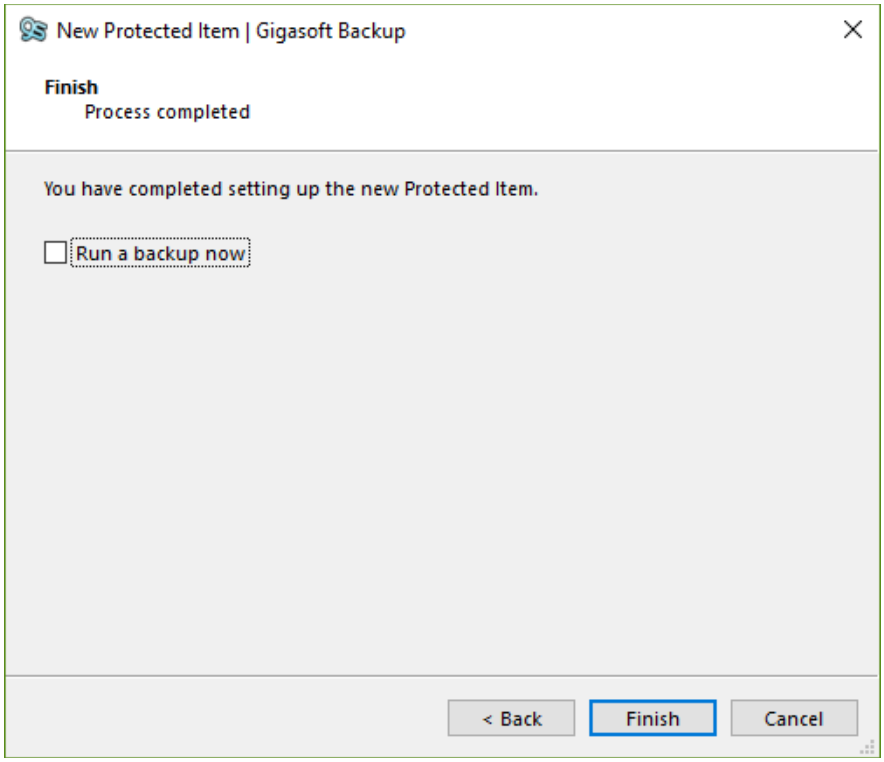
Use the drop-down selection box to choose a retention schedule that suits you, in this example we will select *Last […] backups*. In the next box we will select *3* this will allow us to keep the last 3 backups, this can be changed to anything you require. Once you have completed your selection click the **[OK]** button.



You will now be taken back to the overview page, you can set other schedules for this same protected item if you wish else please click the **[OK]** button.



Now we are back to the retention overview page, once you are happy you have all the settings you need click the **[Next]** button.



You will now be asked if you would like the run the backup now, if you do leave the box ticked and click **[Finish]** if you do not wish to run the backup now remove the tick in the **Run a backup now** box and click **[Finish]**

After clicking finish you are taken back to the main dashboard, from here you can create further protected items if you need to.

6.5.2 MySQL (Mac)

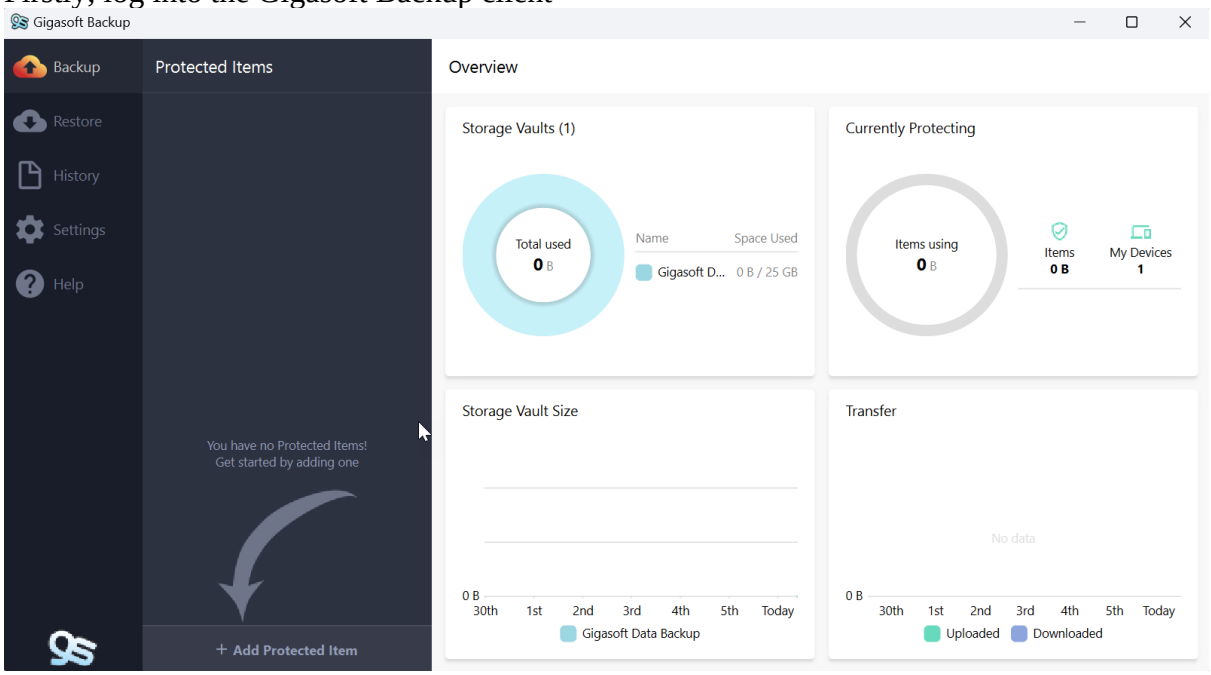
The process to backup MySQL on MacOS is almost identical to the Windows version, please follow these steps and let us know if you have any problems.

6.5.3 MySQL (Linux)

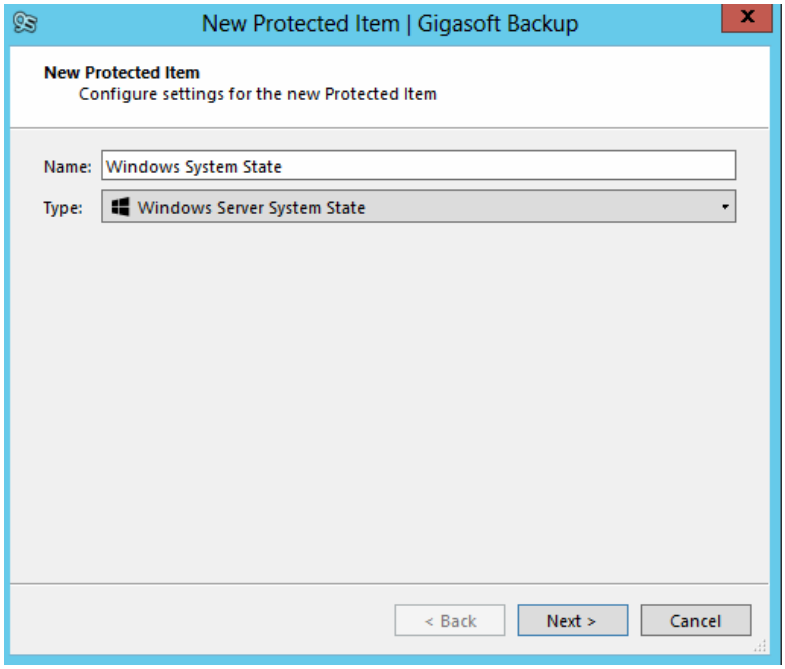
Currently the Linux version is command line only, any changes to the account need to be performed via the customer portal, you will need the exact paths and port numbers required to access the MySQl databases in order to configure this via the portal.

6.6 Windows Server System State protected item

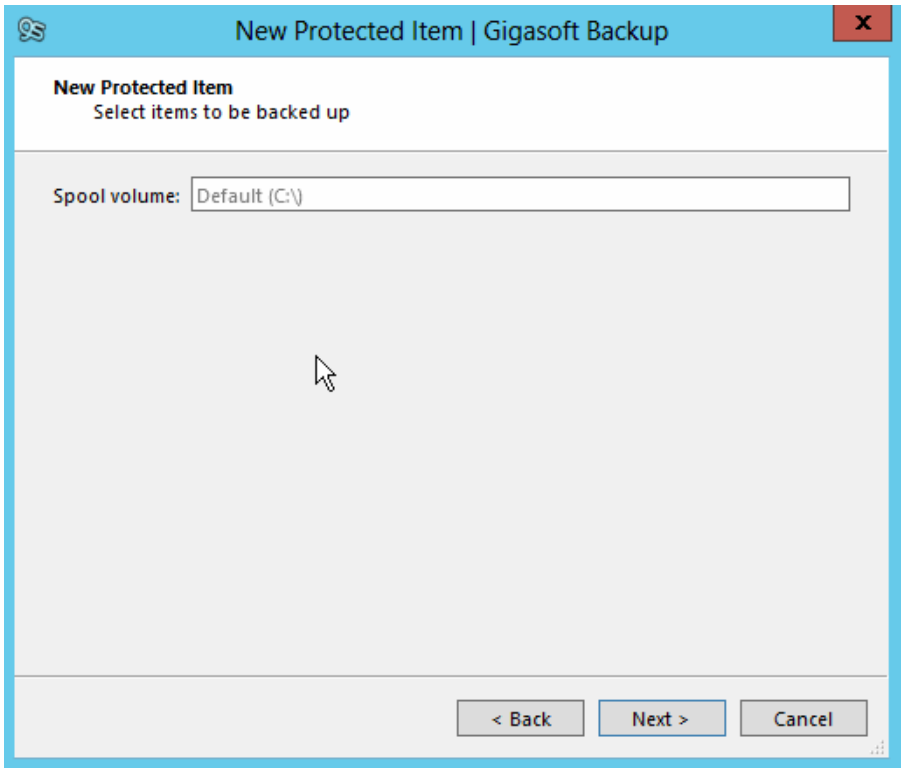
In this section we will guide you through the process of creating a Windows Server System State protected item. This backup type can only be done on a Windows Server and not on desktop machine, The System State takes a snapshot of the server and is ideal for restoring Active Directory etc to the same instance it was taken from, this cannot be used to restore a failed system where the Operating System has had to be reinstalled.
Firstly, log into the Gigasoft Backup client



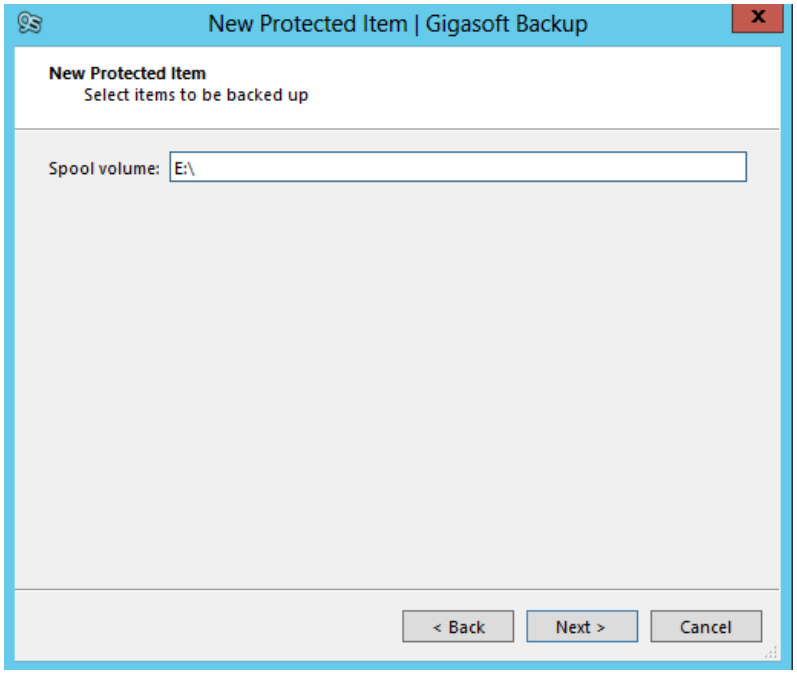
Click on the **[+ Add Protected Item]** button at the bottom of the page.



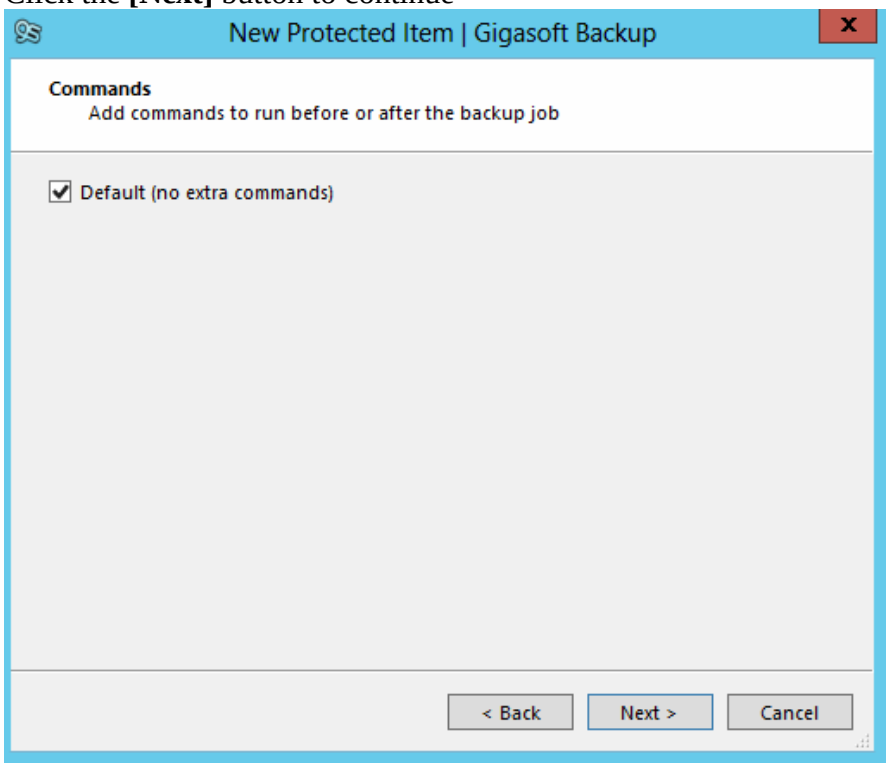
From the drop-down menu select the **[Microsoft Server System State]** option and then change the name to a more meaningful protected item name, in our example we will use *Windows System Backup*, now click on the **[Next]** button.



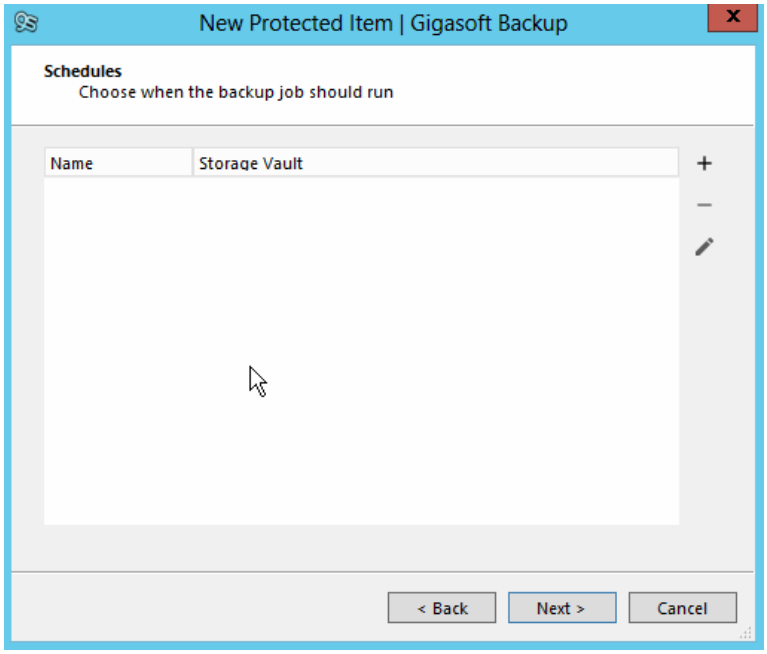
Change the **[Spool volume]** location to a different volume, you cannot spool to the same location you are trying to take a system state from. This could be another drive within the server or a USB drive directly attached to the server.



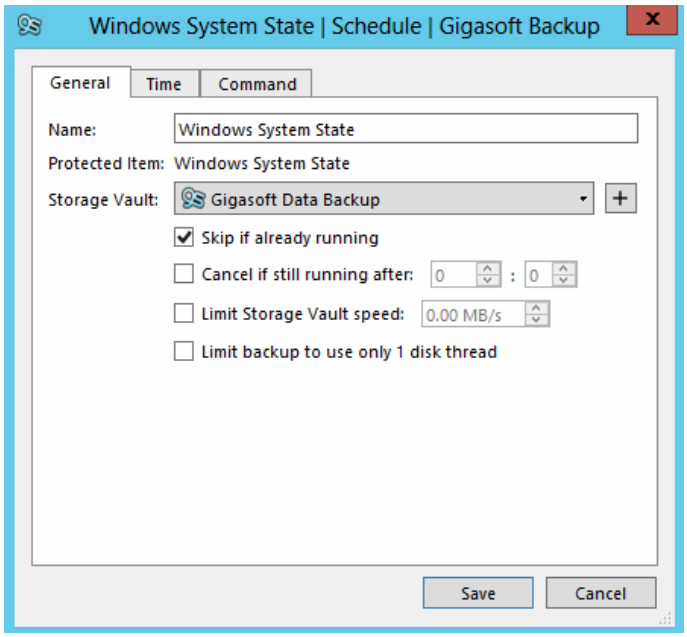
Click the **[Next]** button to continue



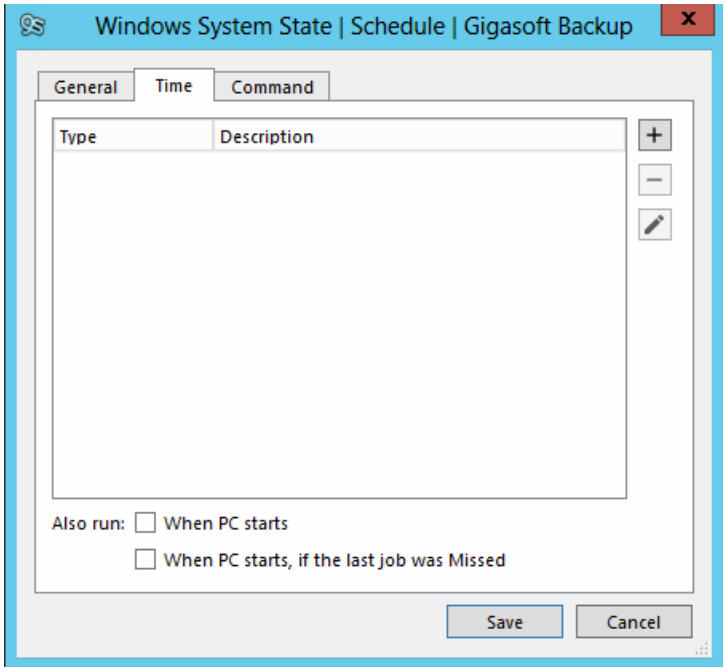
If you need to run any commands, you can add them here by unticking the **Default (no extra commands)** tick box and following the prompts else leave this ticked and click on the **[Next]** button.



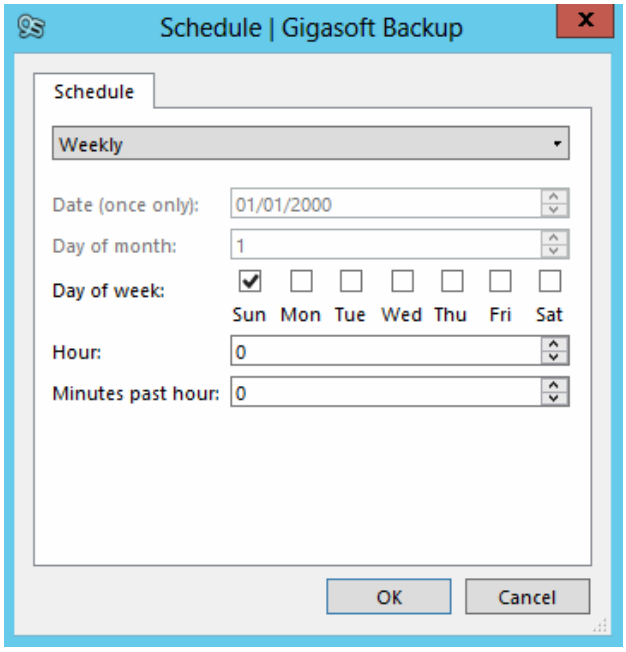
Click the **[+]** button to add a new schedule.



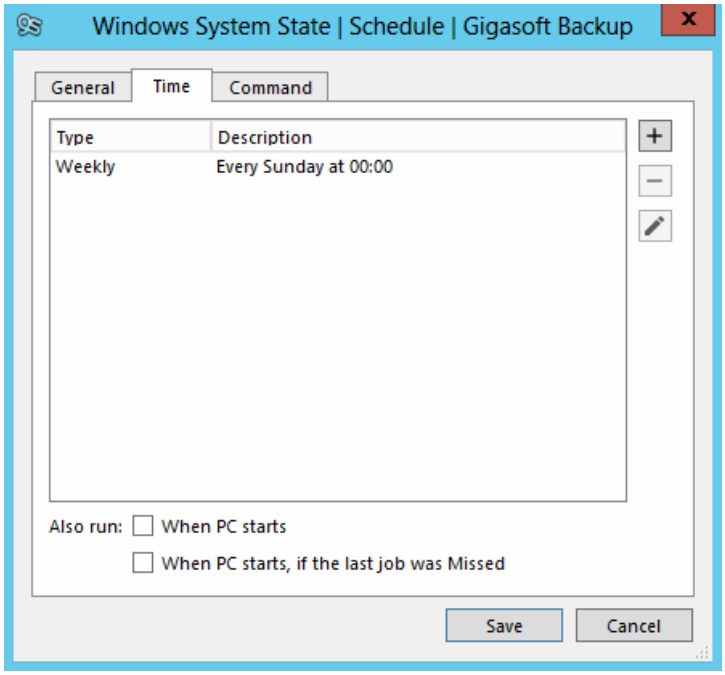
Enter a meaningful name into the Name box, we have used *Windows System State*, select which vault this backup will go to. In this example we will use the default offsite storage vault. Change the options if you want the job to stop after a certain amount of time or to skip another backup if there is one already running, you can also limit the bandwidth available to this protected item, this is especially useful if you have a large amount of data and you don't want it to use all of the available upload bandwidth.
On older machines or machines that are busy we can now request that GBM uses a single disk thread, this causes the backup to take a bit longer but uses less resources, this is useful if you find your machine is running slower than normal when the backup is running, now click on the **[Time]** tab.



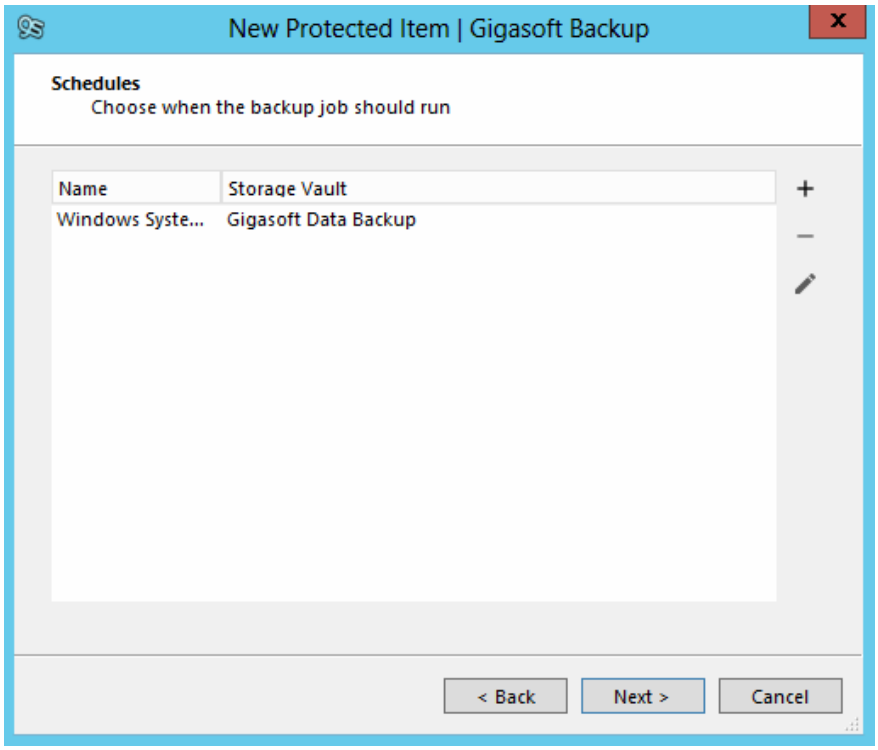
Here we can set a schedule for this protected item, click on the **[+]** button to add a schedule



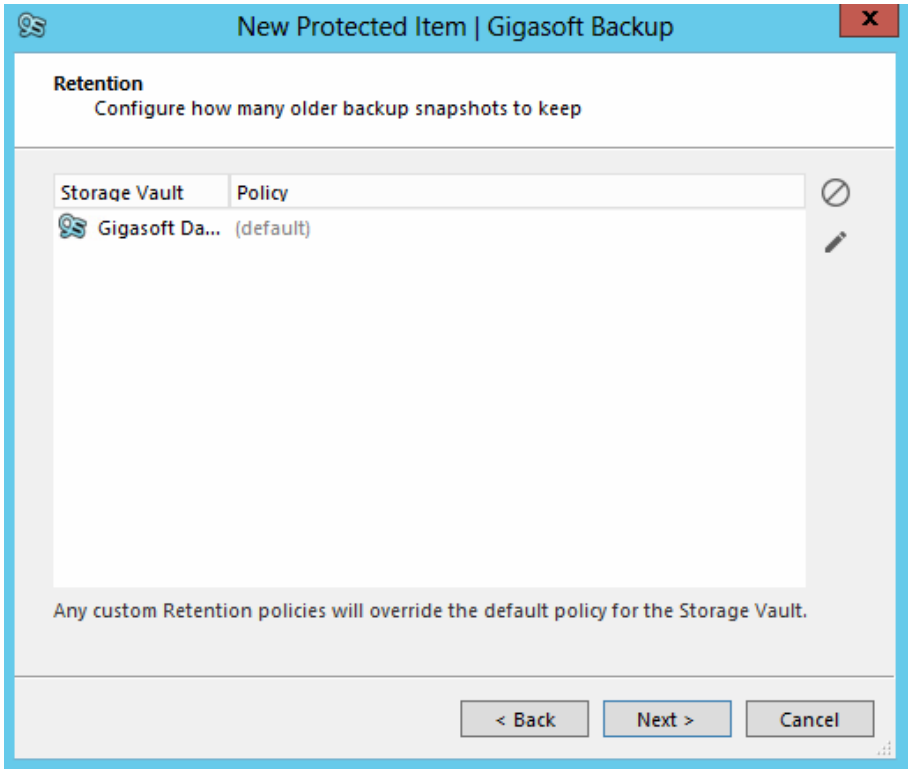
Use the drop down to select the desired type of schedule, in this example we will set the schedule to run *Weekly on a Sunday* at *00:00*, click **[OK]** once you are done.



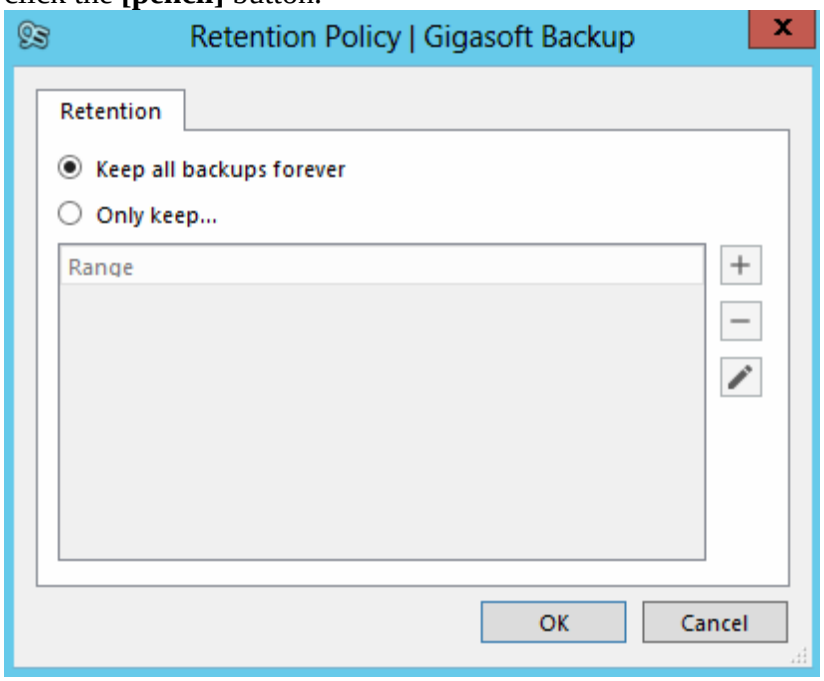
We are taken back to the schedule overview page, here you can add more schedules if needed, you can also set any pre or post commands if required else click the **[Save]** button to move on.



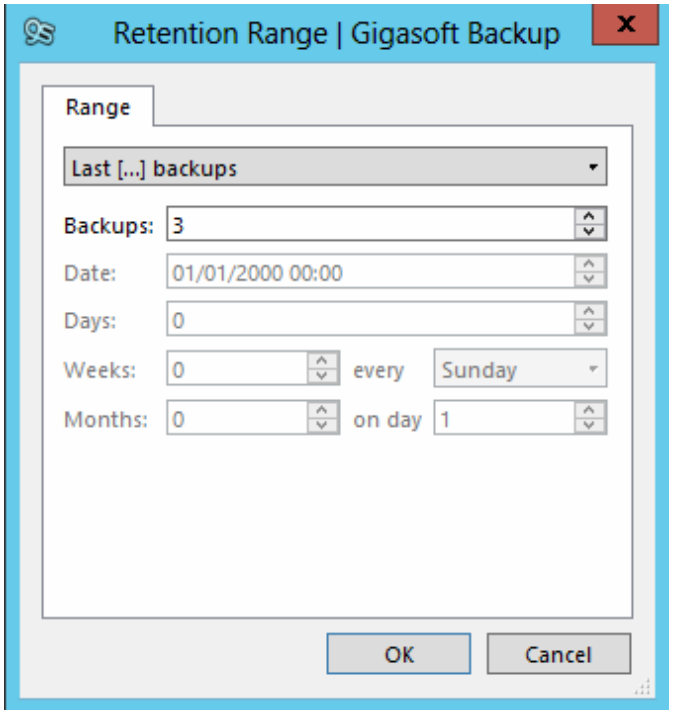
We are now back to the scheduled item overview page, we now need to set the retention policy for this set. Click on the **[Next]** button.



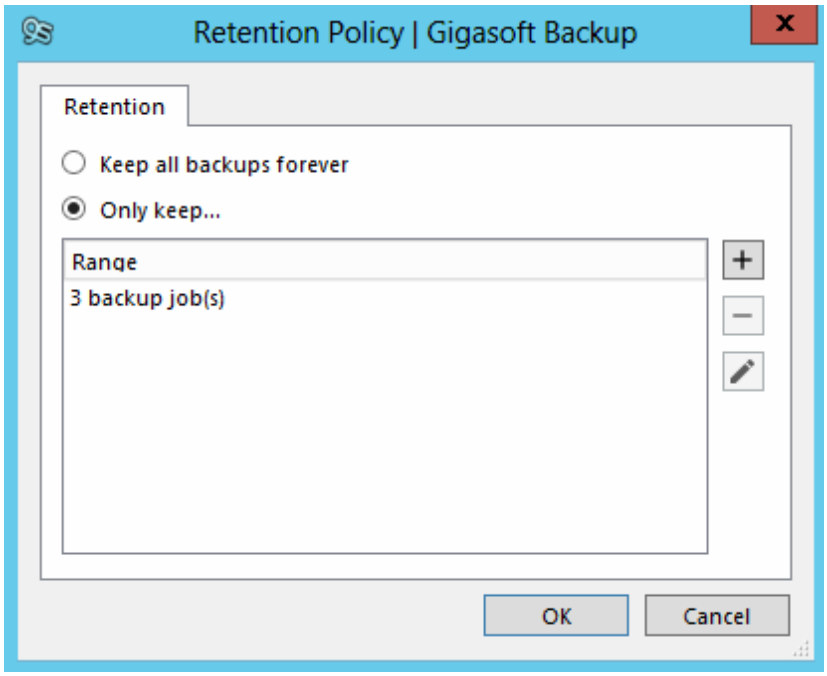
Here you can see there is a default retention policy set, this is to keep all the data forever, to change this to one that suits your needs click on the current policy to highlight it and then click the **[pencil]** button.



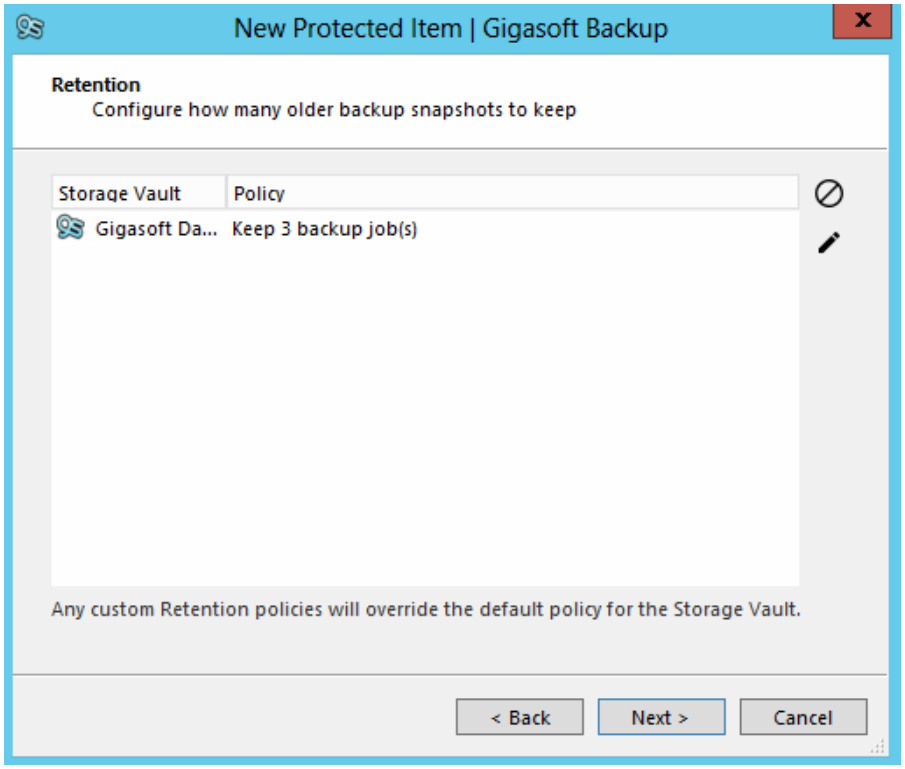
Here you can see the retention will be kept forever, change the radio button to **[Only keep…]** and then click on the **[+]** button.



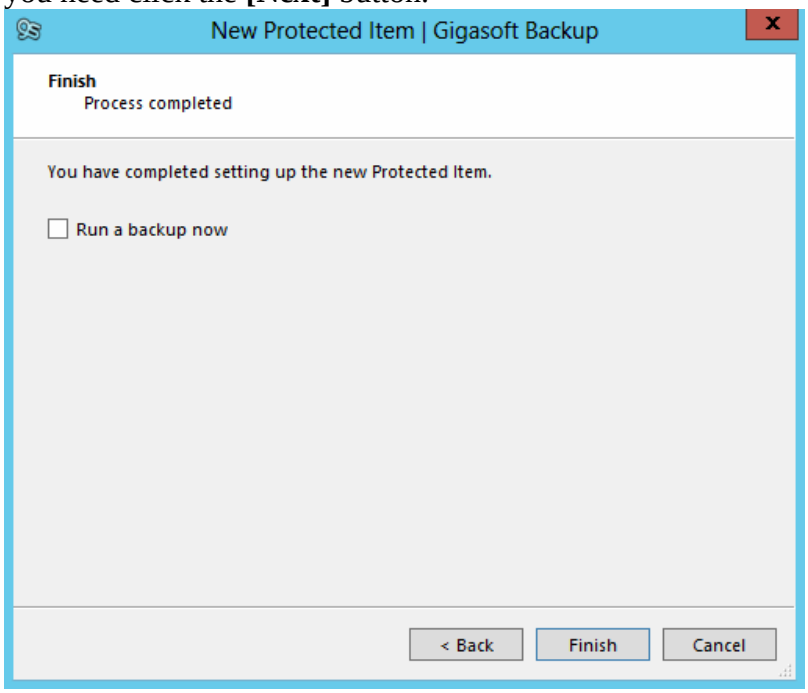
Use the drop-down selection box to choose a retention schedule that suits you, in this example we will select *Last […] backups*. In the next box we will select *3* this will allow us to keep the last 3 backups, this can be changed to anything you require. Once you have completed your selection click the **[OK]** button.



You will now be taken back to the overview page, you can set other schedules for this same protected item if you wish else please click the **[OK]** button.



Now we are back to the retention overview page, once you are happy you have all the settings you need click the **[Next]** button.

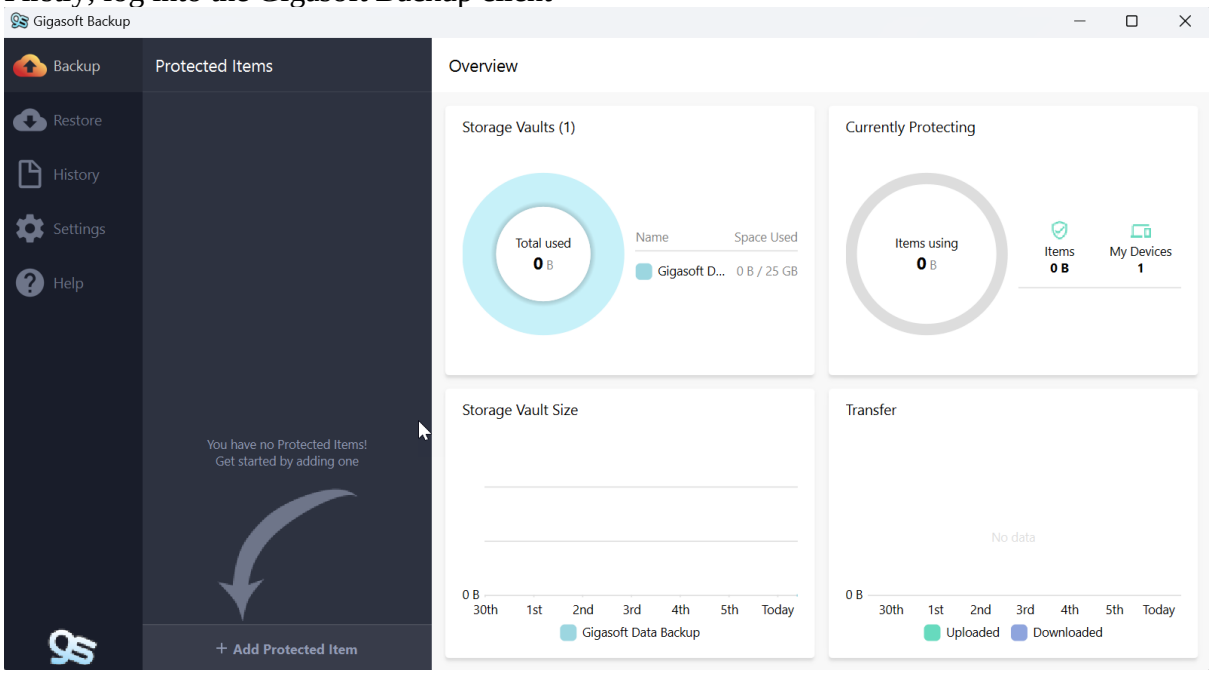


You will now be asked if you would like the run the backup now, if you do leave the box ticked and click **[Finish]** if you do not wish to run the backup now remove the tick in the **Run a backup now** box and click **[Finish]**

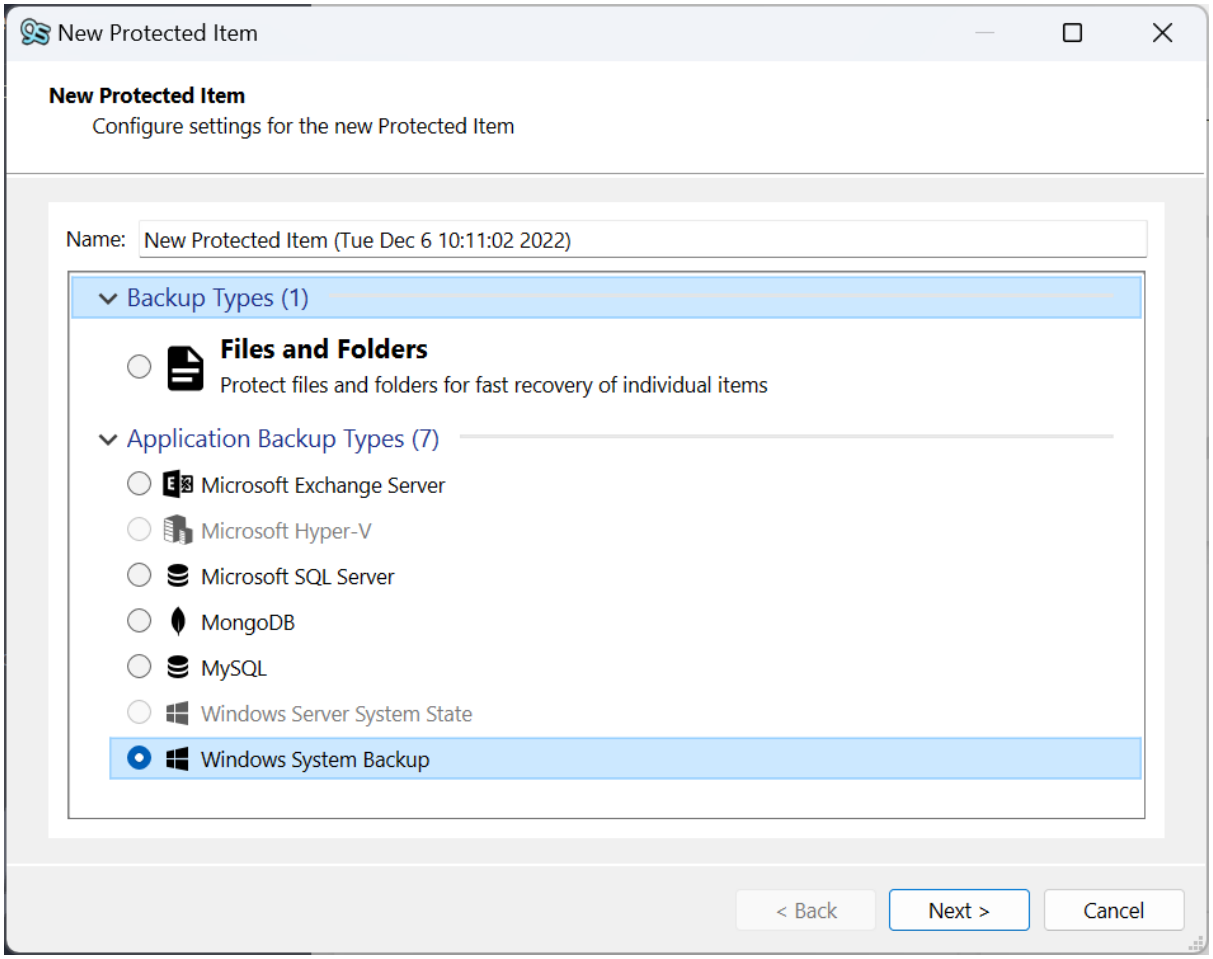
After clicking finish you are taken back to the main dashboard, from here you can create further protected items if you need to.

6.7 Windows System Backup protected item

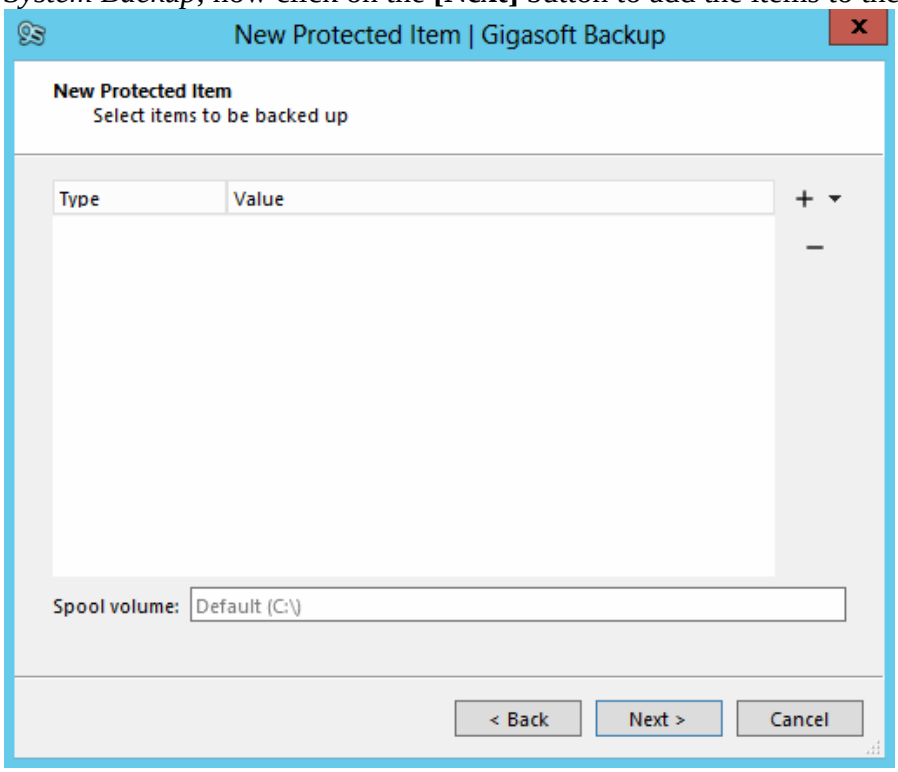
In this section we will guide you through the process of creating a Windows Server Backup protected item. The Windows System Backup is used to take a backup of your internal disks and can be used to restore data in the event of a failure, it cannot be used to recover a failed system as the backup does not include any boot partitions although these can be manually set. It can also be possible to restore individual items in needed but this is not recommended, the use of a file protected item would perform much better in this scenario.
Firstly, log into the Gigasoft Backup client



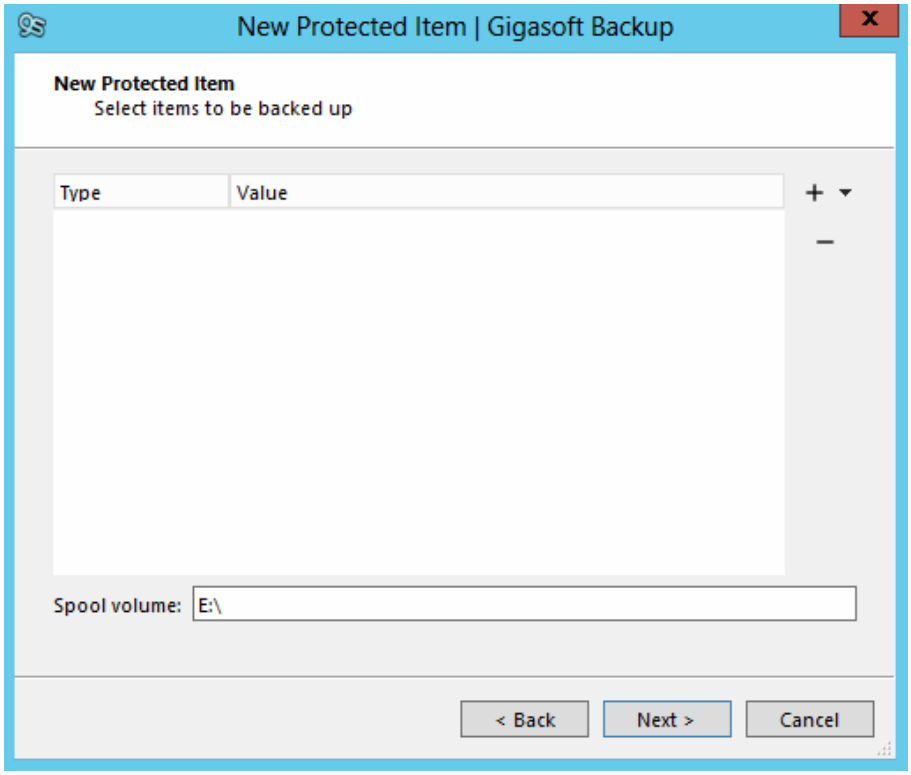
Click on the **[+ Add Protected Item]** button at the bottom of the page.



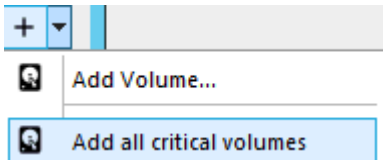
From the drop-down menu select the **[Windows System Backup]** option and then change the name to a more meaningful protected item name, in our example we will use *Windows System Backup*, now click on the **[Next]** button to add the items to the protected item.



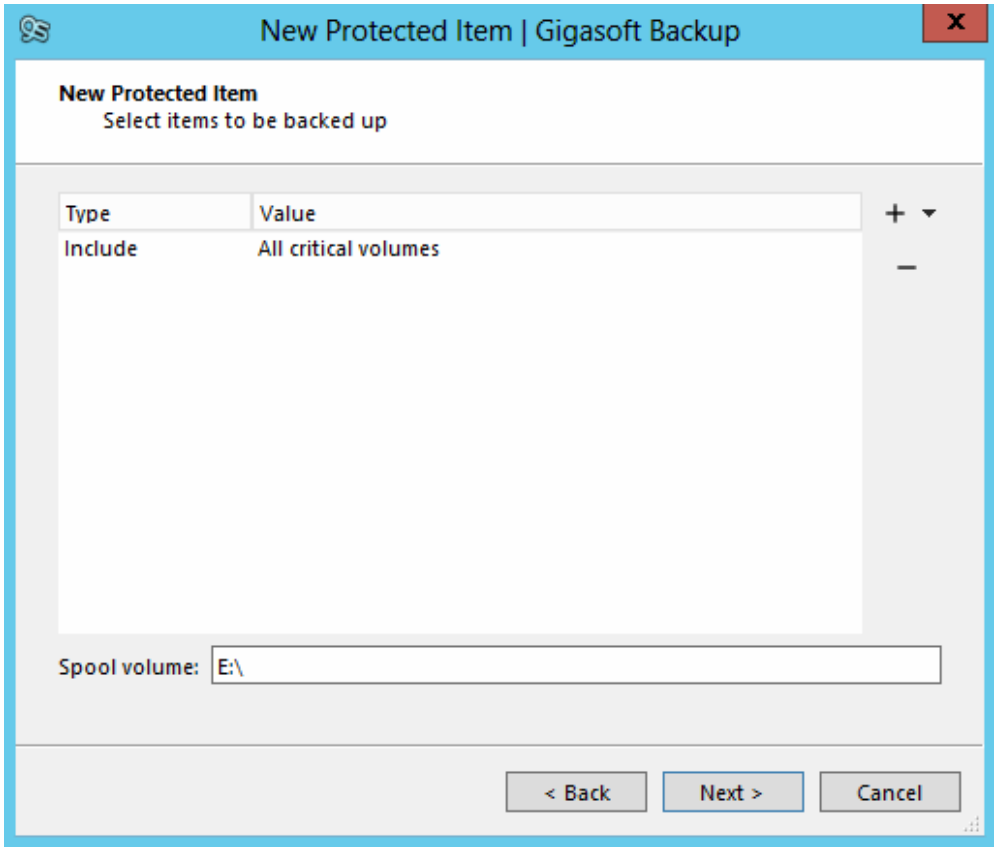
Change the **[Spool volume]** location to a different volume, this could be another drive within the server or a USB drive directly attached to the server as long as it's not one of the systems critical volumes, i.e. a different volume with Windows Exchange on will be part of the critical volumes as would the System Reserved Partition.



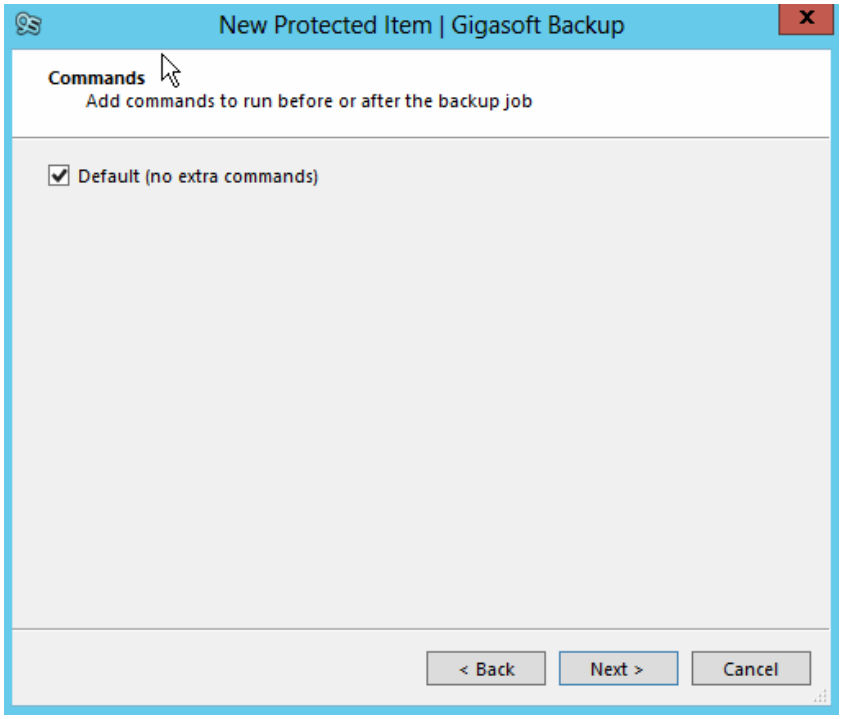
In this example we will use the E drive, this is a non-critical drive in our test setup.



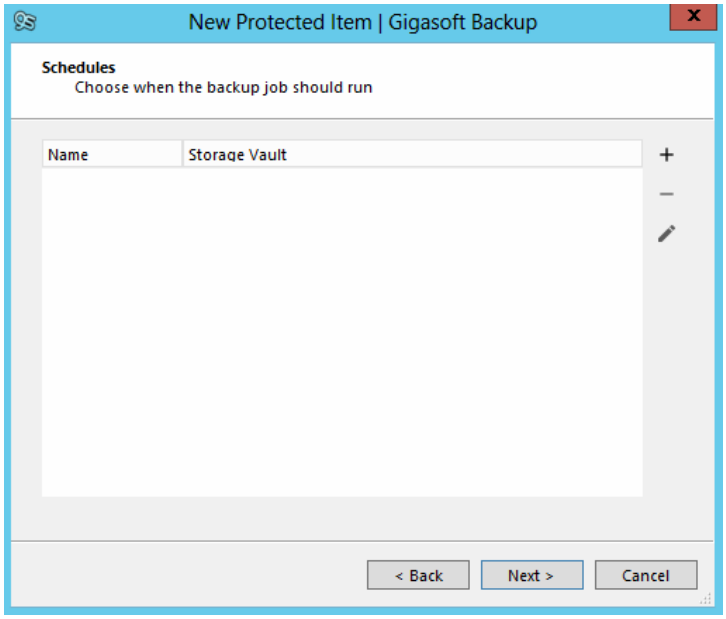
Click on the down arrow next to the **[+]** button and then choose **[Add all critical volumes]** you can specify the individual volumes you wish to back up if you prefer but in the event of a failure you may be unable to restore all the information required to bring your system online, you may be able to use the restore to extract single files or folders but this is a slower process than using a file protected item.



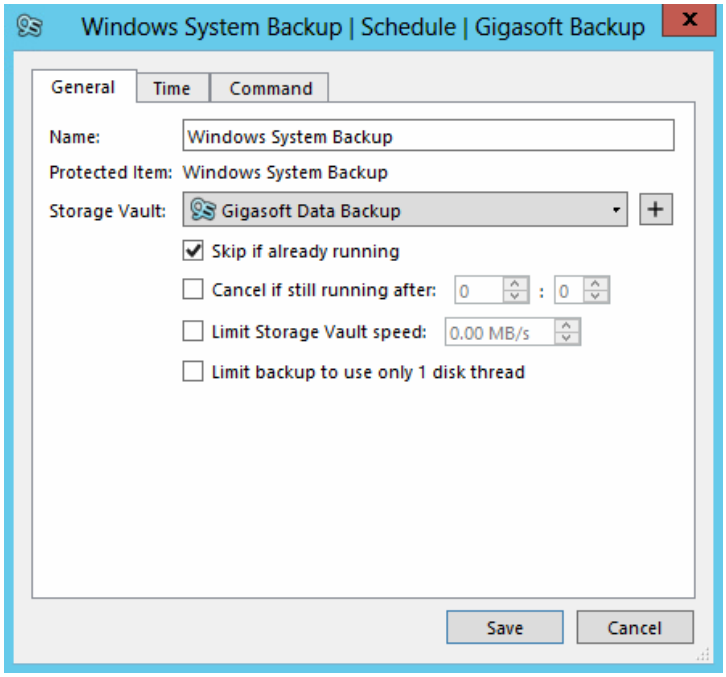
Click the **[Next]** button to continue.



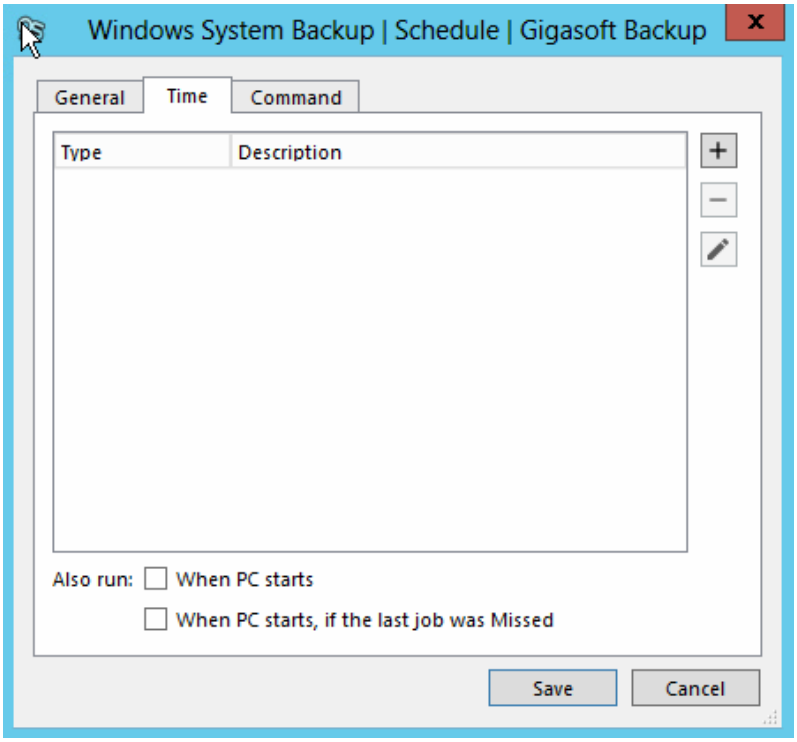
If you need to run any commands, you can add them here by unticking the **Default (no extra commands)** tick box and following the prompts else leave this ticked and click on the **[Next]** button.



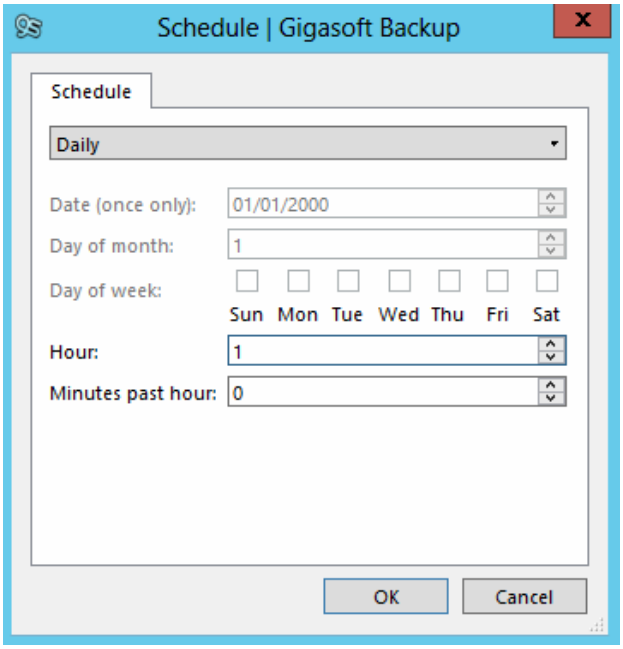
Click the **[+]** button to add a schedule for this protected item.



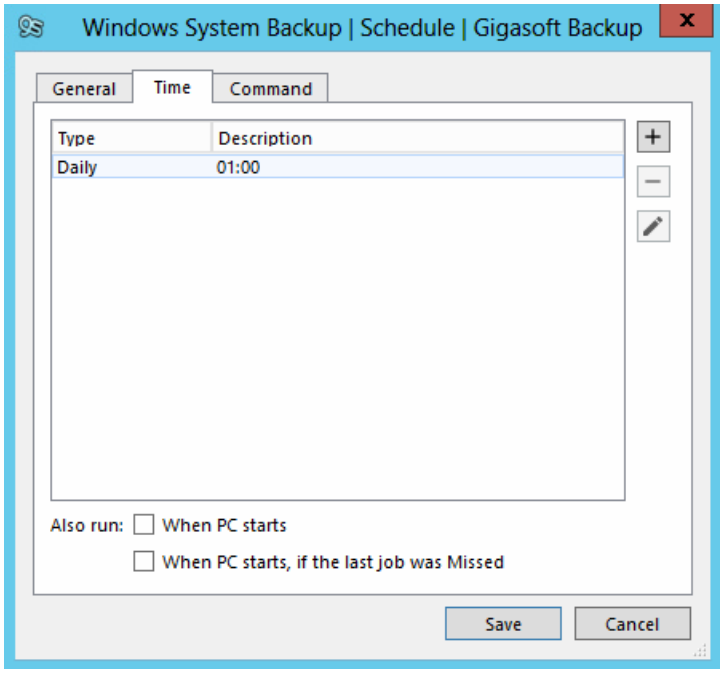
Enter a meaningful name into the Name box, we have used *Windows System Backup*, select which vault this backup will go to. In this example we will use the default *offsite storage vault*. Change the options if you want the job to stop after a certain amount of time or to skip another backup if there is one already running, you can also limit the bandwidth available to this protected item, this is especially useful if you have a large amount of data and you don't want it to use all of the available upload bandwidth.
On older machines or machines that are busy we can now request that GBM uses a single disk thread, this causes the backup to take a bit longer but uses less resources, this is useful if you find your machine is running slower than normal when the backup is running, now click on the **[Time]** tab.



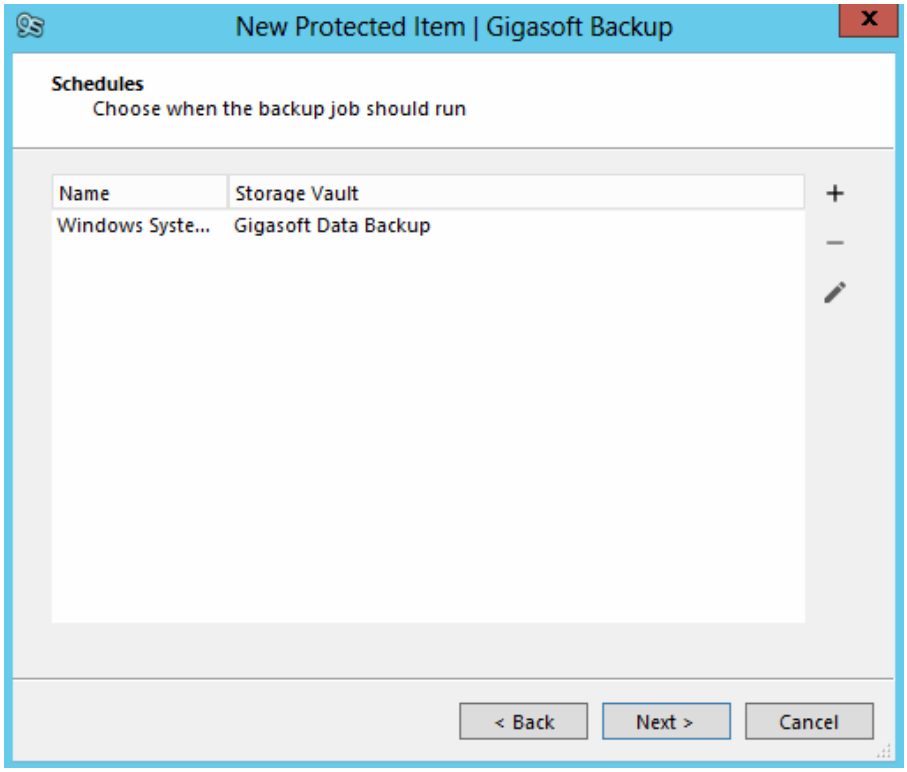
Here we can set a schedule for this protected item, we can create multiple schedules if needed but in this example, we will just create the one. Click on the **[+]** button to add a schedule.



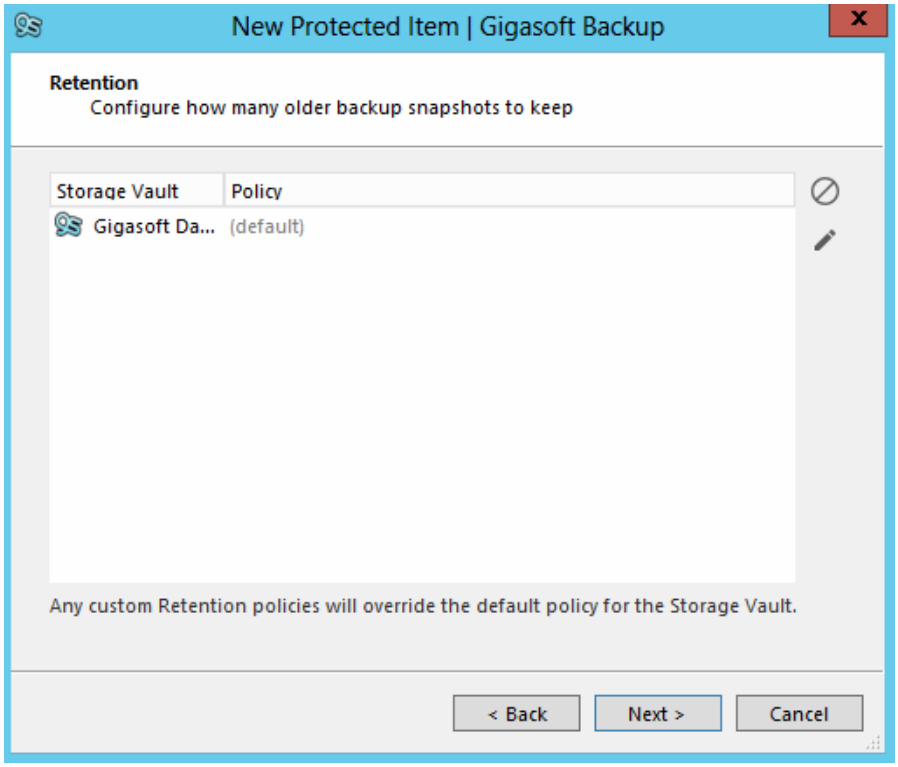
Use the drop down to select the desired type of schedule, in this example we will set the schedule to run *daily at 01:00*, click **[OK]** once you are done.



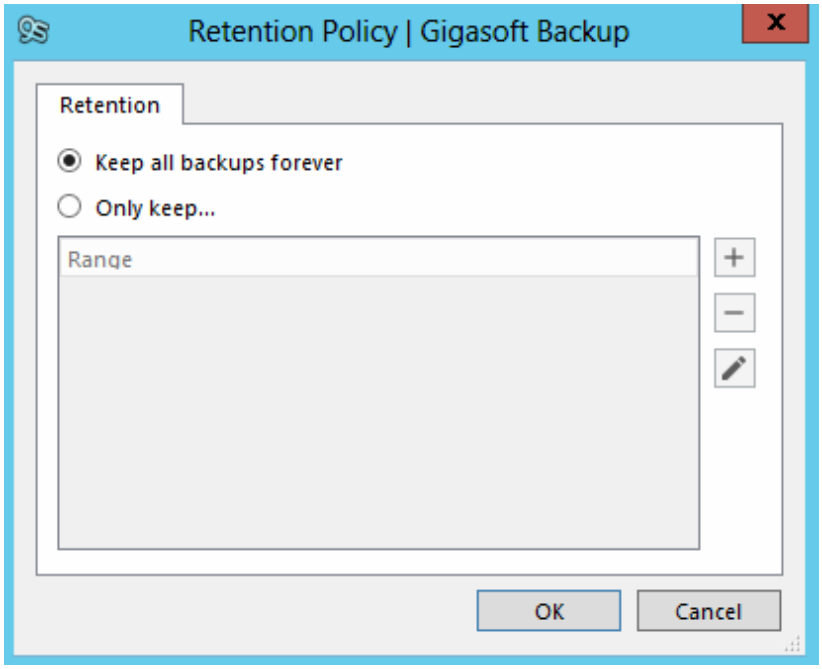
We are taken back to the overview page, here you can add more schedules if needed, you can also set any pre or post commands if needed else click the **[Save]** button to move on.



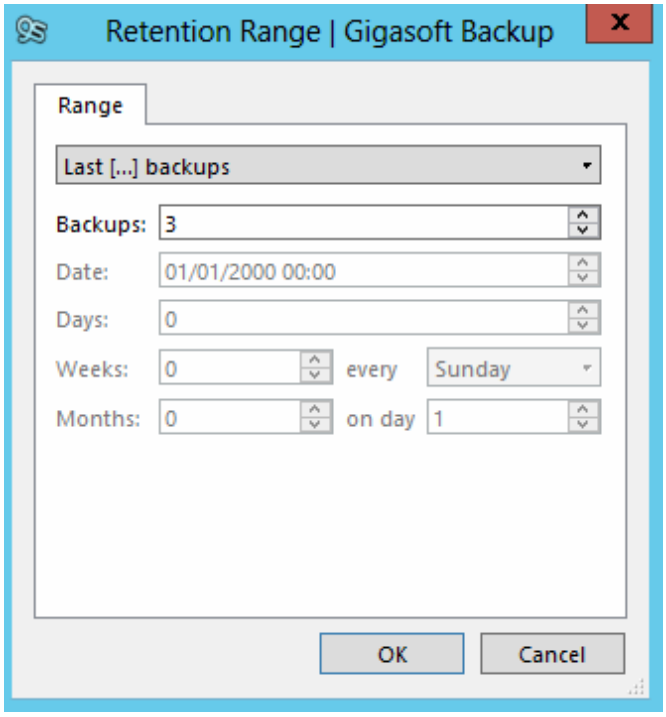
We are then taken back to the schedule overview page, we now need to set the retention policy for this set. Click on the **[Next]** button.



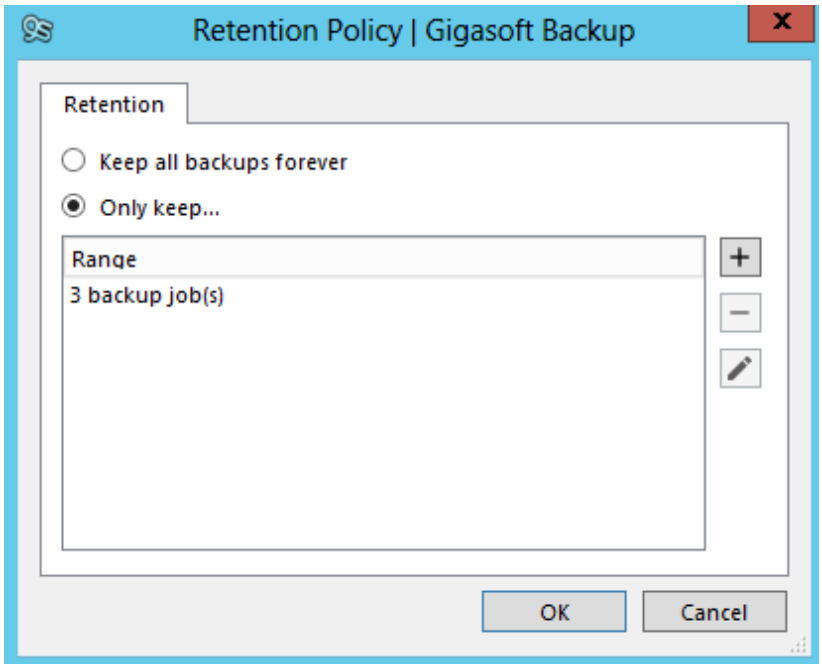
Here you can see there is a default retention policy set, this is to keep all the data forever, to change this to one that suits your needs click on the current policy to highlight it and then click the **[pencil]** button.



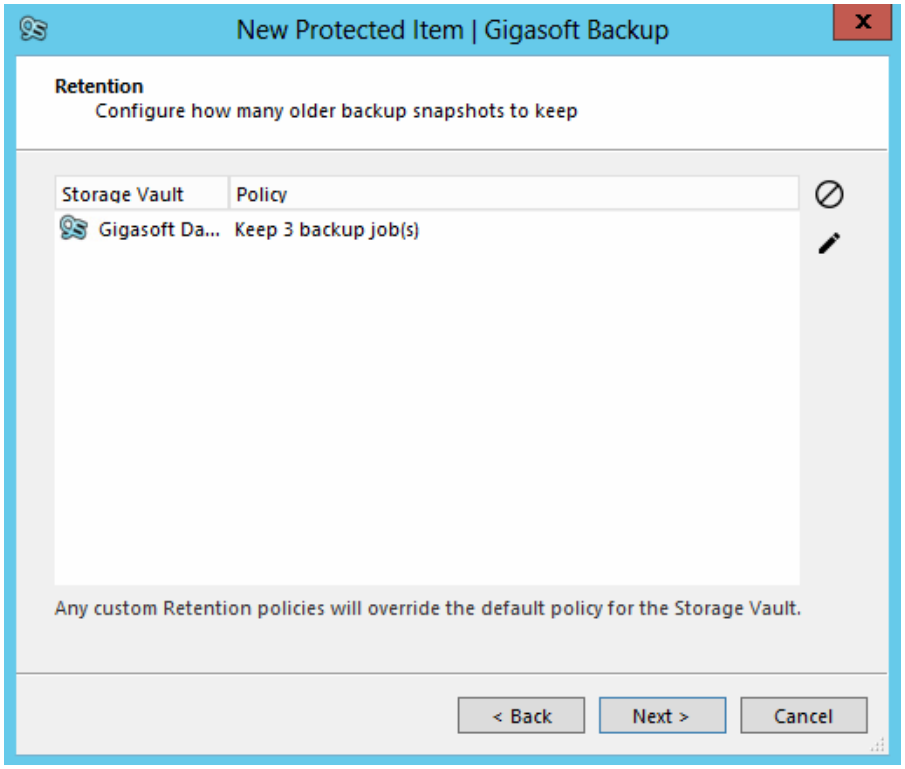
Here you can see the retention will be kept forever, change the radio button to **[Only keep…]** and then click on the **[+]** button.



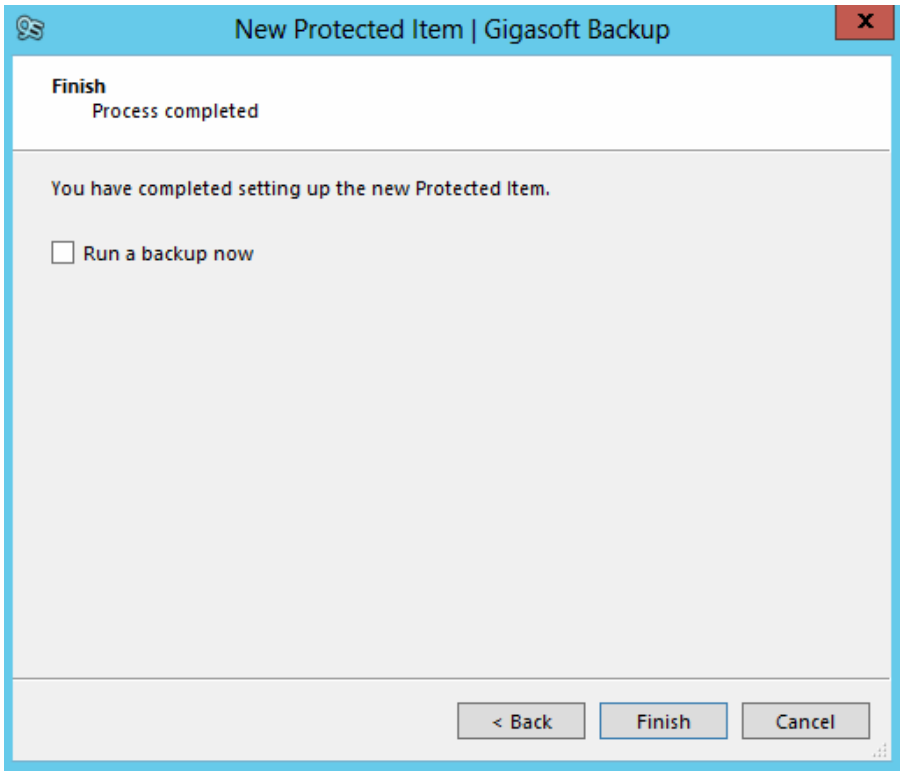
Use the drop-down selection box to choose a retention schedule that suits you, in this example we will select *Last […] backups*. In the next box we will select *3* this will allow us to keep the last 3 backups, this can be changed to anything you require. Once you have completed your selection click the **[OK]** button.



You will now be taken back to the overview page, you can set other schedules for this same protected item if you wish else please click the **[OK]** button



Now we are back to the retention overview page, once you are happy you have all the settings you need click the **[Next]** button.



You will now be asked if you would like the run the backup now, if you do leave the box ticked and click **[Finish]** if you do not wish to run the backup now remove the tick in the **Run a backup now** box and click **[Finish]**

After clicking finish you are taken back to the main dashboard, from here you can create further protected items if you need to.

6.8 Office 365 Backup (SharePoint, OneDrive & Email)

Using this Protected Item type may incur additional charges.

This feature requires GBM Backup 21.9.x or later.

The "Microsoft Office 365" Protected Item type allows you to back up data from your Office 365 cloud account. The backup job runs on the local device, using GBM's client-side encryption, compression and deduplication to store data efficiently.

The following Office 365 services are supported:

- Exchange Online
  - Mailbox (Email)
  - Calendar
  - Contacts
- Sites
  - SharePoint
  - OneDrive for Business
  - Teams Files

NOTE: Microsoft Online Services are responsible for the availability of the Office 365 online service and meeting their SLA guarantees. There are first-party archival and history solutions such as Retention Policy and Litigation Hold. Back up your Office 365 cloud account, for purposes of data safety; redundancy; resilience to tampering, misconfiguration, and accidental loss; legal compliance; unified reporting with other backup sources; and ease of restoring single items.

6.8.1 Overview

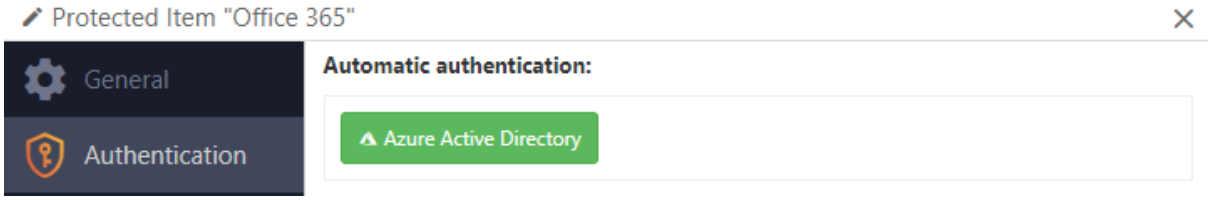
Services	Backup	Restore to Local	Restore to Cloud	Supported	Not Supported
Exchange Online					
Mailbox (Email)	Yes	Yes	Yes	Active users, shared mailboxes	Guest users, Deleted users, Discovery mailbox, Archive mailbox, Journal mailbox, Outlook group mailboxes
Calendar	Yes	Yes	Yes	Restore to local:JSON format	
Contacts	Yes	Yes	Yes	Restore to local:JSON format	
Tasks	No	No	No		
SharePoint Online					
Sites	Yes	Yes	No	Restore lists, documents and pages individually	
Lists	Yes	Yes	Yes		
Pages	Yes	Yes	No		
OneDrive for Business					
Document Library (Word, Excel, PowerPoint, OneNote)	Yes	Yes	Yes	Displayed under "Documents" in associated SharePoint site	
Teams					
Files	Yes	Yes	Yes	Displayed under "Documents" in associated SharePoint site	
Chat	No	No	No		
Calendar	No	No	No		
Meetings	No	No	No		
Call	No	No	No		

6.8.2 Authentication

For backups, grant GBM the ability to read data from your Office 365 account. Please pay attention to the credentials provided as a significant amount of access to the Office 365 organization occurs. This grant is done by creating an "Application" inside Azure AD. This application can be created automatically or manually.

Automatic application registration

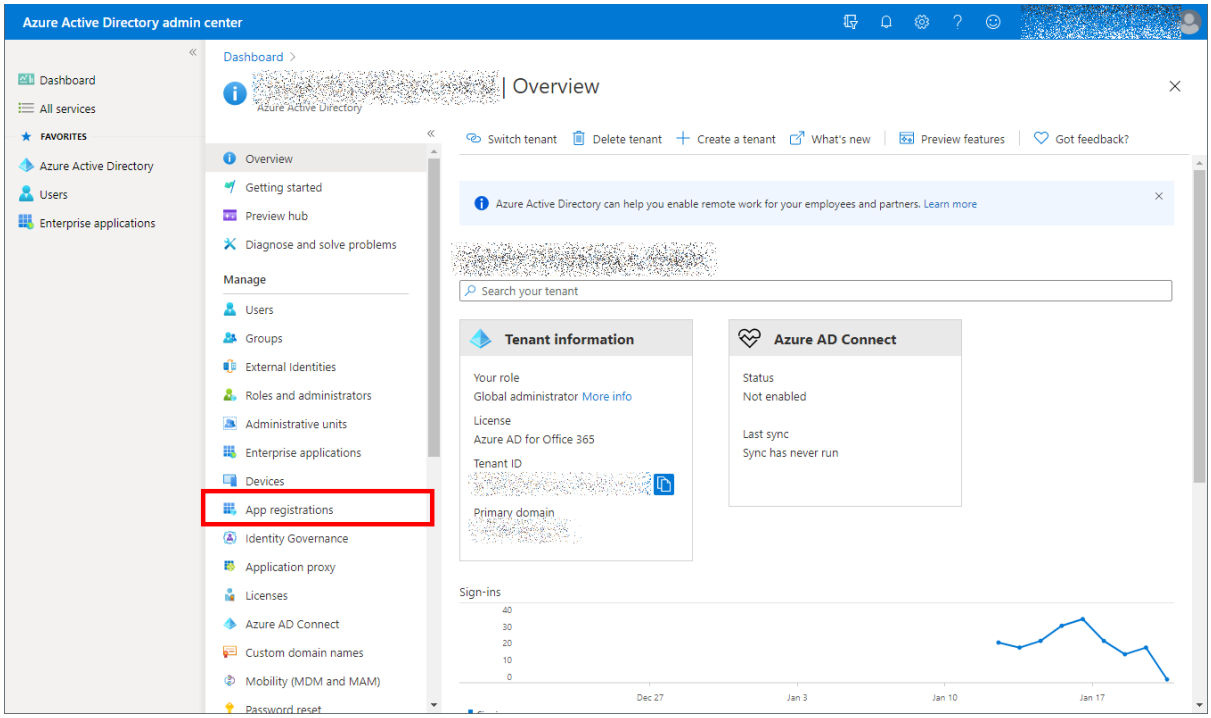
Click the "Azure Active Directory" button. This opens a registration application wizard dialog that steps you through the process to automatically register. Authenticate with Azure as a top-level administrator.



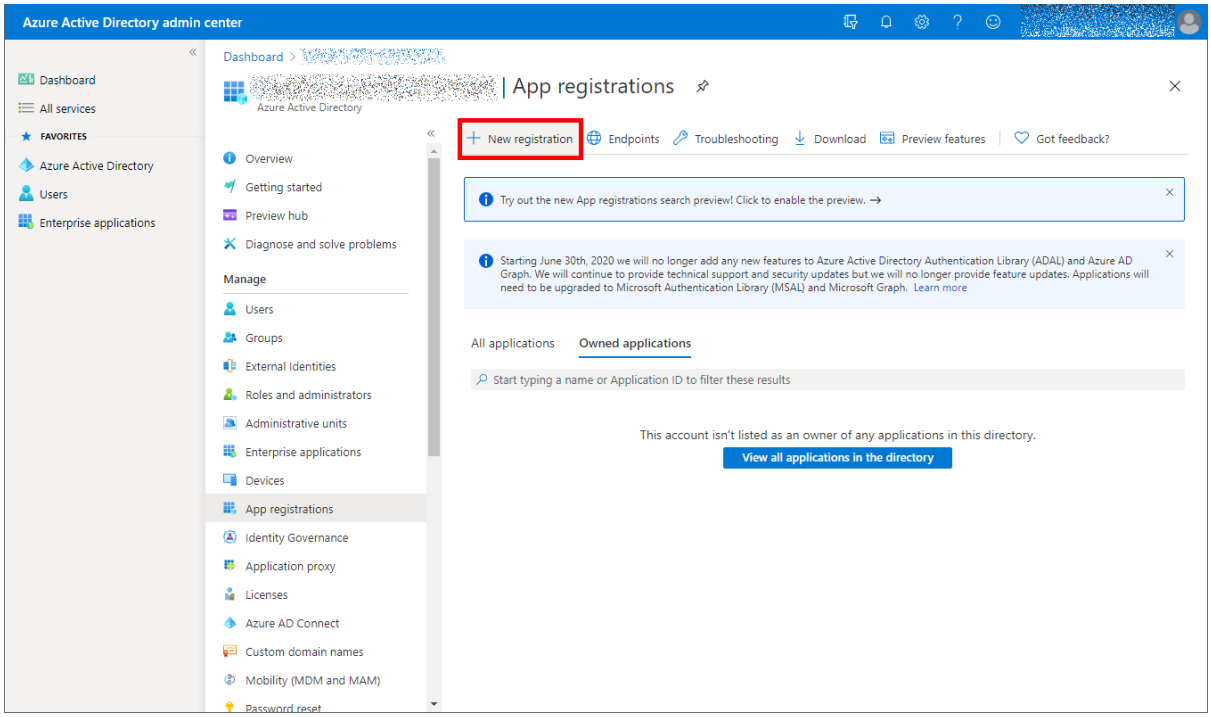
Manual application registration

If you are unable to use the automatic application registration, you can register the application manually via the Azure AD web interface via the following steps:

1. Register a branded application inside the Azure Active Directory panel:



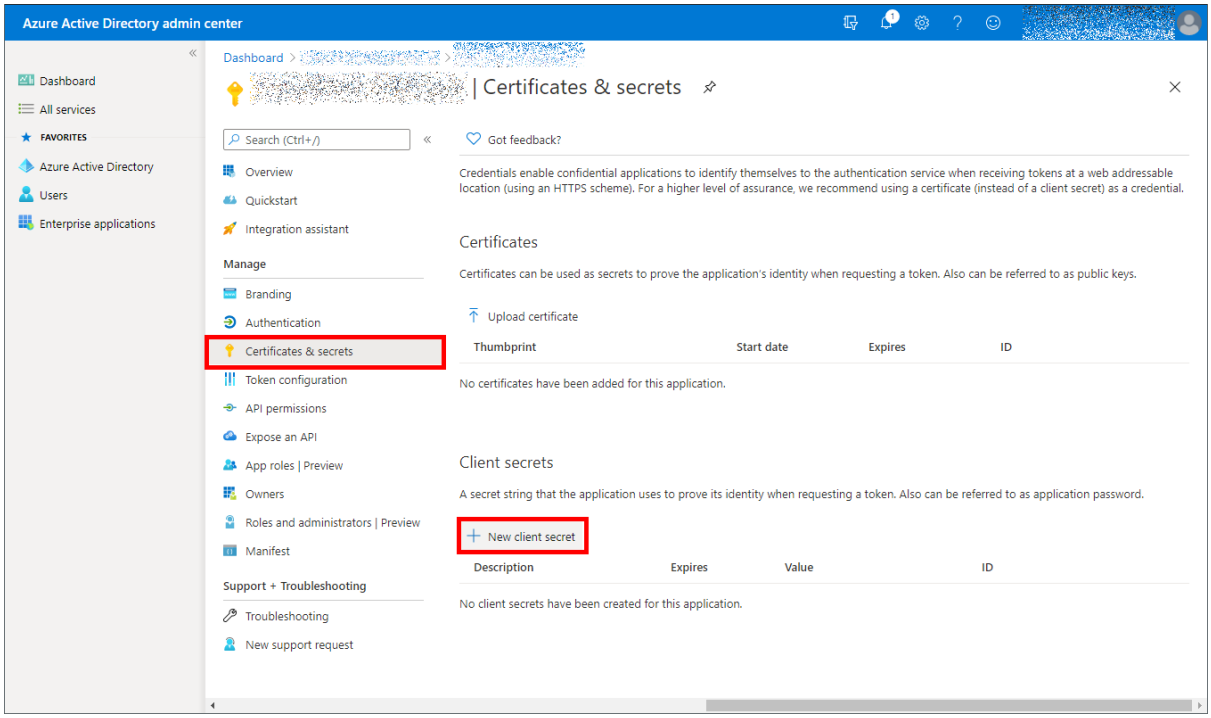
- Visit https://aad.portal.azure.com/
- Click "Azure Active directory"



- Click "App registrations" > "New registration"
- Enter an application name (e.g. "My Branded Office 365 Backup Product"). The other options can be left as default
- Click the "Register" button.
- Copy the `Application (client) ID` field into GBM's `Application ID` field
- Copy the `Directory (tenant) ID` field into GBM's `Tenant ID` field

Ensure that there are no extra spaces in the field after the Tenant ID

2. Register an authentication secret for the application:

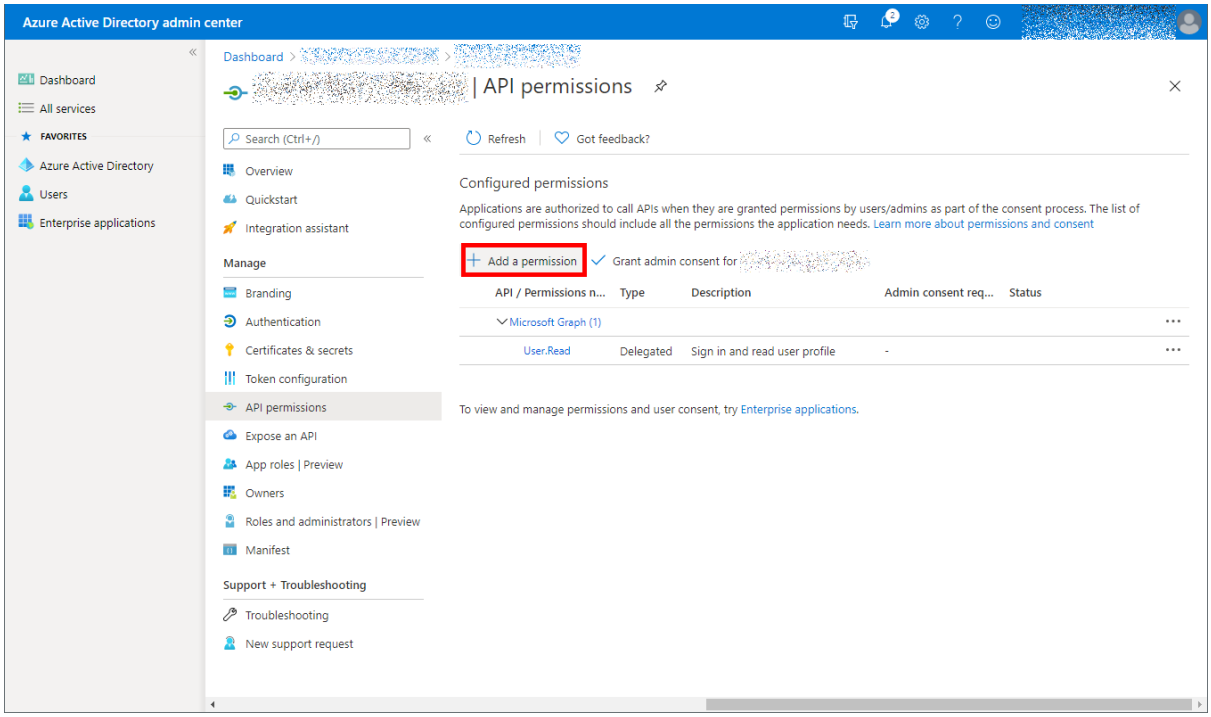


- Click the "Certificates & secrets" left-hand tab
- In the "Client secrets" section, click the "New client secret" button
- Create a new secret

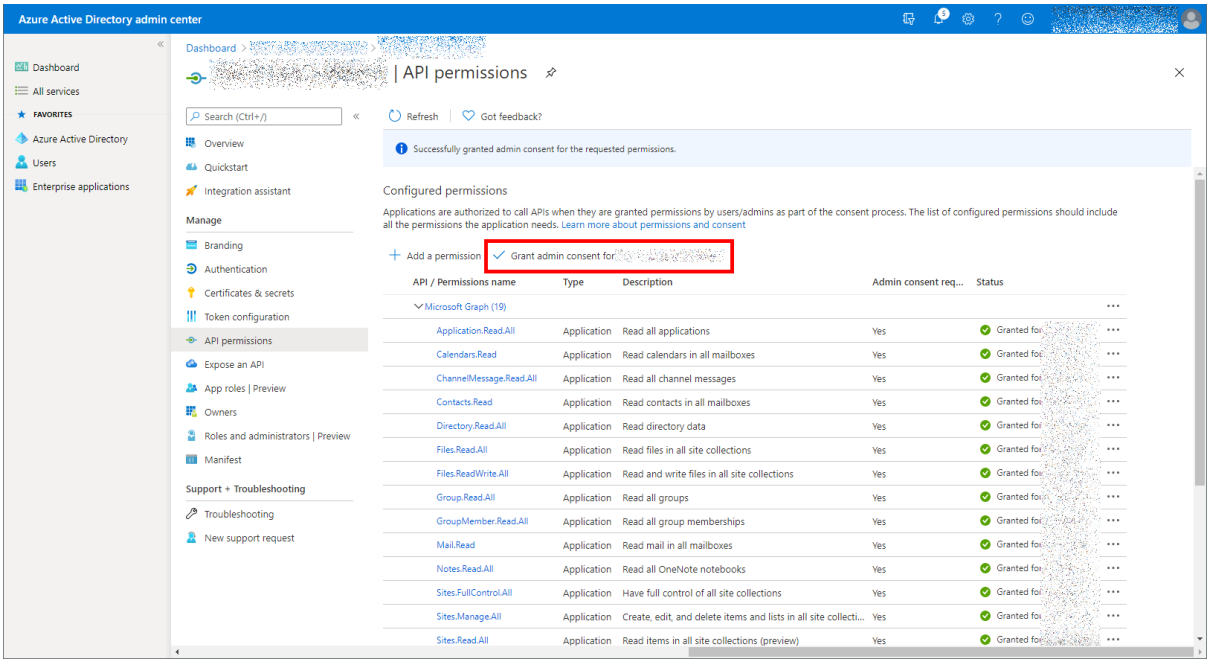
  Specify any name (e.g. "My GBM integration credentials") and any expiry (e.g. "Forever / No expiry")

- Copy the `Value` column into GBM's `Application Secret` field

3. Grant this application permission to read Office 365 data:
   - Click the "API permissions" left-hand tab
   - Click the "Add a permission" button



- Find and add the following permissions:
    1. "APIs my organization uses" > "Office 365 Exchange Online" > Application permissions > ...
        1. "Other permissions" > `full_access_as_app`
    2. "Microsoft APIs" > "Microsoft Graph" > Application permissions > ...
        1. `Application.Read.All`
        2. `Calendars.Read`
        3. `ChannelMessage.Read.All`
        4. `Contacts.Read`
        5. `Directory.Read.All`
        6. `Files.Read.All`
        7. `Files.ReadWrite.All`
        8. `Group.Read.All`
        9. `GroupMember.Read.All`
        10. `Mail.Read`
        11. `Notes.Read.All`
        12. `Reports.Read.All`
        13. `Sites.FullControl.All`
        14. `Sites.Manage.All`
        15. `Sites.Read.All`
        16. `Sites.ReadWrite.All`
        17. `TeamMember.Read.All`
        18. `TeamMember.ReadWrite.All`
        19. `User.Read.All`



- Back on the API permissions page, click the top "Grant admin consent for (My Organization Name)" button

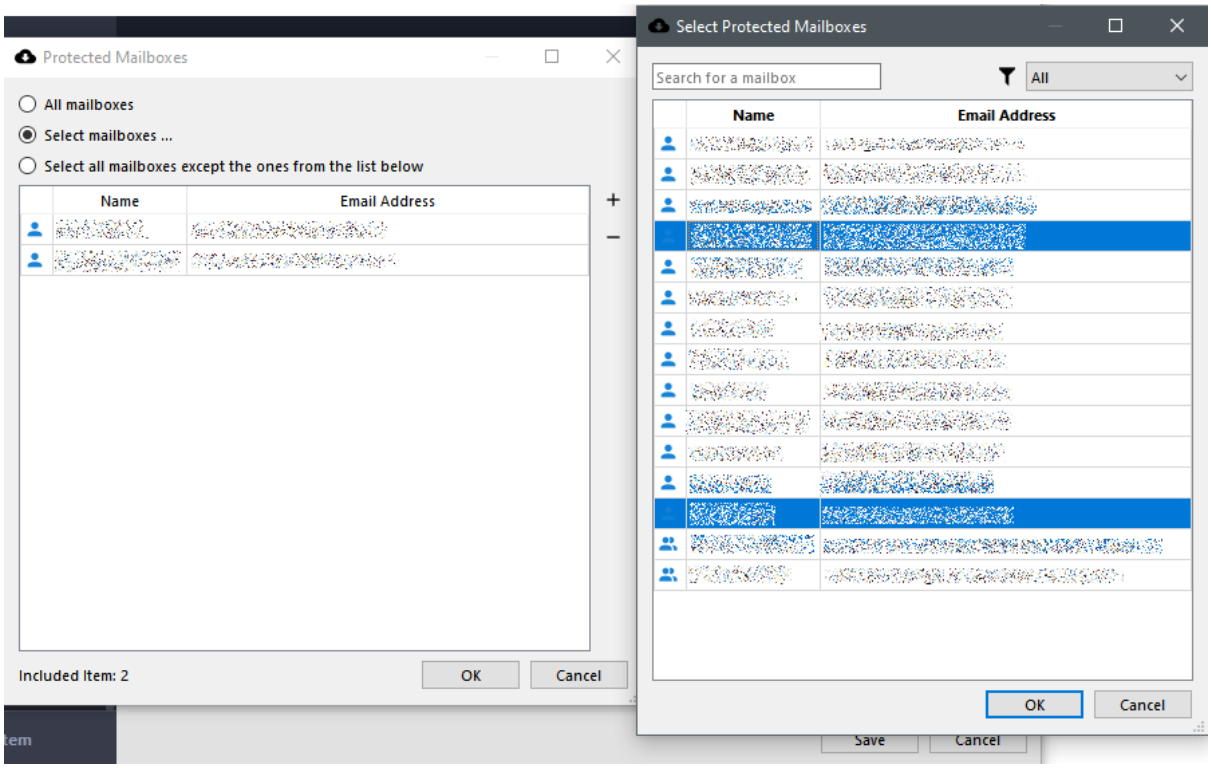
The authentication details are automatically populated in the desktop app, use the "Test Connection" button to validate the Office 365 credentials.

6.8.3 Configuring Selections

GBM supports backing up different items from your Office 365 account. Use the pencil button in the desktop app to configure which mailboxes and sites will be backed up. Make separate selections for both mailboxes and sites using the dropdown arrow beside the plus button.

User has the following options for backups:

- Back up all mailboxes/sites
- Back up only the selected mailboxes/sites
- Back up all mailboxes/sites except for the selected ones



When selecting users or sites for backup, the first dialog shows your current selection. Inside the first dialog, click the plus button to open a second dialog, to find users and sites from the Office 365 server.

The Search field in the second dialog box can be used to quickly filter for a known user or site.

When selecting users, the dialog also shows groups (Azure AD groups of user accounts). If you select a group, GBM will backup all the mailboxes for user accounts belonging to this group.

GBM supports Azure AD groups of user accounts, but does not currently support Outlook groups. If email messages are in an Outlook group, GBM will not be able to back them up. You can see the Outlook groups via the Sites view, but group messages are not included via the Sites backup job.

The only mailboxes available for selection are

- Active Users (as shown in the Office 365 Admin Center), and
- Shared Mailboxes (created with an Exchange E5 license plan or higher).
    - GBM supports backing up Shared Mailboxes. Shared Mailboxes are counted as a full separate mailbox for the purposes of billing, regardless of the number of other accounts with access to the Shared Mailboxes.

The Protected Item configuration is also available remotely via the GBM Server web interface. This feature can be used when the device is online with a live-connection to the GBM Server.

6.8.4 Performance Considerations

The backup job uses Microsoft Office 365 API to read data from the cloud and store it in the Storage Vault. A large amount of data will be downloaded to the local device.

The backup job takes advantage of Office 365 server-side delta change APIs to efficiently perform incremental backup jobs.

- This applies to Mailbox (Email), Calendars, Contacts, OneDrive files, and Teams files, allowing for high-performance incremental backup.
    - Deleting any file from within a backup job snapshot will disassociate the backup job snapshot from the server-side delta change. If you delete a file from the most recent backup job snapshot, the next incremental backup job will require a longer duration.
- This does not apply to SharePoint lists, which may re-download data during each backup job, reducing performance.

The Office 365 API imposes some rate-limiting on the backup operation. This may limit the total performance of the backup job.

- One of the multiple imposed rate-limit rules is based on the target mailbox account. Each mailbox has its own rate limits. GBM backs up multiple mailboxes in parallel; if the Office 365 tenant has a large number of mailboxes, the overall backup job performance would be balanced evenly across all the mailboxes. If the Office 365 tenant contains mailboxes with very different sizes, the single largest mailbox may reduce performance owing to the tail effect.

Hosting the GBM device inside Microsoft Azure provides the lowest possible latency to the Office 365 servers improving the performance.

6.9 VMware backups

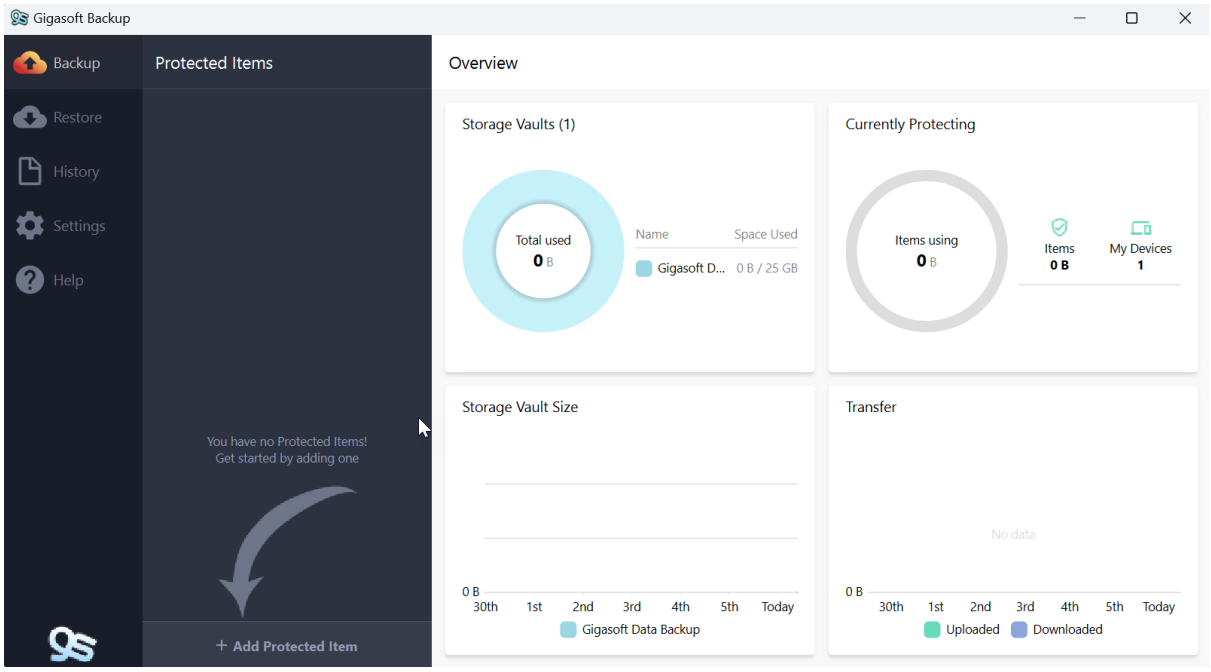
Coming soon

7 How to edit a protected item

In this section we will cover the basics of how to edit a protected item that has already been created.

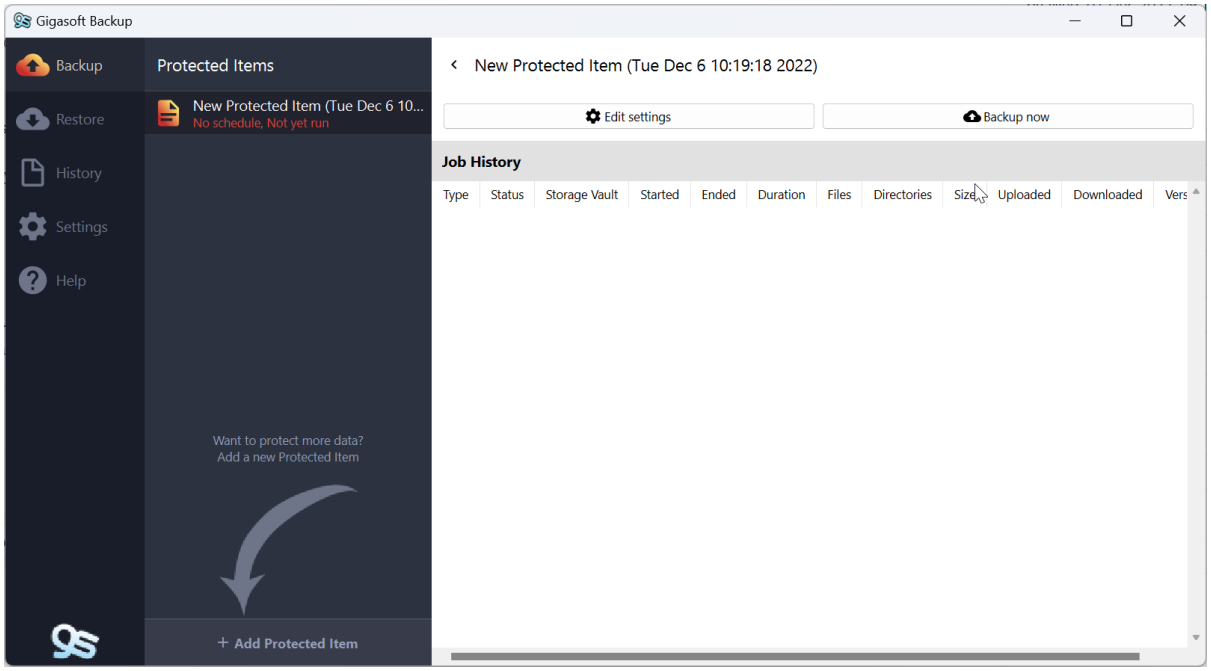
7.1 Windows

Log into the client and you will be presented with the dashboard.



Click on the name of the protected item you wish to edit.

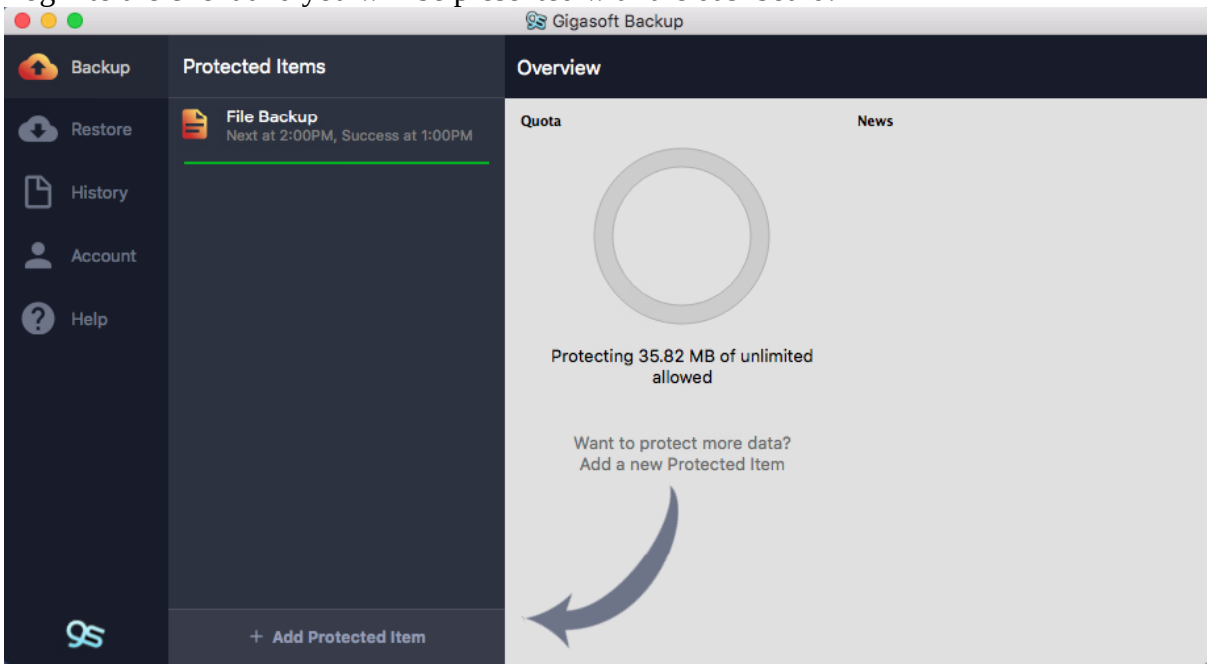
On the right-hand side panel click the **[Edit settings]** button and then navigate through the tabs to make the necessary changes.



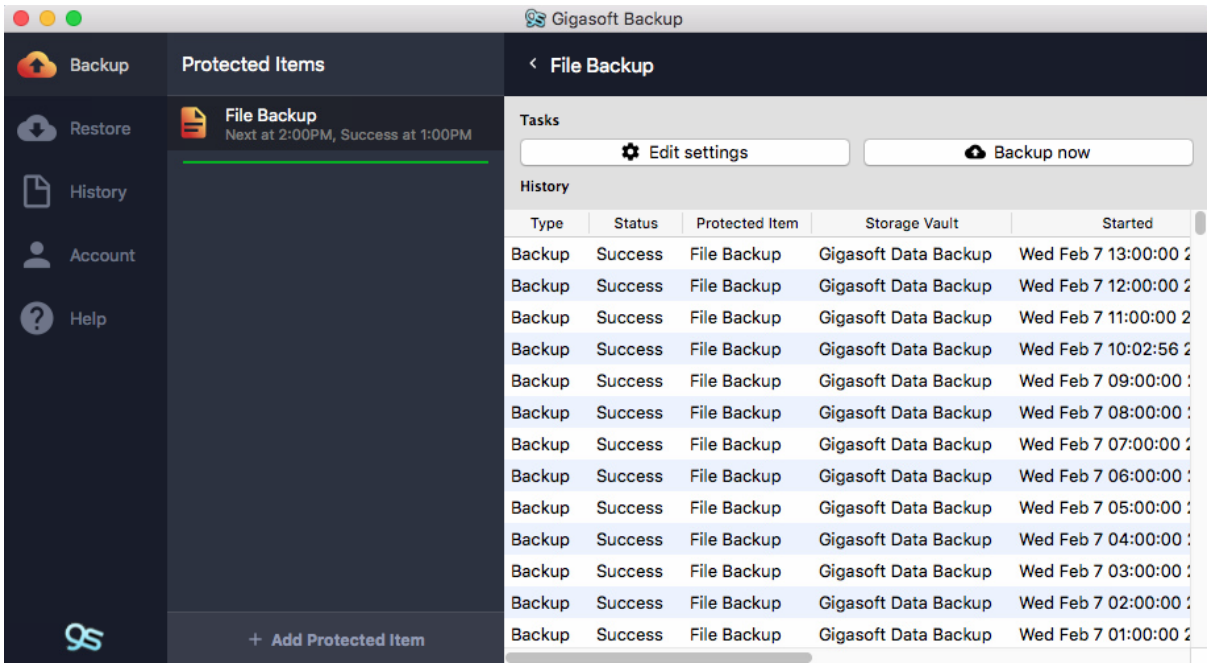
Once you have finished make sure you click the **[Save]** button to save the changes.

7.2 MacOS

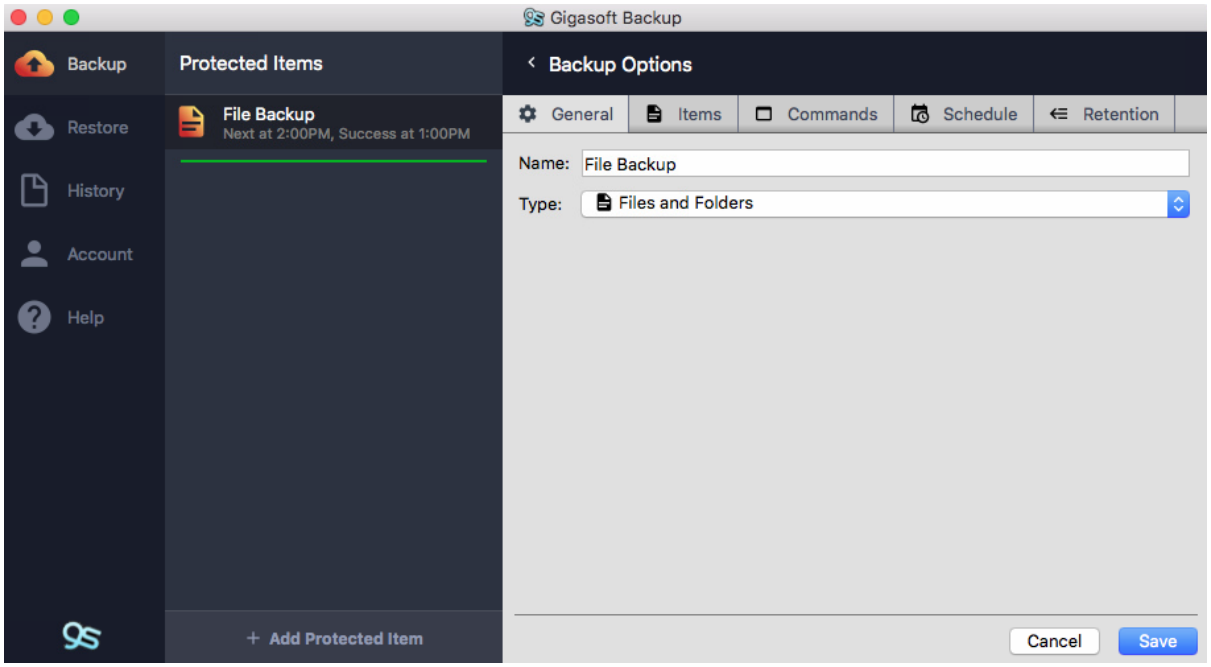
Log into the client and you will be presented with the dashboard.



Click on the name of the protected item you wish to edit.



On the right-hand side panel click the **[Edit settings]** button and then navigate through the tabs to make the necessary changes.



Once you have finished make sure you click the **[Save]** button to save the changes.

7.3 Linux (command Line)

Currently the Linux version is command line only, any changes to the account need to be performed via the customer portal.

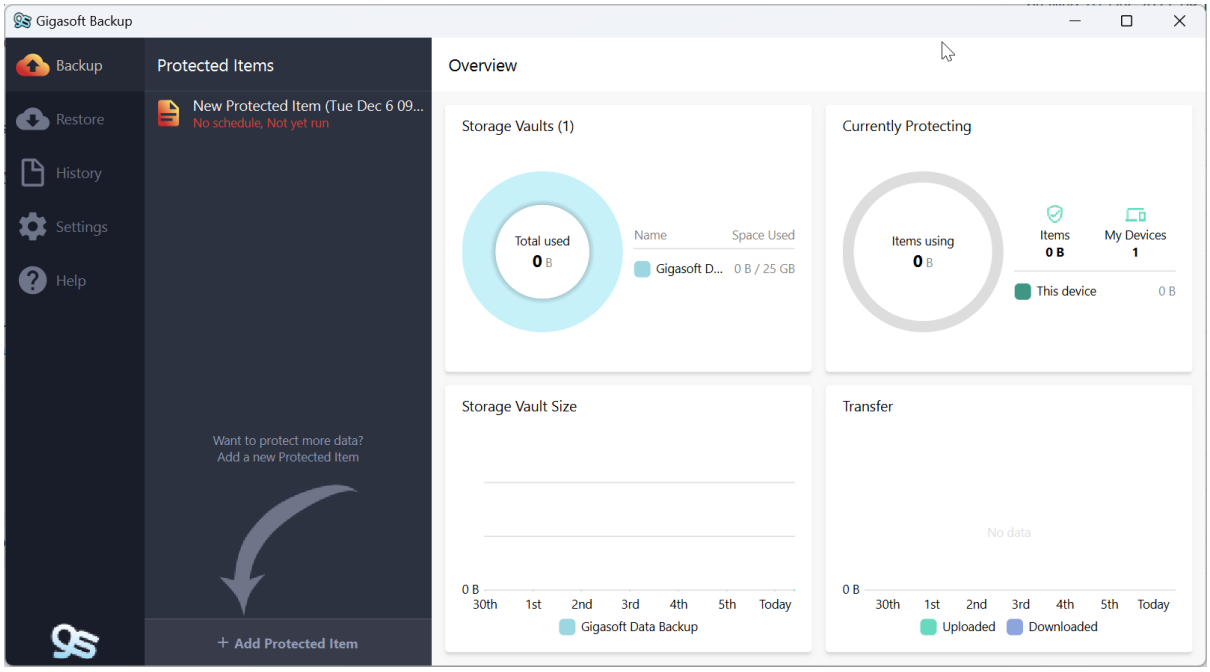
8 Restoring protected items

In this section we will cover the basics of a restoration using the different clients.

8.1 file protected items

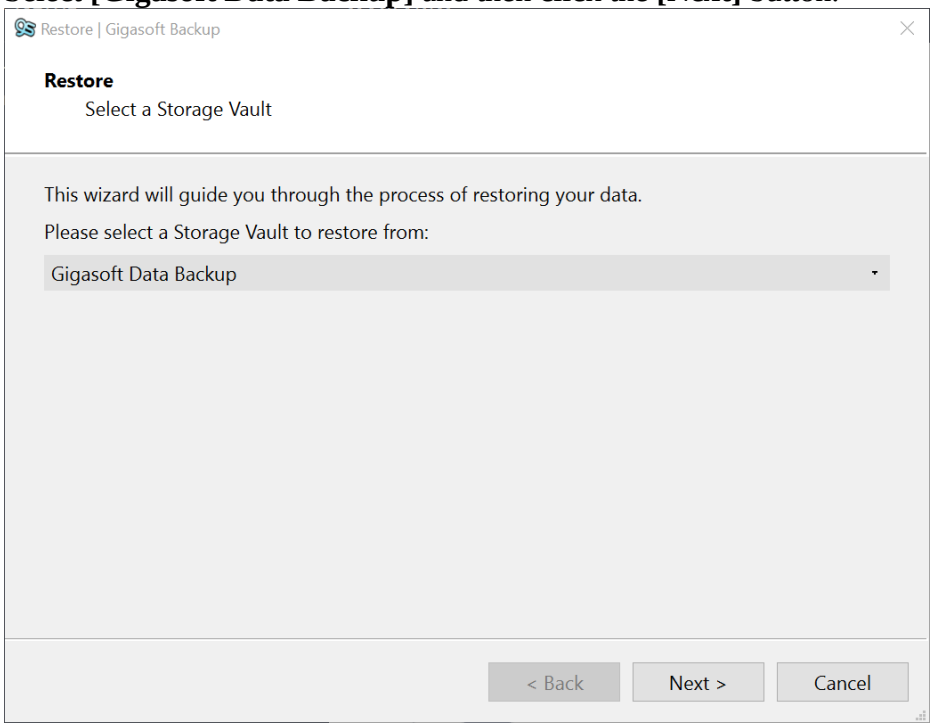
8.1.1 Restoring a file protected item (windows)

In this section we will go through the steps to restore a file protected item using the Windows Client.
Once you have logged in to Gigasoft Backup you will be presented with the main dashboard click the **[Restore]** button on the left-hand side of the screen.

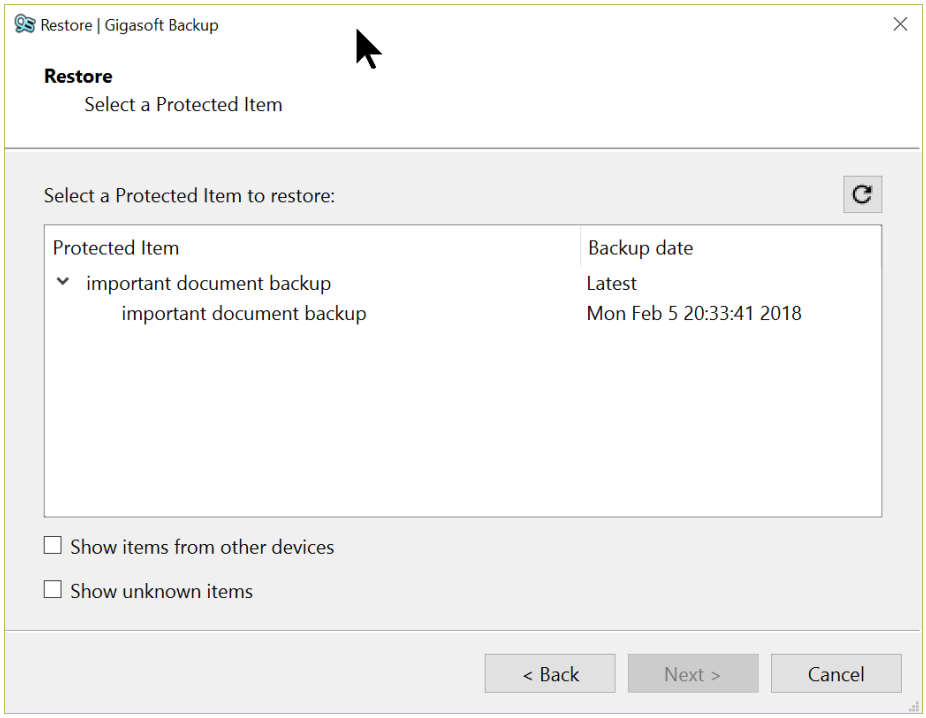


On the next screen you will be asked which storage vault you would like to restore your data from, if this is an offsite backup you would need to use the Gigasoft Data Backup Vault, if this was a local backup then you would select the name of your local vault (please refer to the section Local backups for more information).

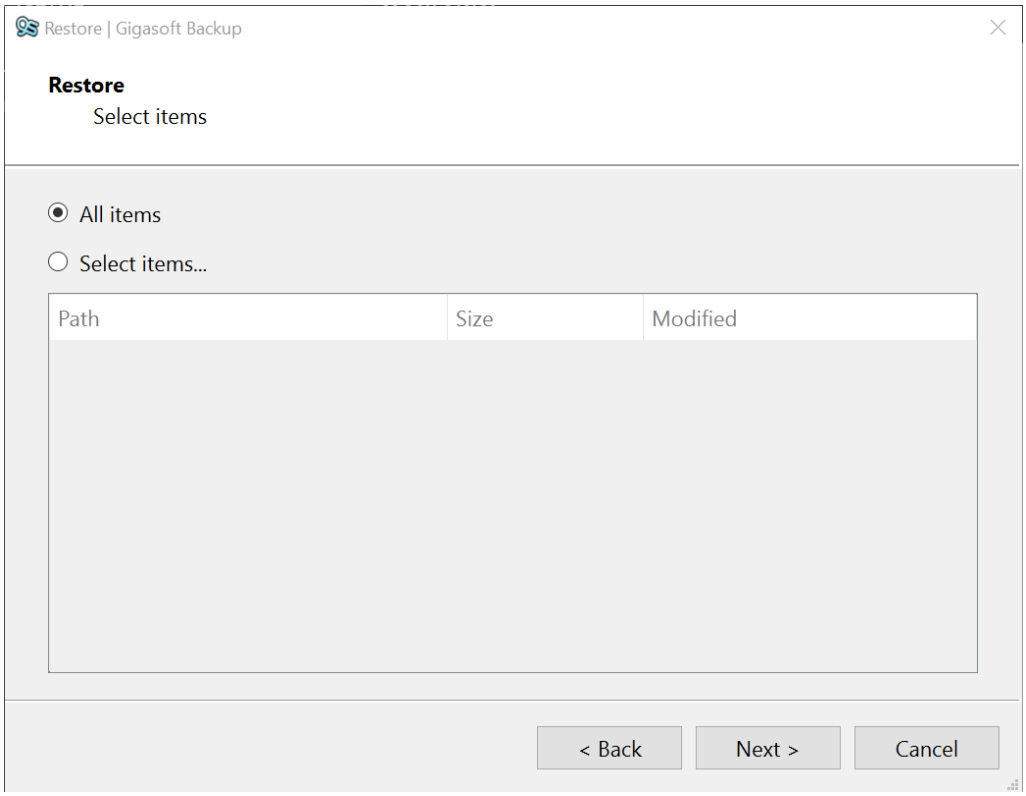
Select **[Gigasoft Data Backup]** and then click the **[Next]** button.



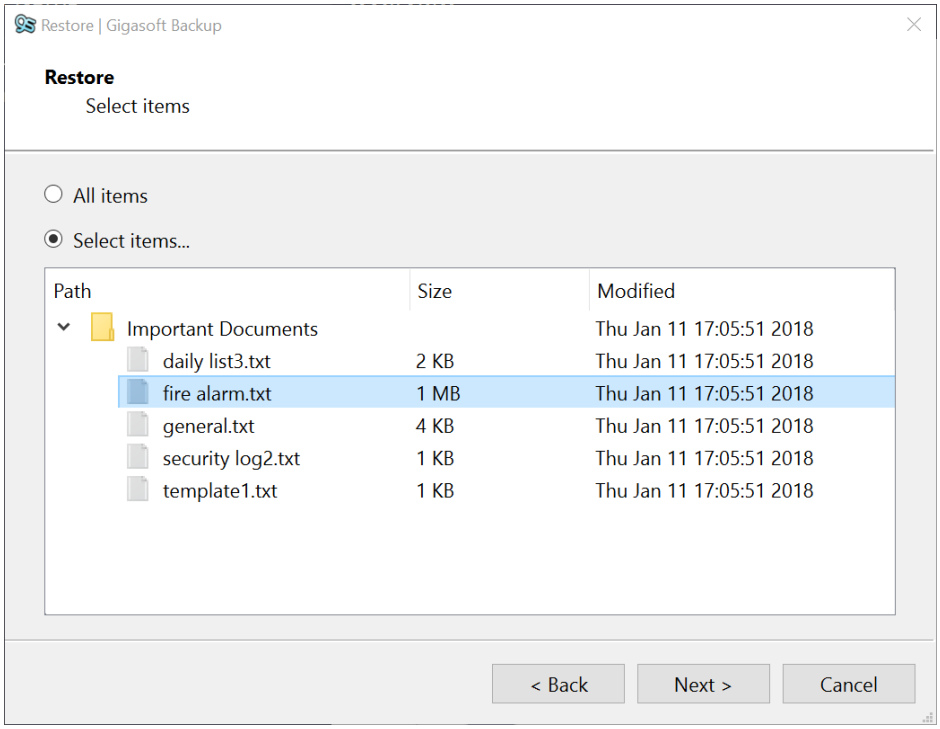
On the next screen you will be shown a list of protected items held by this account on this storage vault, select the drop-down arrow next to the file backup and then click on a point in time that you wish to restore, click **[Next]** to continue



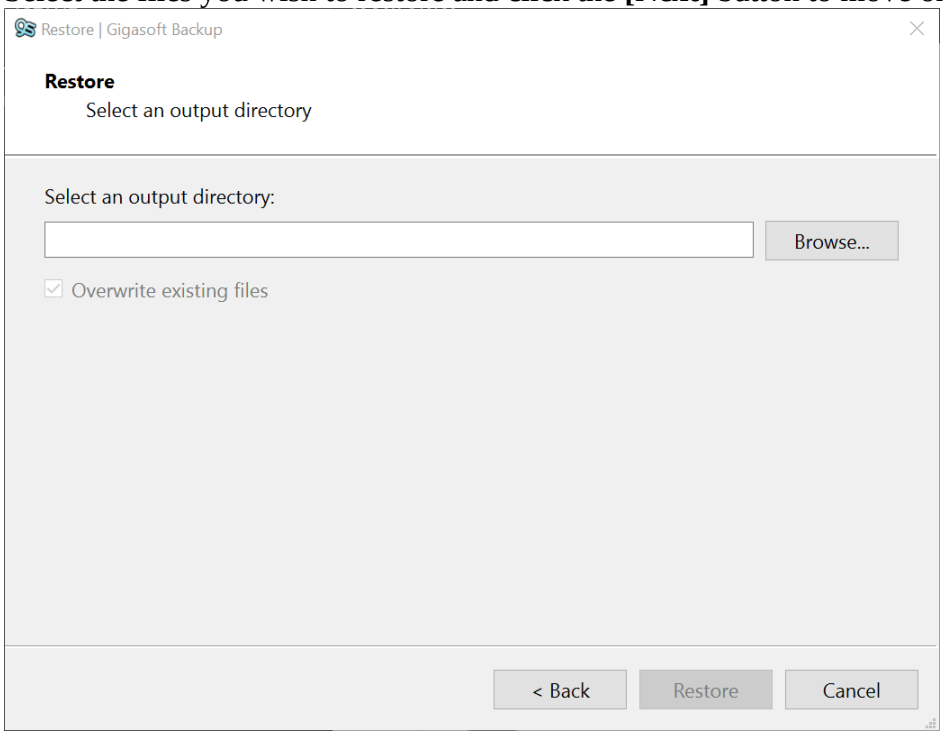
The next screen gives you the option to fully restore all the data up to and including this backup job, to do so click the **[Next]** button or if you need specific files click the **[Selected items]** radio button, click the **[Next]** button to continue to the next step.



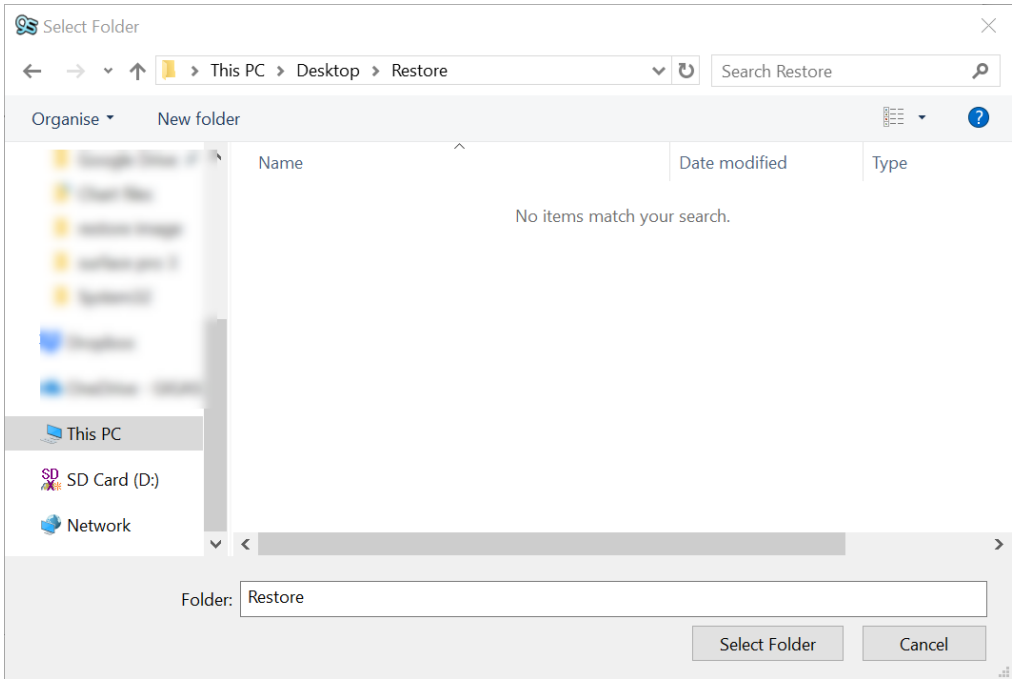
The next screen allows you to drill down and select the files you wish to restore.



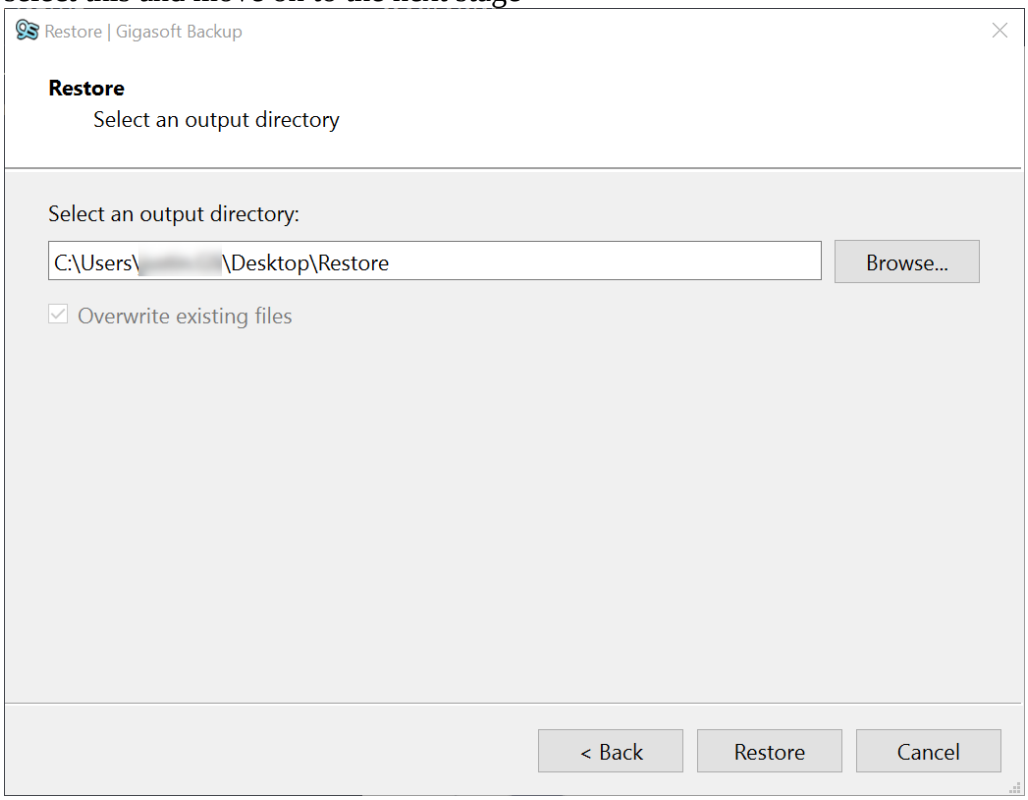
Select the files you wish to restore and click the **[Next]** button to move on to the next stage.



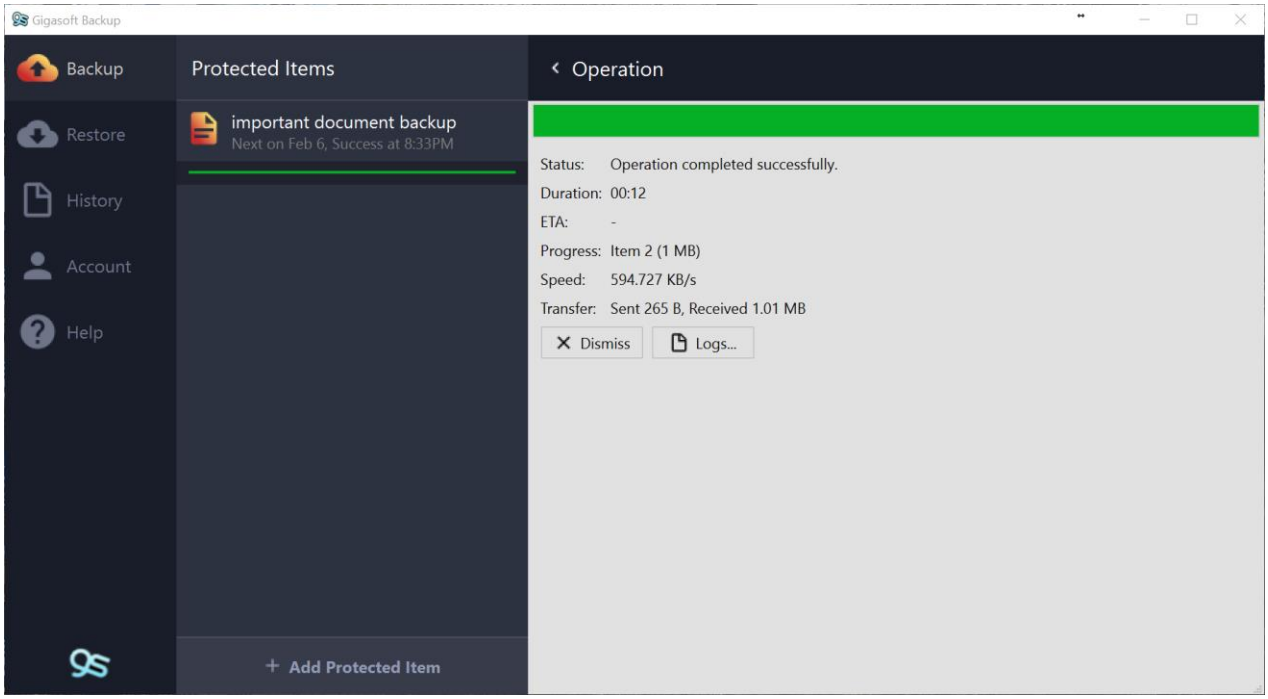
On this screen we are asked where we would like to restore the data to, best practise is to restore the data to a temporary location to make sure you have the data you need and then copy over to the original location ready for use. Click the **[Browse]** button to open the explorer view or if you have a location ready type the full path name and click **[Restore]**



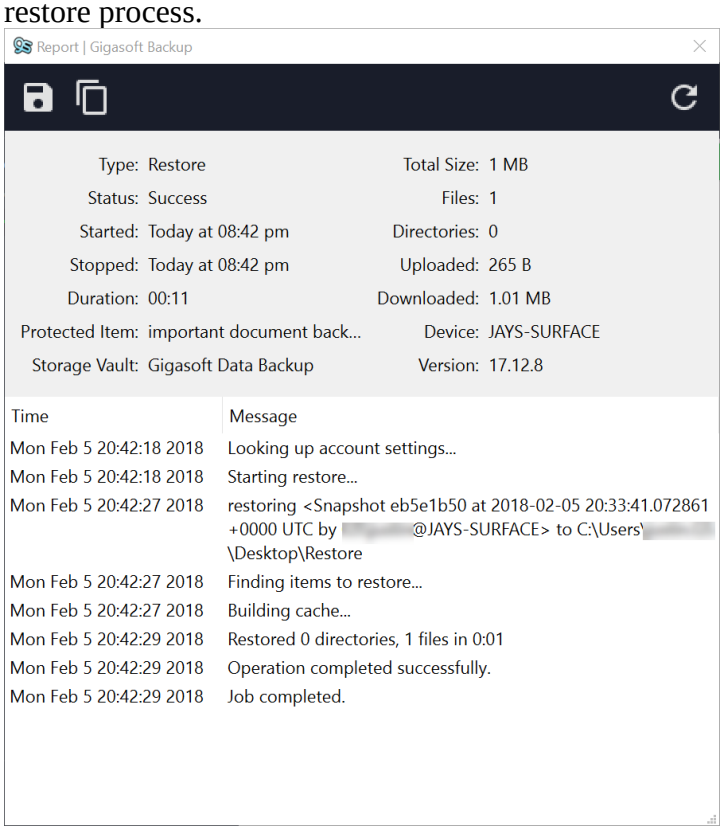
Create a folder that you wish to restore the data to or if you have a location already simply select this and move on to the next stage



You will be presented with the directory option again with the location selected ready for the restore. If this is correct click the **[Restore]** button to start the restore process.



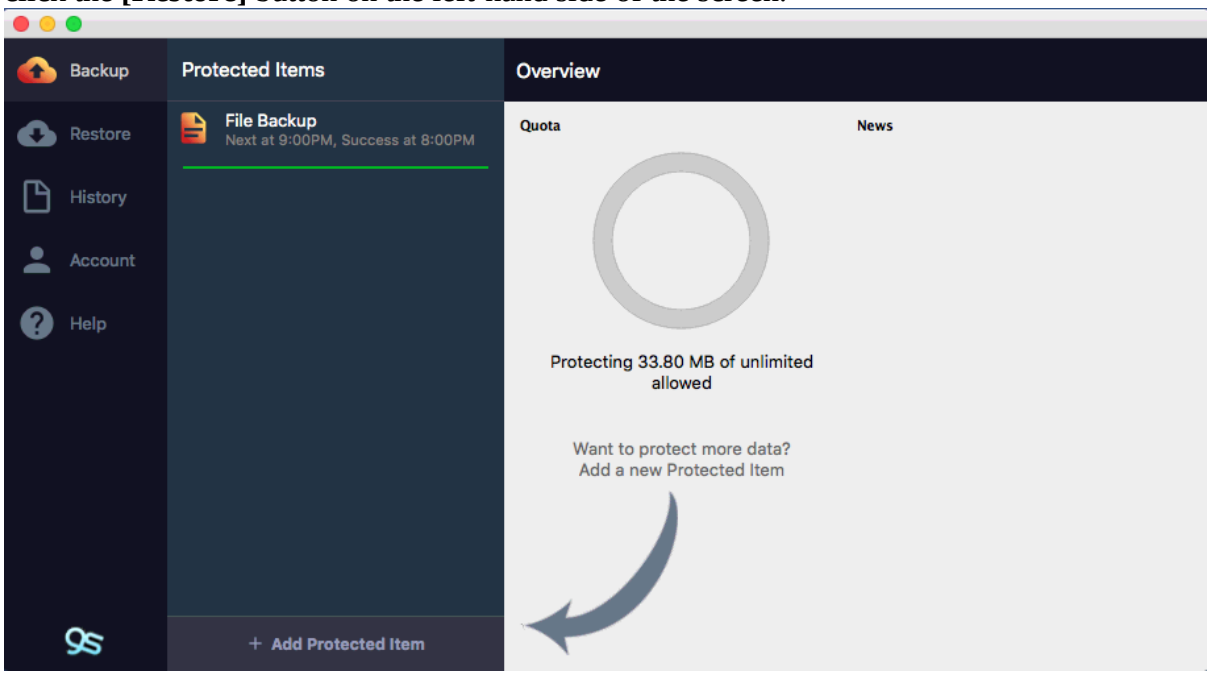
The restore will begin and you will see the green progress bar move as the restore progresses. Once it completes you will be shown the operation page.
Clicking on the **[Logs]** button will bring up a restore report giving you more detail of the restore process.



Clicking on the X in the top right will close the report and take you back to the operation page.
Clicking the **[Dismiss]** button will close the restore page and take you back to the main dashboard.

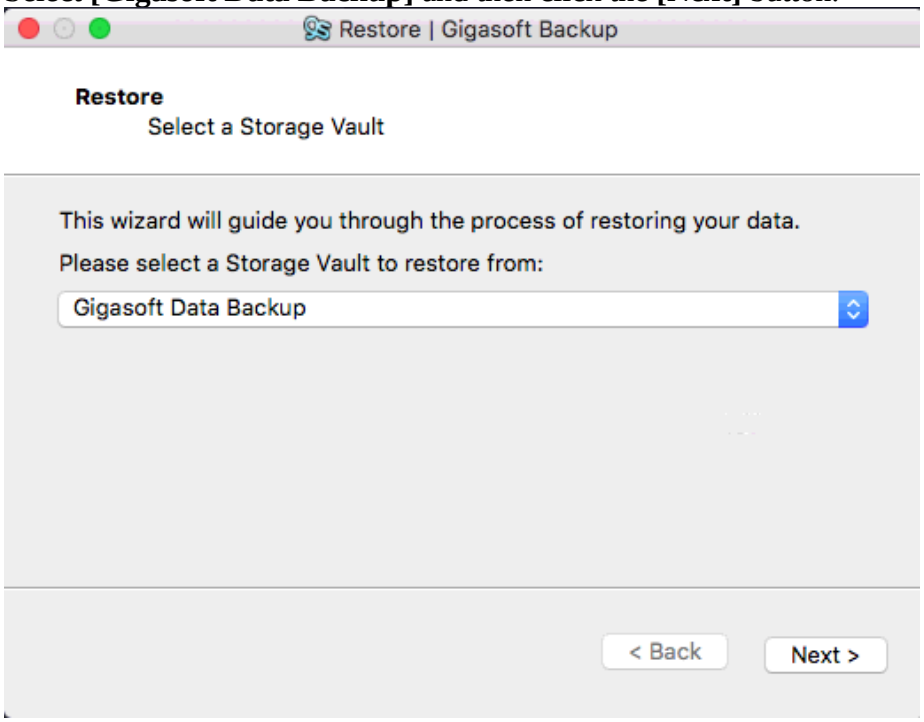
8.1.2 Restoring a file protected item (MacOS)

In this section we will go through the steps to restore a file protected item using the MacOS Client.
Once you have logged in to Gigasoft Backup you will be presented with the main dashboard click the **[Restore]** button on the left-hand side of the screen.

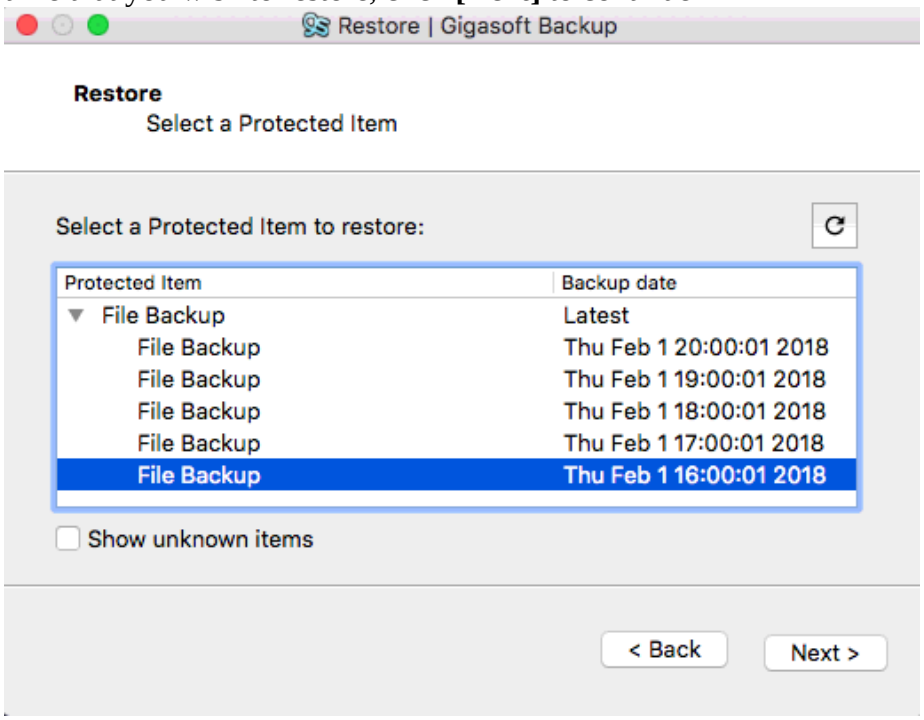


On the next screen you will be asked which storage vault you would like to restore your data from, if this is an offsite backup you would need to use the Gigasoft Data Backup Vault, if this was a local backup then you would select the name of your local vault (please refer to the section Local backups for more information).

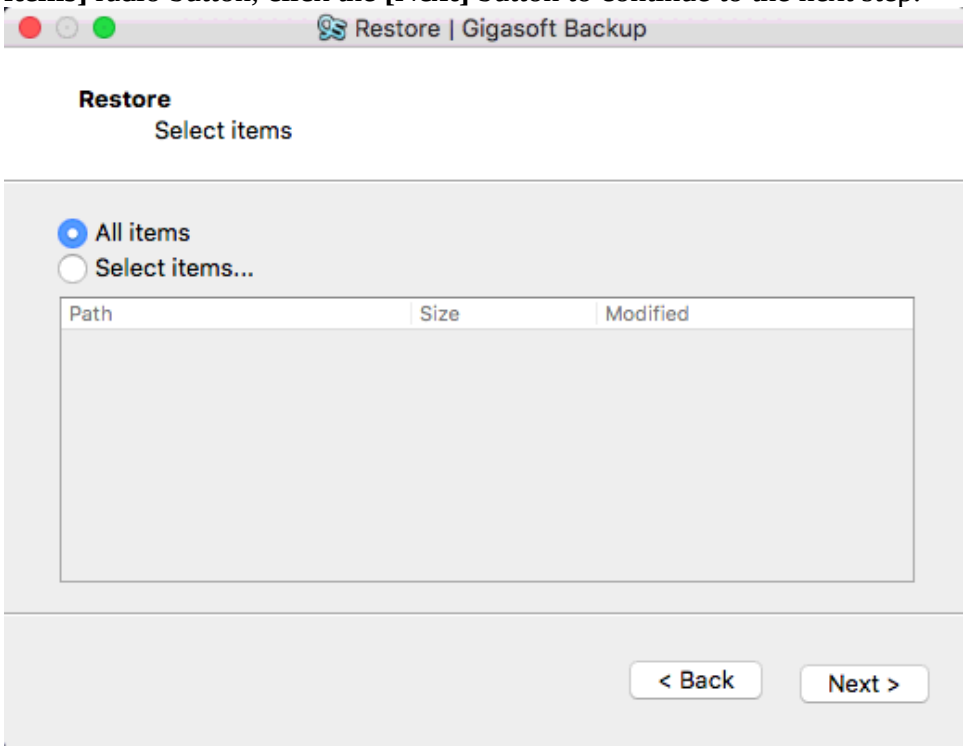
Select **[Gigasoft Data Backup]** and then click the **[Next]** button.



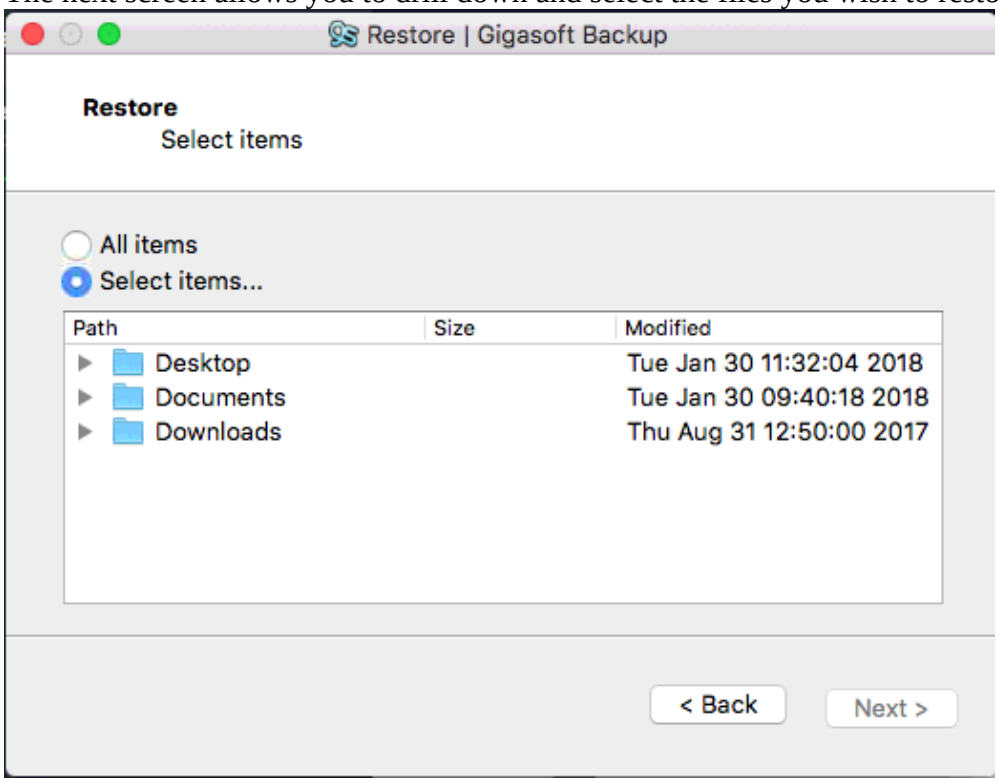
On the next screen you will be shown a list of protected items held by this account on this storage vault, select the drop-down arrow next to the file backup and then click on a point in time that you wish to restore, click **[Next]** to continue



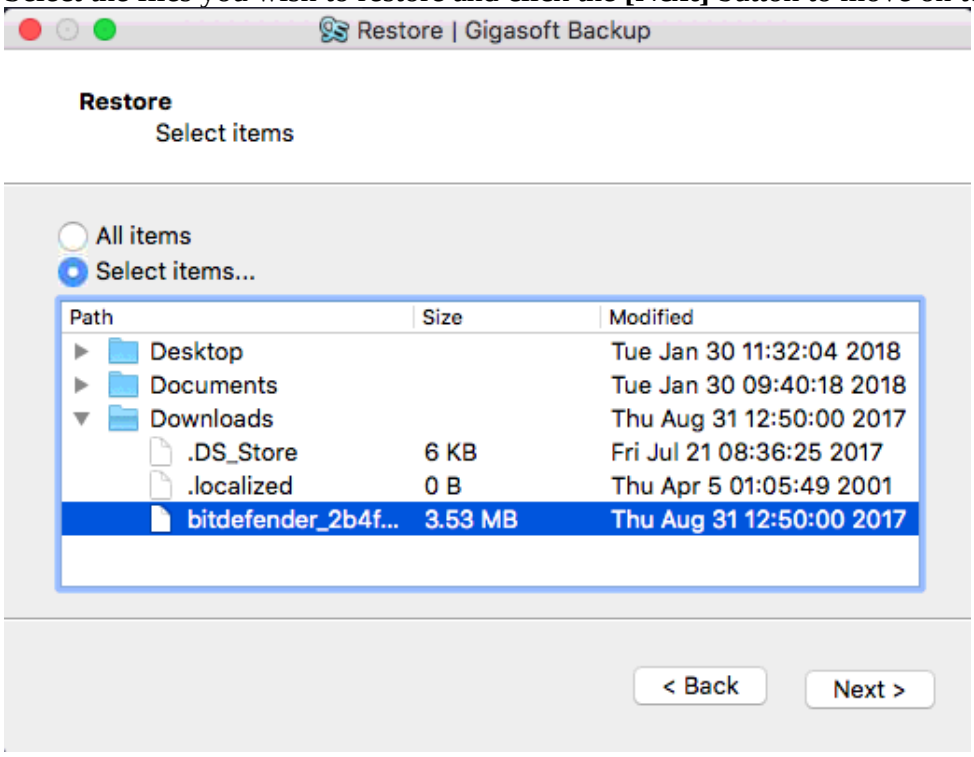
The next screen gives you the option to fully restore all the data up to and including this backup job to do so click the **[Next]** button or if you need specific files click the **[Selected items]** radio button, click the **[Next]** button to continue to the next step.



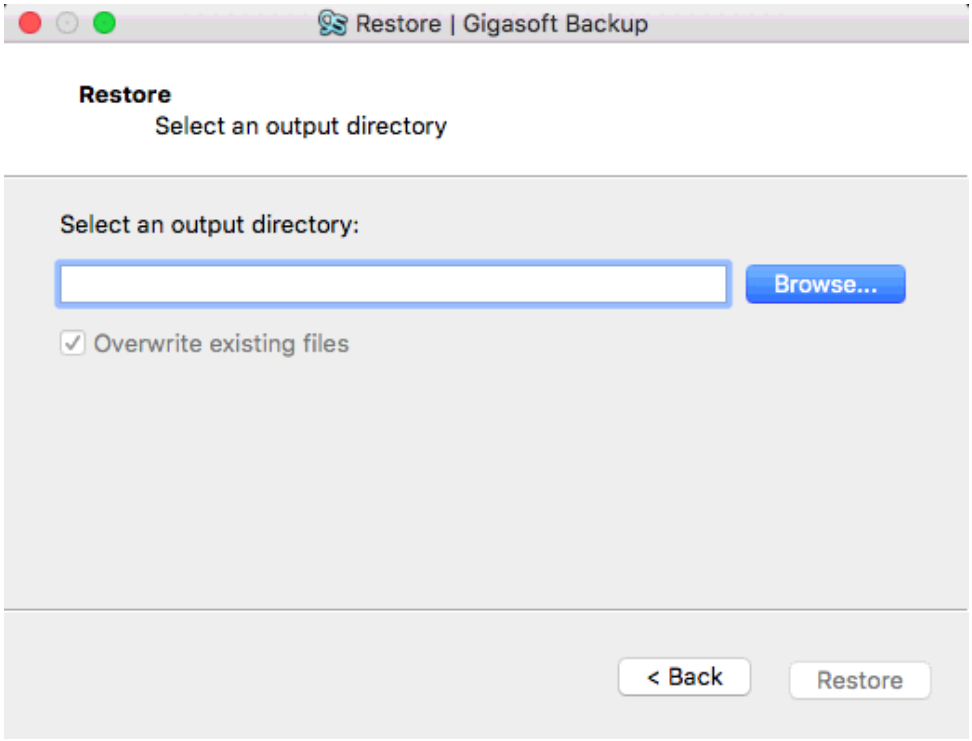
The next screen allows you to drill down and select the files you wish to restore.



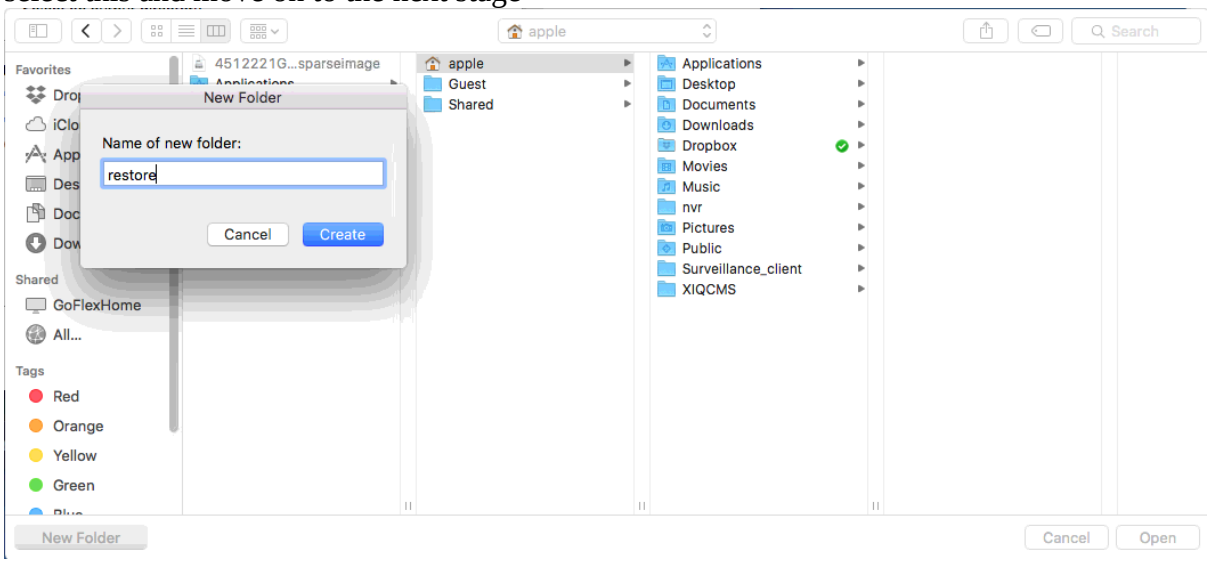
Select the files you wish to restore and click the **[Next]** button to move on to the next stage.



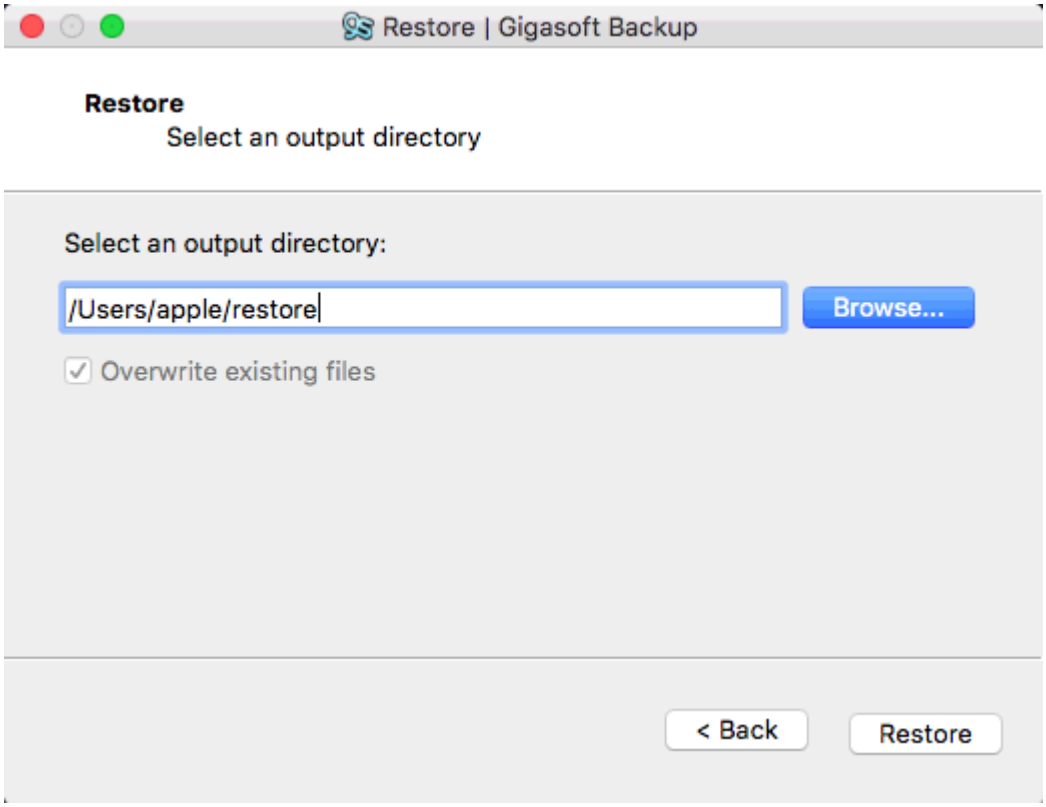
On this screen we are asked where we would like to restore the data to, best practise is to restore the data to a temporary location to make sure you have the data you need and then copy over to the original location ready for use. Click the **[Browse]** button to open the explorer view or if you have a location ready type the full path name and click **[Restore]**



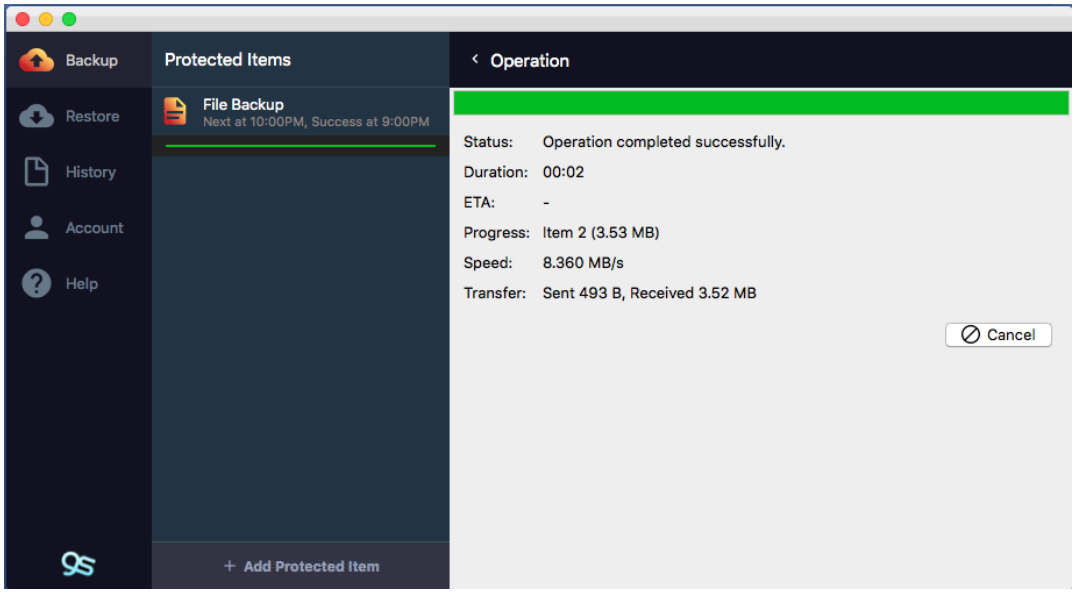
Create a folder that you wish to restore the data to or if you have a location already simply select this and move on to the next stage



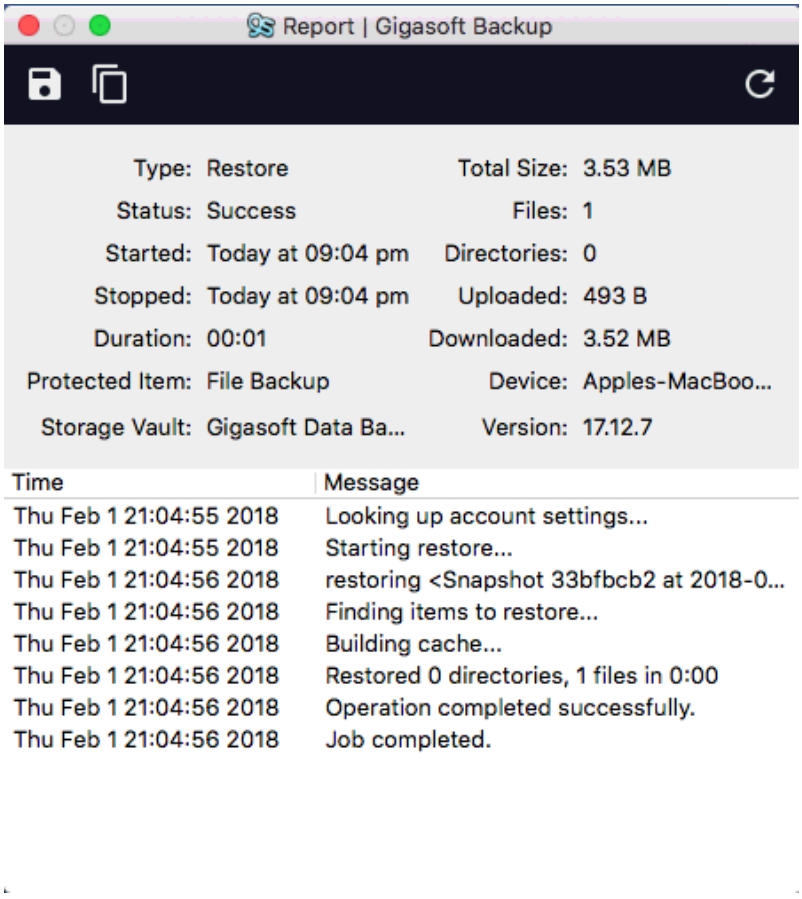
You will be presented with the directory option again with the location selected ready for the restore. If this is correct click the **[Restore]** button to start the restore process.



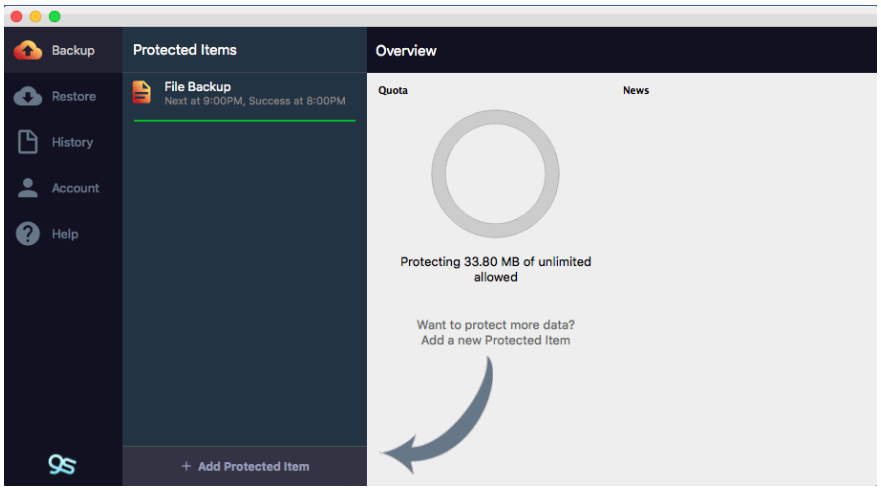
The restore will begin and you will see the green progress bar move as the restore progresses. Once it completes you will be shown the operation page.



Clicking on the **[Logs]** button will bring up a restore report giving you more detail of the restore process.



Clicking on the red dot will close the report and take you back to the operation page. Clicking the **[Dismiss]** button will close the restore page and take you back to the main dashboard.



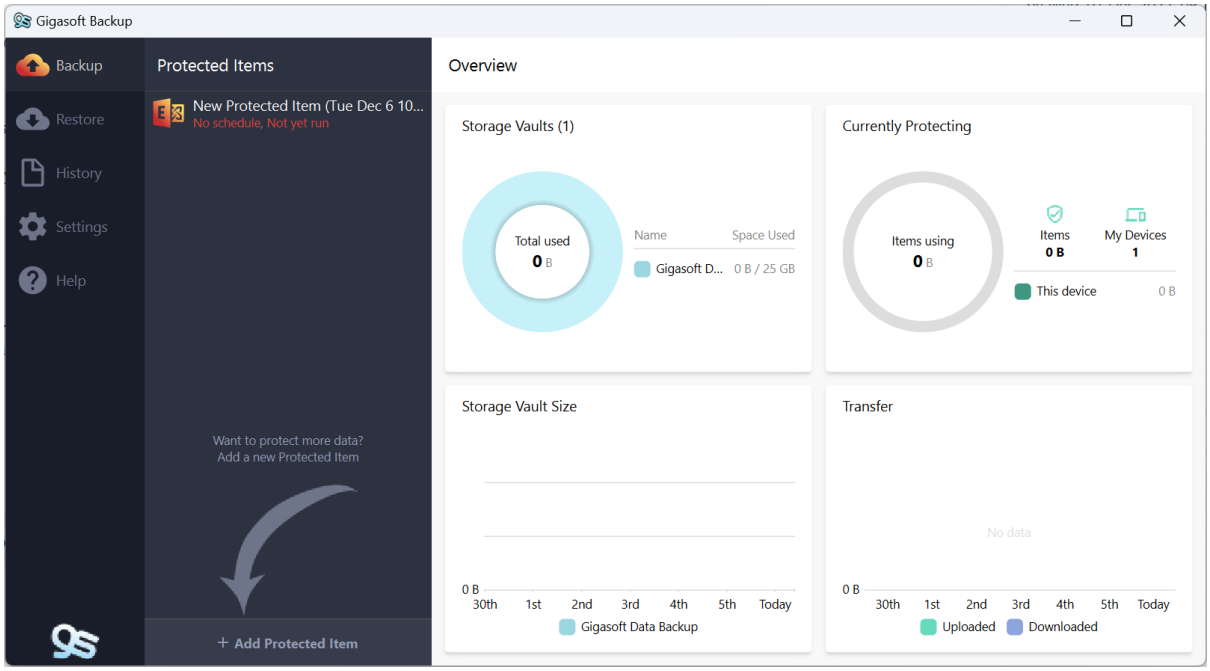
8.1.3 Restoring a file protected item (Linux)

As there currently is no customer portal available you have the option to restore via a windows client or if you provide us with a path to an empty location we can perform the restore remotely from any point in time, this would be a complete restore from that day so there would need to be plenty of space to receive the restore, once the restore has started there is no way to stop and you would need to wait until we tell you before moving any data from

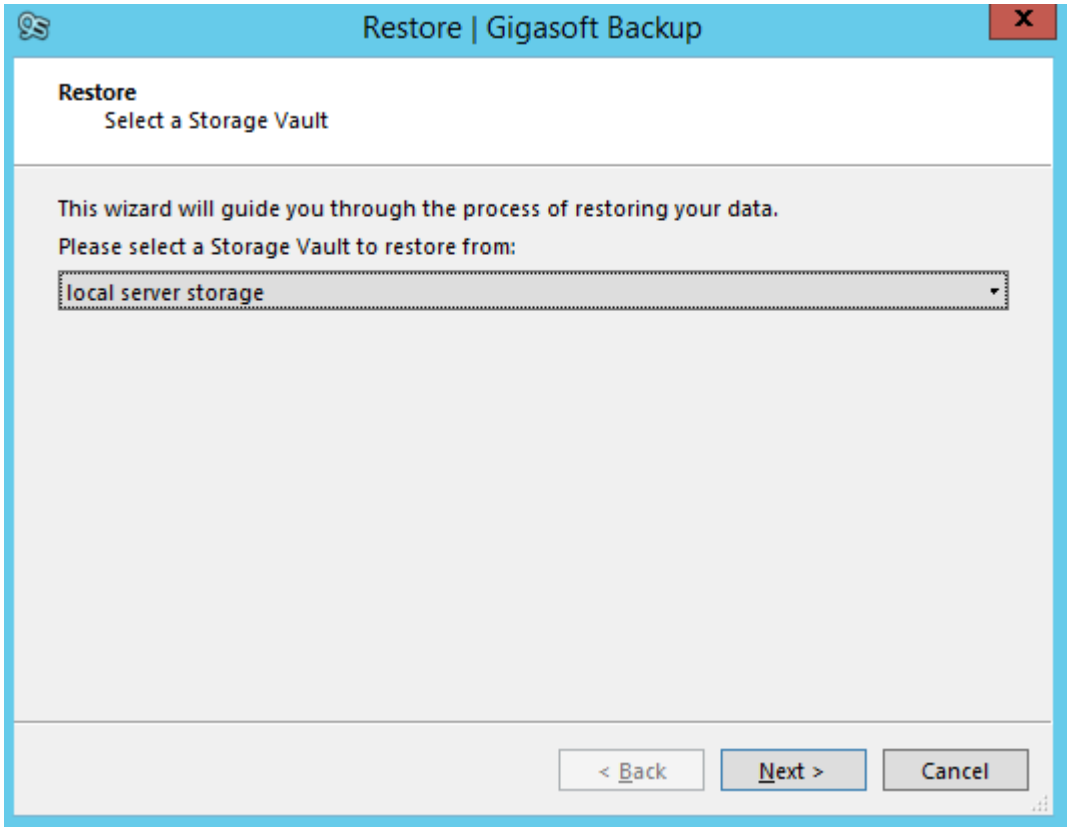
the restore location back into your live area, we don't have any way of knowing how long the restore would take as there is no progress bar or ETA so you may find restoring to a windows machine more flexible for you.

8.2 Exchange protected item

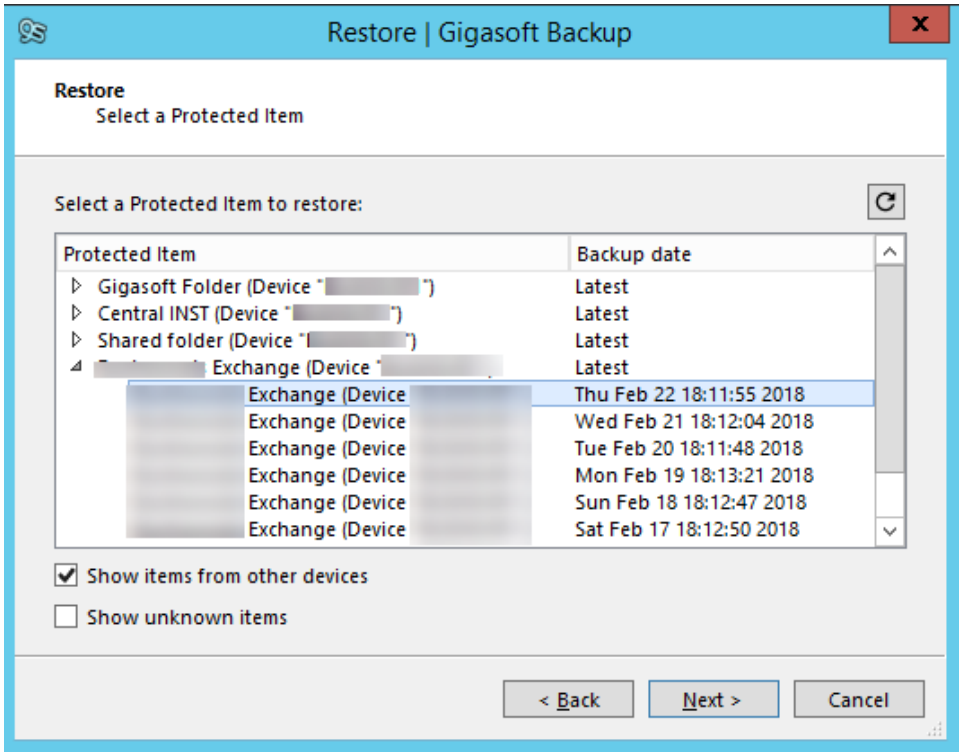
In this section we will guide you through the process of restoring an Exchange database, as each version of Microsoft Exchange is different there will be further steps needed to mount the databases that you will need to follow as per Microsoft guides, we will not cover these here.



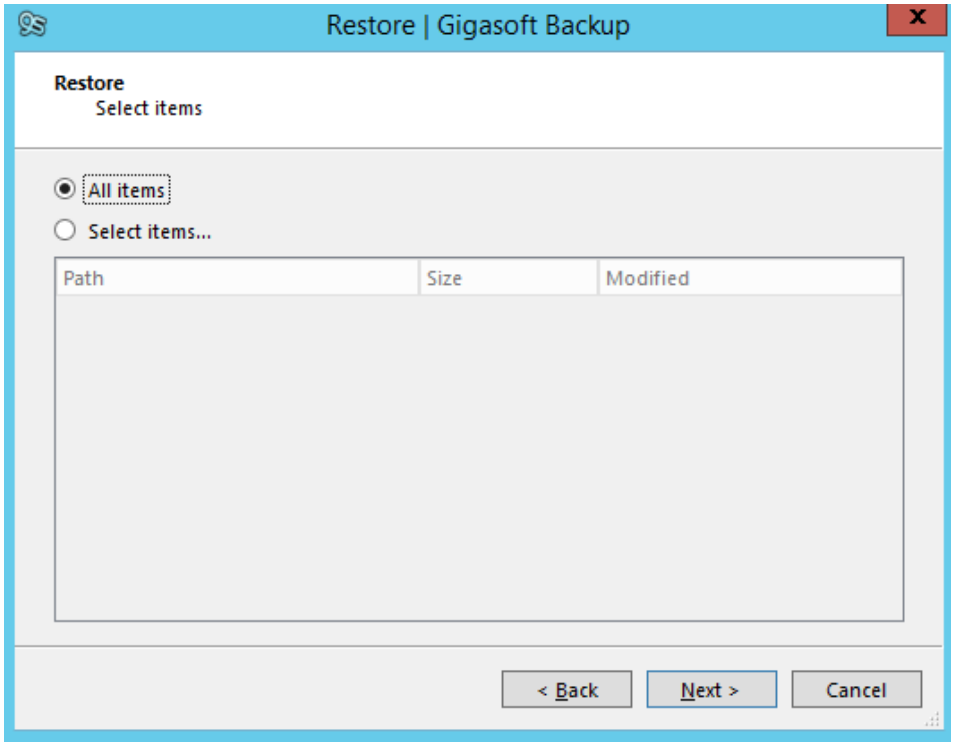
Firstly, log in to the Gigasoft Backup Manager.



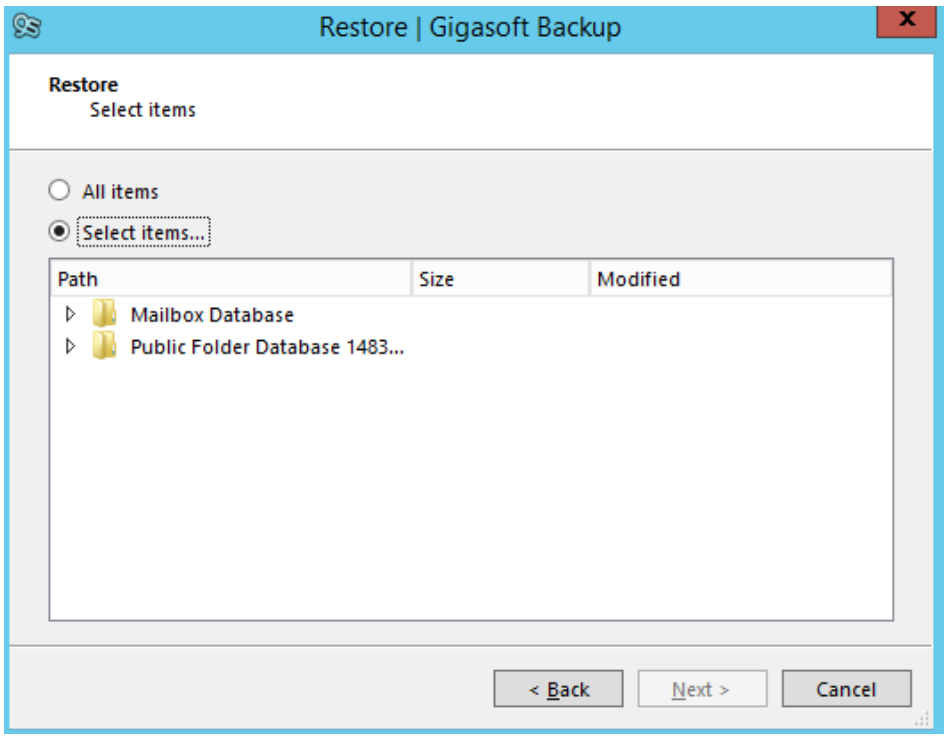
Select the restore tab and choose the storage vault from the drop-down menu, click **[Next]** to continue



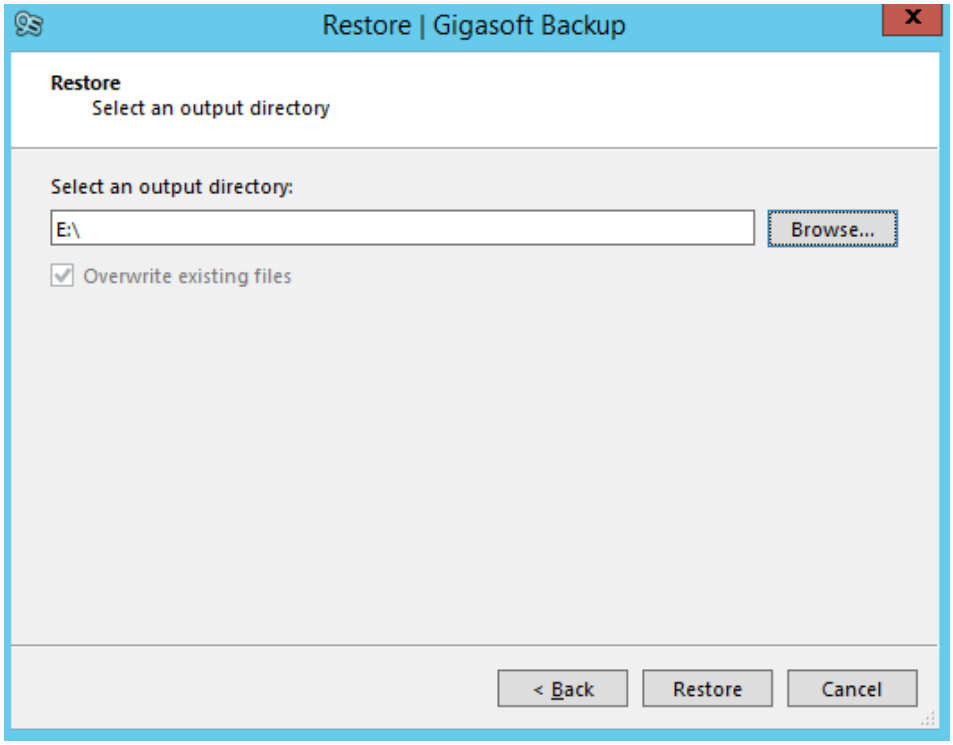
If this is a restore to the same server then select the Exchange database you wish to restore. If this is a new Exchange server click on the **[Show items from other devices]** tick box and then drill down to the instance of Exchange you wish to restore.



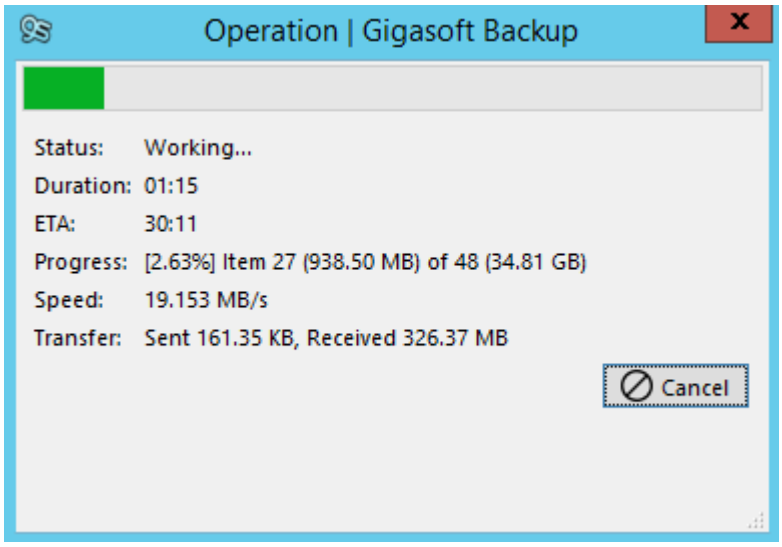
If you wish to restore all databases leave the default settings and click **[Next]**



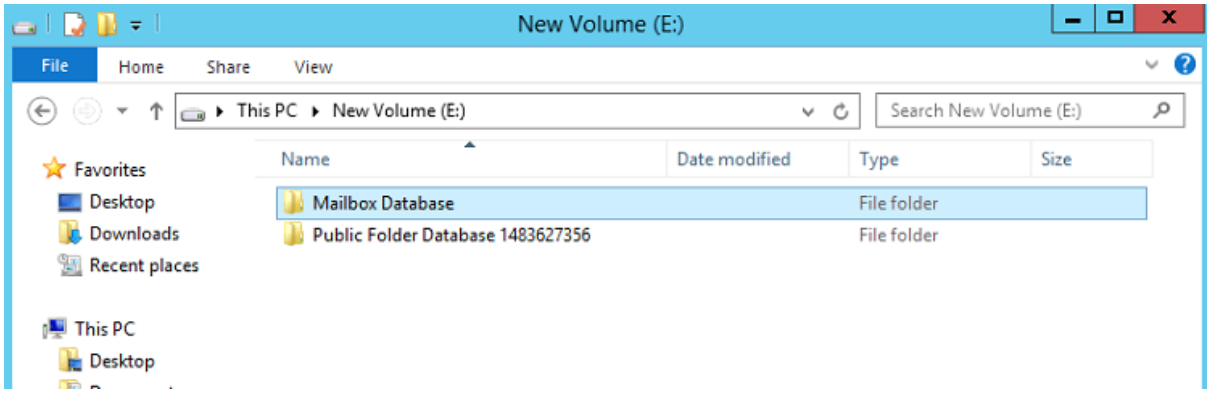
Or if you only wish to restore one database, select **[Select items…]** and then highlight the database you wish to restore before clicking **[Next]**



Select a suitable location for the restore, this needs to be large enough to take all of the data, once you import this back into Exchange this location can be cleared if needed, click **[Restore]** to start the restore process.



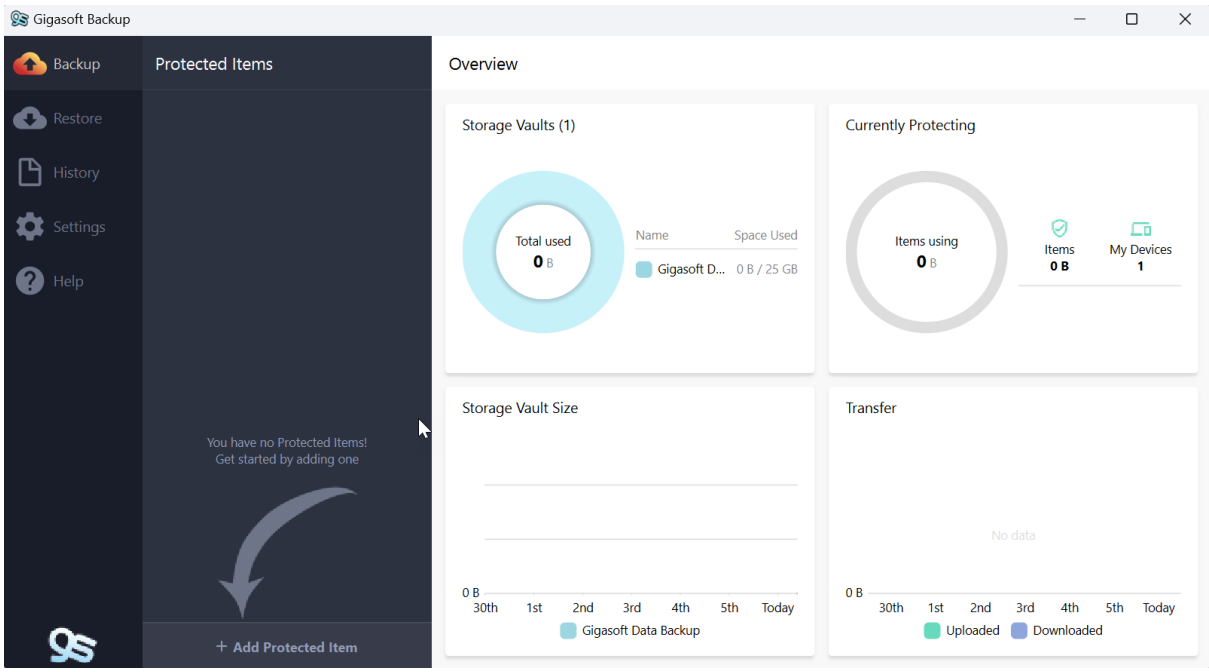
You will now see the restore progress bar, if you click on this a more detailed restore window will appear.



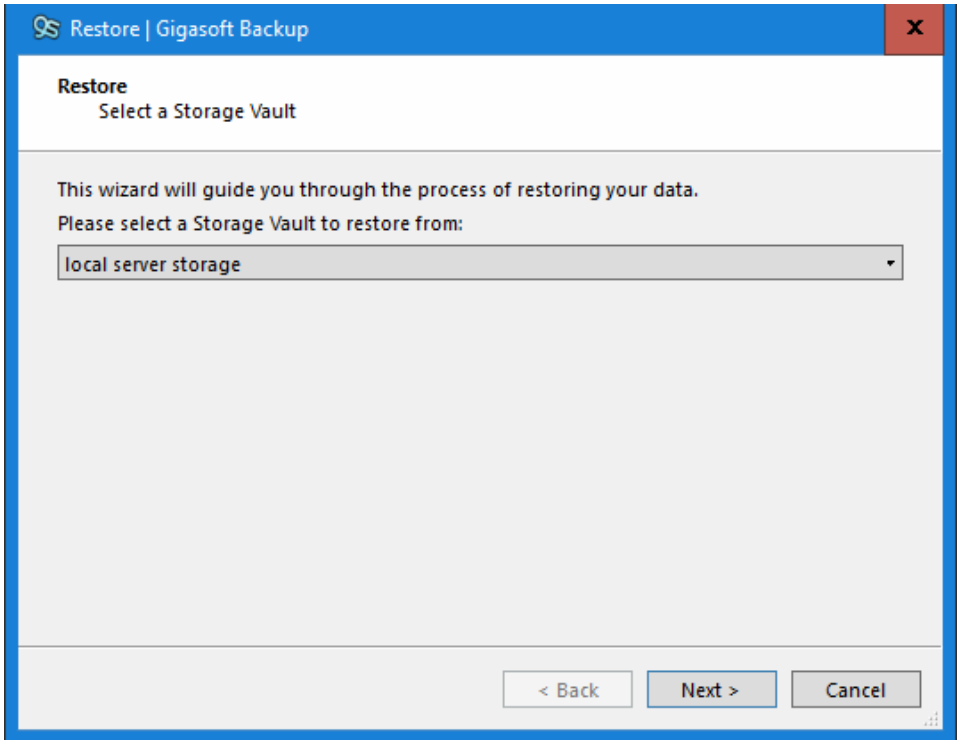
Once the restore has completed you will be able to see the restored files in the restore location, now follow the relevant guide from Microsoft to import this database back into your Exchange server and mount if needed.

8.3 Hyper V Protected item

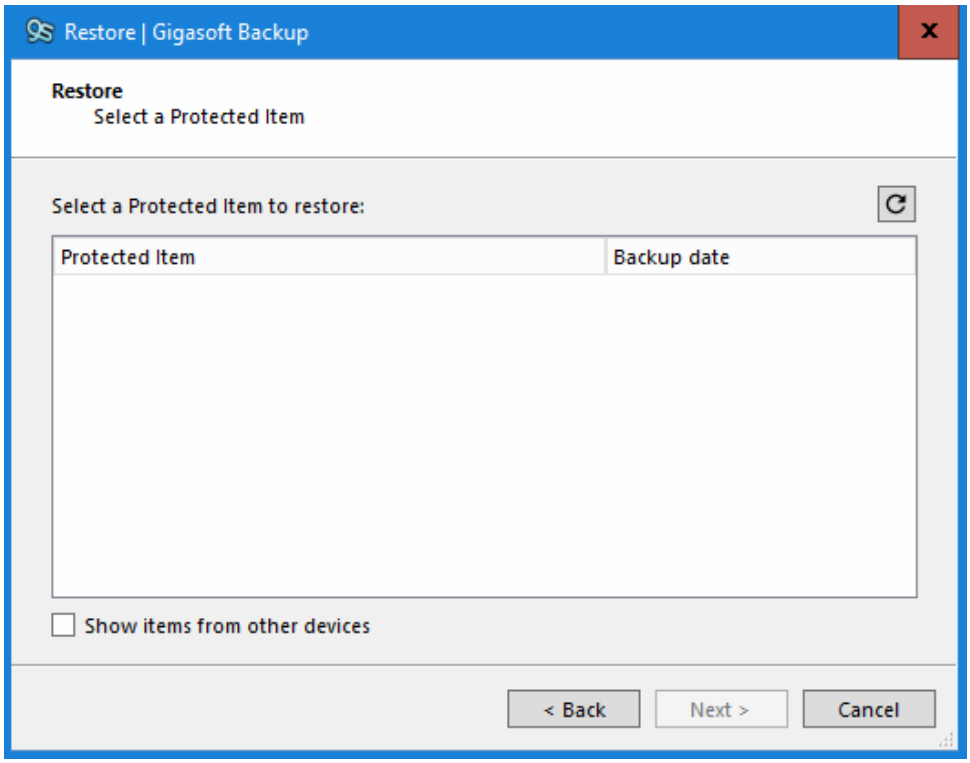
This section will guide you through the process of restoring a Hyper-V machine.
Hyper-V backups can only be performed from a Windows Server running Hyper-V.
In this example we will be restoring a Hyper-V machine from one hypervisor to another (assume hypervisor has failed) but restoring to the same hypervisor would be very similar.
Make sure the Hyper-V service is running and that you can access the Hyper-V Manager.
First, we need to install the Gigasoft Backup client onto the new hypervisor, please refer to the install section and the section for registering for the 1st time.
Once you have the client installed log in as you would normally you will see an empty dashboard.



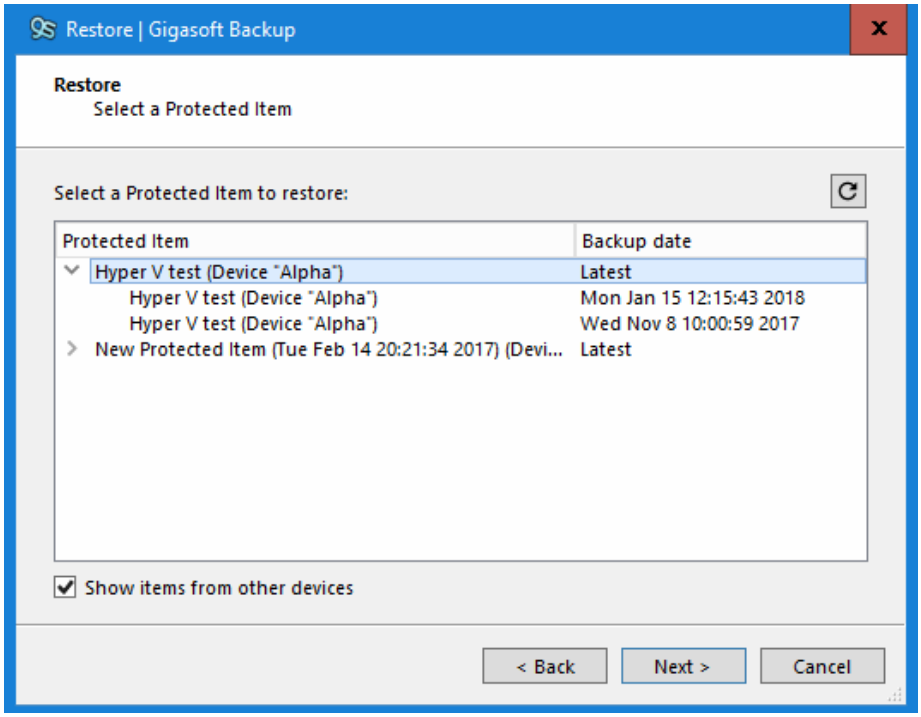
We can now start the restore to this server.



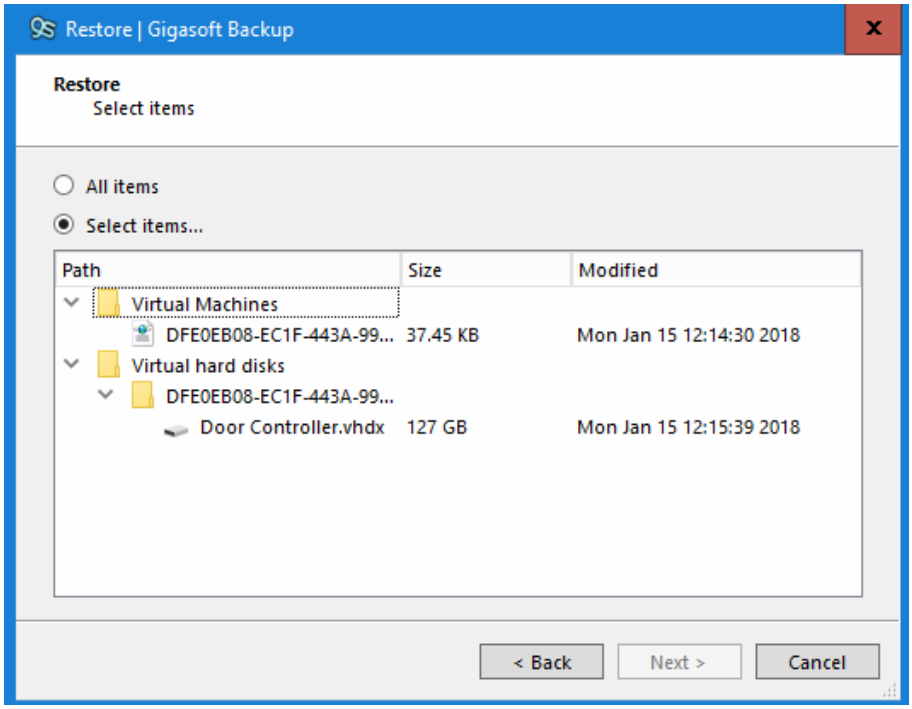
Click on the **[Restore]** tab, select the Vault from the drop-down list that contains your Hyper-V backups and click **[Next]** (in this example we are using a local vault for the Hyper-V backups).



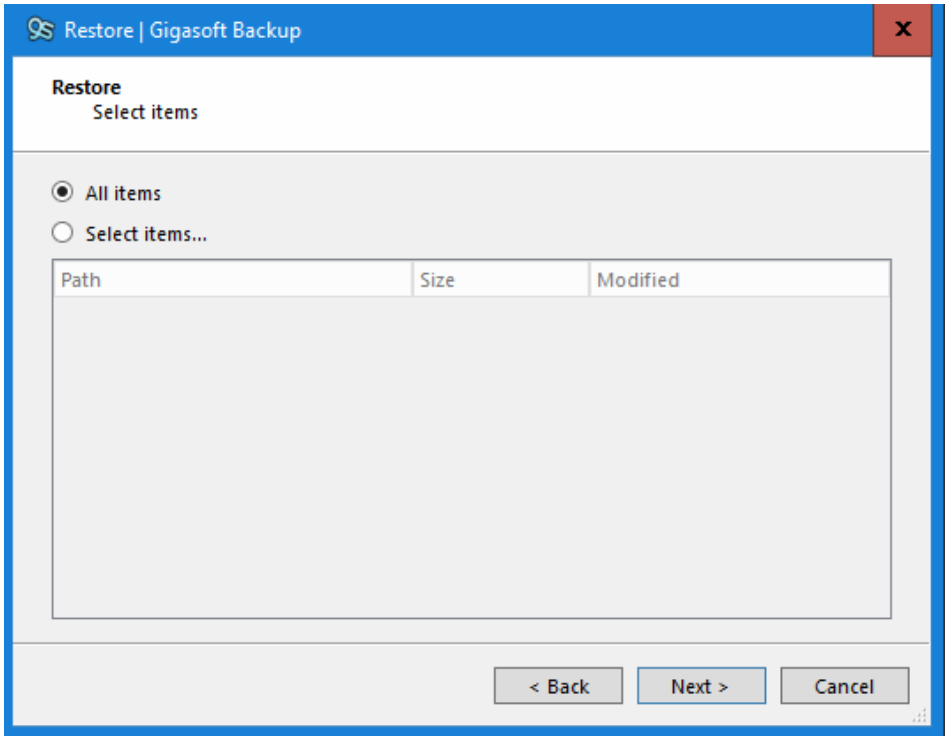
You will see there is no data able to be restored, this is because there are no protected items on this machine, click the **[Show items from other devices]** radio button and the list will begin to populate.



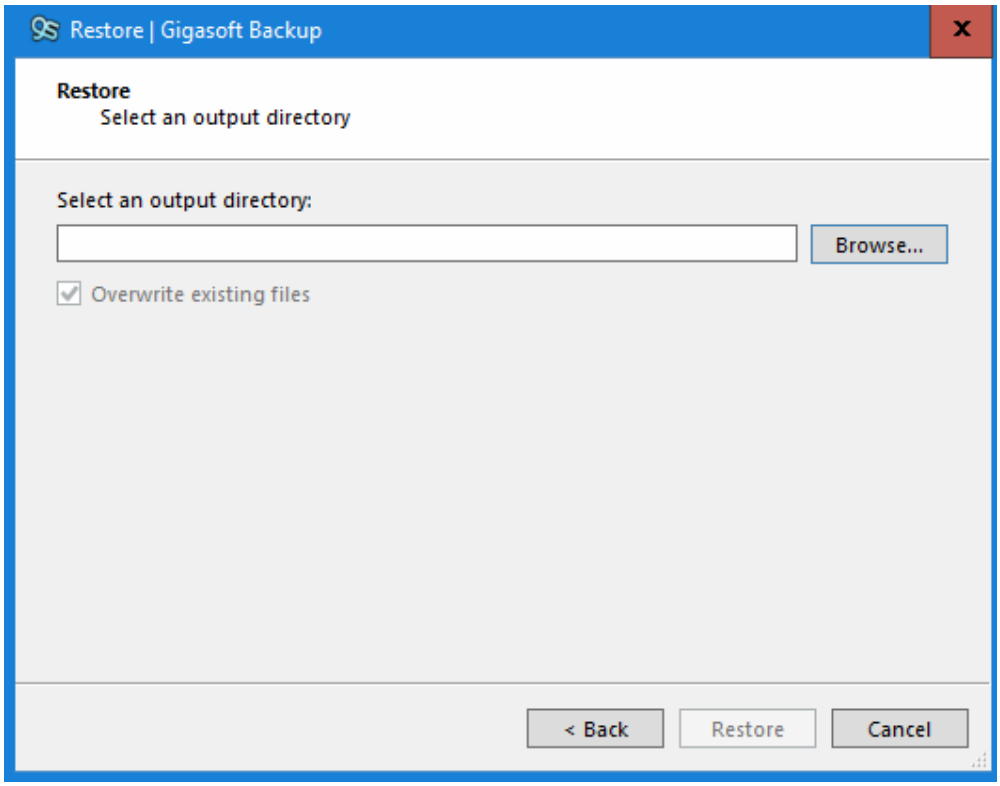
Click the down arrows to drill down into the correct protected item to reveal the snapshots available. In this example we will restore the latest version, highlight the version you wish to restore and then click the **[Next]** button.



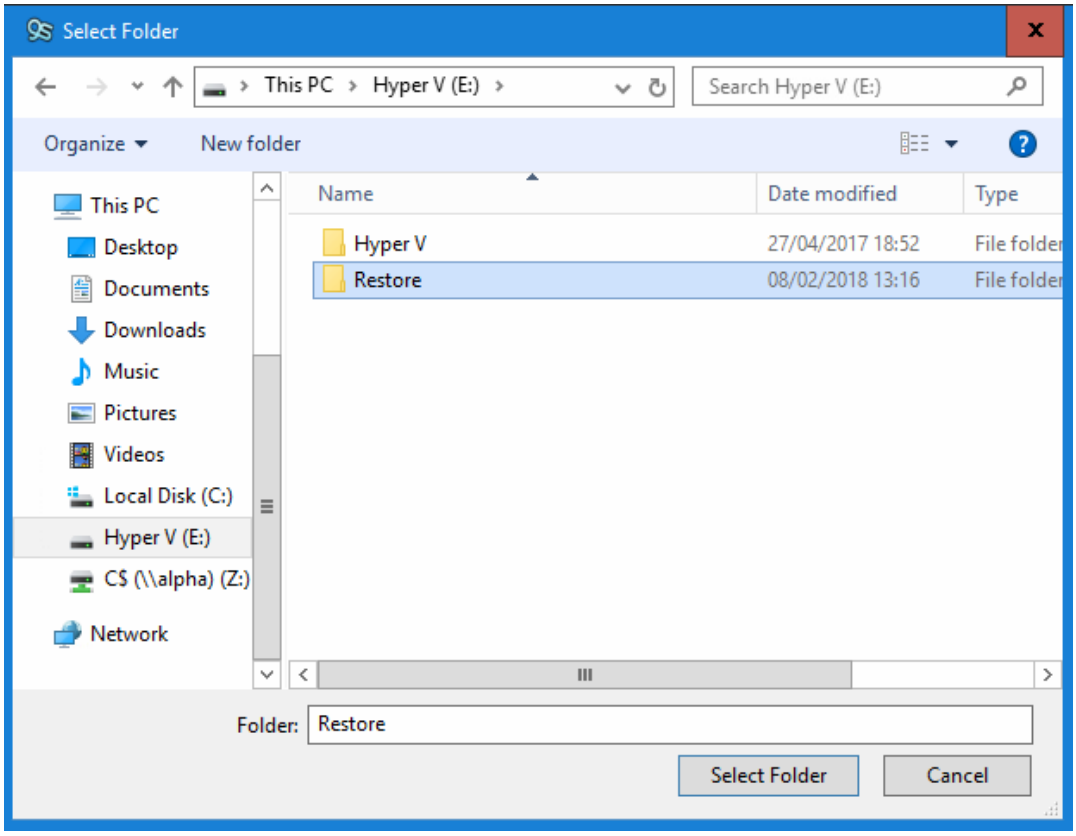
If this was a partial recovery or you have multiple virtual machines you would choose the **[Select items]** and drill down and restore only the parts / machines you needed.



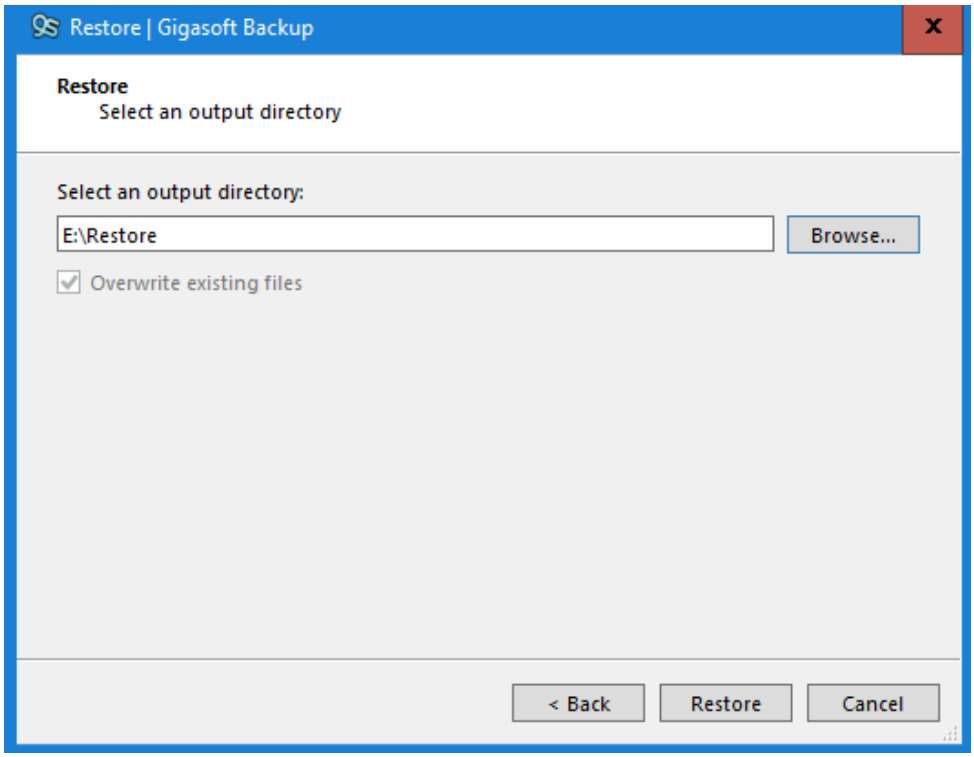
In our example we only have one virtual machine being backed up so we will select the **[All items]** option and then click **[Next]**.



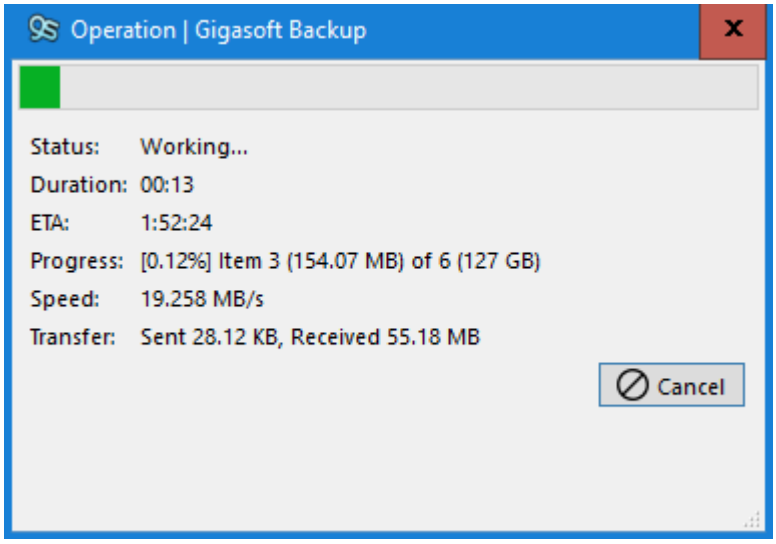
Now we need to select an output directory, this needs to be somewhere large enough for the recovered virtual machine. Click the **[Browse]** button to open the explorer view.



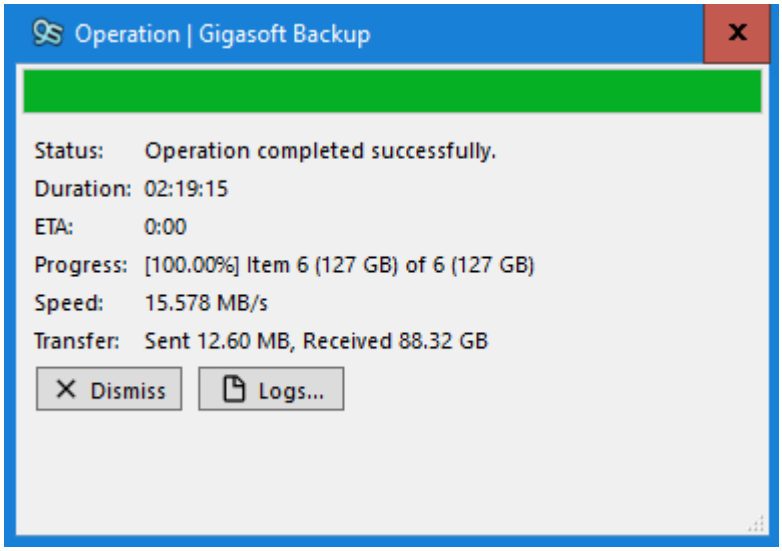
Create a folder somewhere, in this example I have created a folder called *restore* on the E drive, now click on the **[Select Folder]** button.



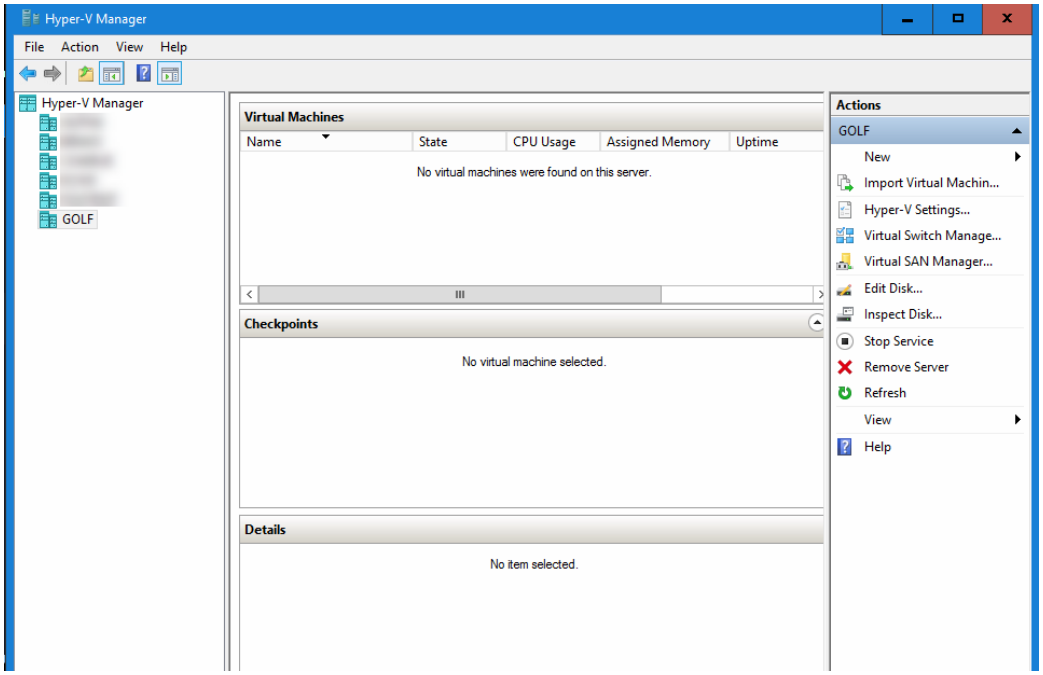
You can now see the folder has been selected ready for the restore, click **[Restore]** to begin the restore process.



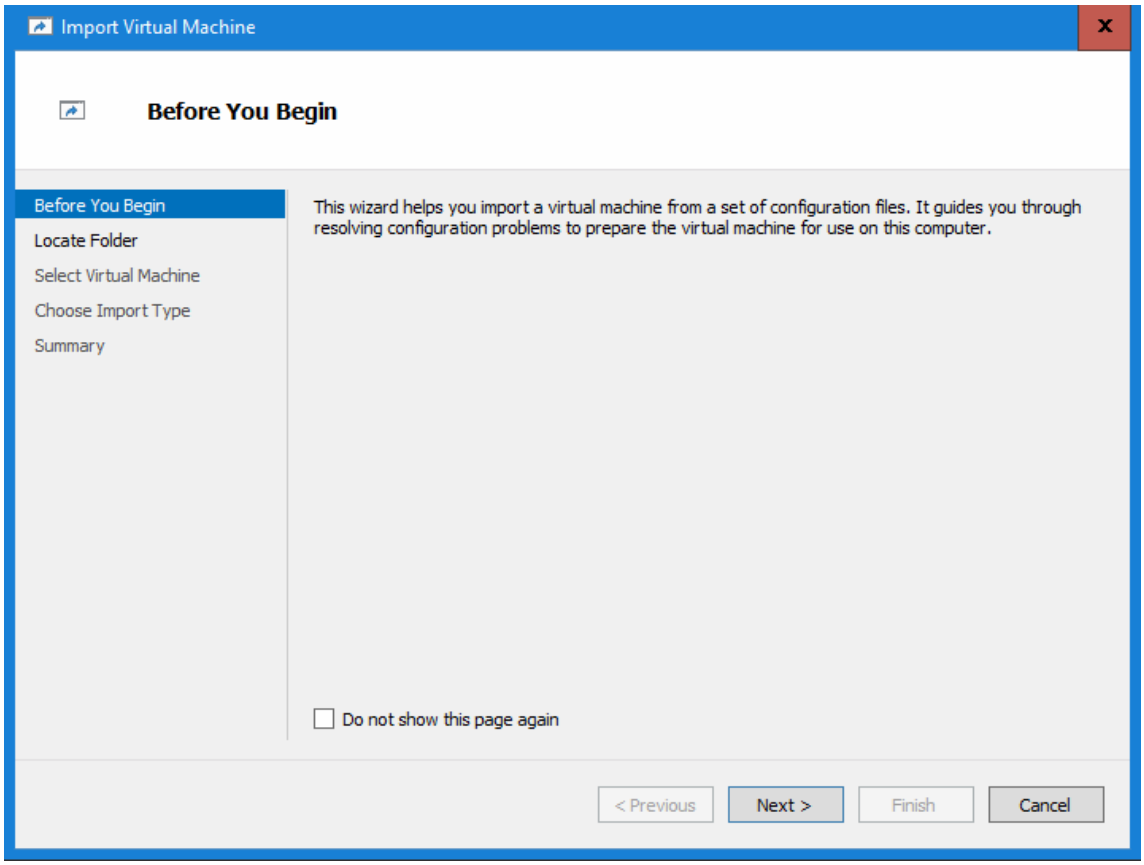
The restore will begin and you will see a progress screen like this one.



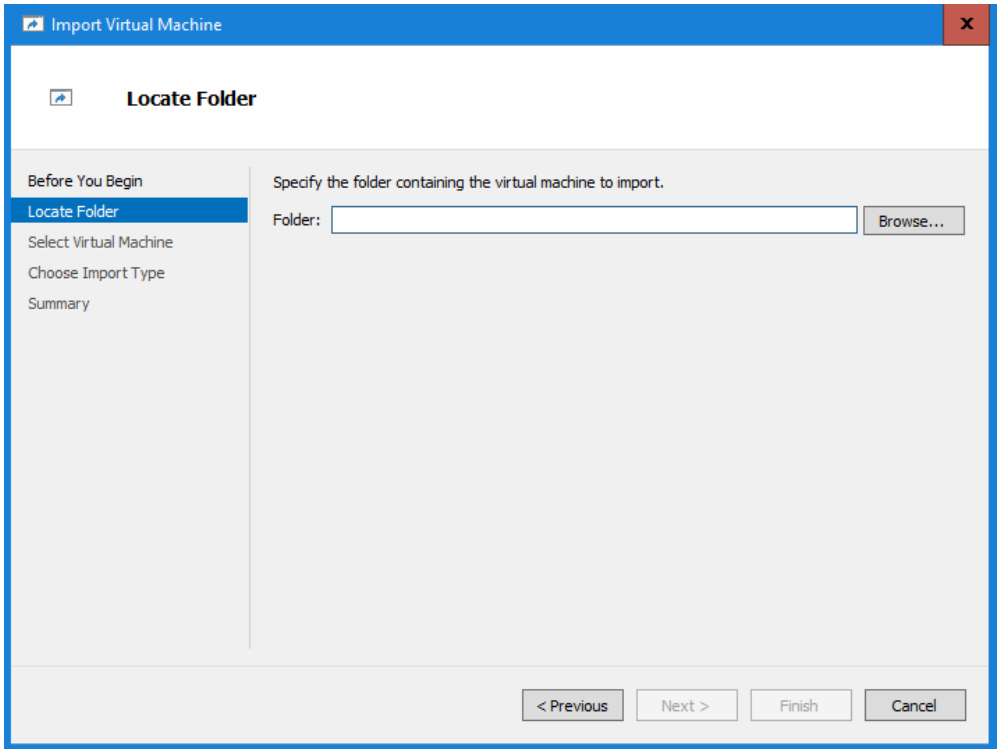
Once the restore has complete you will see a screen like this, click **[Dismiss]** to close the window.



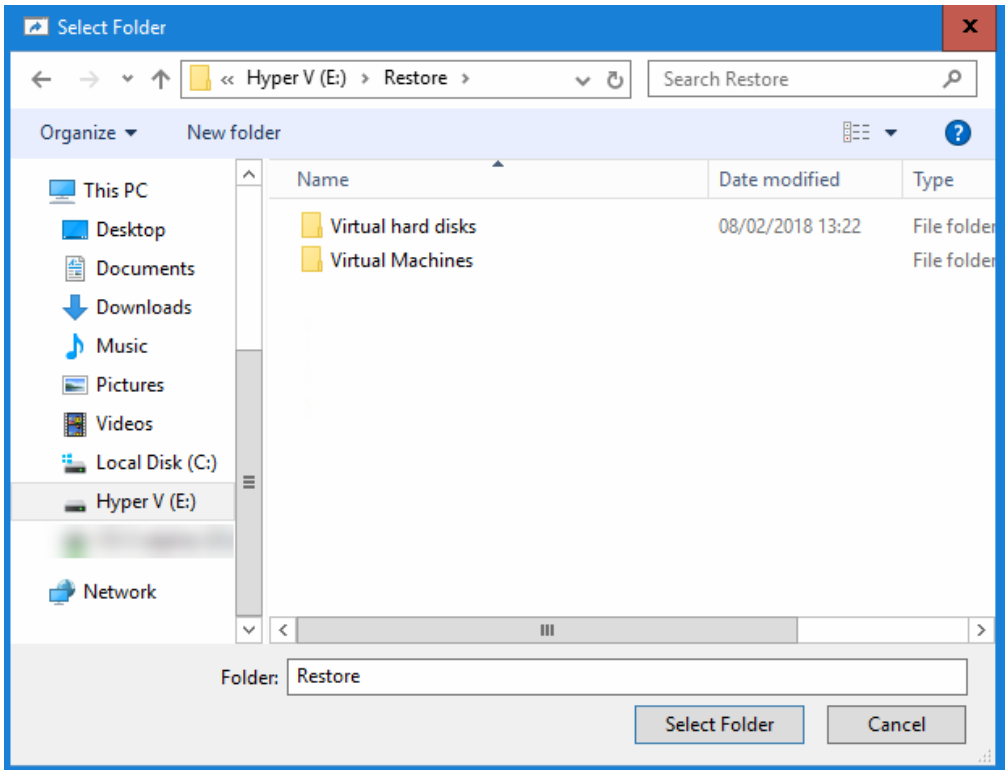
In order to start the virtual machine, open up Hyper-V Manager, now we need to start the import process, click **[Import Virtual Machine]**.



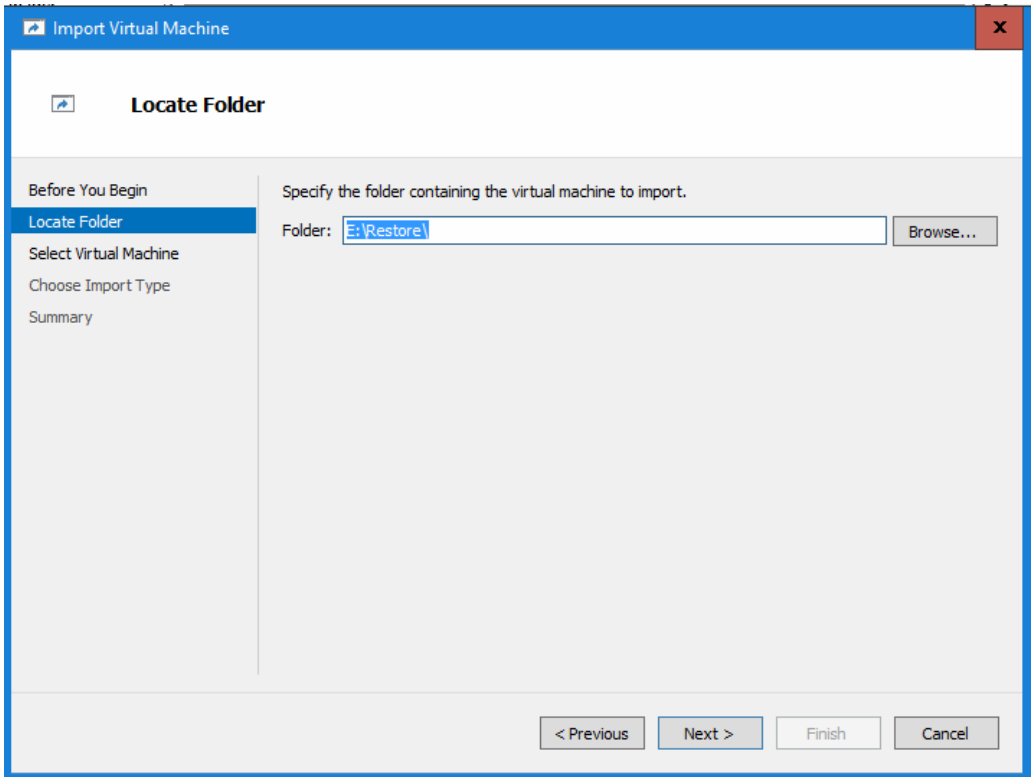
Click **[Next]** to move on to the next stage.



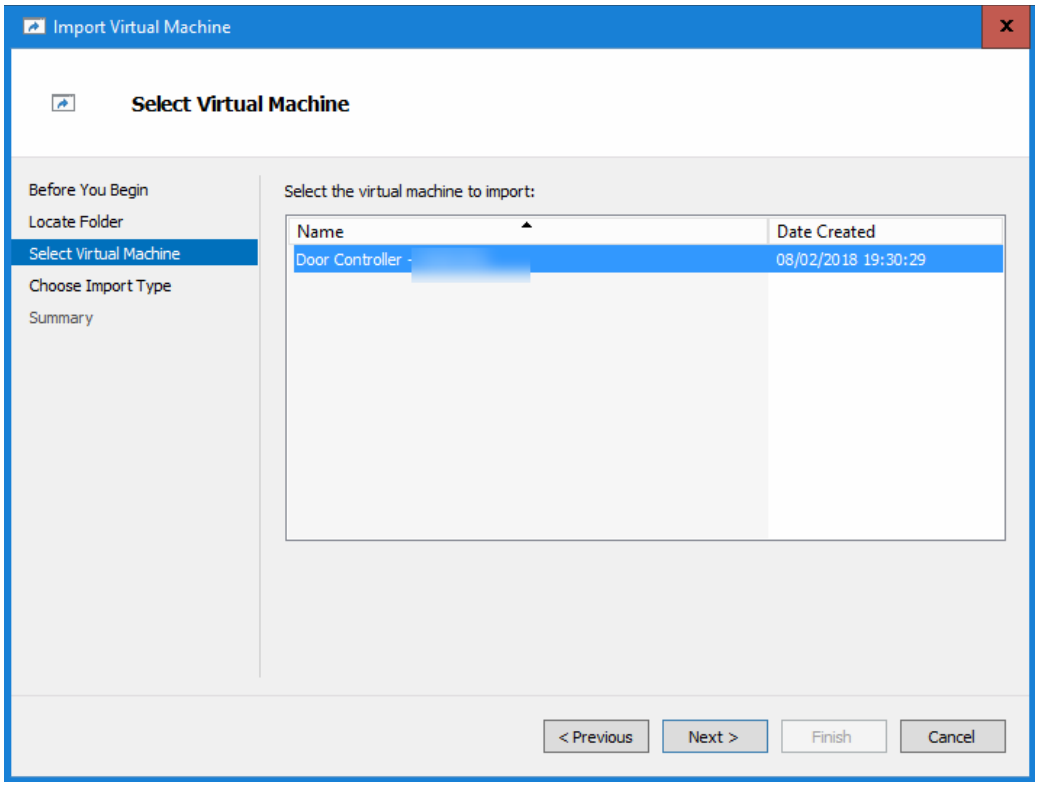
Now we need to locate the folder we just performed the restore to click **[Browse]**.



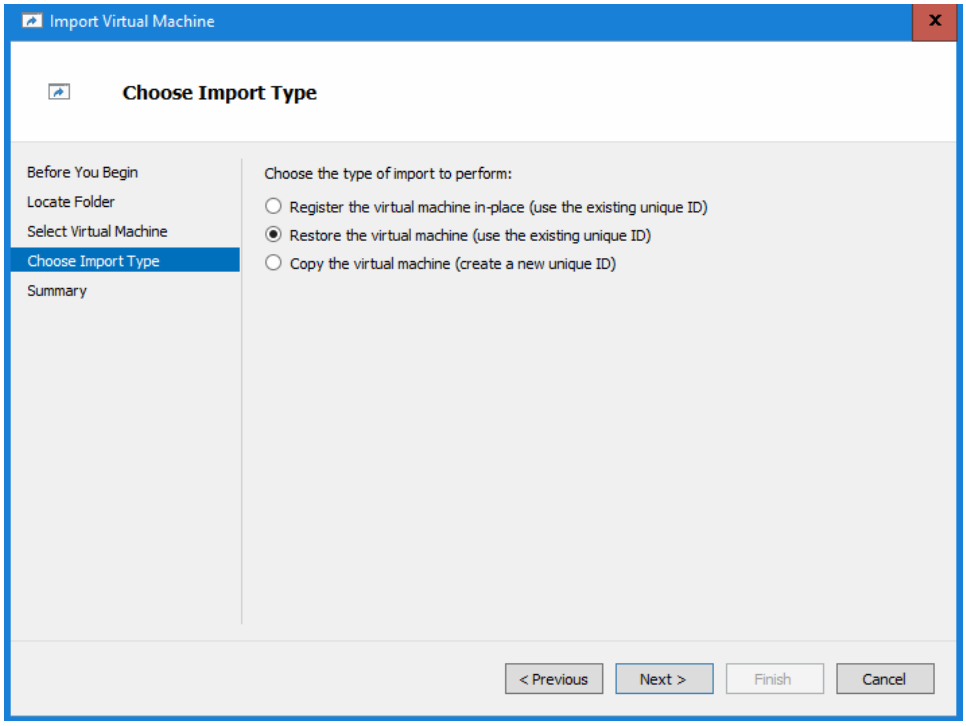
Use the explorer window to navigate to the restore folder, in our example we used *E:/Restore* now click **[Select Folder]**.



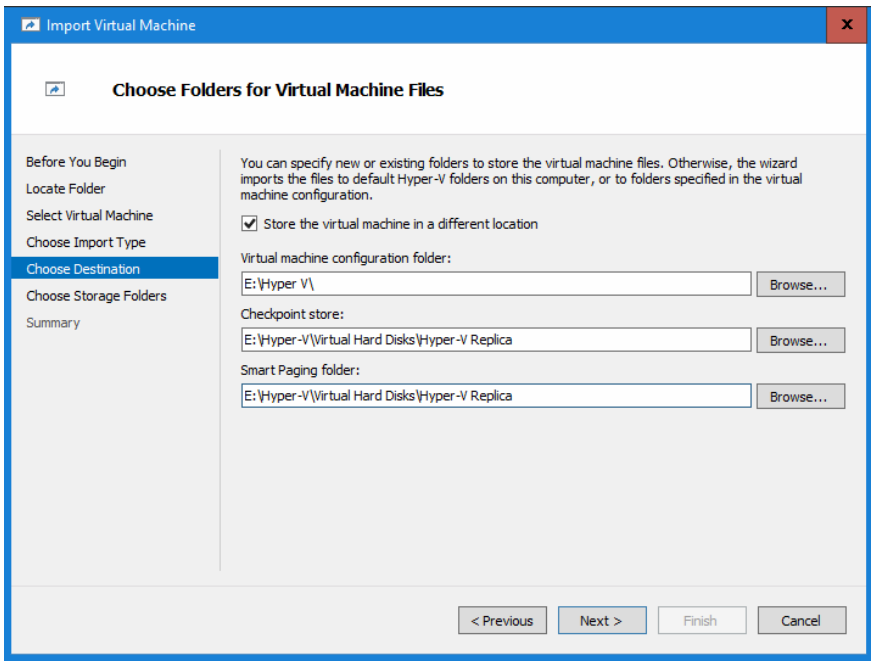
You will be taken back to the Locate Folder menu but the Folder name will now be populated with the restore path, click **[Next]**.



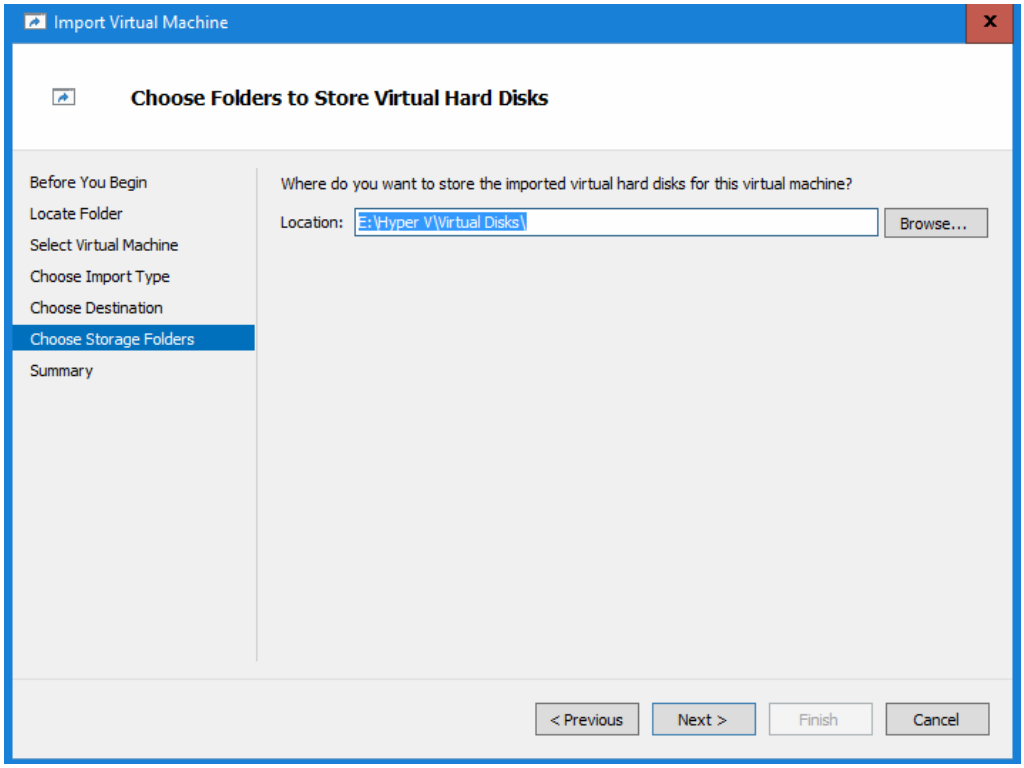
The wizard will search the Folder selected and return the name of the Virtual Machine it finds. In our example it has found a machine called *Door Controller*, Click **[Next]**.



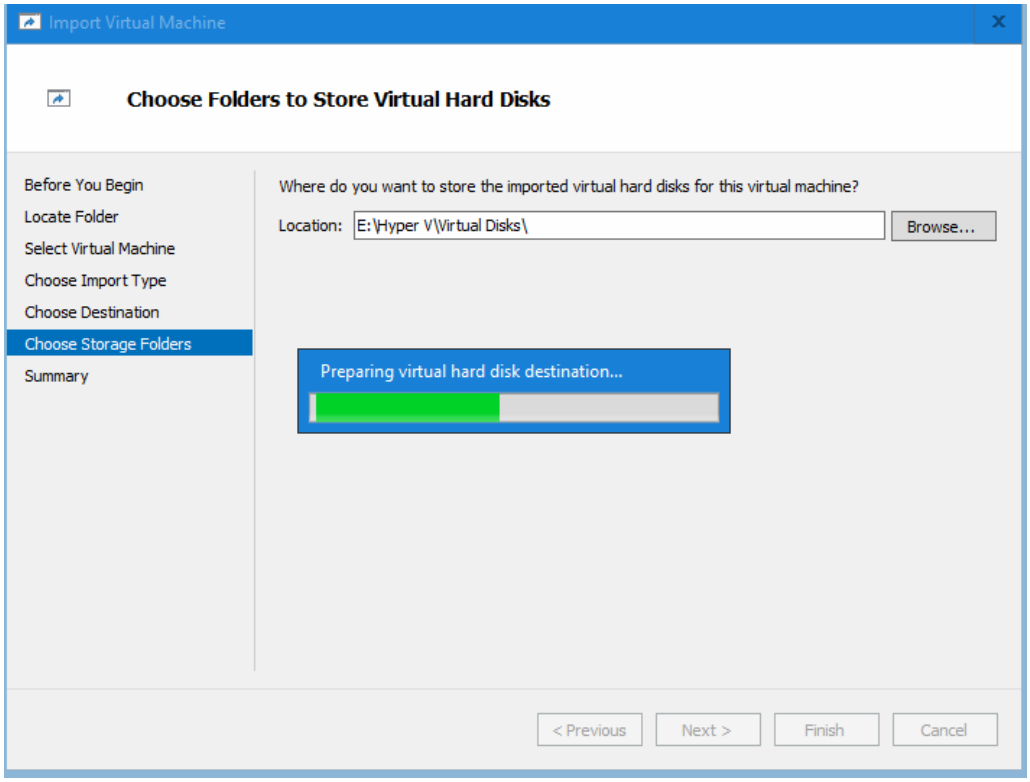
Now we need to choose the type of import. If this is a recovery of a machine to a new hypervisor then one of the first two options should be fine, if you are restoring to the same hypervisor and the previous machine is still present then the **copy** option would be the best solution, this will give you another instance of the same machine. Choose the option you need and click **[Next]** in our example this is a different hypervisor and the previous machine is gone so we will use **Restore**.



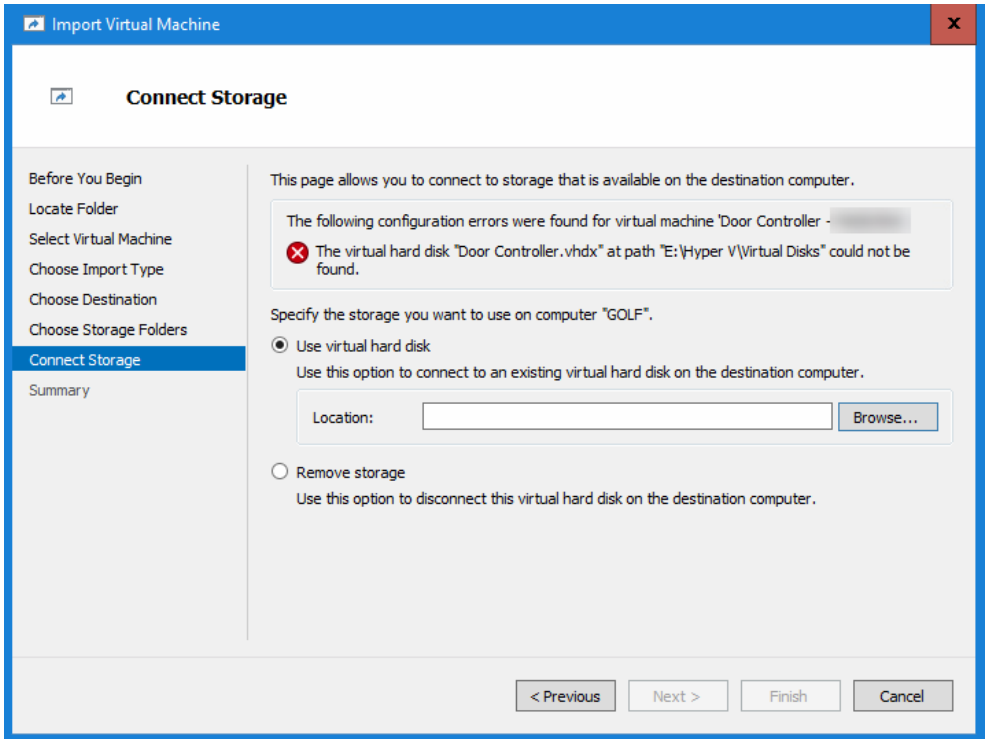
Now we need to select where you would like the recovered machine to be imported to, these settings will be prefilled for you but if they are from a different hypervisor they may be incorrect, clicking the tick box will allow you to make changes and save the import to a location that suits you. When you are finished click **[Next]**.



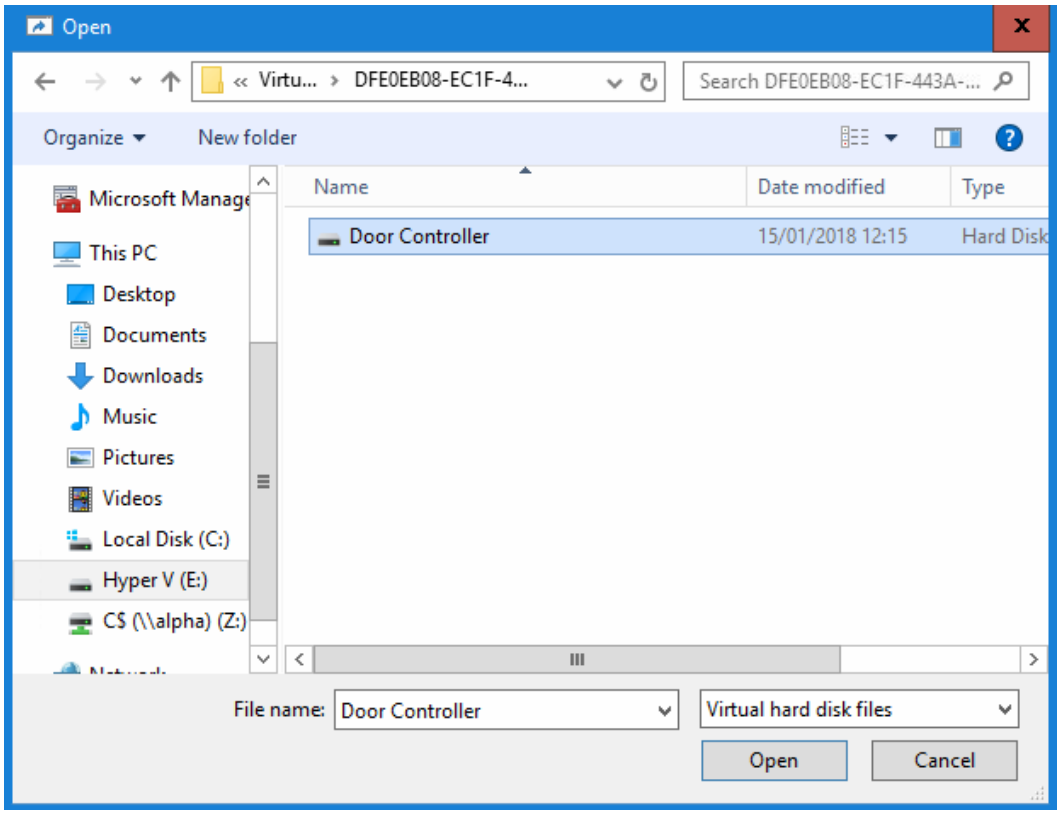
Chose the location of where you would like to import the Virtual Machine Hard drive and click **[Next]**



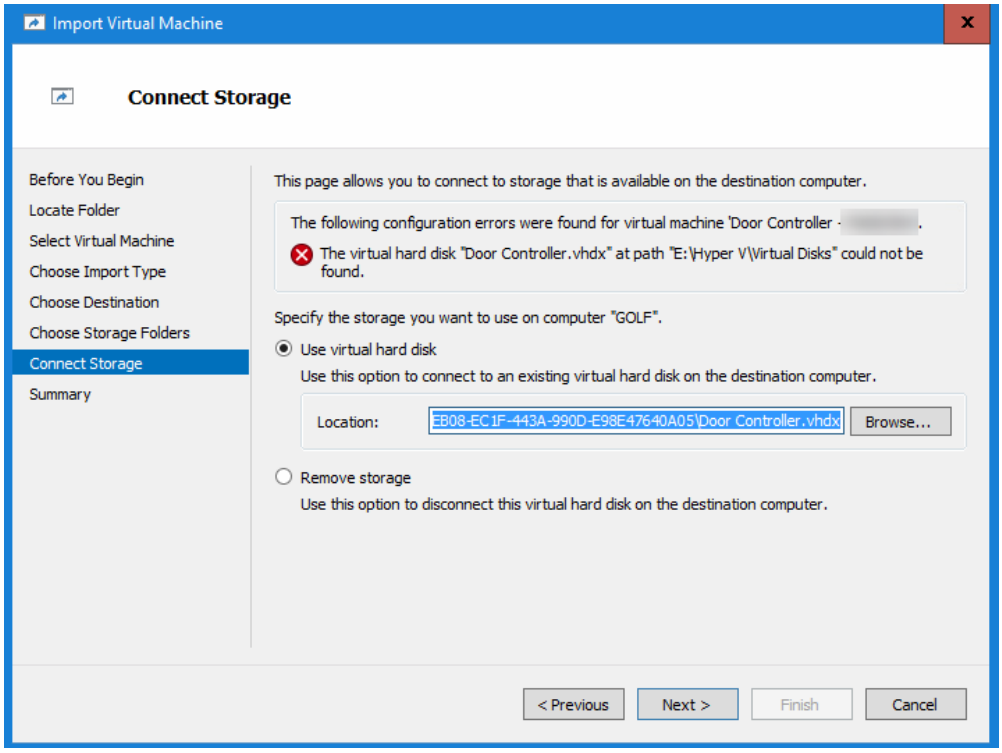
The system will now start the process of preparing the virtual hard disk destination.



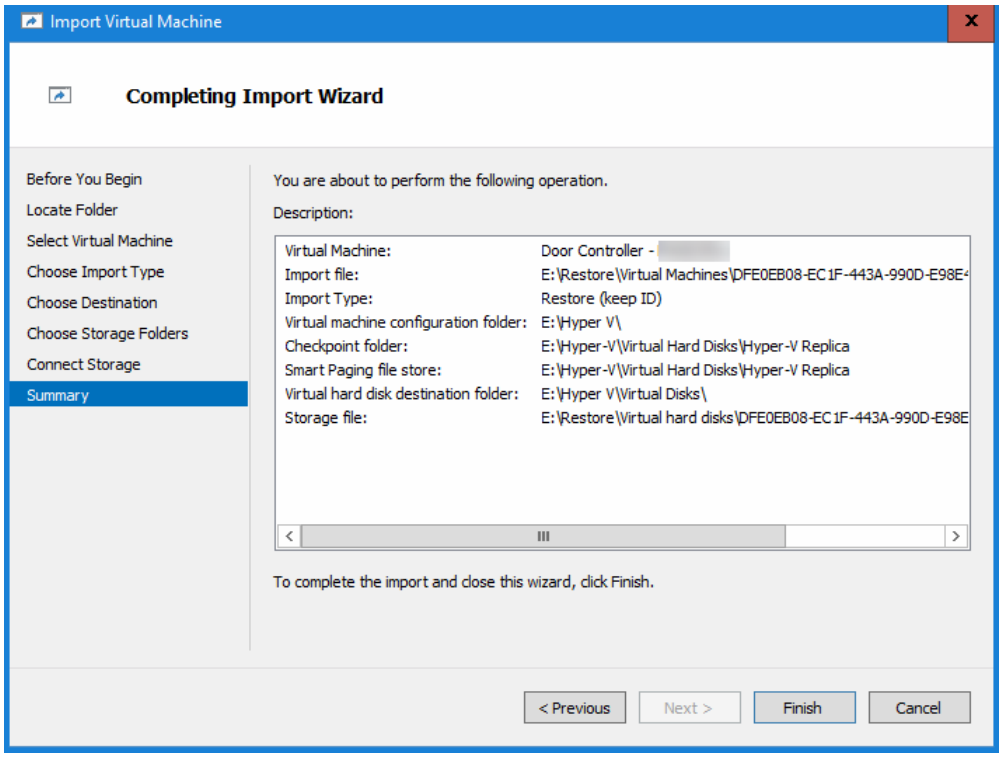
Now we need to point the wizard to the restored machines hard drive, click the **[Browse]** button



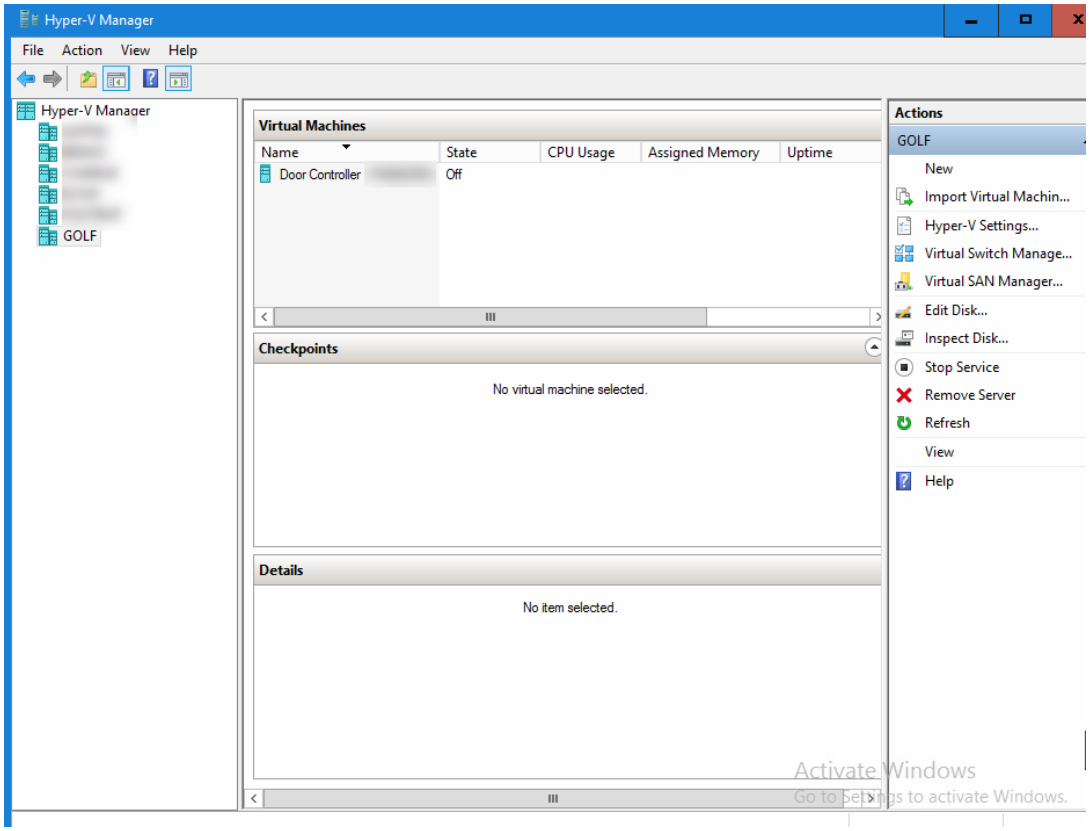
Navigate to where we restored the virtual machine and drill down into the hard drive folder until you see the hard disk file, in out example we restored the virtual machine to *E:/Restore* when you have found the hard drive file click **[Open]**.



Now click the **[Next]** button to proceed.



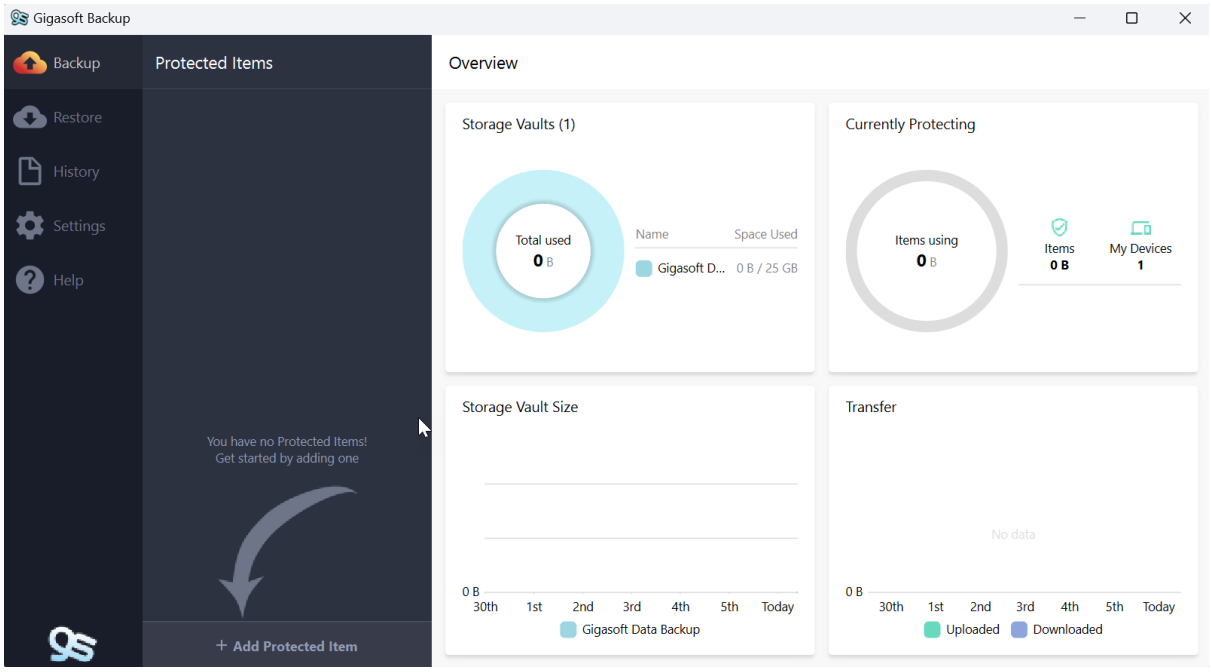
We now get a summary of the import wizard, check to make sure everything looks ok and then click the **[Finish]** button to start the import process.



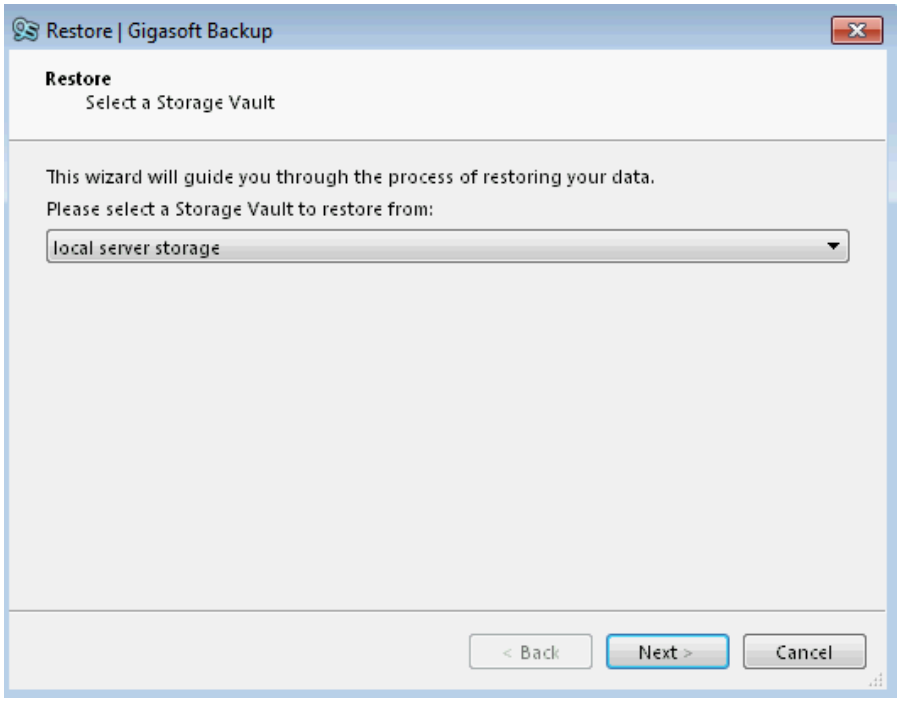
Here you can see the import has completed and the machine has been restored and left in the off state, now is the time to edit the machines settings to make any changes needed then it can be started, remember to modify the Gigasoft Backup client to back up the virtual machine in its new location.

8.4 SQL protected item

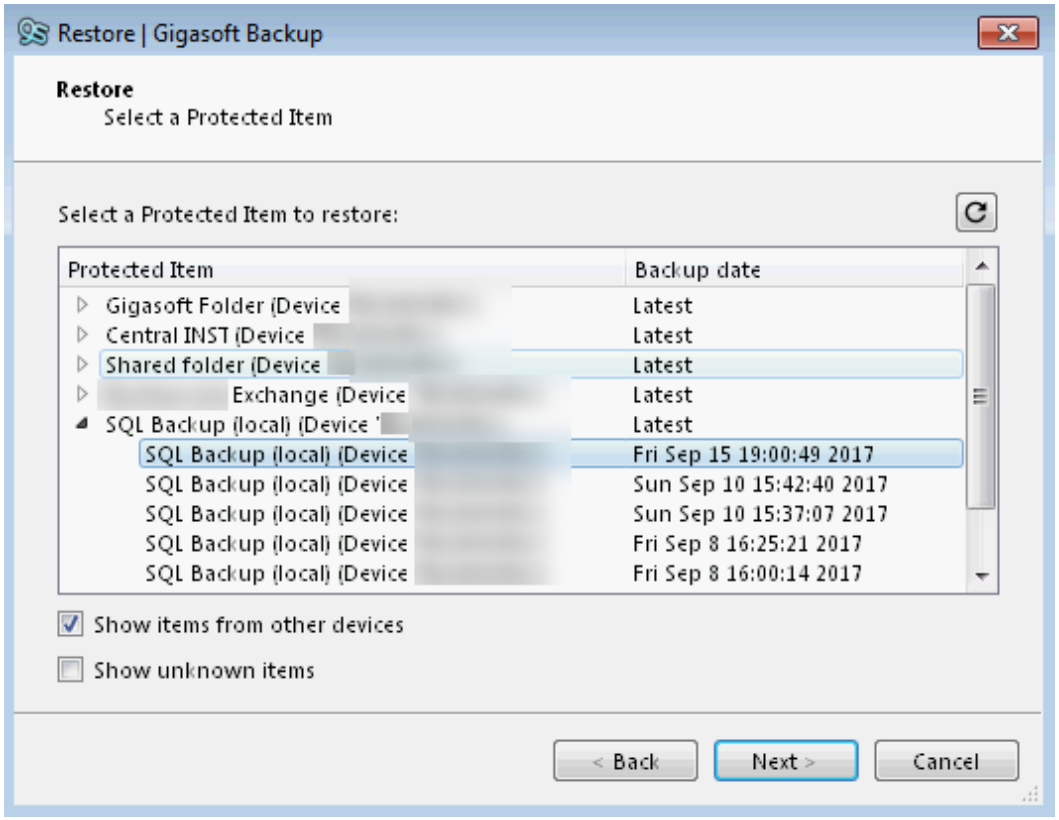
In this section we will guide you through the process of restoring a SQL backup to a new or existing SQL server, your steps may differ slightly and there maybe additional steps involved to allow your particular software to interact with the restore databases.



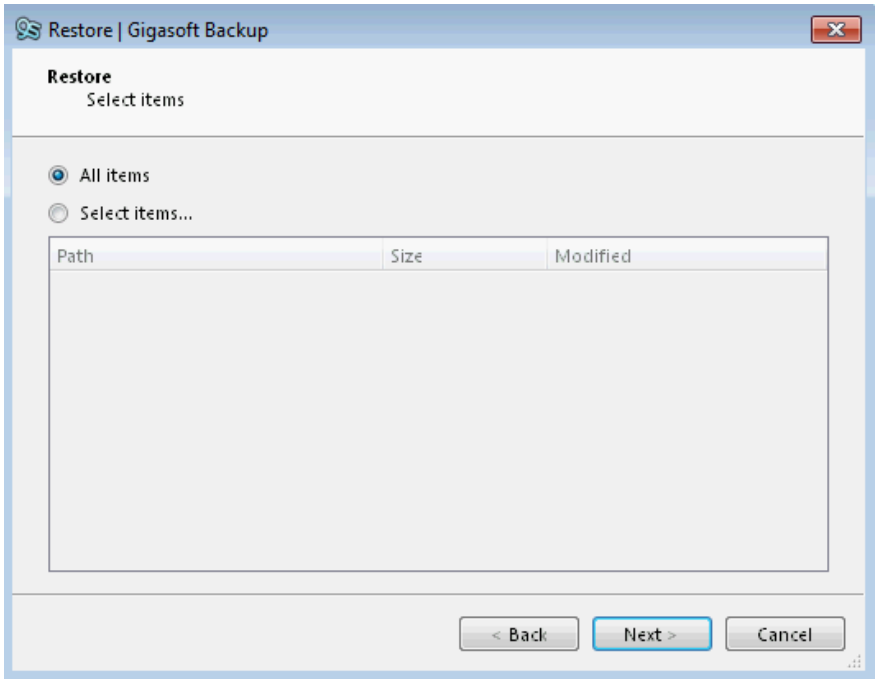
Log in to the Gigasoft Backup Manager Client.



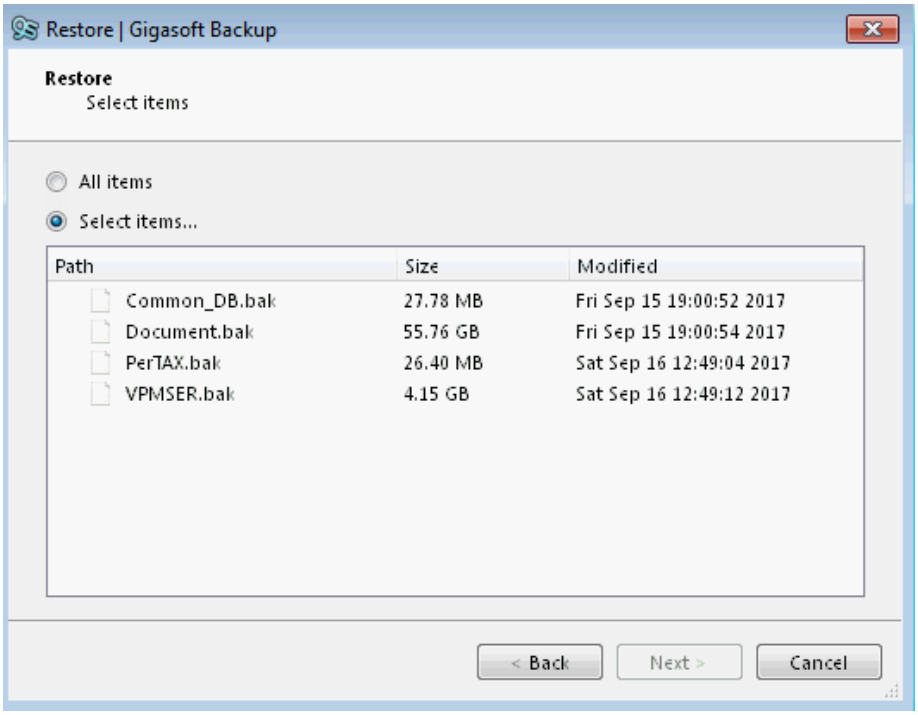
Select the **[Restore]** tab and then choose the location of the protected item, in this example the databases were stored on a local disk, click **[Next]** to continue.



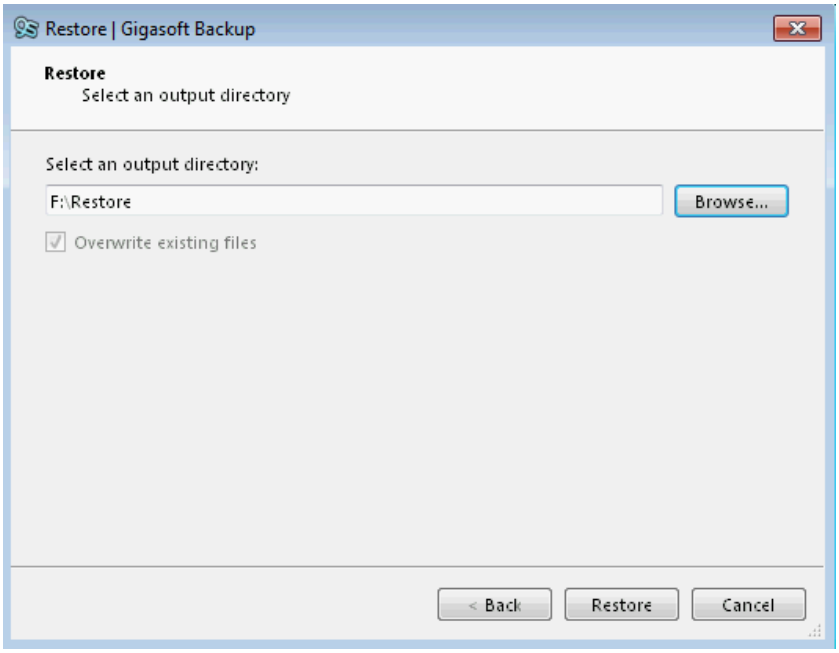
Select the **[Show items from other devices]** radio button and then drill down into the SQL protected item for the point in time you wish to restore, in this example we wish to restore the databases from September 15th, click the **[Next]** button to proceed.



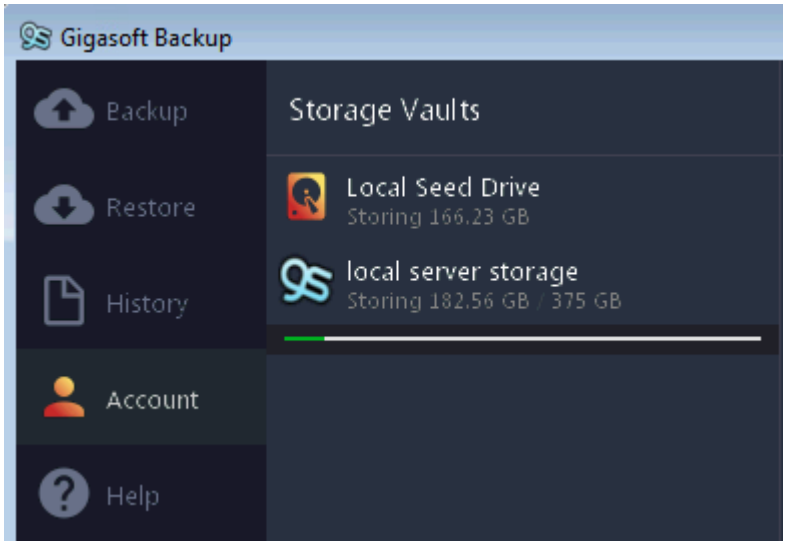
By default, the system selects the option to restore all the data from that protected item for that job.



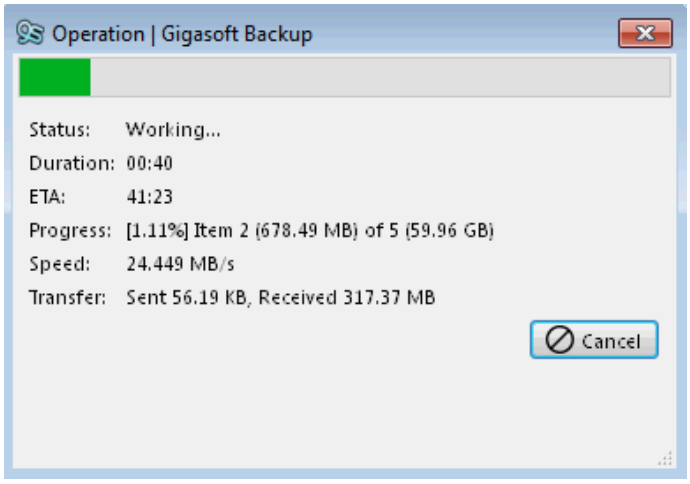
by clicking **[Selected Items]** you can choose the individual databases if you need to, in our example we will leave the default selected and then click **[Next]** to restore all the databases from that date.



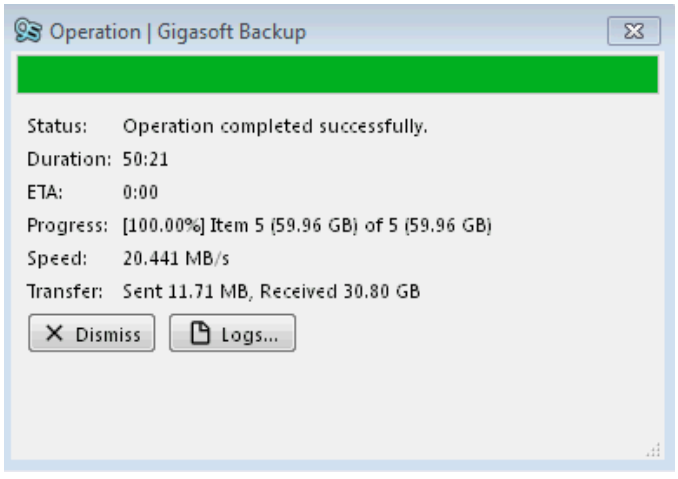
On the next screen we need to select the restore location, click on the **[Browse]** button to open an explorer window so you can choose where you wish to restore the data, it is advisable to restore the data to a different location to the current data so that you can compare the files if needed. Once you have selected a suitable restore location click the **[Restore]** button to start the restore process.



The restore process will start and you will see a green progress bar slowly move up as the data is restored.

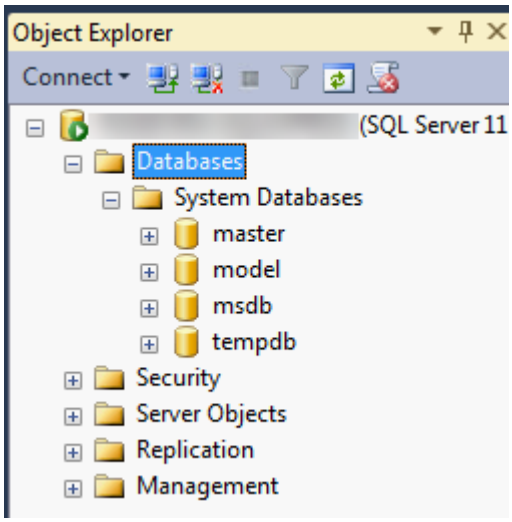


If you click on the green progress bar a more detailed restore window will open.

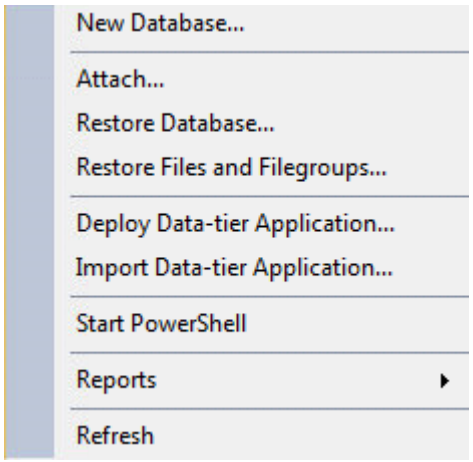


Once the restore has completed click on **[Dismiss]** and then we can move on to importing the databases back in to SQL Server.

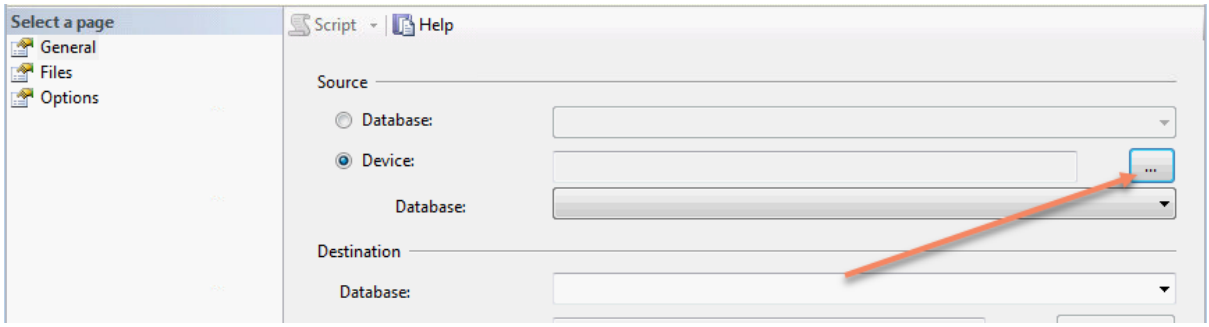
Open SQL Studio Manager and login using the necessary credentials.



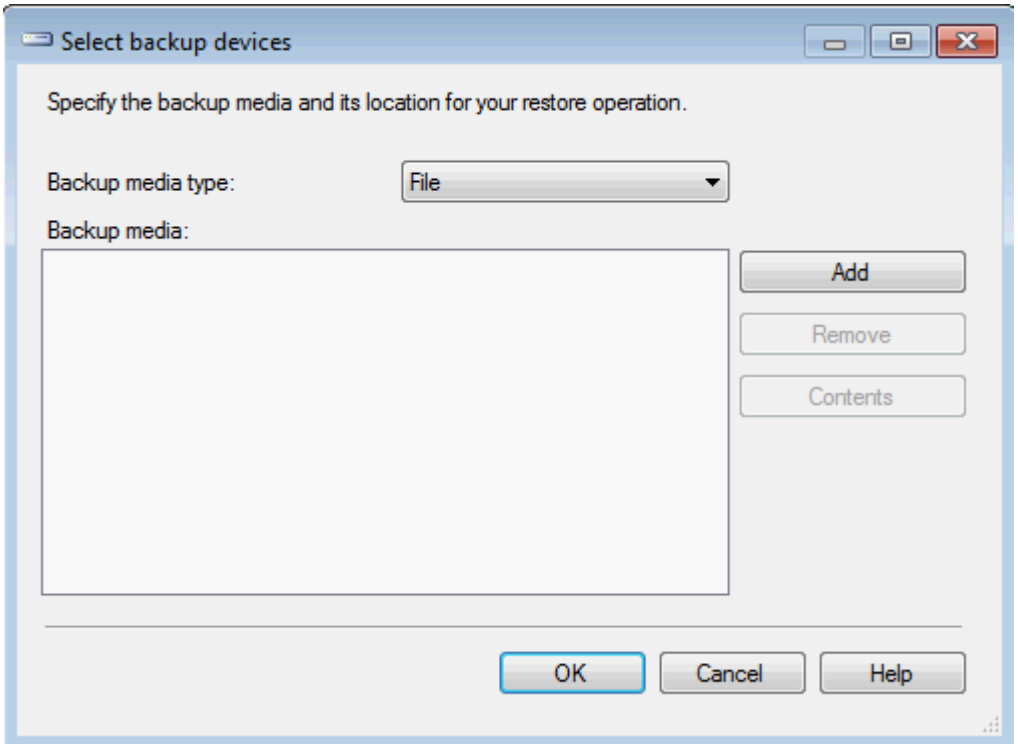
Expand the server name at the top left of the Object Explorer window and then right click on the **[Databases]** option.



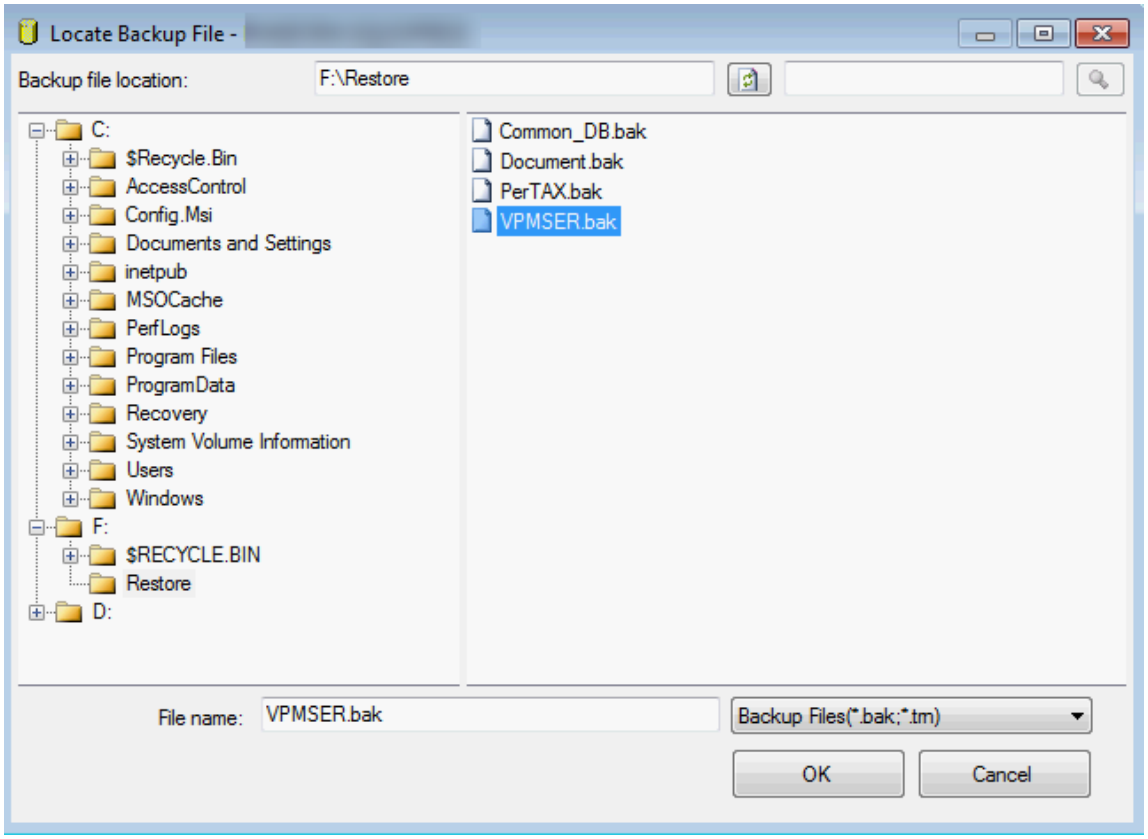
Chose the **[Restore Database…]** option.



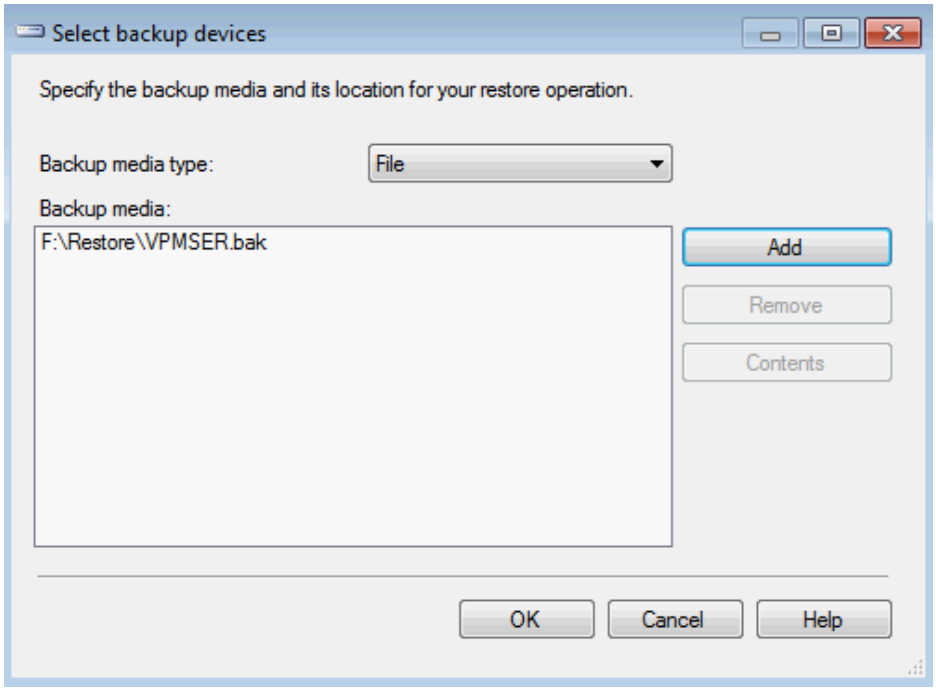
On the restore page select the **[Device]** radio button and then click on the **[…]** button (arrowed)



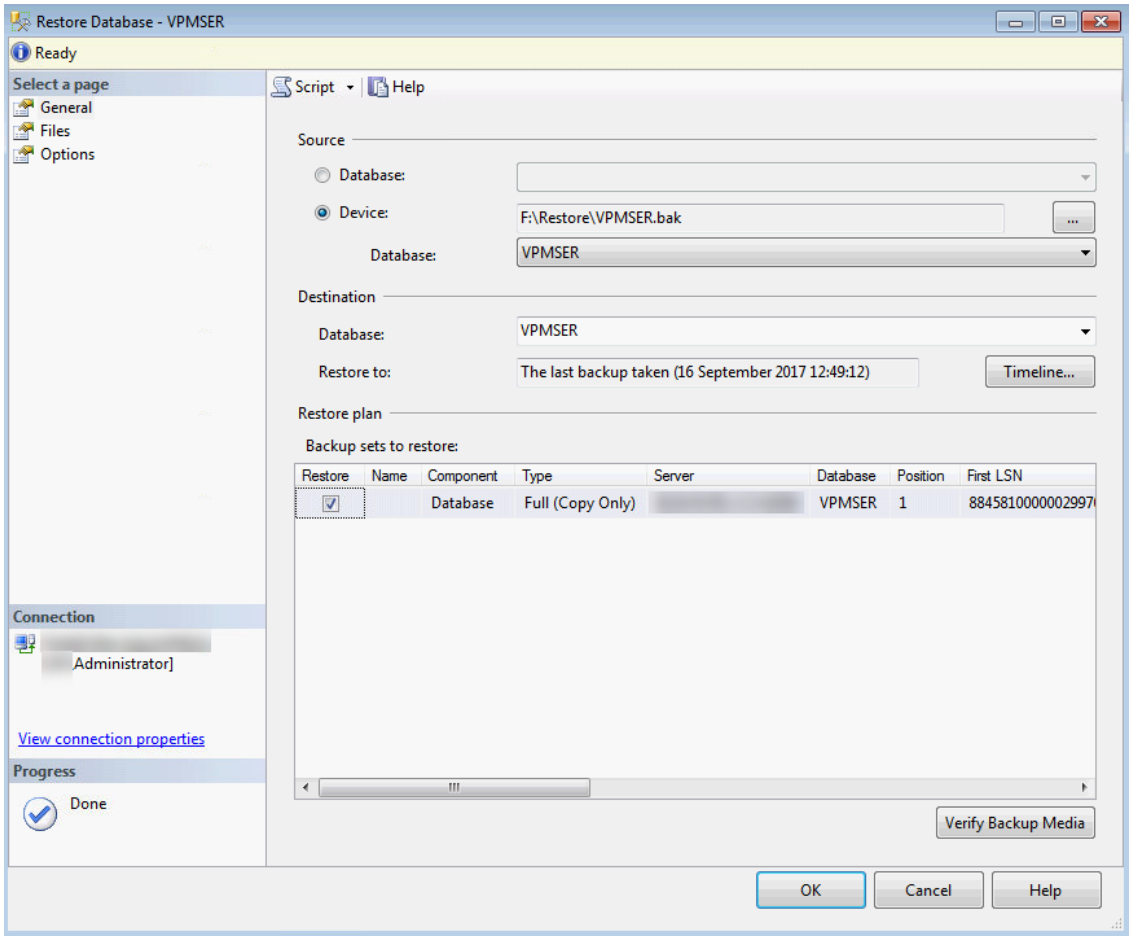
Click the **[Add]** button.



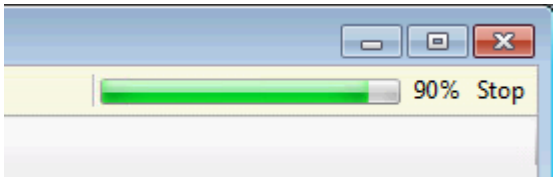
Use the explorer window to navigate to the restore location you created earlier, select one of the databases you need to restore and click **[OK]** in this example we have selected the ***VPMSER.bak*** database



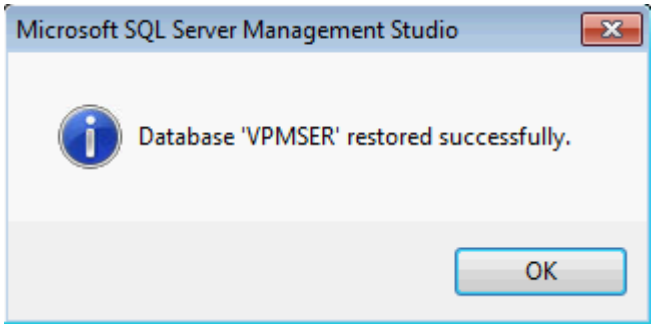
At this point you can click **[Add]** to add more databases or just click **[OK]** to restore just the one.



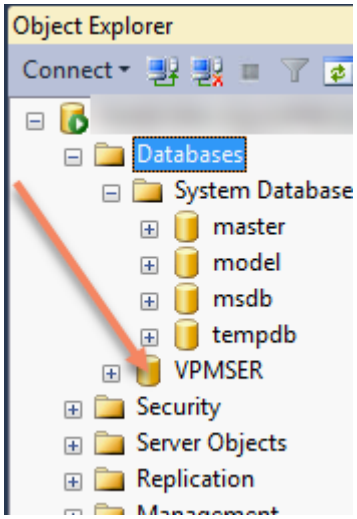
Check the settings are correct and click **[OK]** to start the restore / import process.



In the top right of the screen there will be a green progress bar indicating the restore progress



Once the restore completes you will be given a new window indicating if the restore completed successfully or if it errored, click **[OK]**

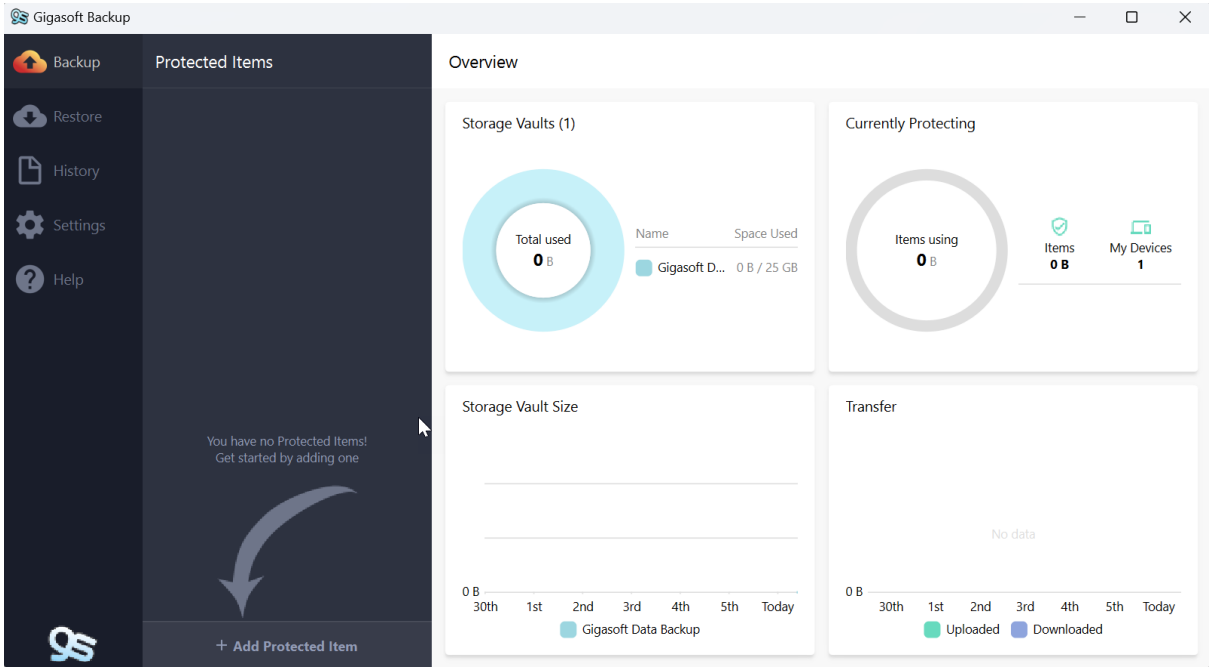


In the Object Explorer window, you can now see the database has been restored back into SQL Server and is ready for any additional steps that you may need to allow your software to communicate with it.

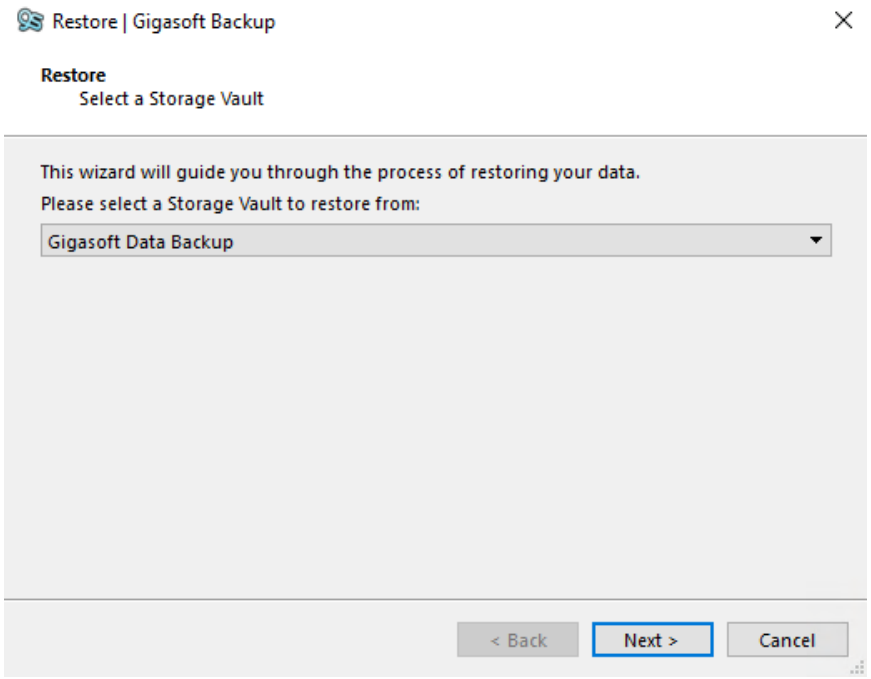
8.5 MySQL protected item

8.5.1 Windows

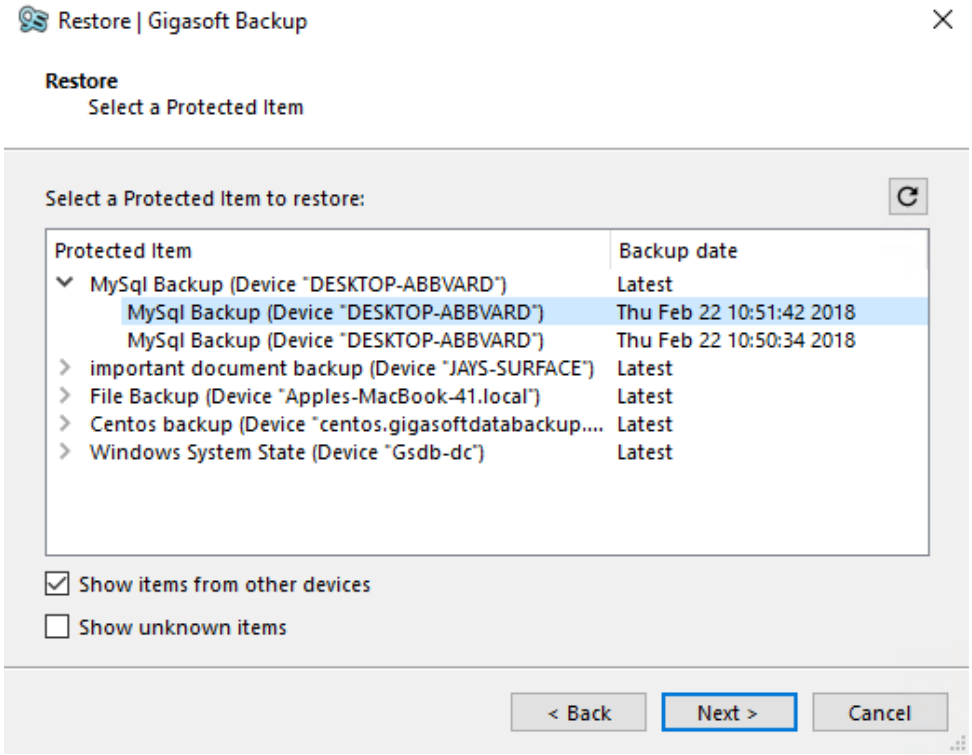
In this section we will guide you through the process of restoring a MySQL backup to a new or existing MySQL server, your steps may differ slightly and there maybe additional steps involved to allow your particular software to interact with the restore databases.



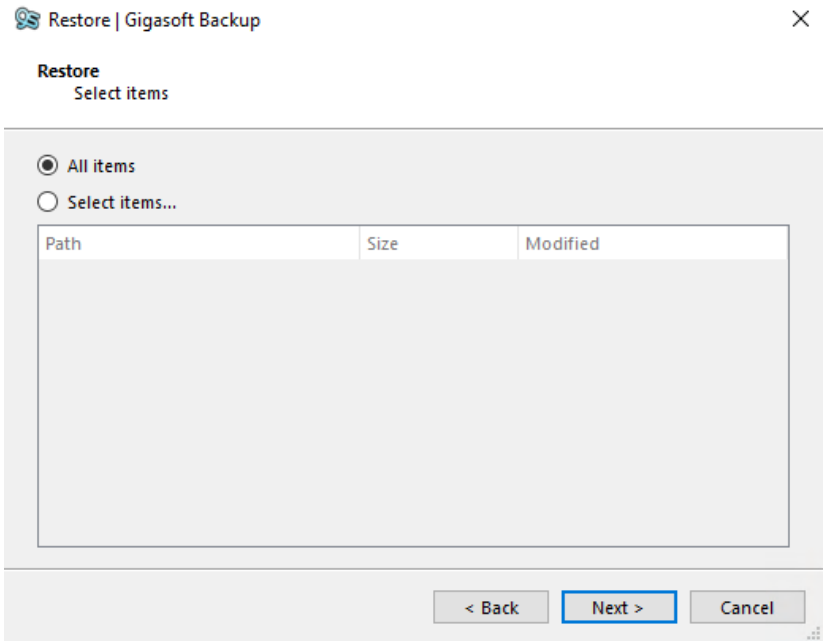
Log into the client software



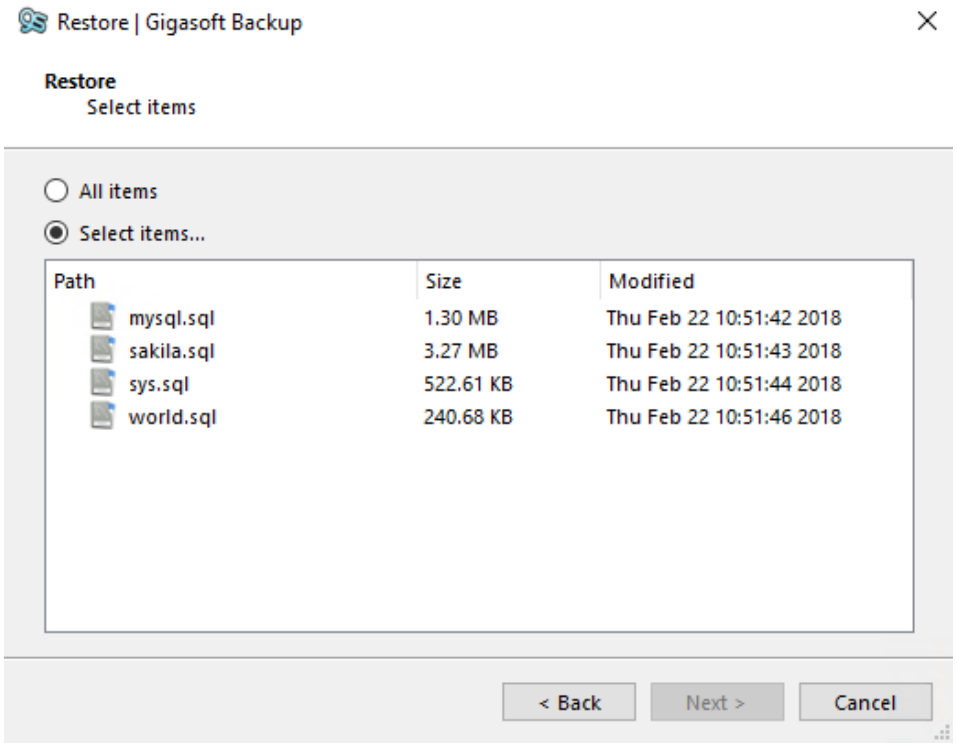
Select the **[Restore]** tab and then select the storage vault this protected item used, in this example we are using the **[Gigasoft Data Backup]** storage vault, click **[Next]** to continue.



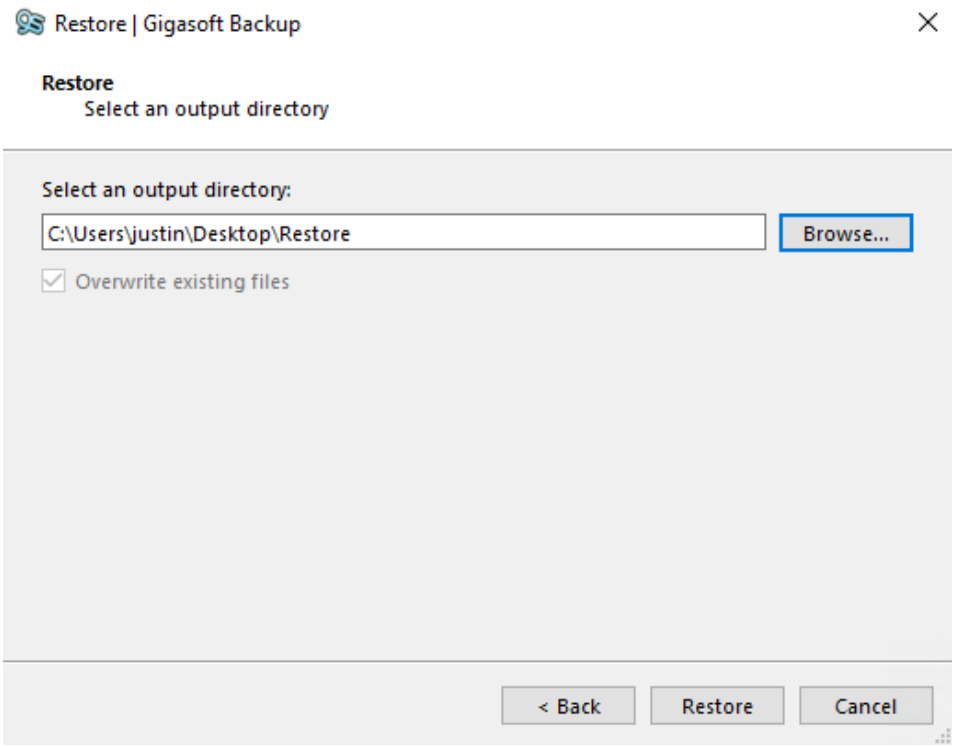
If this is a different server to where the backup was taken you will need to select the **[Show items from other devices]** tick box to show the protected items from the other devices, drill down into the protected items to find the point in time you wish to restore to, in this example we are selecting the **[Thursday 22nd]** job, click **[Next]**.



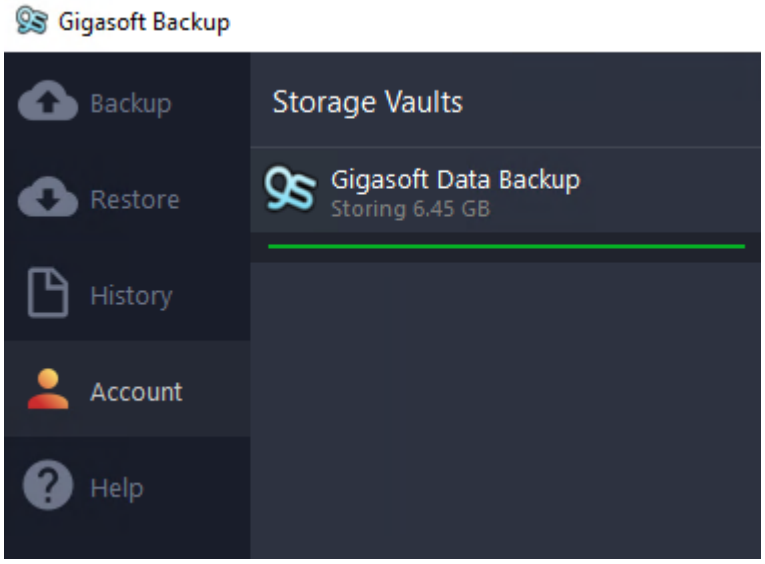
By default, the client selects to restore all items, if you only need to restore selected data from this job select the **[Selected Items]** radio button



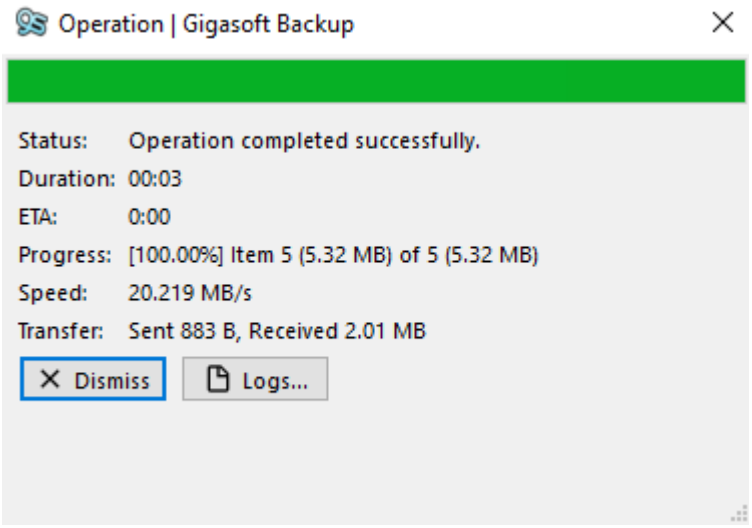
Choose the database(s) you wish to restore and click **[Next]** in our example we are going to leave the default of all items and click **[Next]**.



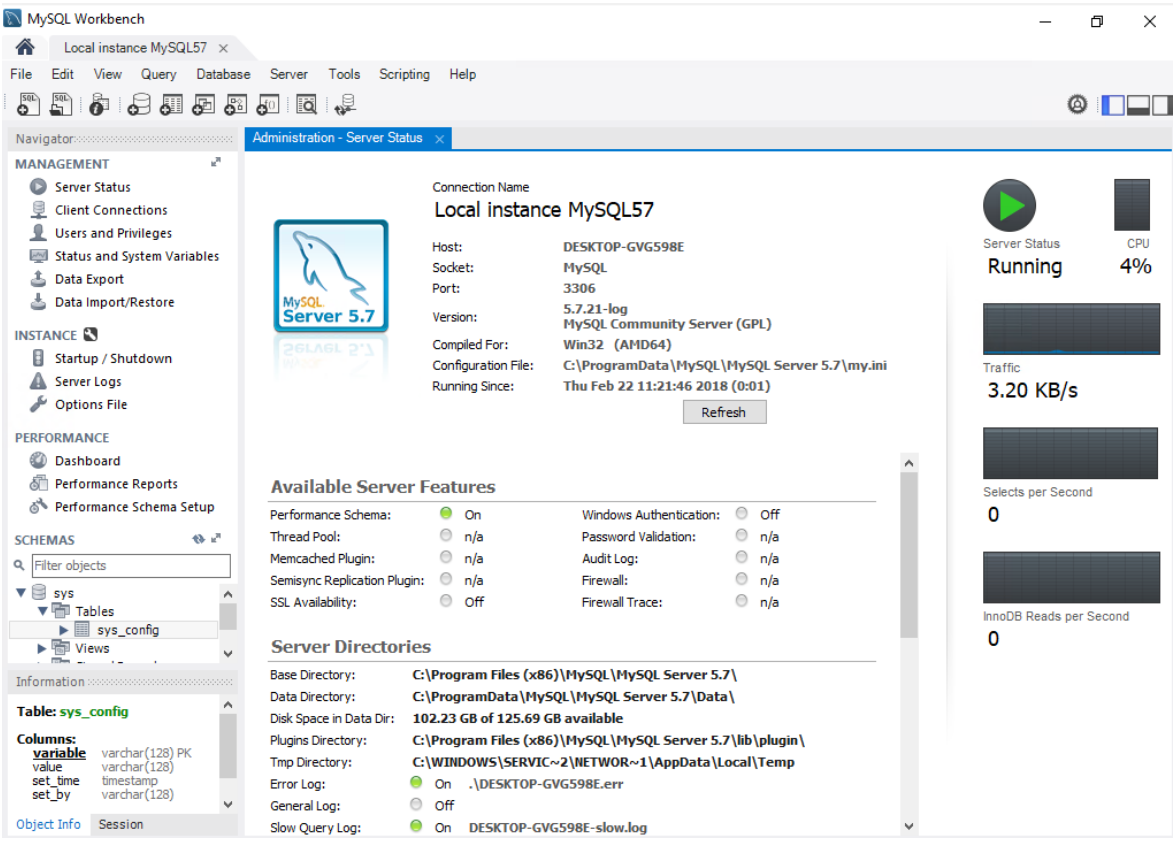
Click on the **[Browse]** button to browse to choose where to restore this data, it is recommended that the data is restored to a different location to where it is backed up from so you can compare the files if needed, once you have selected a suitable location click the **[Restore]** button to start the restore process.



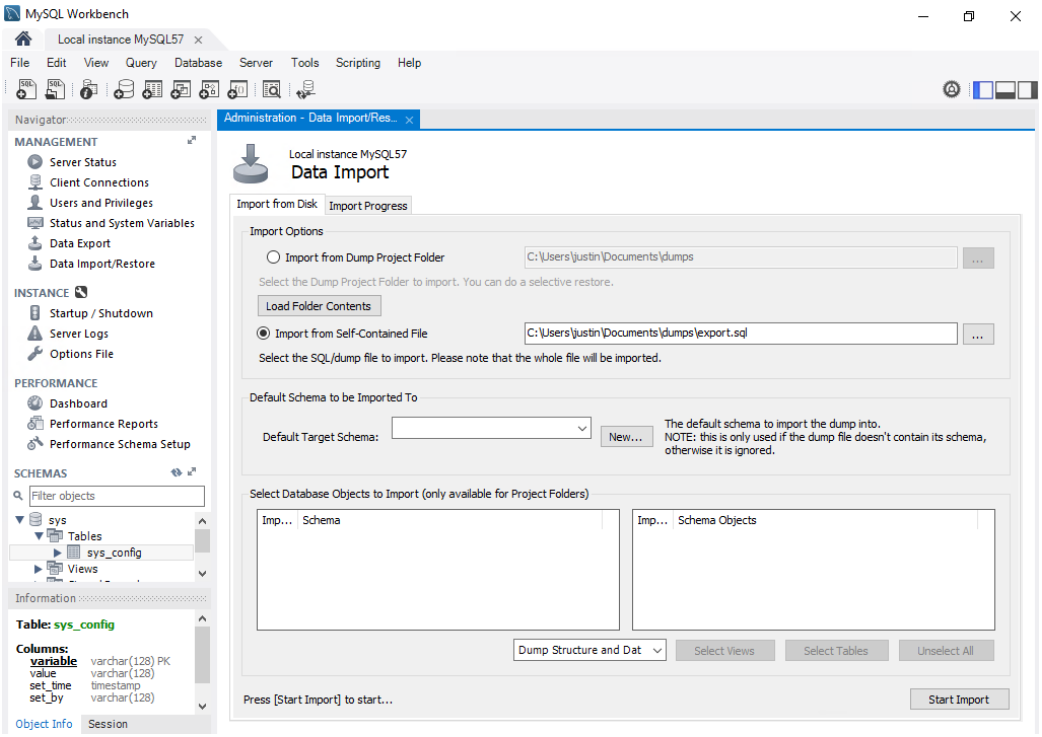
The restore process will start and you will see a green progress bar, this will slowly increase as the databases are restored, you can click on the green progress bar to open a more detailed restore window if you wish.



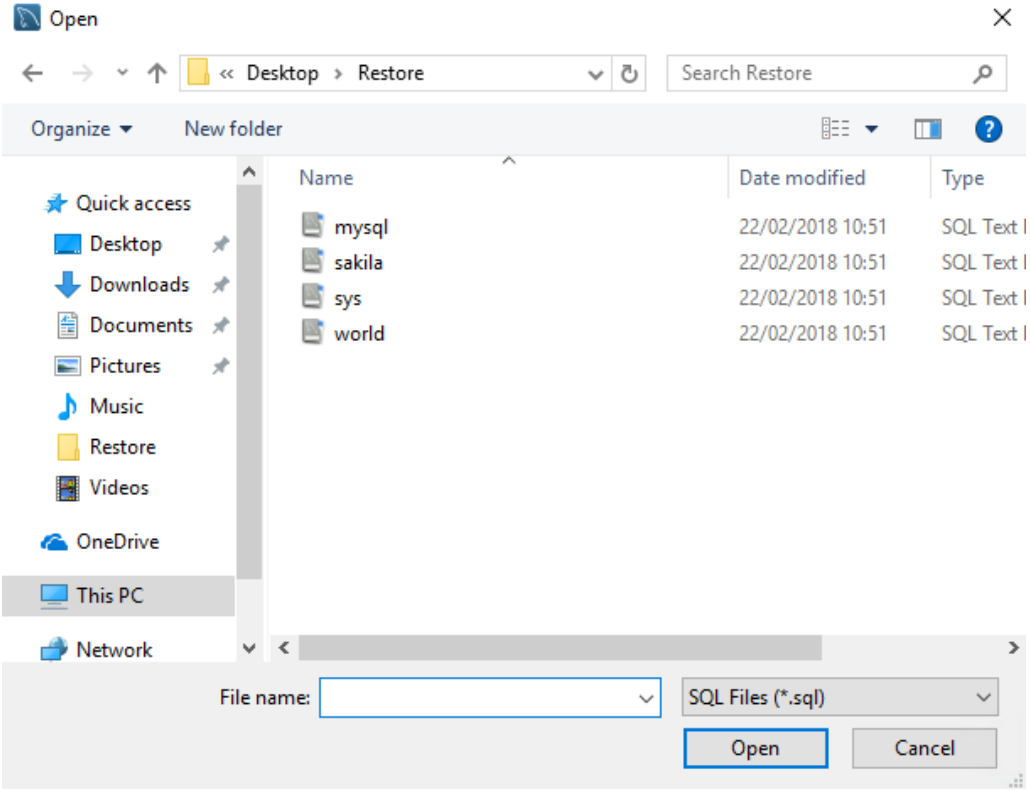
Once the backup process has finished click the **[Dismiss]** button to move on to the next stage.



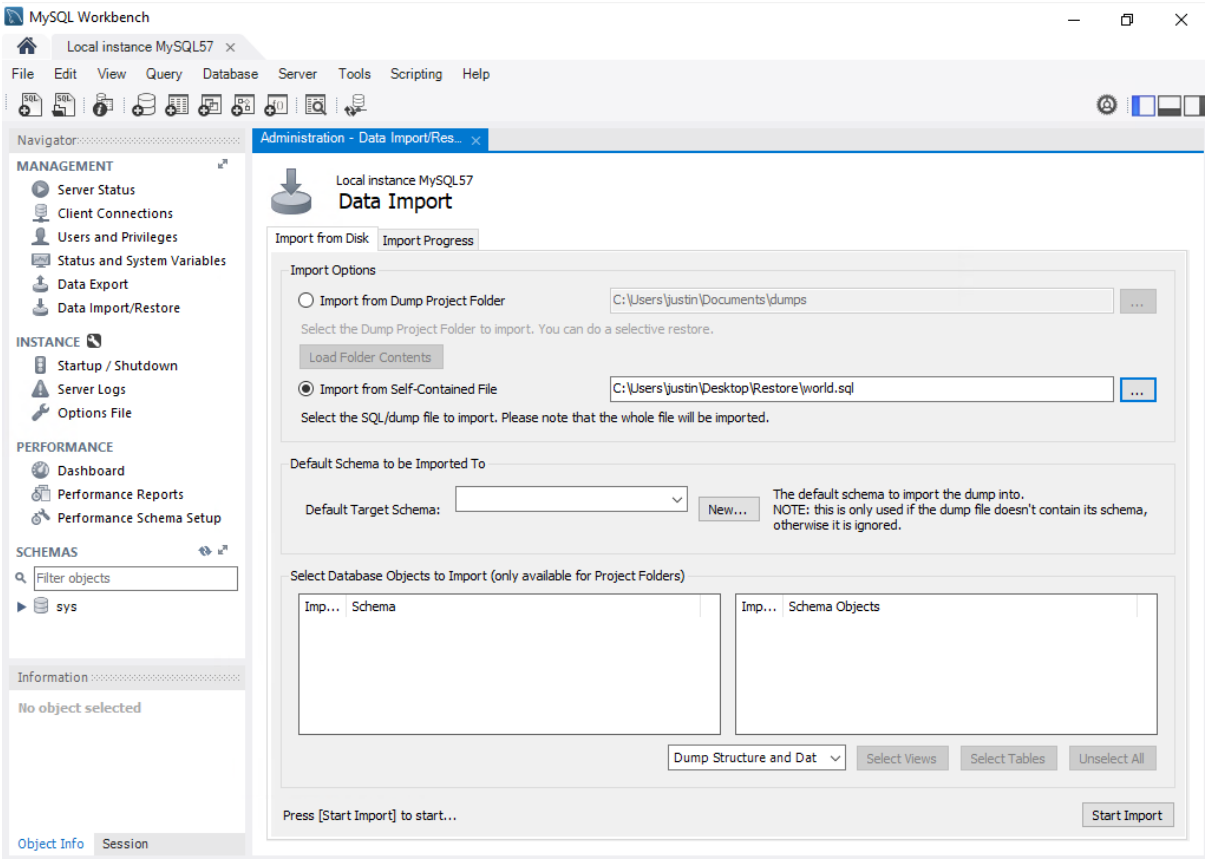
Now we need to restore the databases back into MySQL Server, to do this open MySQL Workbench and login to the current instance.



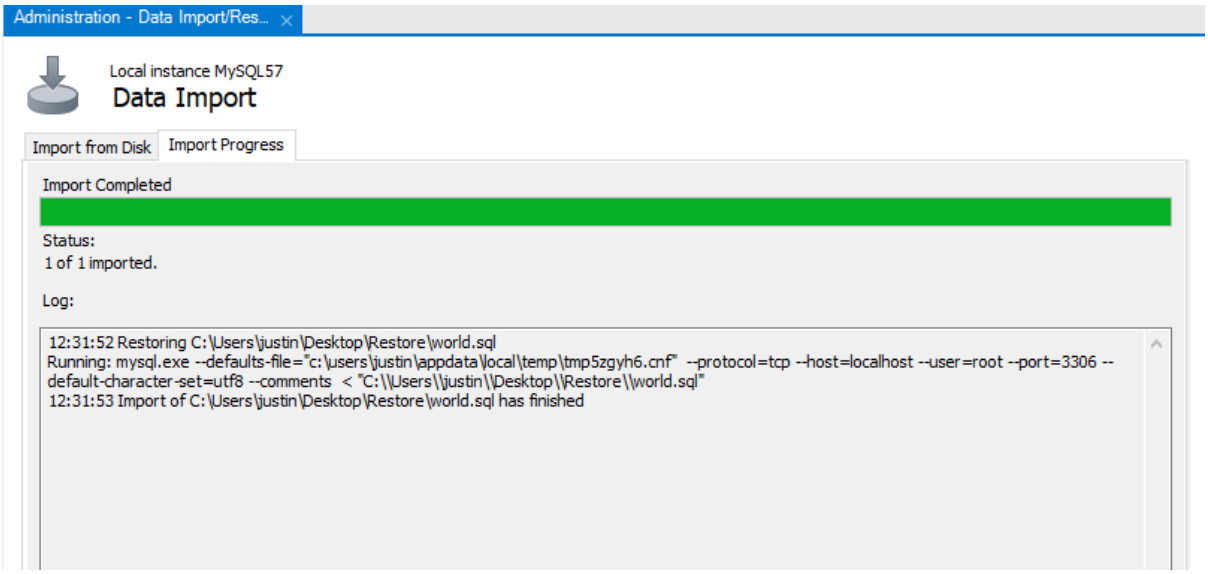
Click on the option **[Data import/Restore]**, now select the **[Import from self-contained file]** radio button and then click on the **[…]** button



Navigate to the restore location you created earlier and select a database you wish to restore, Click **[Open].**



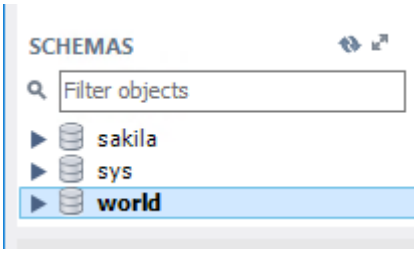
Now click **[Start Import]** button to start the Import process



The database will now begin the import process, keep an eye on the status to look if there are any errors,

One the import has completed press the refresh icon in the Schemas section down in the bottom left of the MySQL Workbench window

You should now see the database you just restored.



If you have any further databases repeat the last few steps to import the remaining ones remembering to refresh the Schemas section to make sure they have imported.
There may be further steps required to allow your software to communicate with the restored databases.

8.5.2 MacOS

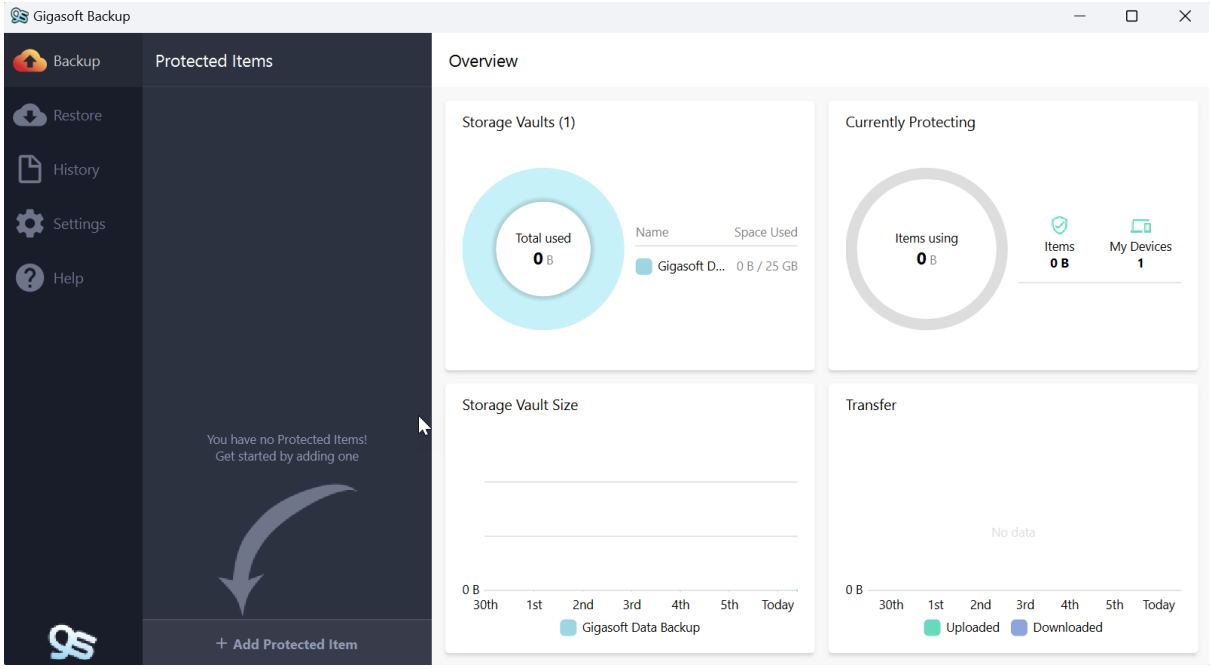
The restore process is almost identical to the Windows version, please follow these steps and let us know if you have any problems.

8.5.3 Linux (command line)

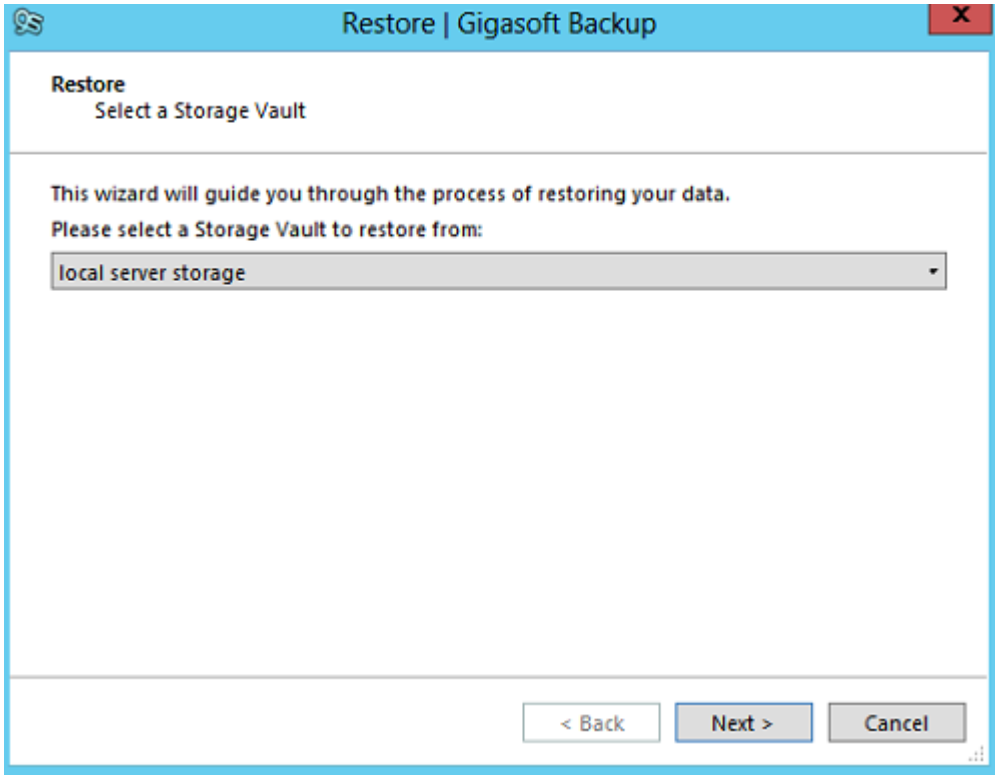
Currently the easiest method is to restore via a GUI enabled client and then copy the data over to the Linux box and import using the command line options. Once the customer portal becomes available you will be able to remotely restore the data to the Linux box.

8.6 Windows server system state

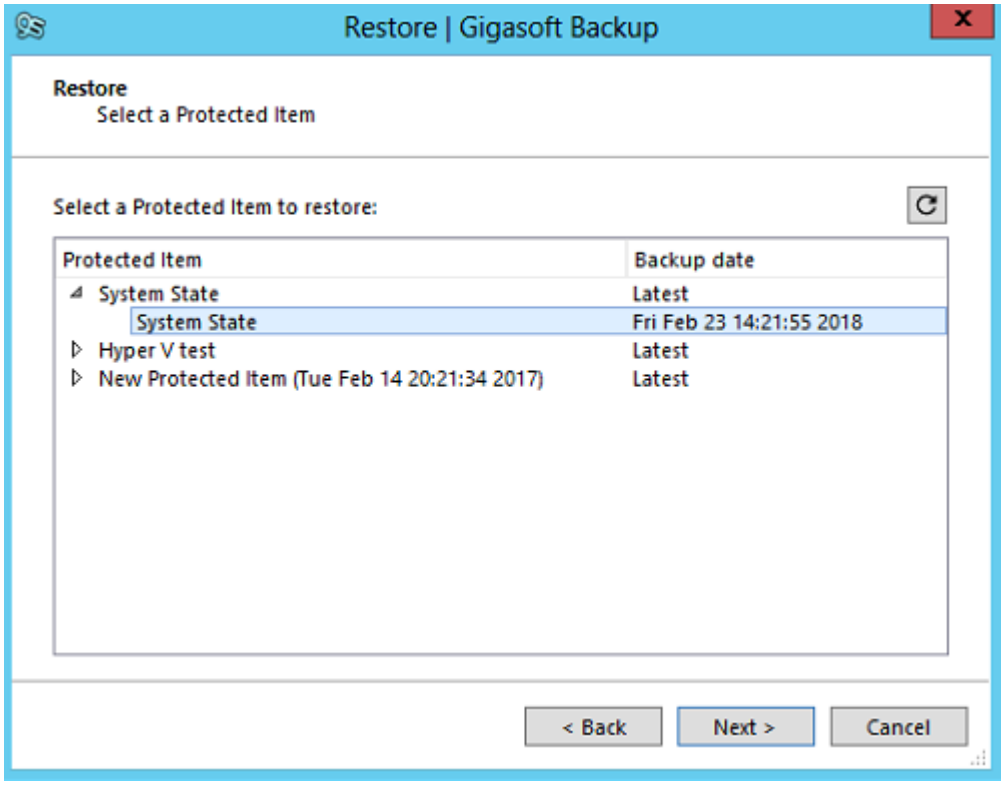
This section of the guide will help guide you through the process of restoring a System State backup, this backup can only be restored to the same instance it was taken from, this is not suitable for a new server install.



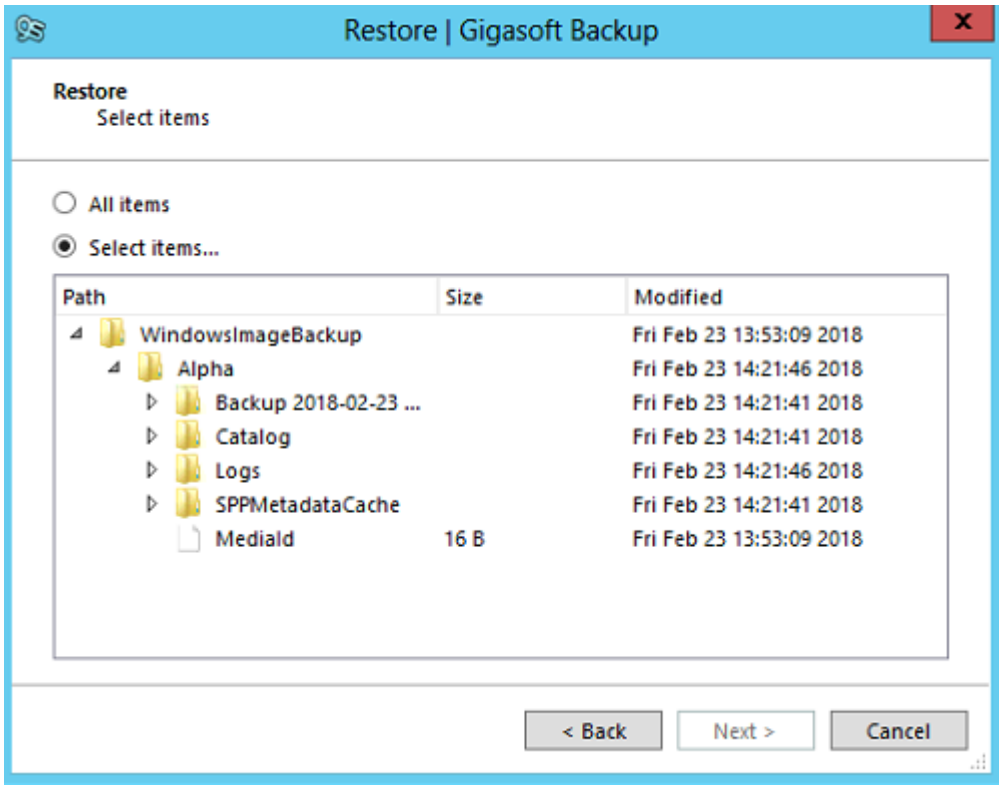
Log in to the Gigasoft Backup Manager client.



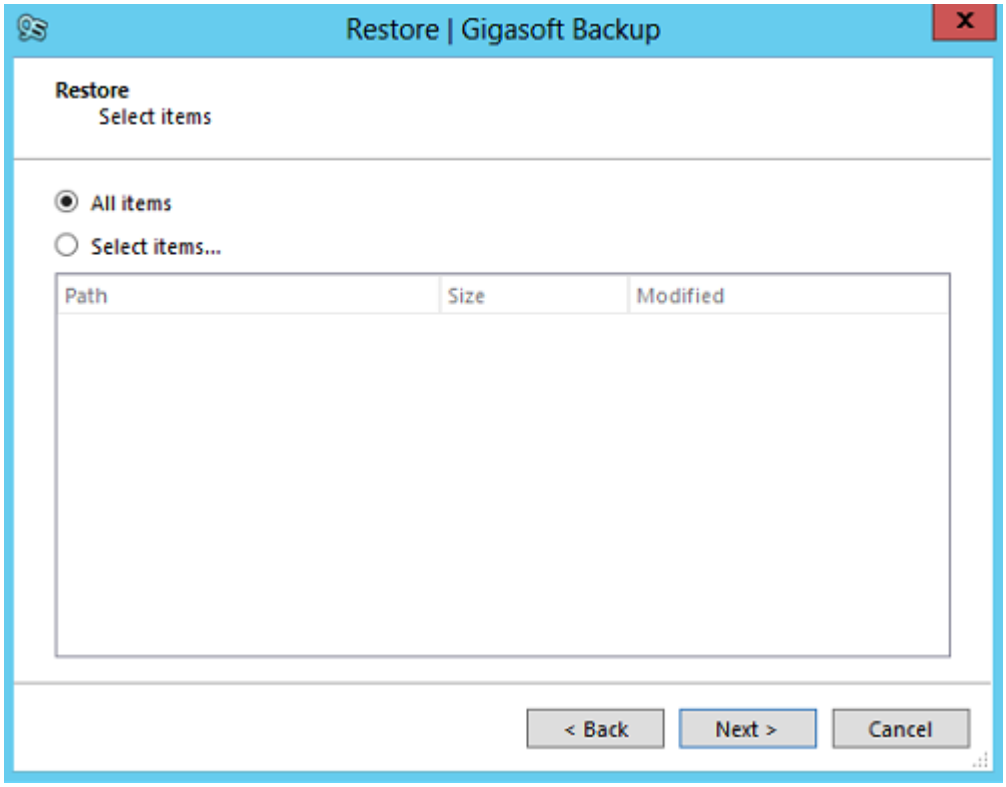
Select the restore tab and choose the storage vault that contains the data for restore, in this example we are using a local vault, click **[Next]**



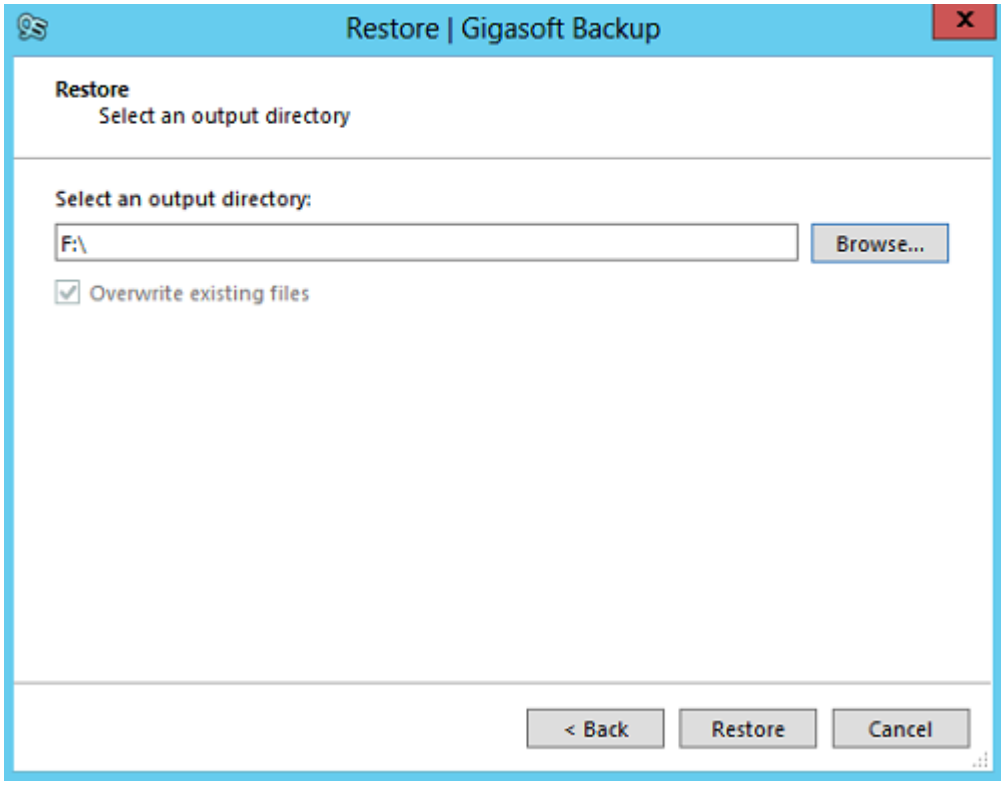
Select the System State protected item and choose the instance you wish to restore, click **[Next]**



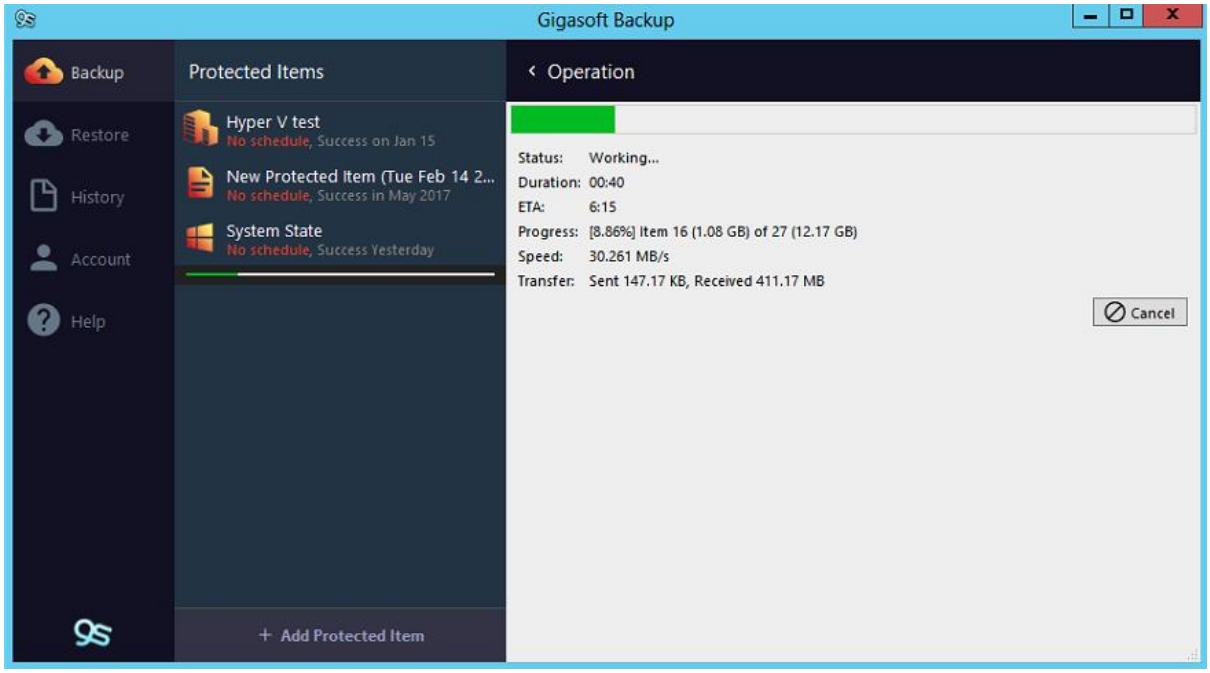
It is possible to select certain items to restore if you wish, just select the **[Select items…]** option and choose the items needed and click **[Next]**



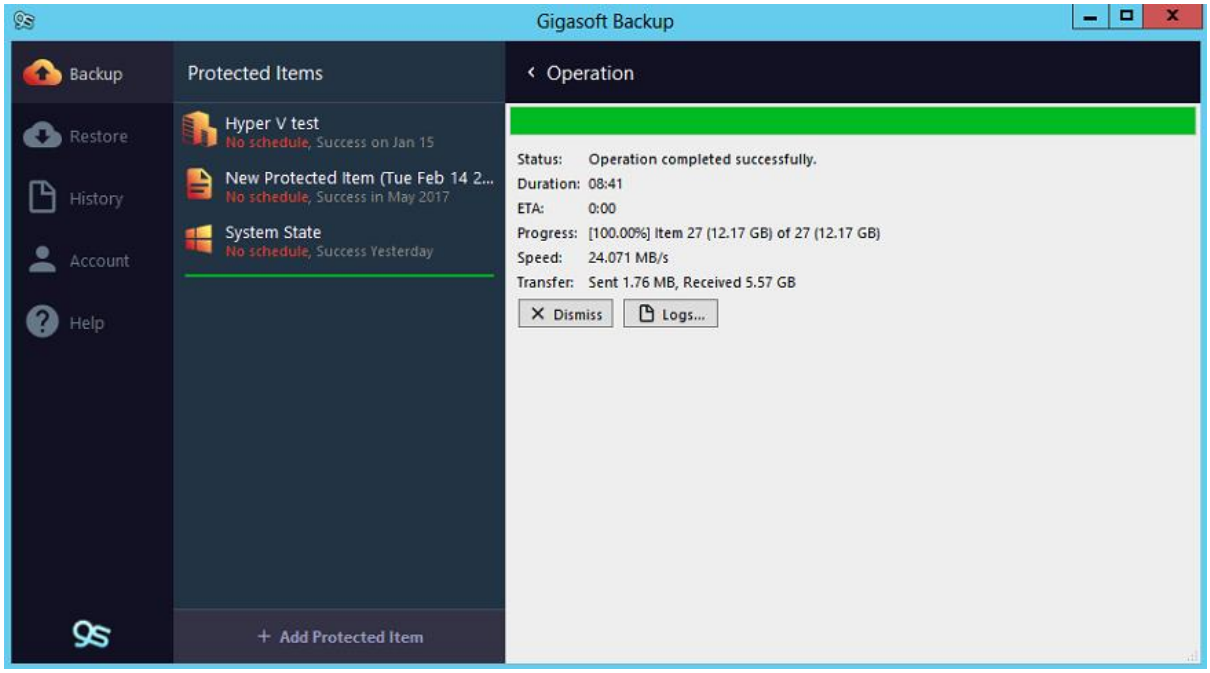
In this example we will choose to restore all the data so we will leave the default selected and click **[Next]**



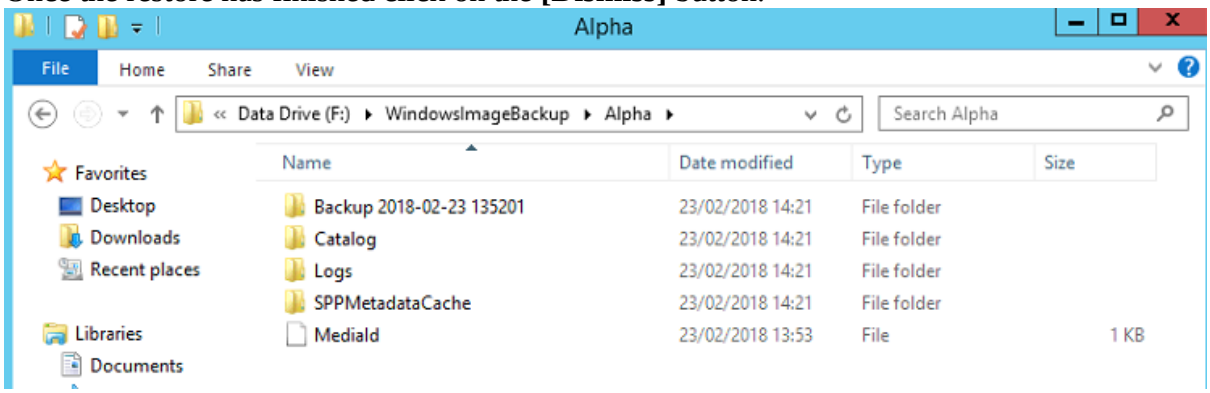
Now we need to choose a location to restore the data to, click on the **[Browse]** button to open an explorer view and choose a location that is suitable to restore the data, once you have selected a location click **[Restore]**



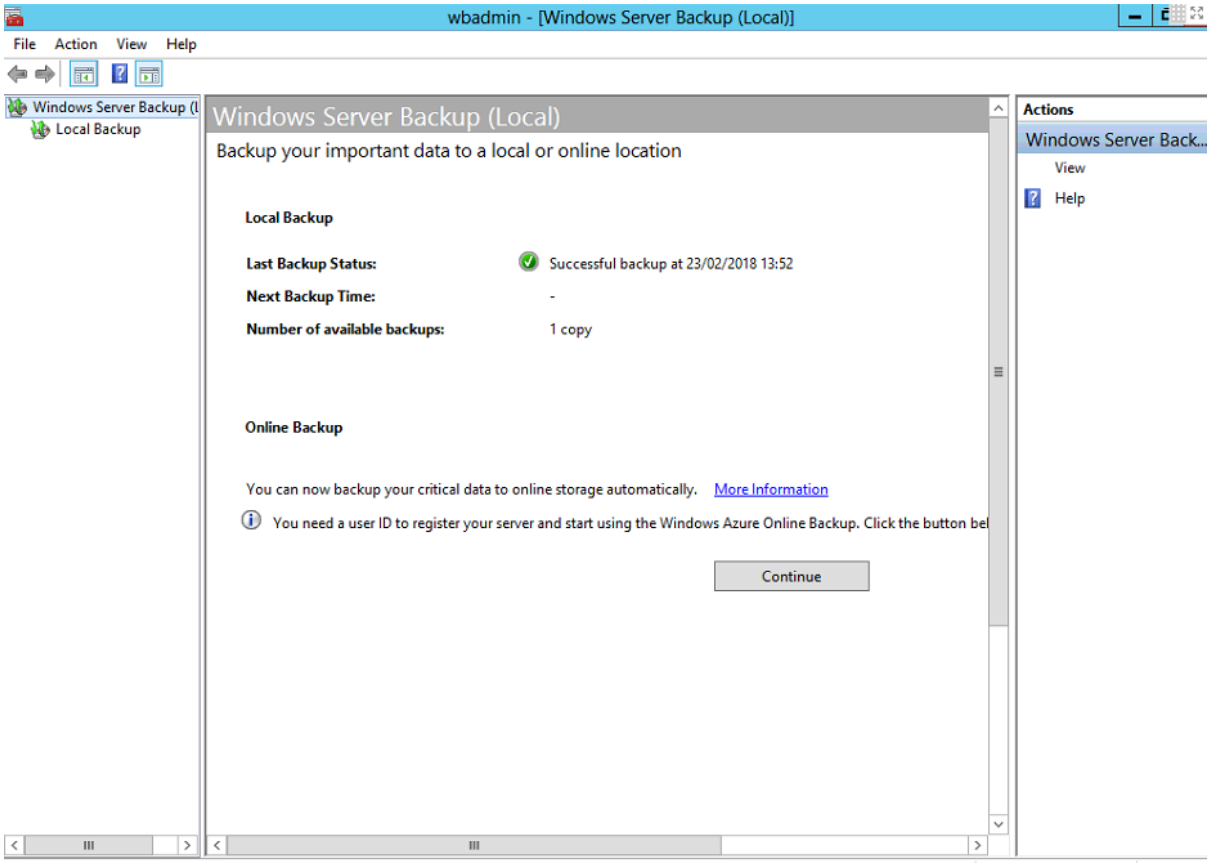
The restore process will begin and you will be presented with a progress window.



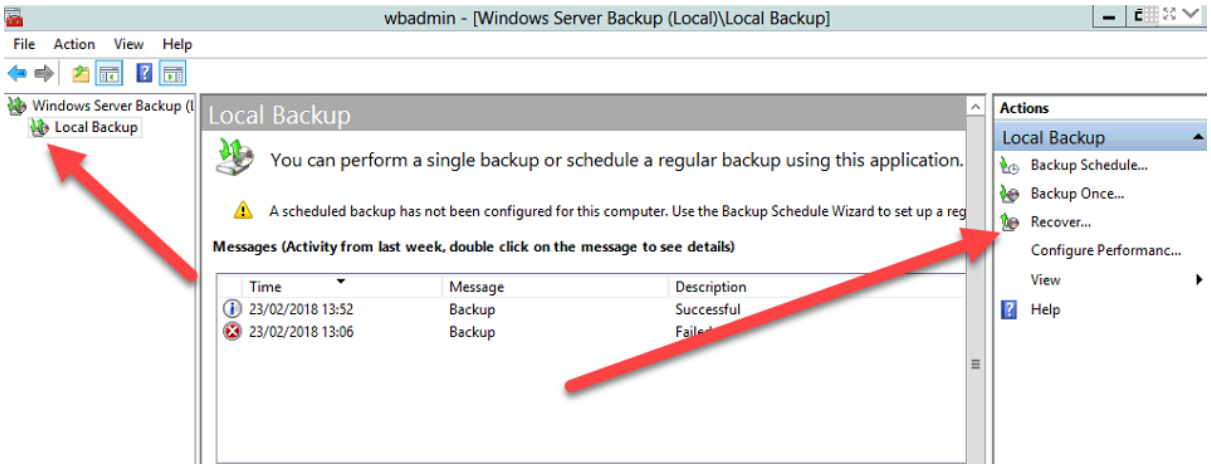
Once the restore has finished click on the **[Dismiss]** button.



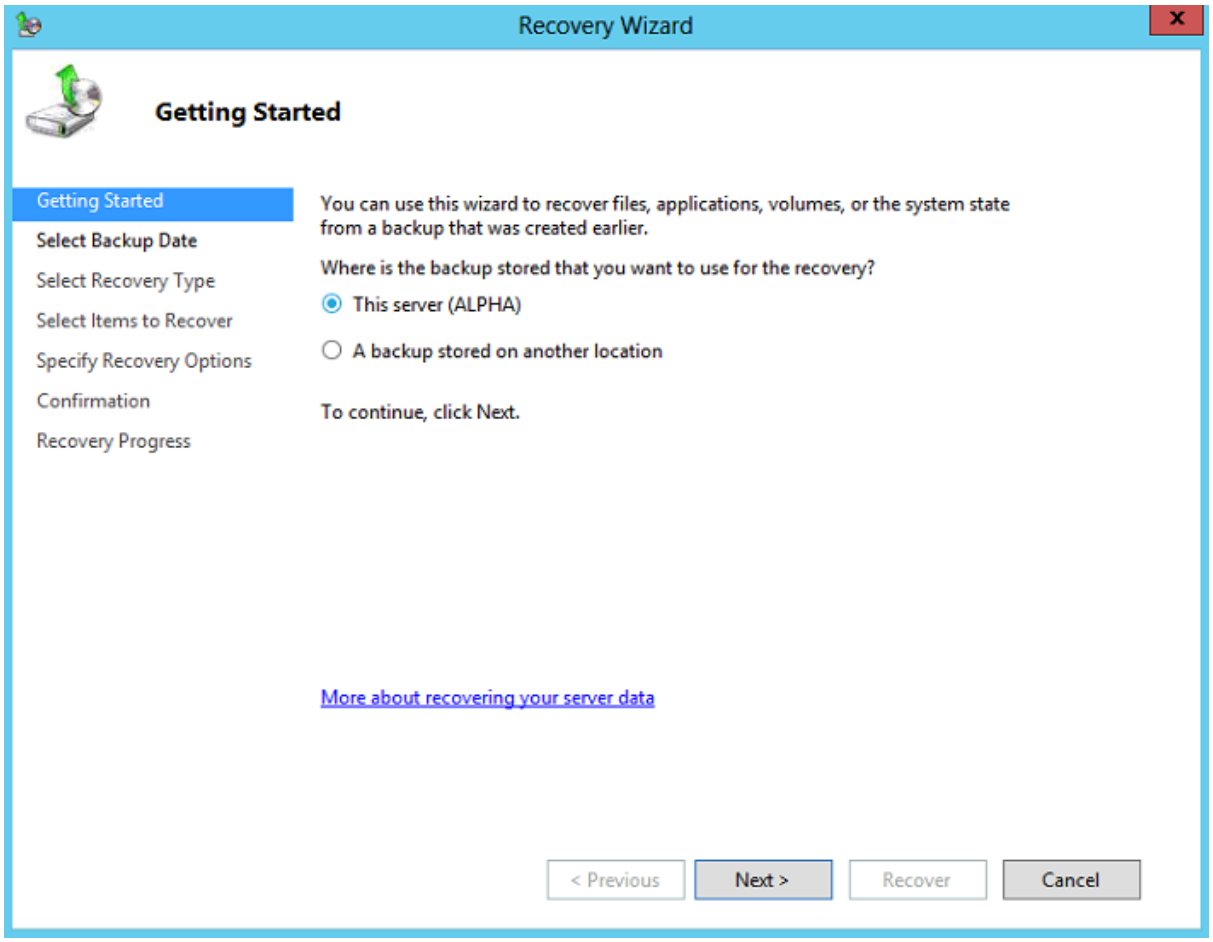
We can now see the data has been restored to the restore location that we selected in an earlier step.



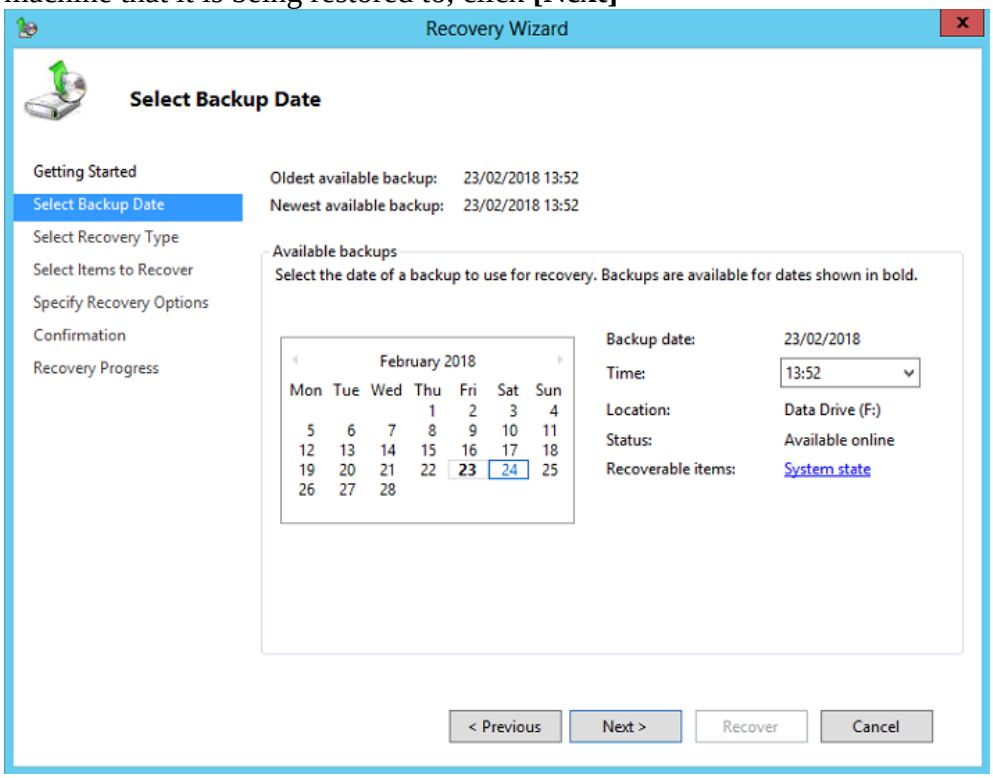
Open the Windows Server Backup application and you will see a screen similar to the one above



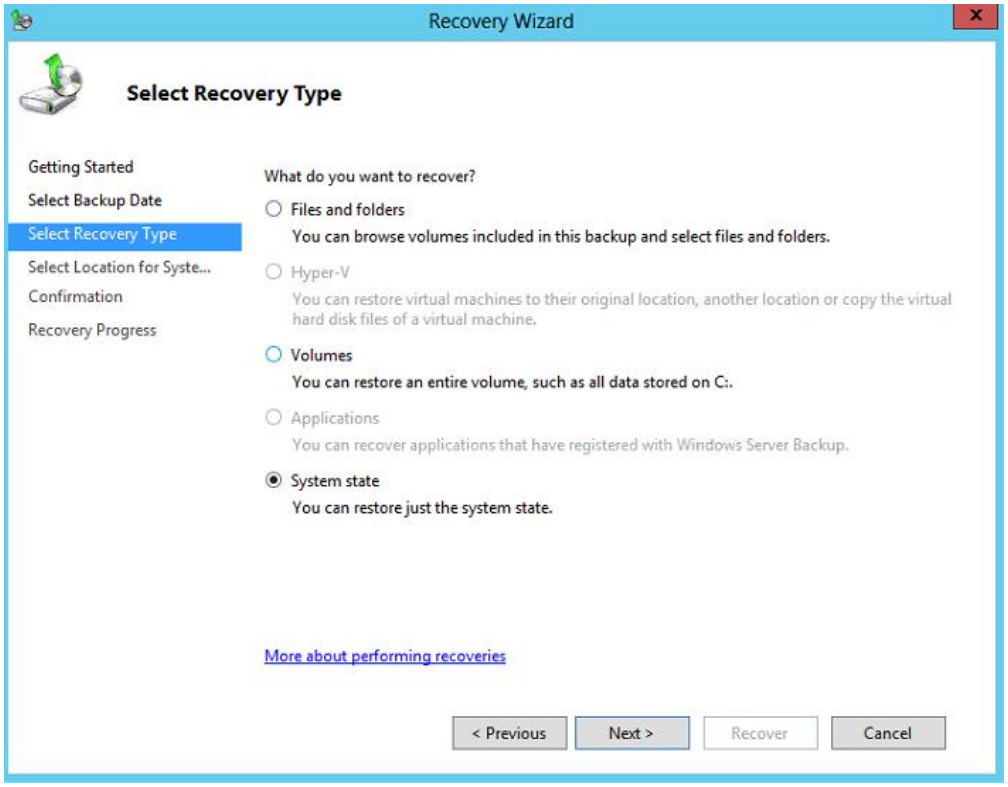
Choose the **local backup** option from the left side of the screen and then choose **Recover** from the right-hand side of the new window



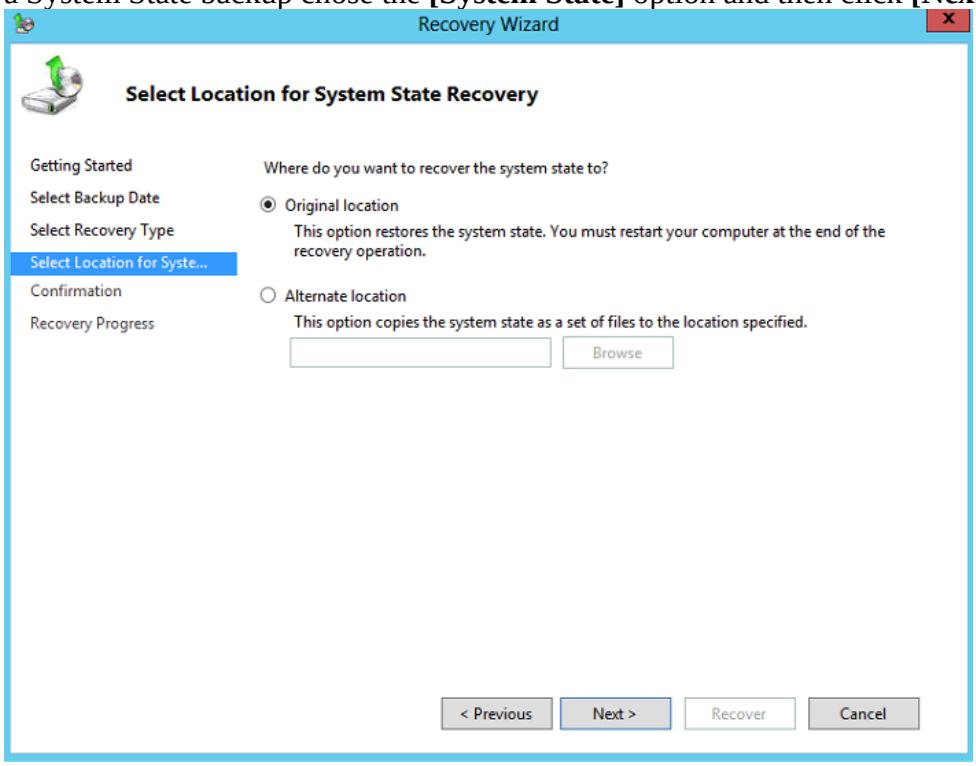
On the next screen we can leave the defaults selected as this backup was taken from the same machine that it is being restored to, click **[Next]**



We can leave the defaults selected on this screen also, you may find your screen may display more restore paths, choose the date of the instance you restored and then click **[Next]**

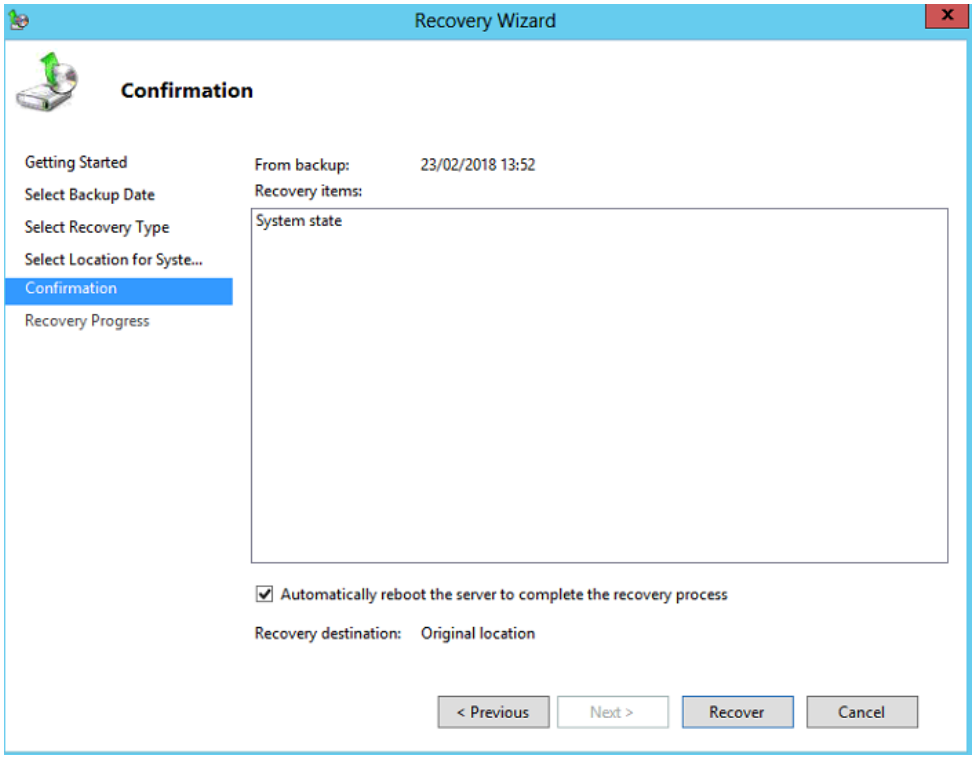


On the next screen we can see there are a few options that we can choose to restore, as this is a System State backup chose the **[System State]** option and then click **[Next]**

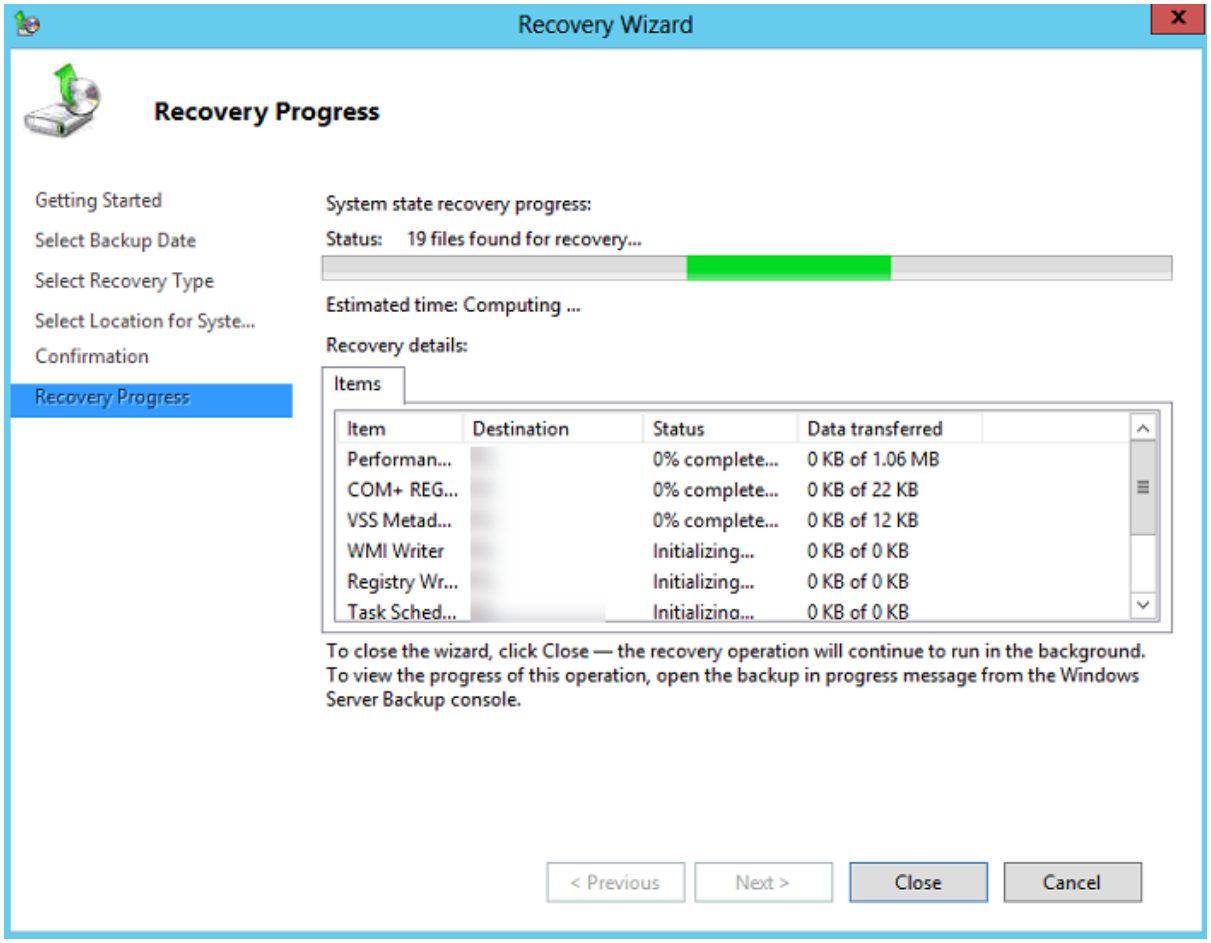


On this screen we can leave the defaults, we will be restoring the System State directly to the server, we can choose to restore to an alternative location if you choose but this will require

further work to restore back into the system. We will leave the default option and click **[Next]**



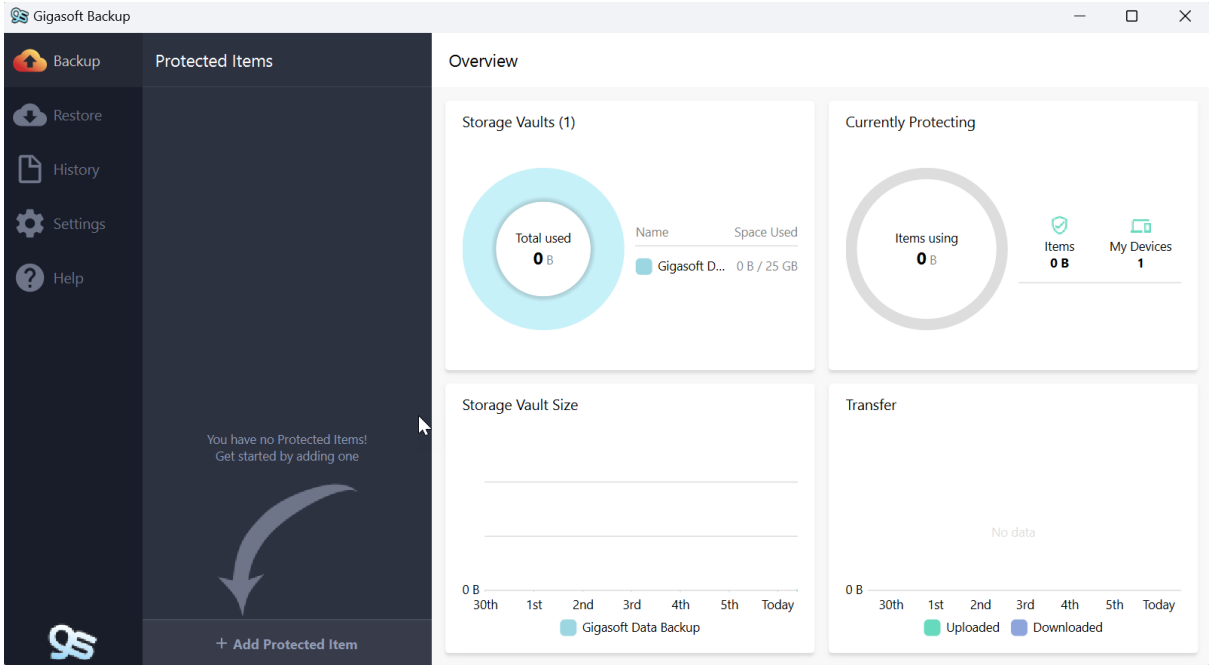
We are now given a confirmation page explaining what we are restoring and allows us to automatically reboot the server once the restore is complete, click the **[Recover]** button to start the restore process



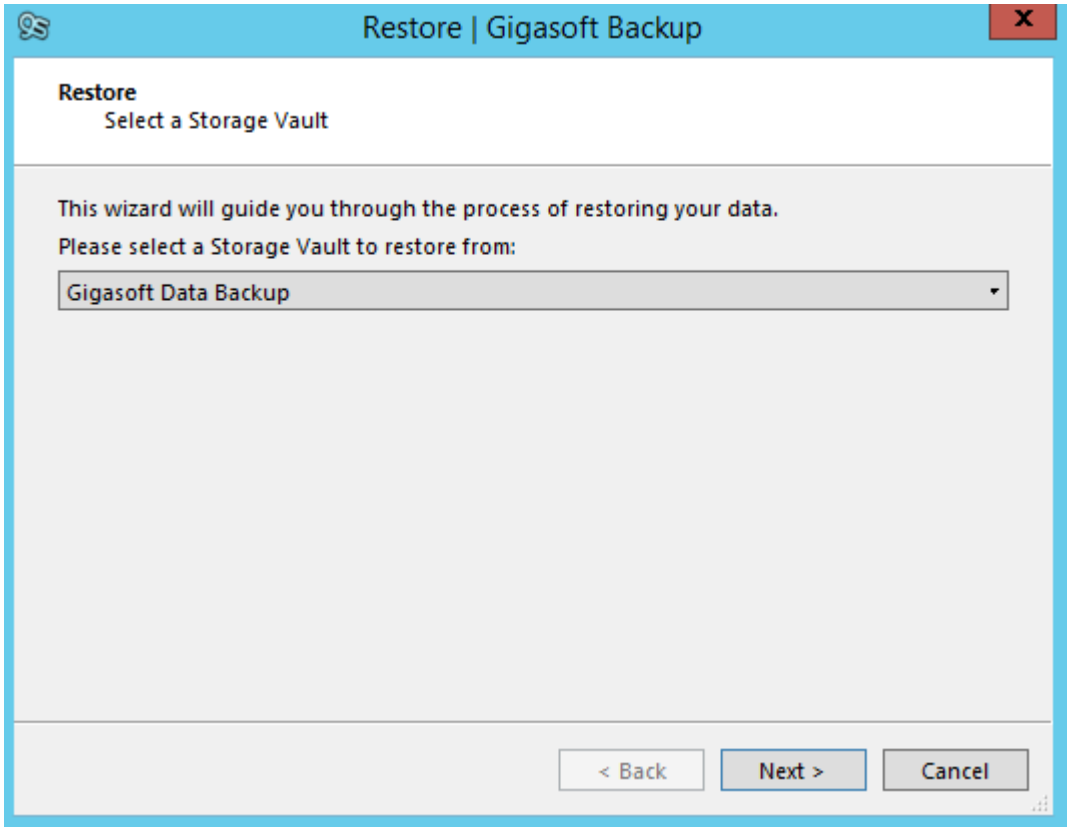
The system will start the recovery process will import the data back into the correct locations, once complete the server will reboot to complete the process.

8.7 Windows system backup

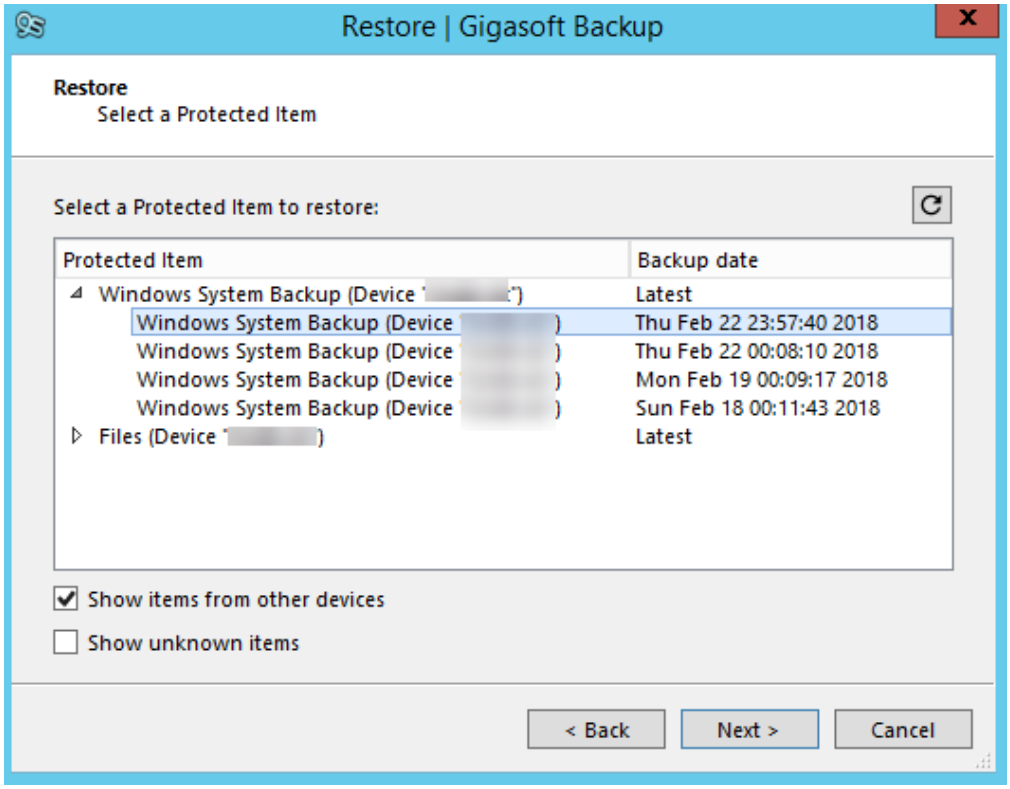
This section will guide you through the process of restoring elements from the Windows system backup. If this is a new machine in which you wish to restore the data to then the windows backup role needs to be enabled before the restore can be used.



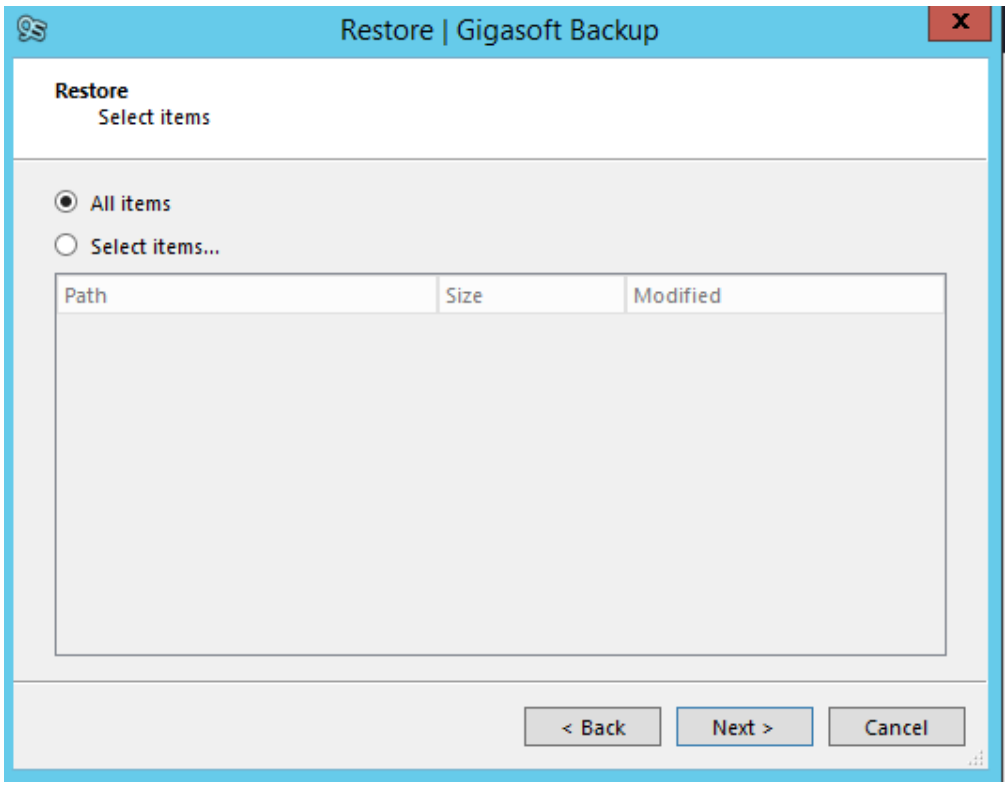
Firstly, log in to the backup client.



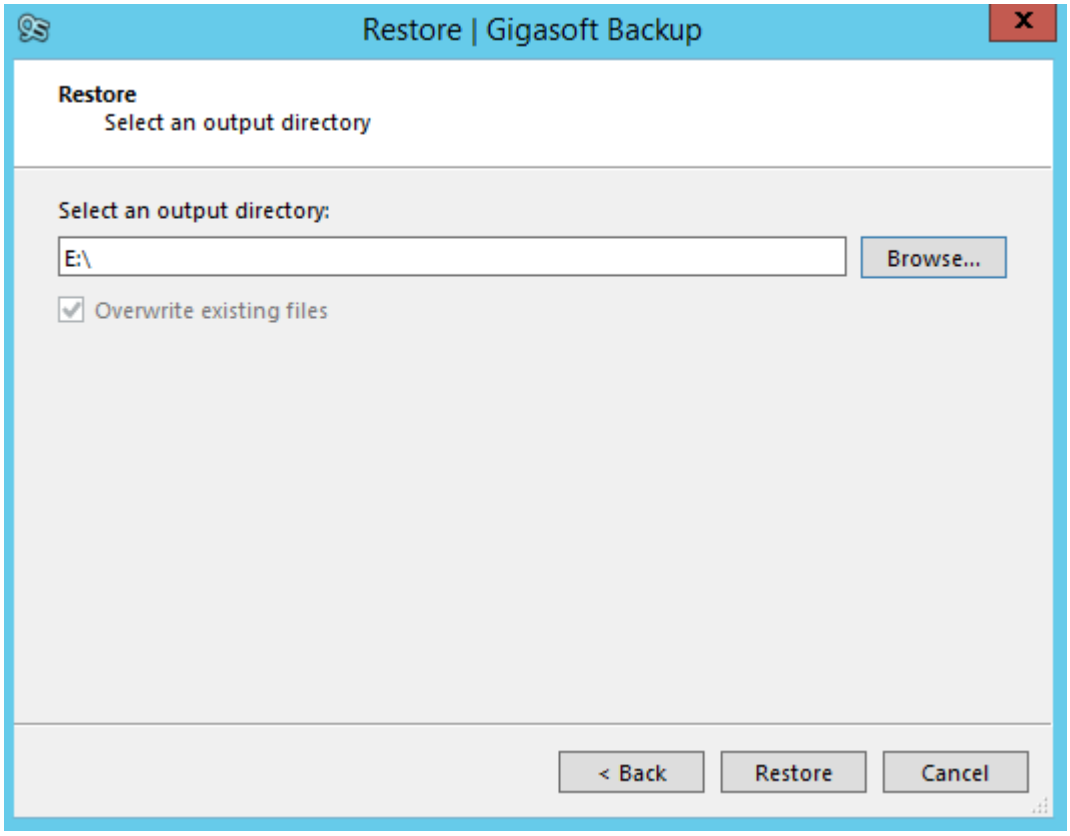
Select the restore tab and then select the required storage vault from the drop sown list and click **[Next]**



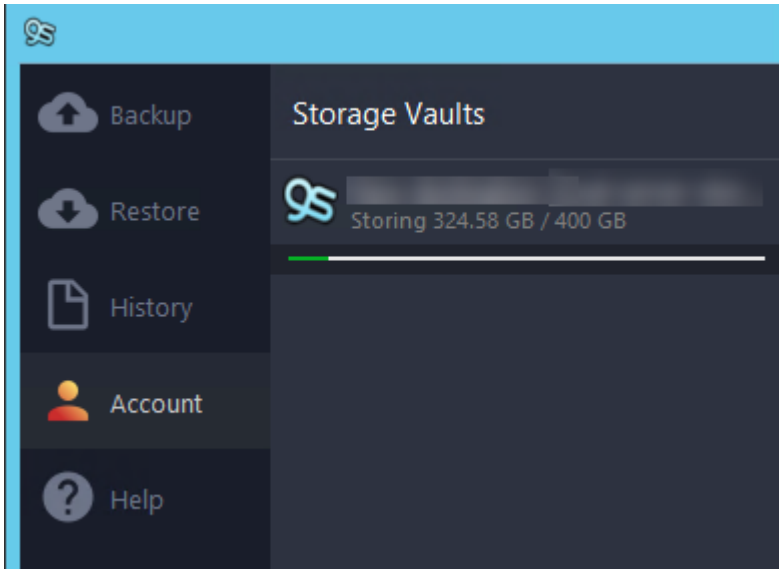
Select the point in time you wish to restore from, you may need to select **[Show items from other devices]** if this is to be restored to a different machine than it was taken from.



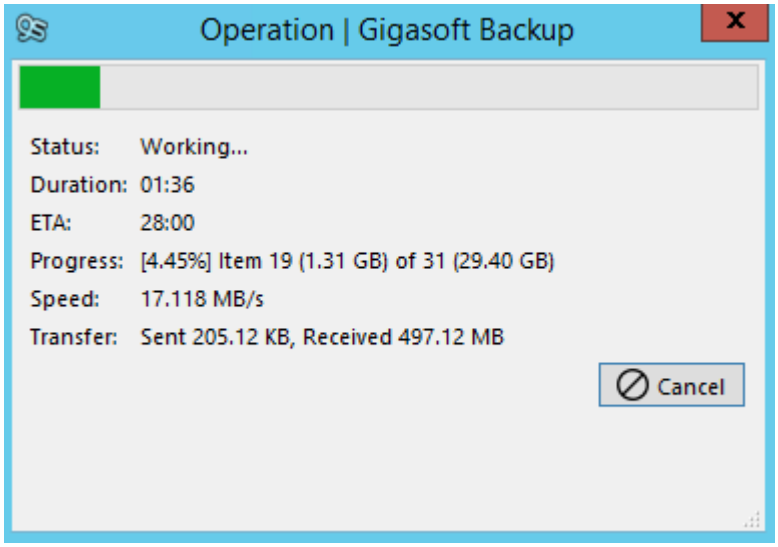
Choose whether to restore all the items or select **[Select items…]** to choose the items you wish to restore, in this example we will choose the default of All



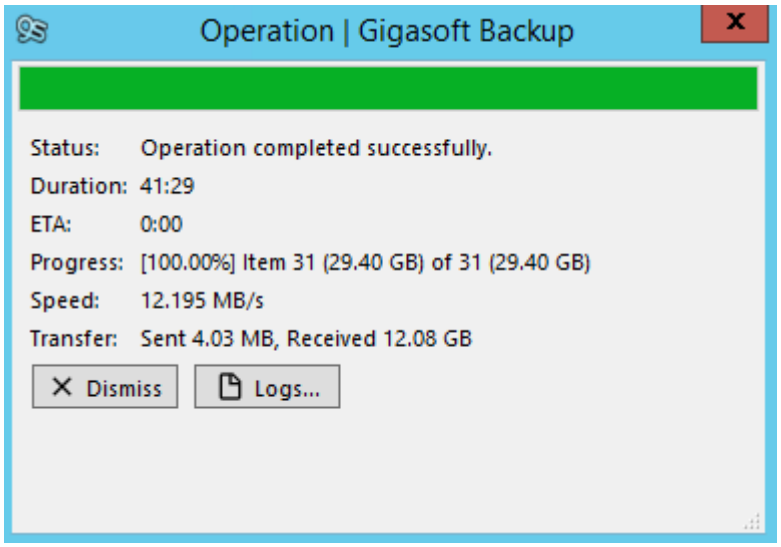
Select a location that is large enough to restore all the selected data and click **[Restore]**



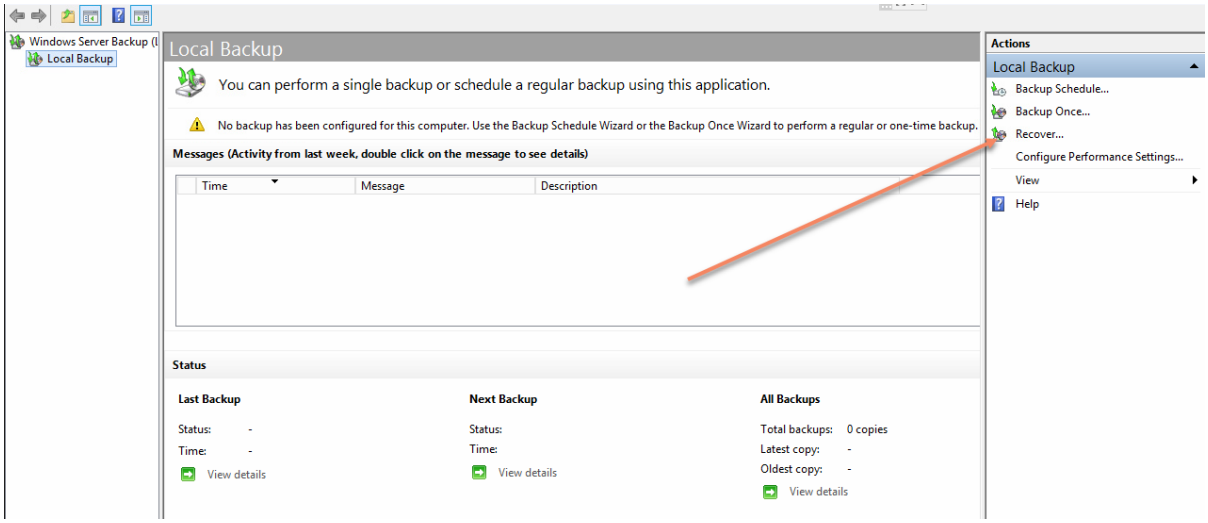
You will now see the restore progress bar, this will increase as the restore process progresses.



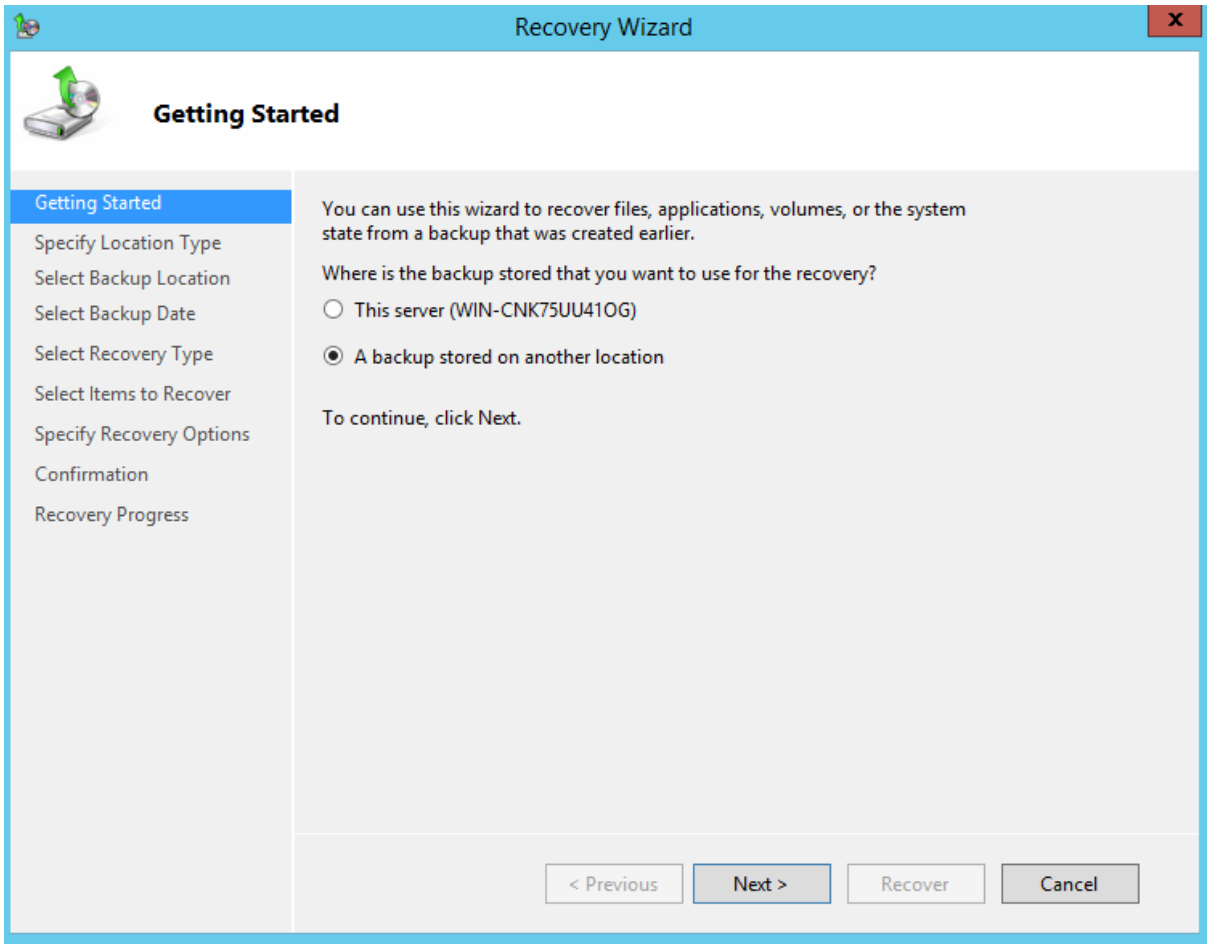
If you click on the green progress bar you can access a more detailed restore progress window.



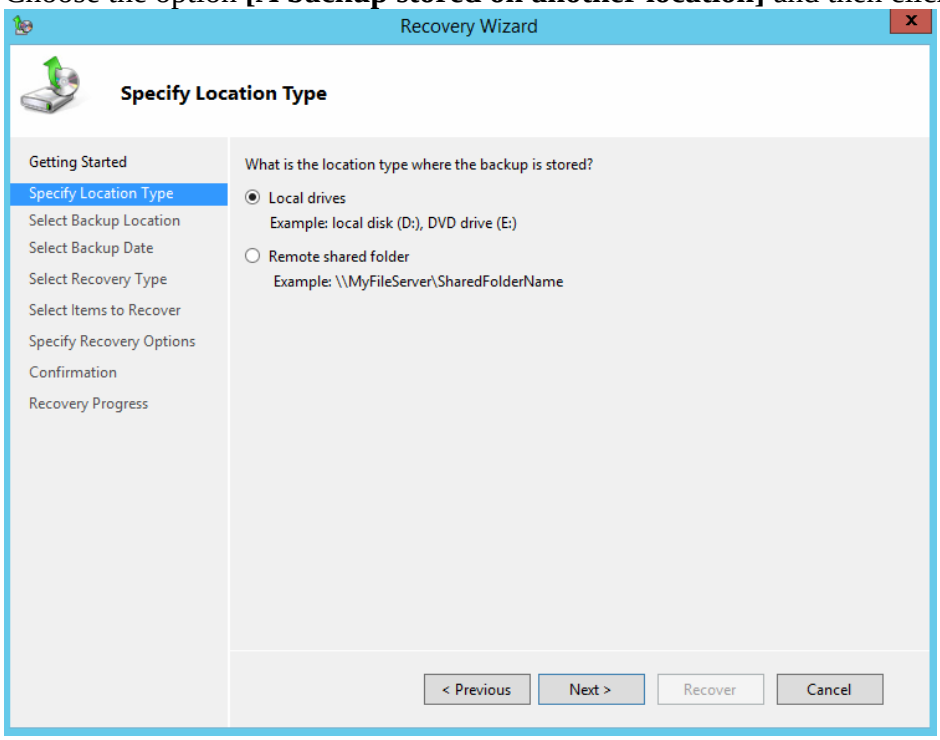
Once the restore has finished click **[Dismiss]**



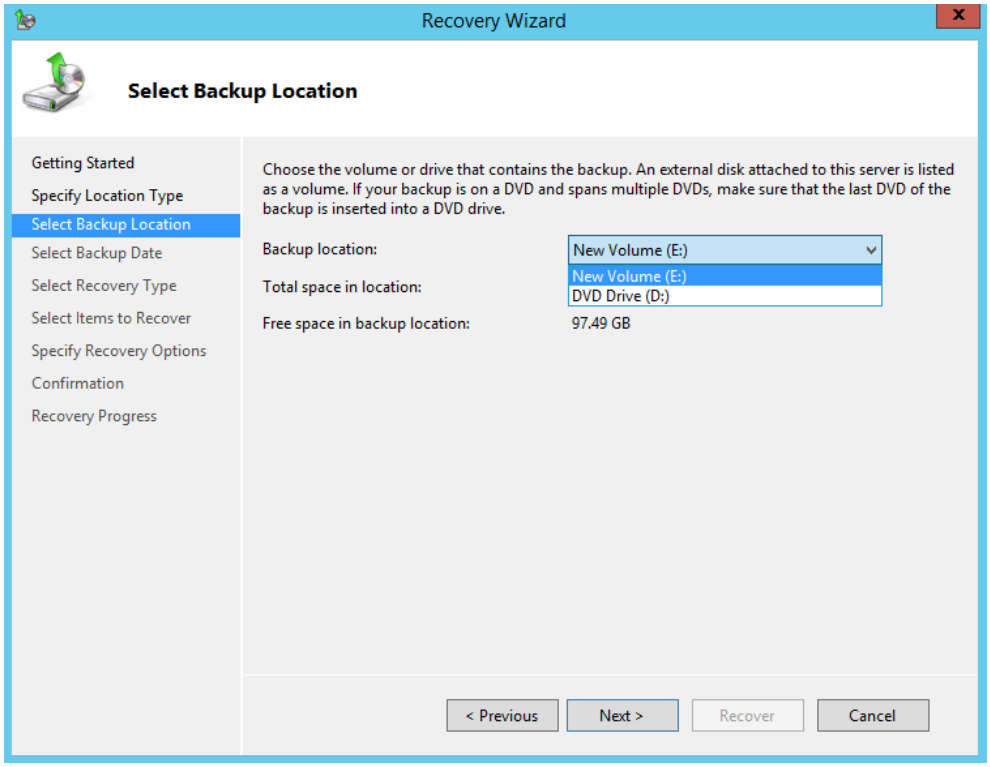
From the Windows Backup application select the **[Restore]** option



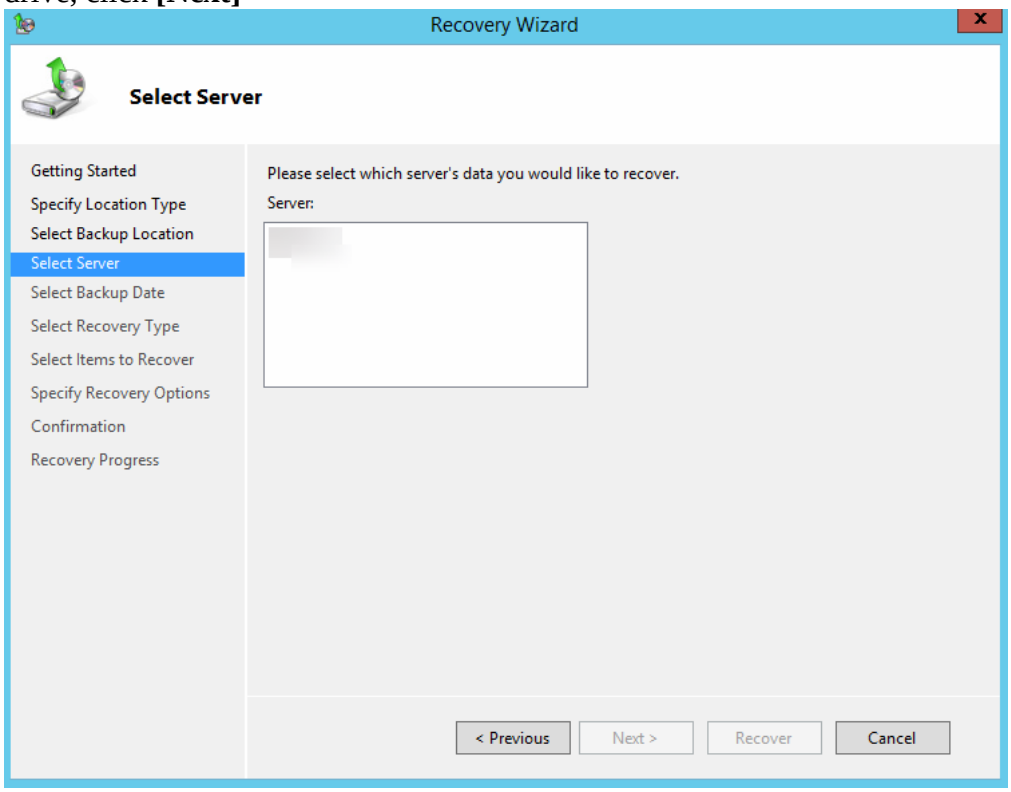
Choose the option **[A backup stored on another location]** and then click **[Next]**



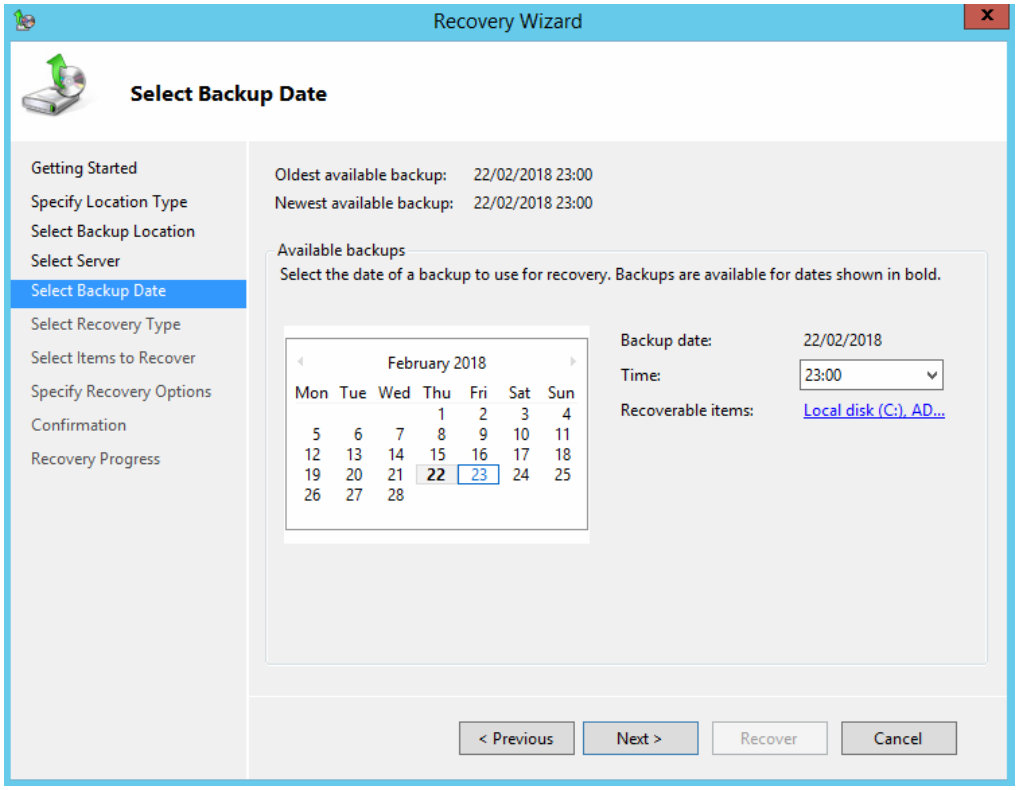
Next choose the option **[Local drives]** and then click **[Next]**



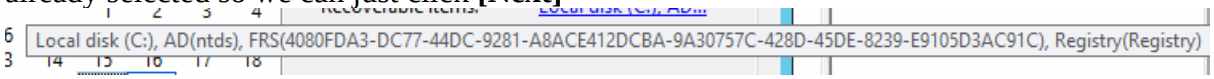
Choose the backup location that you restored the data to, in our example we restored to the E drive, click **[Next]**



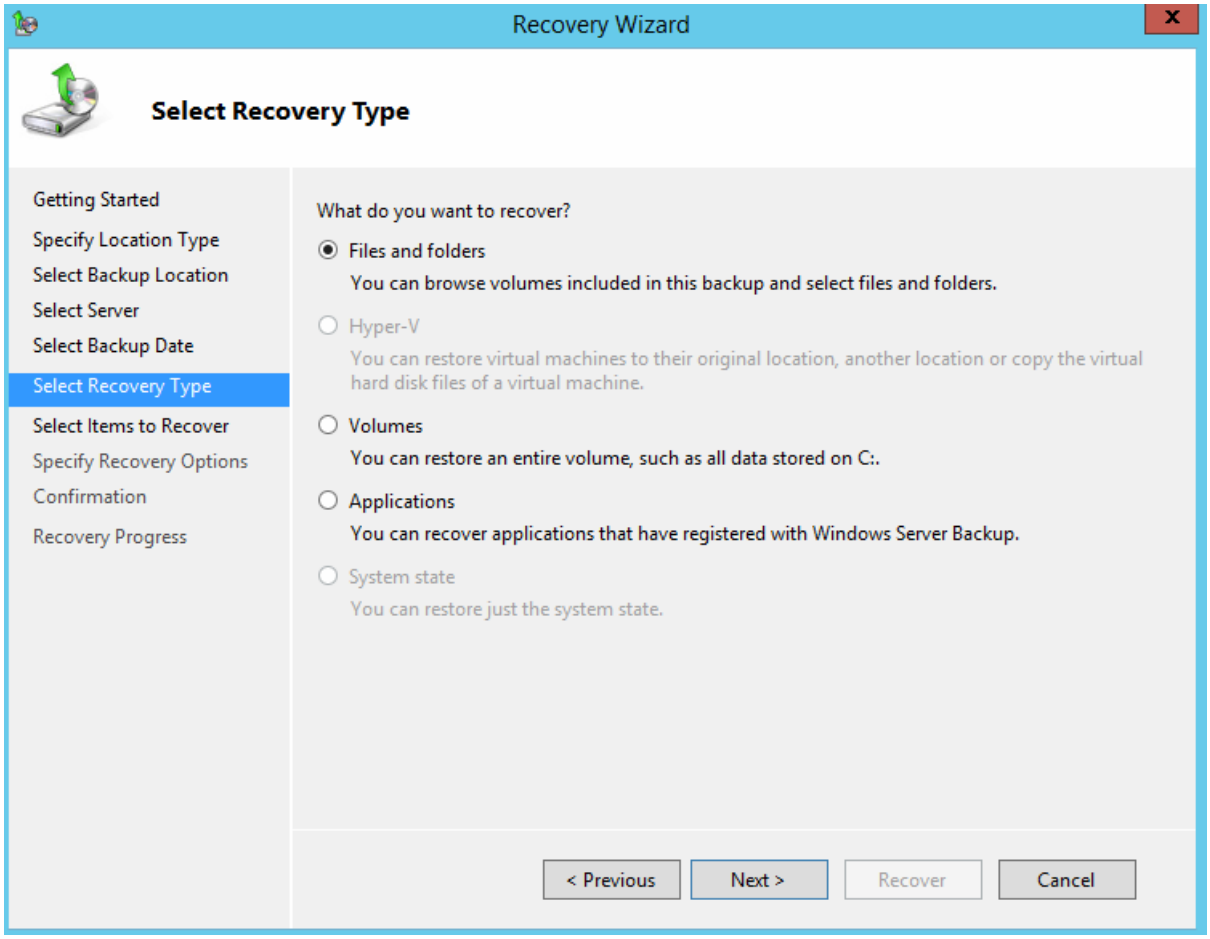
You will now be asked which servers data you wish to restore, click on the server name and then click **[Next]**



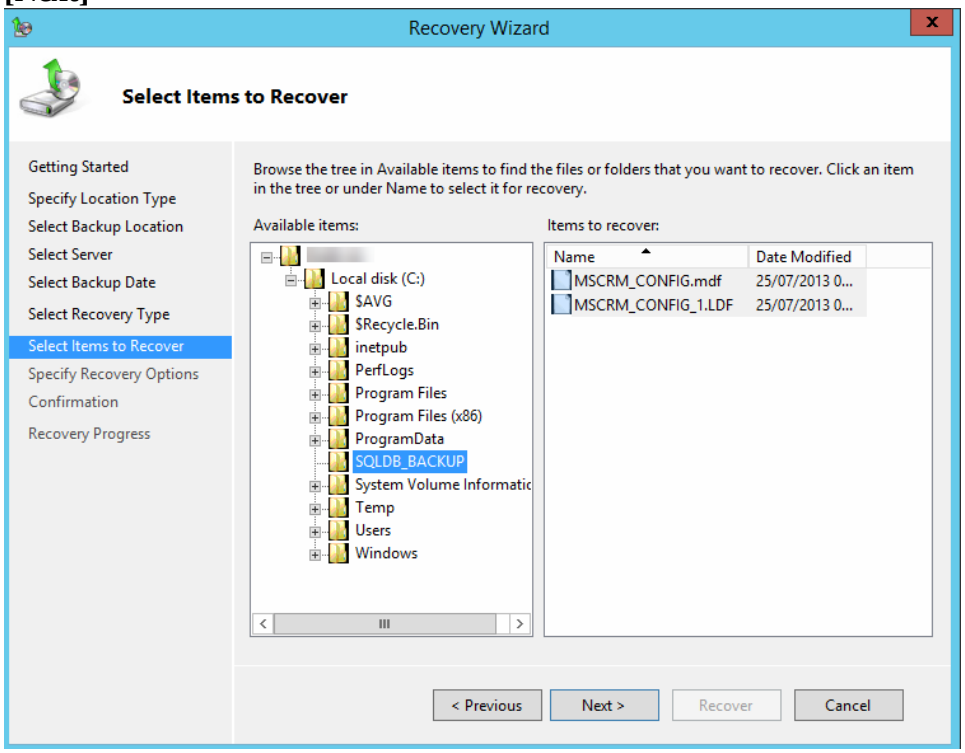
Select a point in time to restore from, in most cases there will only be the option that's already selected so we can just click **[Next]**



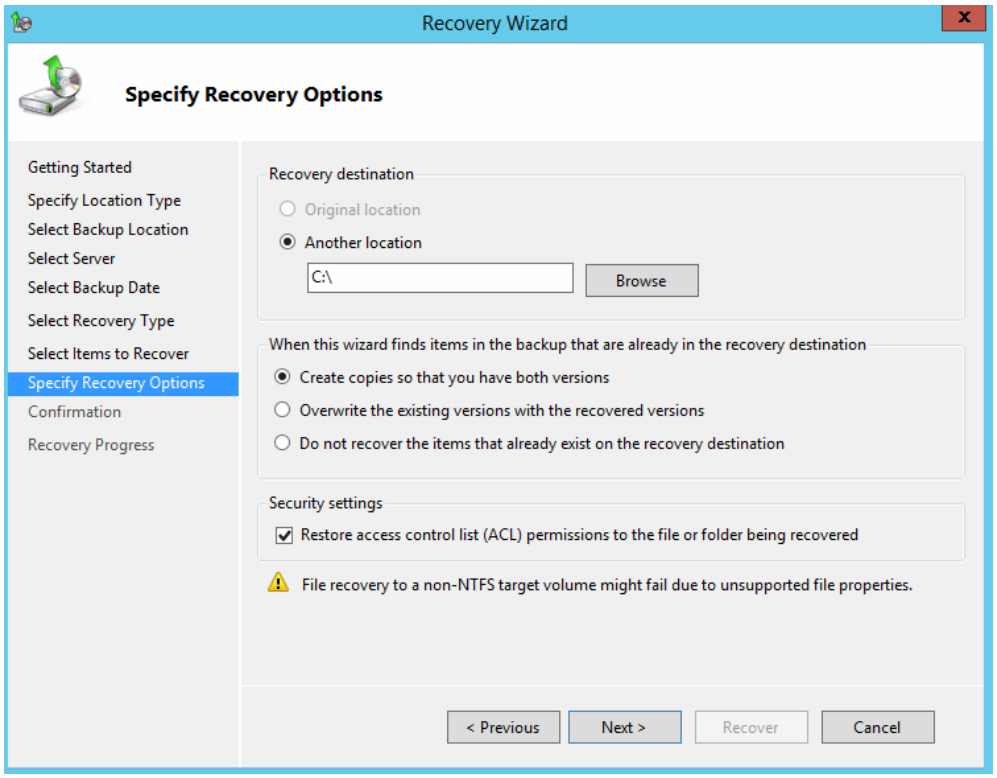
Under the Time field you should see a blue link, hovering over this will give you an idea of what is included in the current backup.



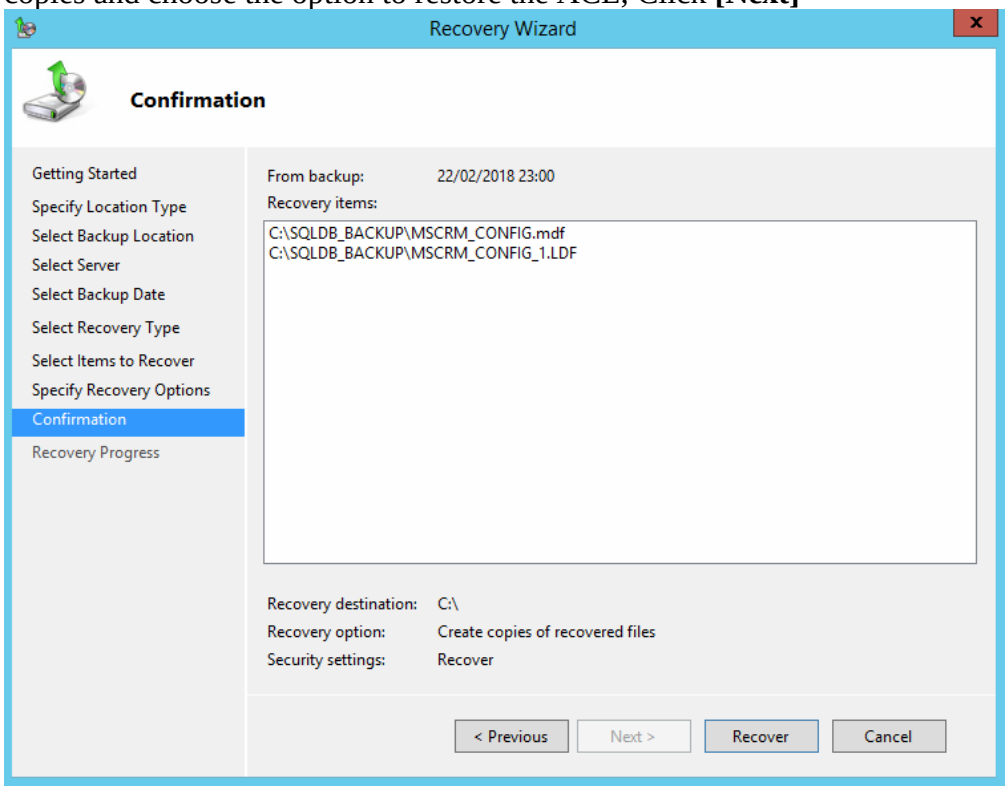
Choose your restore option, in this example we will select **[Files and folders]** then click **[Next]**



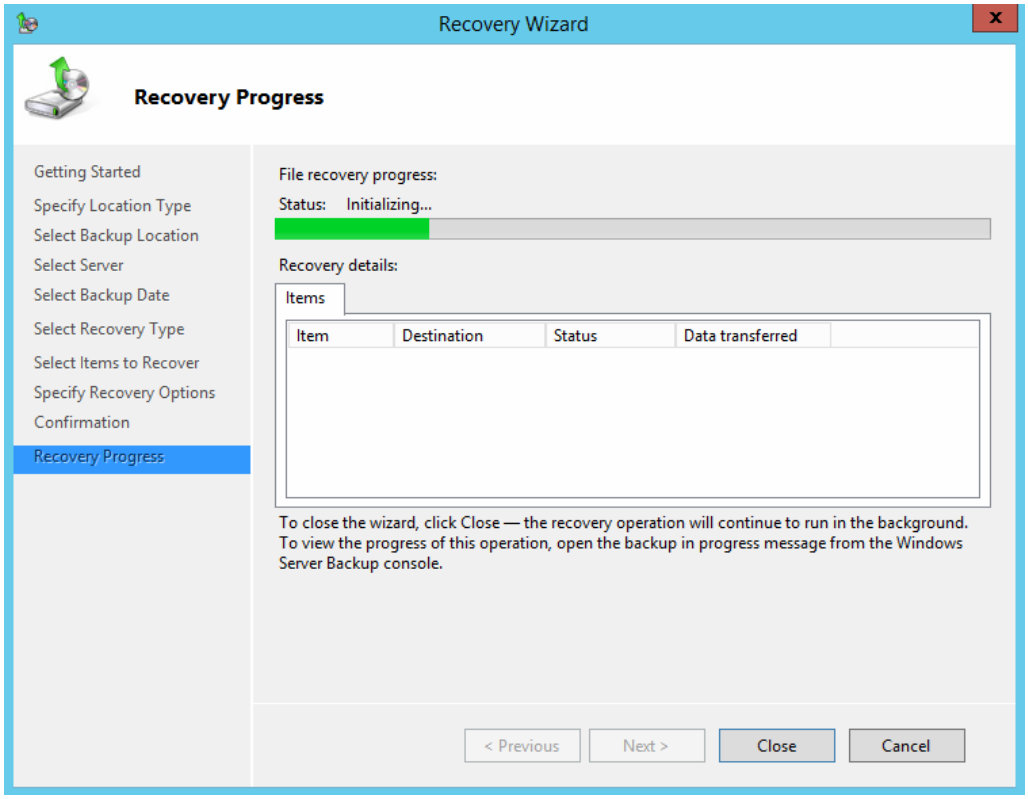
Now use the explorer window to drill down and select the files you wish to restore and click **[Next]**



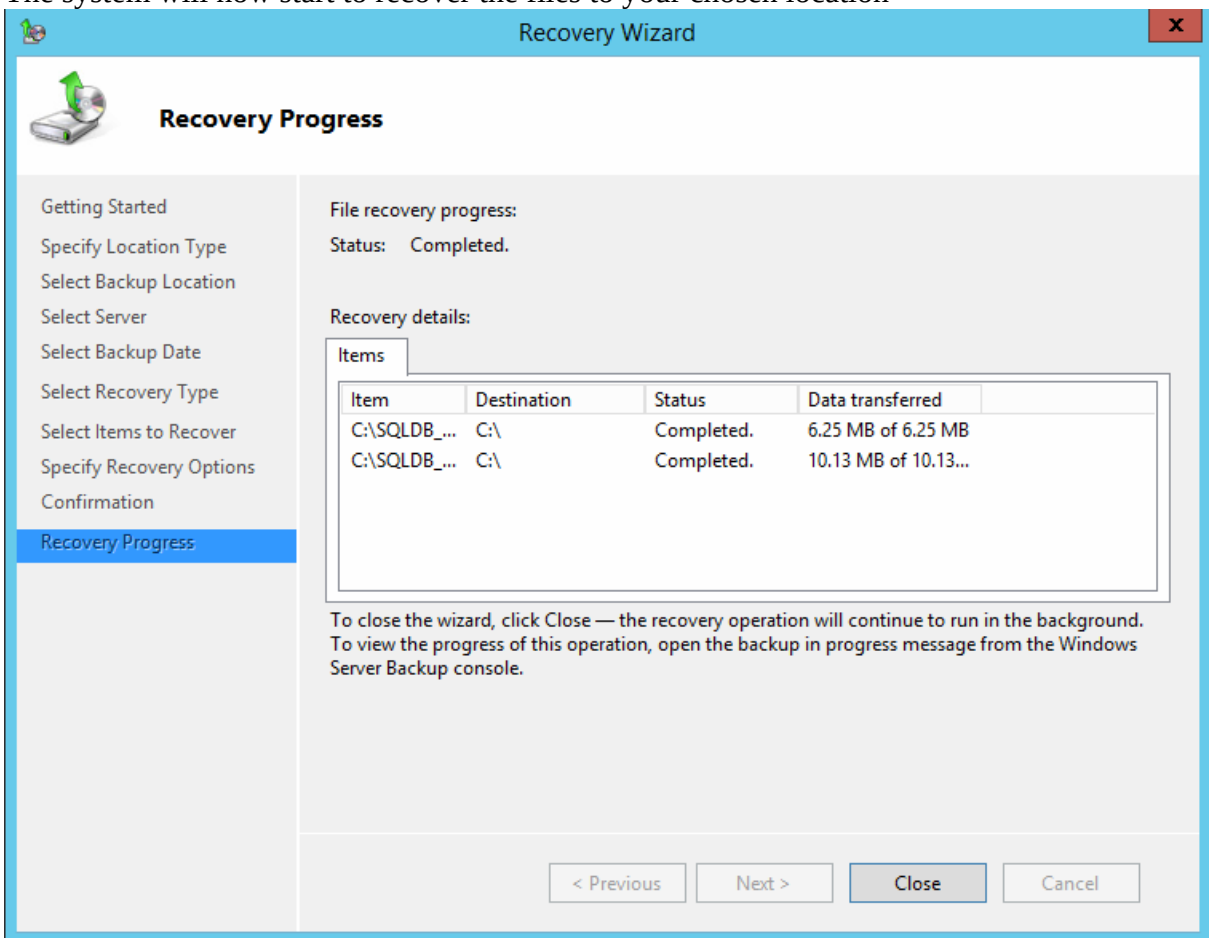
Now specify a location to restore the files to, in this example we will select the C drive, you can also choose to overwrite files that already exist or create copies, we will select create copies and choose the option to restore the ACL, Click **[Next]**



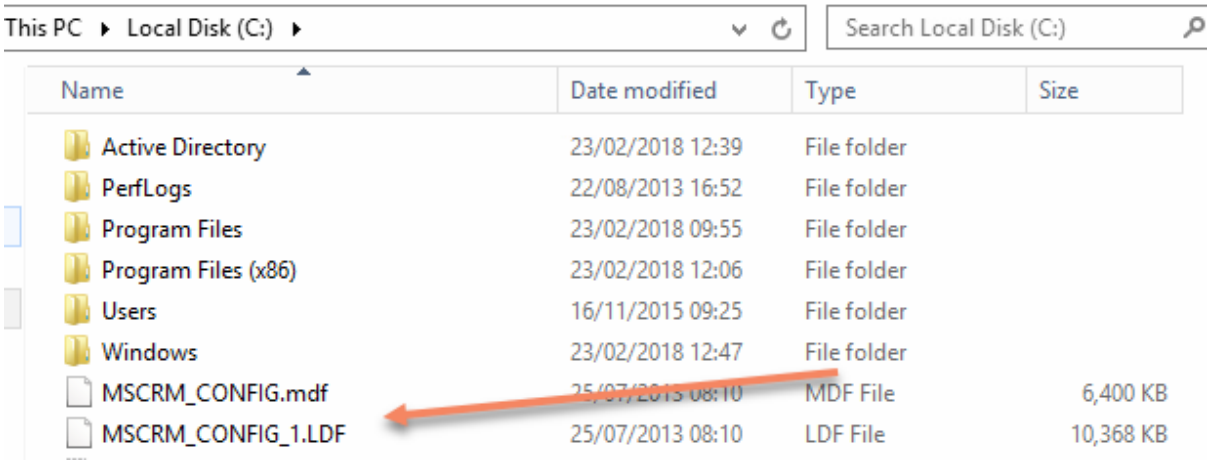
On the final page you will be given a confirmation page, click **[Recover]** to start the recovery process



The system will now start to recover the files to your chosen location



When the recover process is complete click on **[Close]** to finish

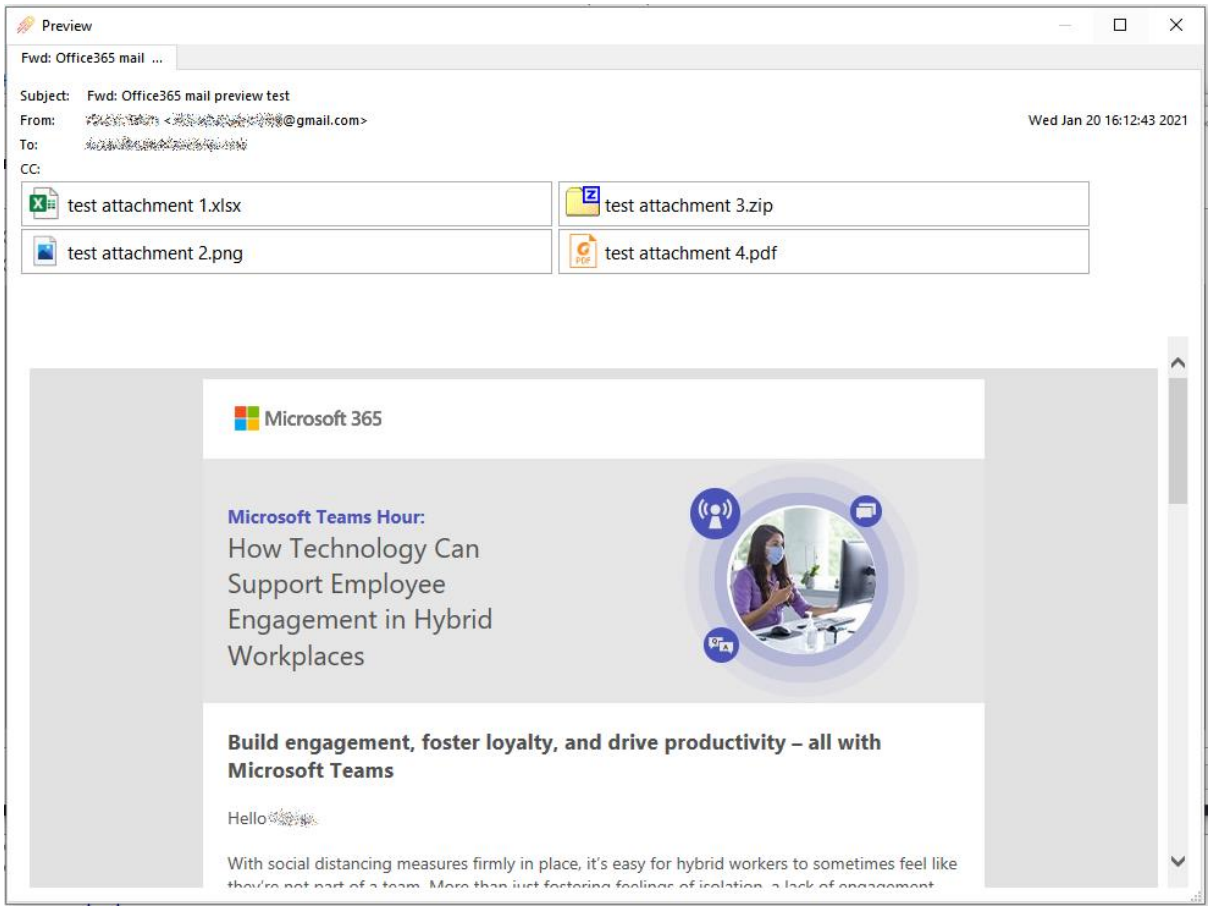


Your files will now be located in the restore location you selected in the previous steps, you can now copy the files into their correct / original locations.

8.8 Restore Office 365 Backup (SharePoint, OneDrive & Email)

Select files for restore. When browsing files to restore, different columns are displayed depending on the type of item being browsed.

Preview an email before restoring it, by using the right-click menu. The email preview shows the rich HTML content if the email contains it. Email preview contains the header fields, such as the `From`, `To`, and `Subject` fields; information about attached files; and embedded images.



8.8.1 Restoring Office 365 items to the local PC

Emails are restored in MIME format (`*.eml`). These files can be opened with Microsoft Outlook on your PC, or in any other email program (MUA) such as Mozilla Thunderbird. Microsoft Outlook supports importing `*.eml` files in bulk by dragging-and-dropping into an Outlook folder.

If the email represents a meeting invite, the email contains a calendar appointment attachment in vCalendar format. These attachments can be renamed to `*.vcf` and opened with Microsoft Outlook on your PC.

Contacts and Calendars are restored in JSON format. These files require further processing to convert to standard vCalendar format (`*.vcf`) before opening with Microsoft Outlook.

SharePoint file attachments, including OneDrive items and Teams files, are found within associated SharePoint site. OneDrive files can be restored as regular files and folders underneath the "Documents" subdirectory of the associated SharePoint site.

8.8.2 Restoring Office 365 items back to the cloud

You can choose to restore Office 365 items back to the cloud. You can choose to restore either to the original Office 365 cloud location, or a custom location.

All items will be restored with the default retention policy.

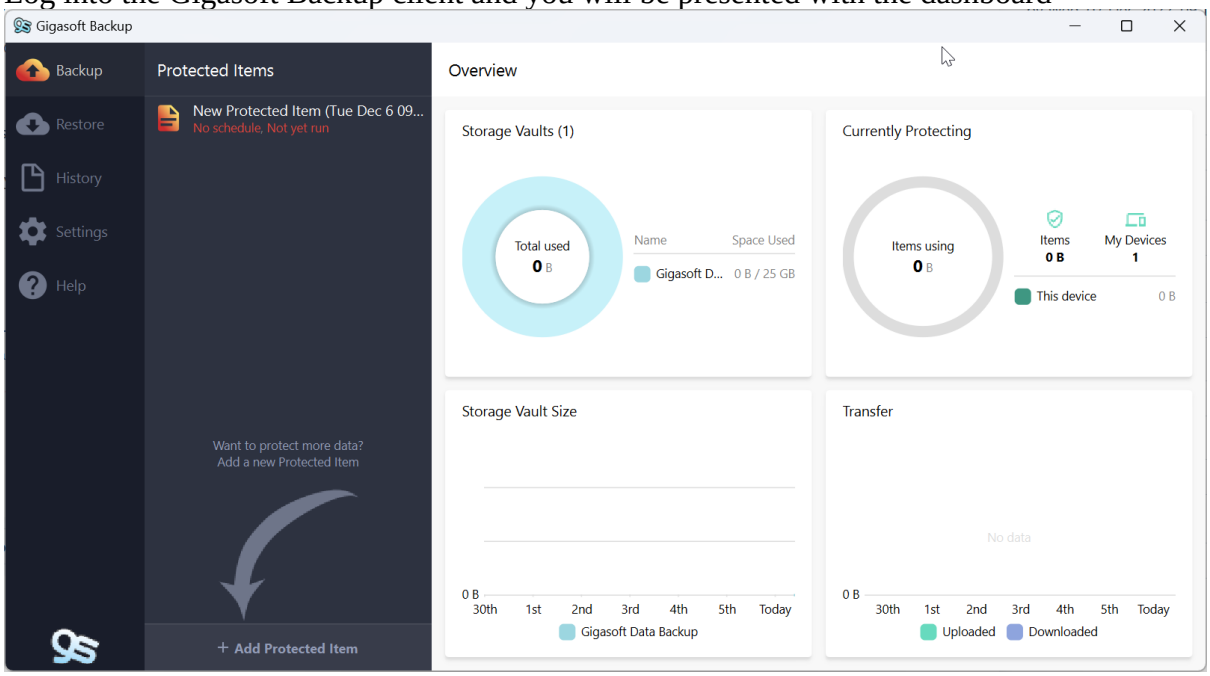
Any existing emails will not be overwritten. If an email selected for restore already exists in the target Office 365 cloud location, it will be restored as a duplicate email.

9 The history tab

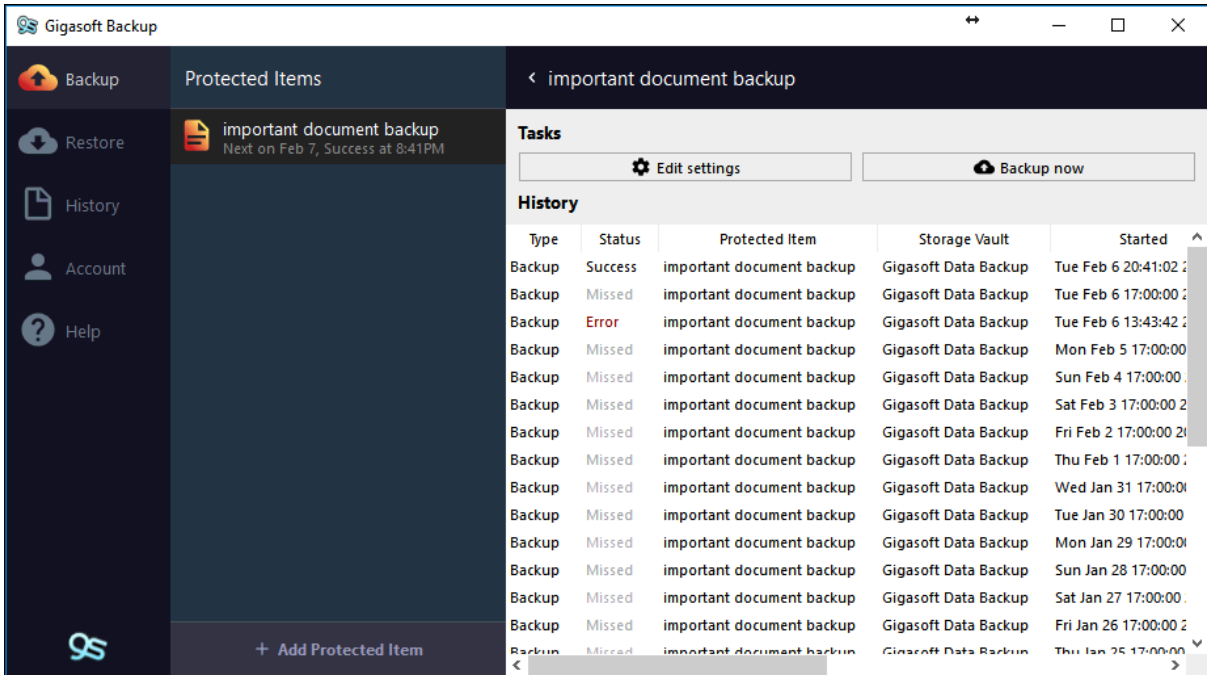
In this section we will cover the History tab and how to view the history of single protected items and of all protected items on the account.

9.1 The history tab (windows)

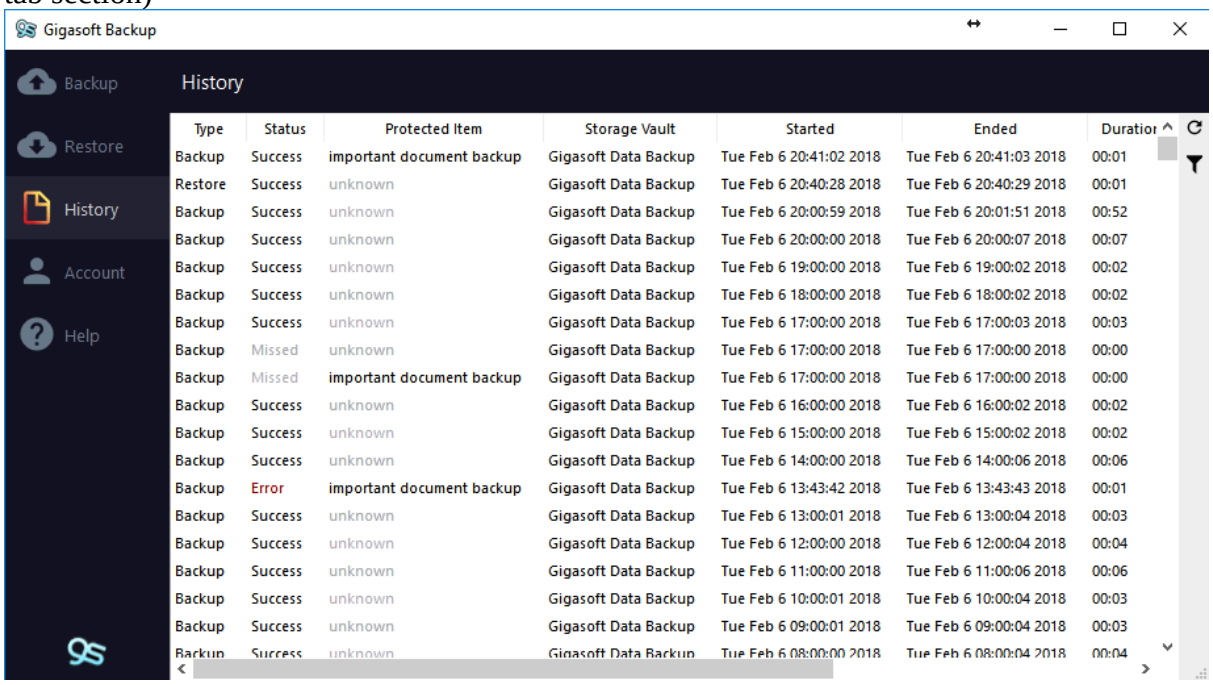
Log into the Gigasoft Backup client and you will be presented with the dashboard



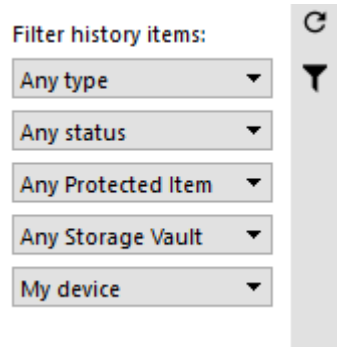
If you click on one of the Protected items you will see the recent activity of this item on the right-hand side of the screen.



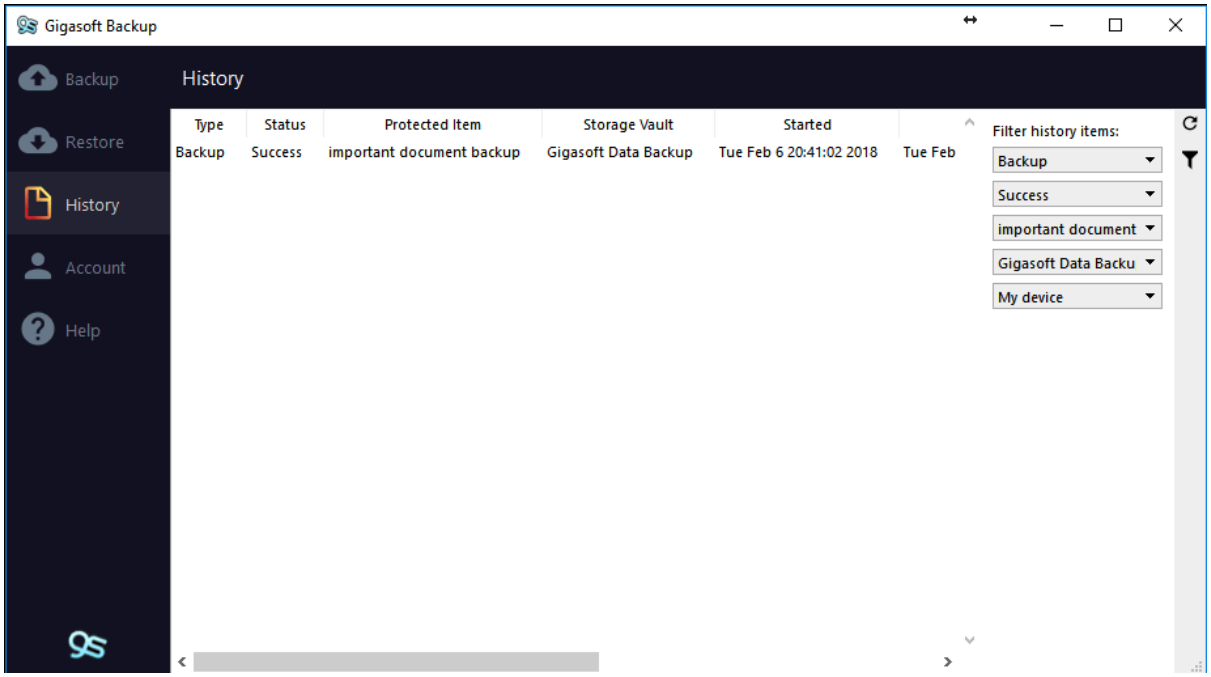
If you now click the **[History]** tab on the left of the client you will be shown the history of the account, any Protected items that run on this machine will be listed as well as unknown ones that relate to other machines on the account (we will cover this a bit more in the account tab section)



From this screen you can apply filters  to sort the columns



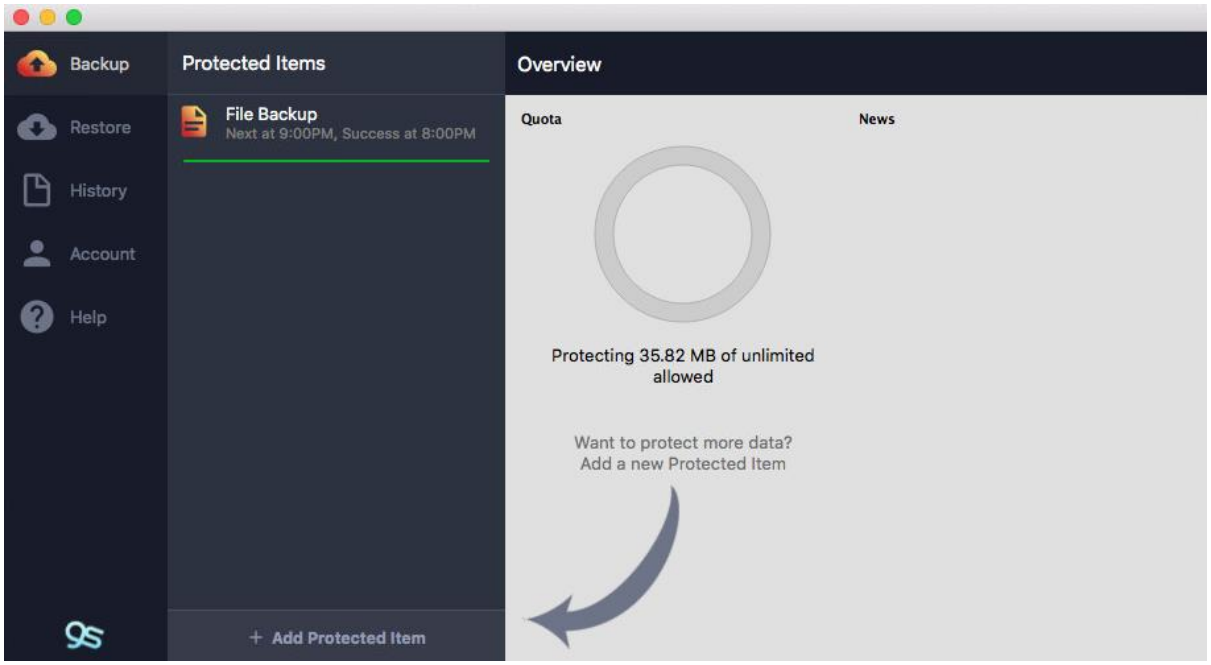
In this example, we will select all backups that were successful called important documents that were backed up to the Gigasoft Data Backup vault from this machine, in this example only one job has been returned as there has only been the one successful job on this test machine.



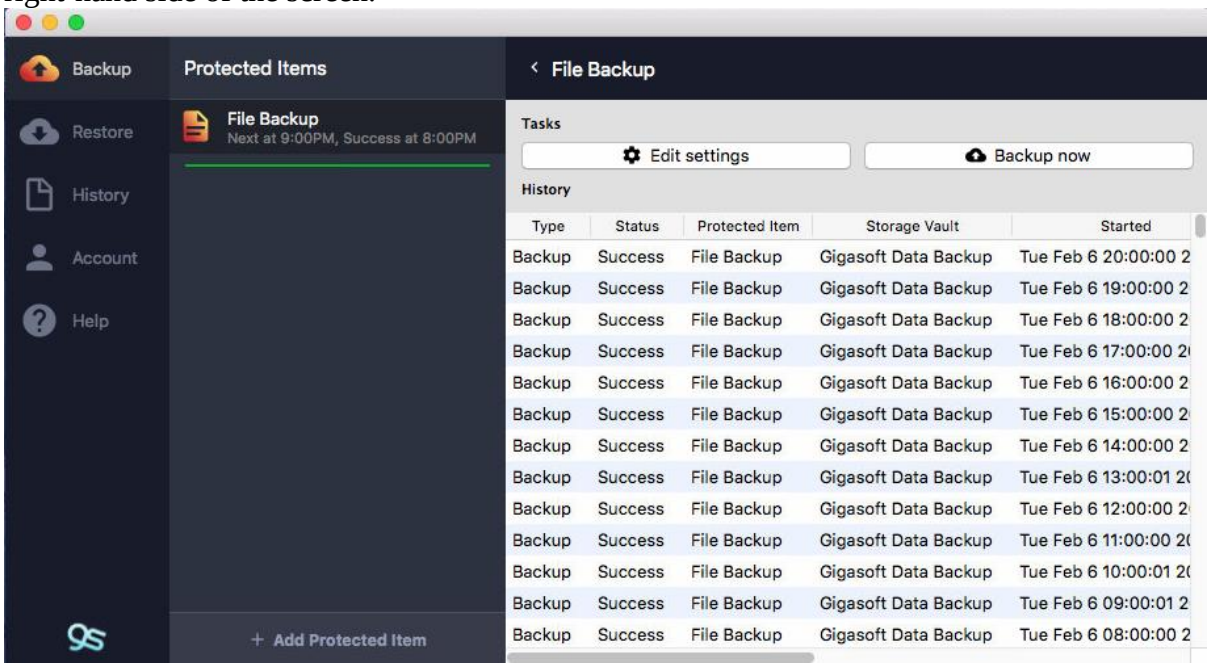
Click the **[Backup]** tab to view the dashboard again.

9.2 The history tab (MacOS)

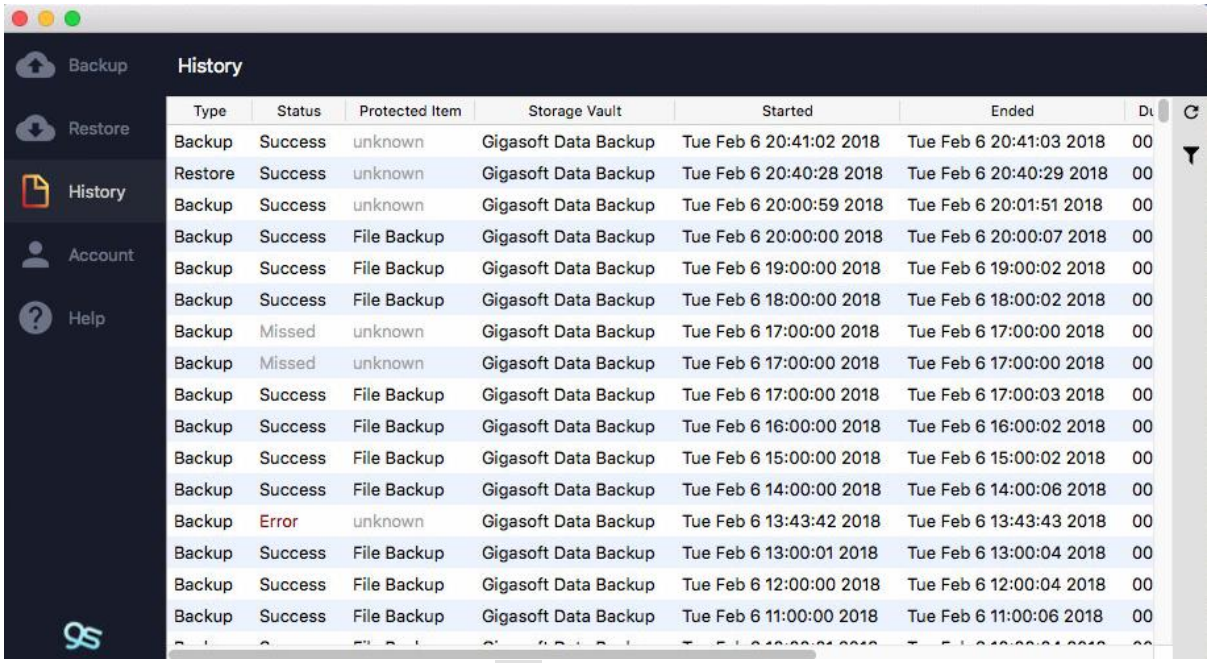
Log into the Gigasoft Backup client and you will be presented with the dashboard



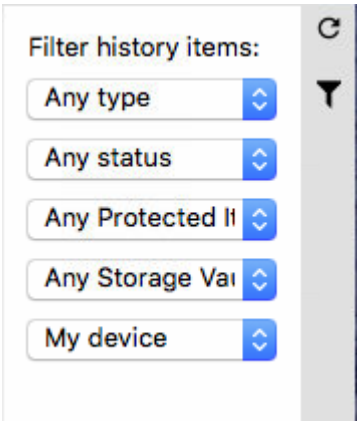
If you click on one of the Protected items you will see the recent activity of this item on the right-hand side of the screen.



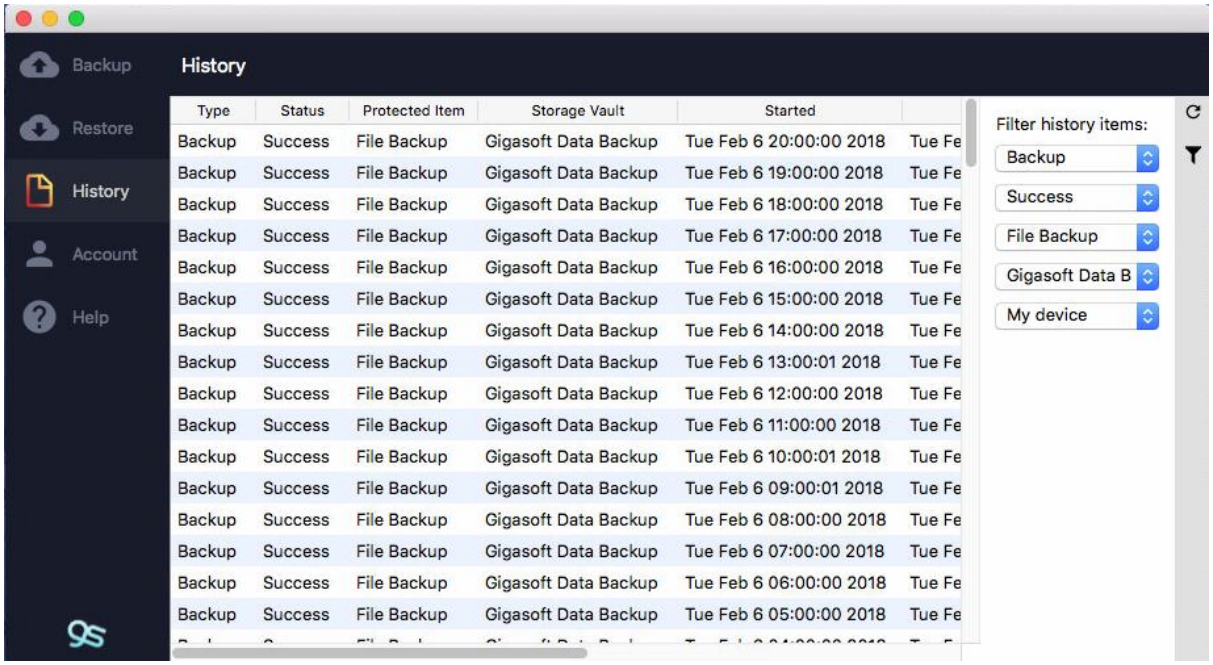
If you now click the **[History]** tab on the left of the client you will be shown the history of the account, any Protected items that run on this machine will be listed as well as unknown ones that relate to other machines on the account (we will cover this a bit more in the account tab section)



From this screen you can apply filters to sort the columns



In this example, we will select all backups that were successful called File Backup that were backed up to the Gigasoft Data Backup vault from this machine, in this example you can see multiple jobs have been returned this is because on this test machine we ran the job every hour.



Click the **[Backup]** tab to view the dashboard again.

9.3 The history tab (Linux)

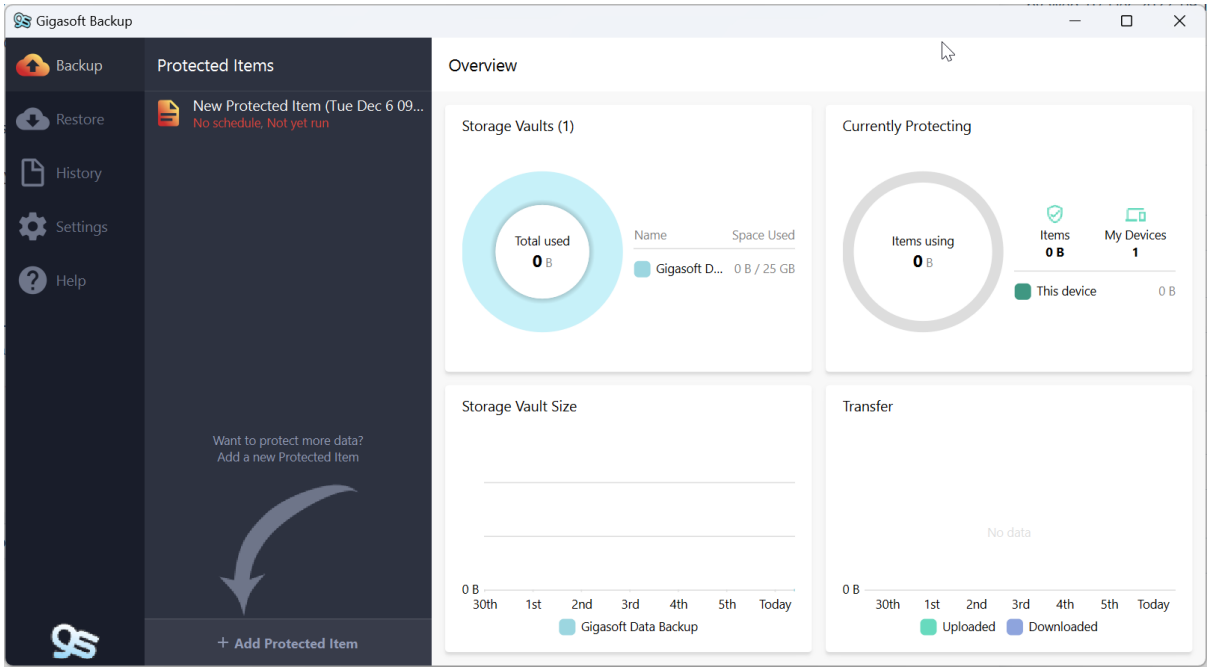
As this version is command only there is no history information available, this will become available via the customer portal once it is released.

10 The account tab

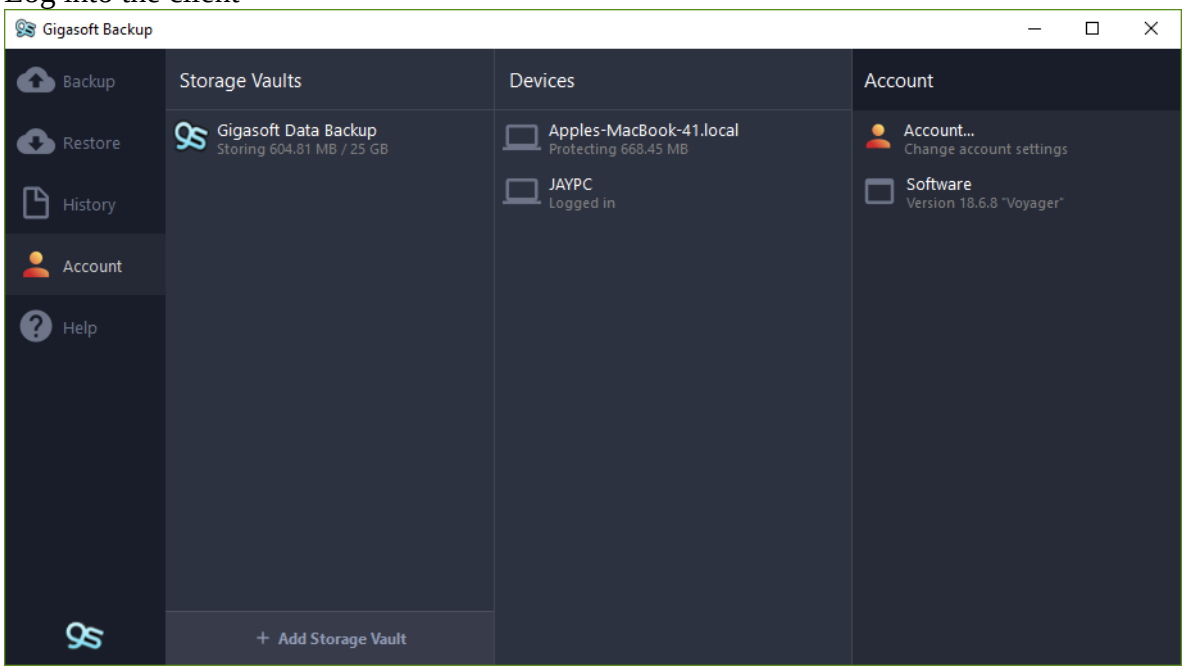
In this section we will explain what the account tab does and how it is used in each of the different client versions.

10.1 Account tab (windows)

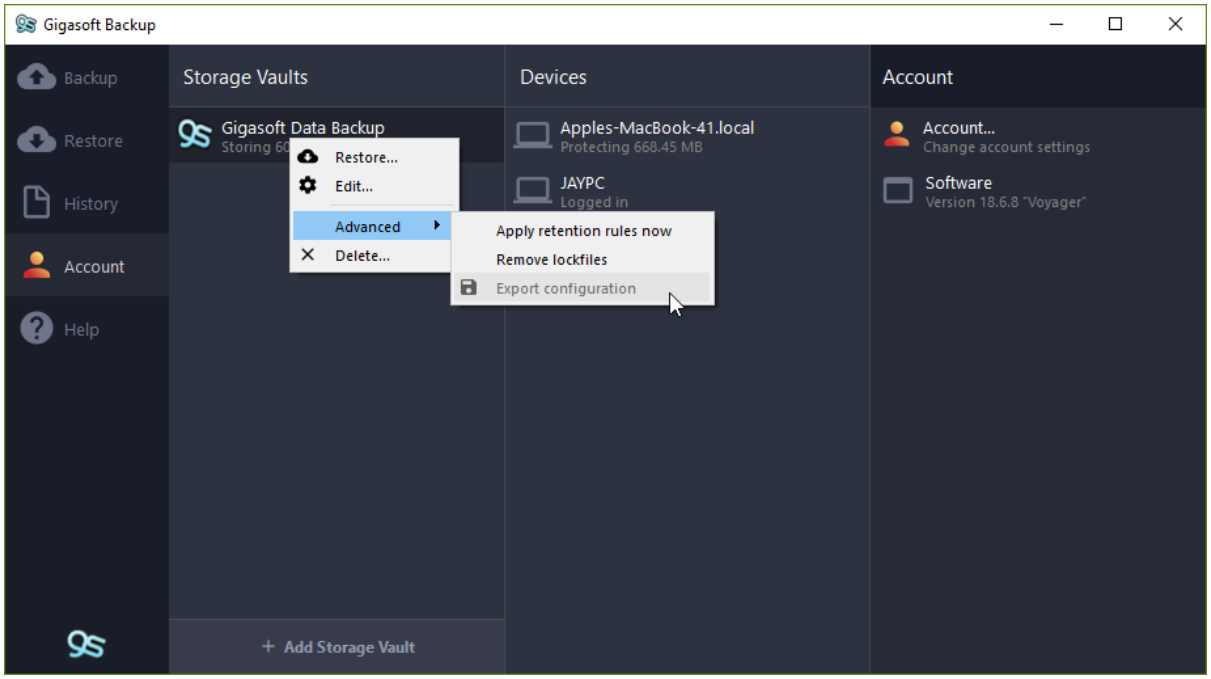
This section of the guide explains what the Account tab is used for. From here we can perform tasks on the storage vaults as well as change the account password and report email address.



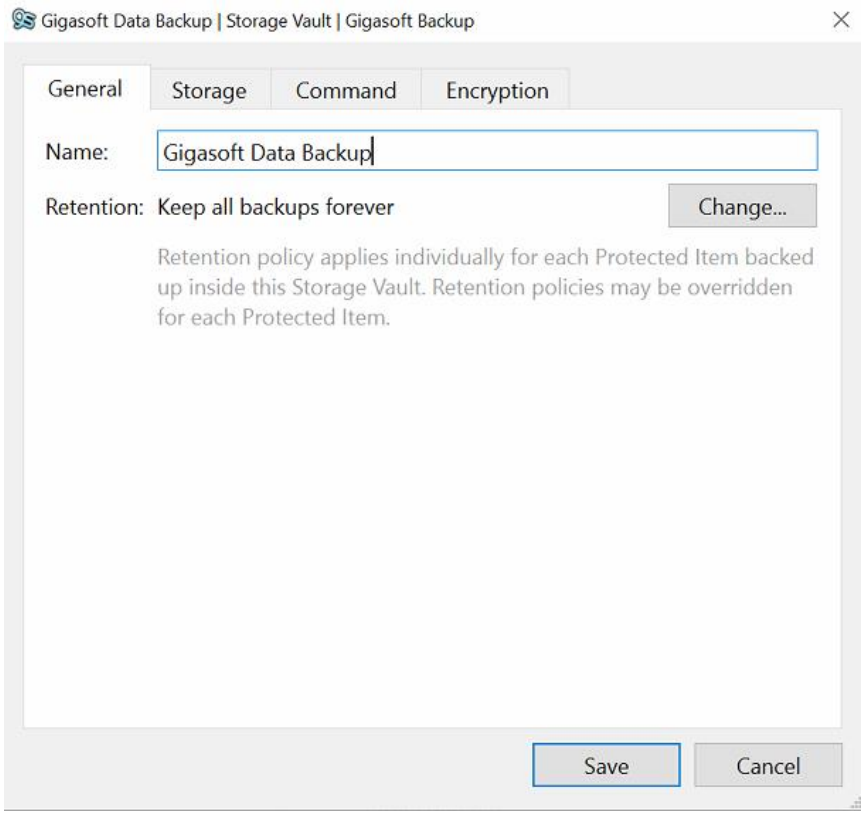
Log into the client



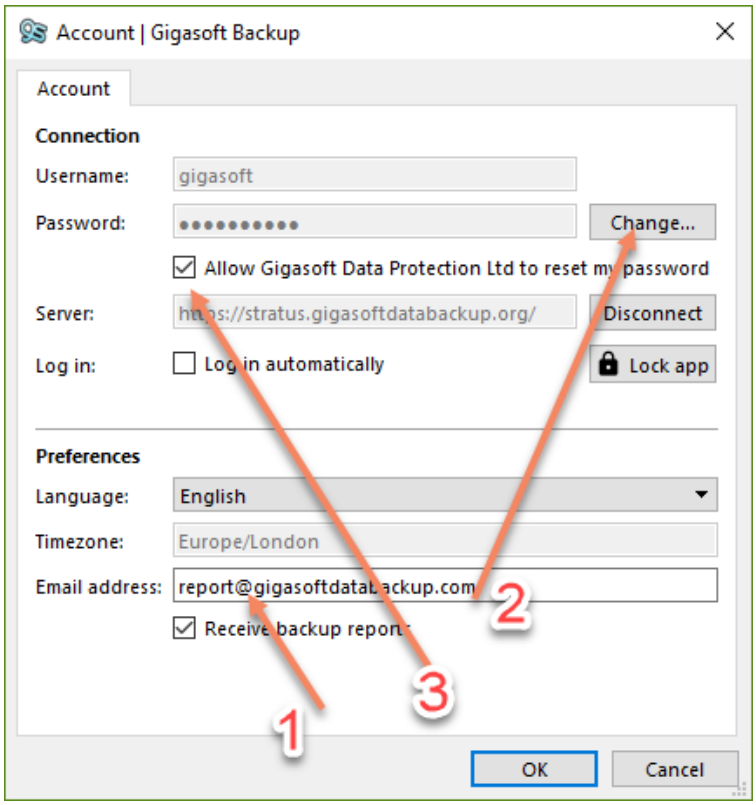
Select the **[Account]** tab



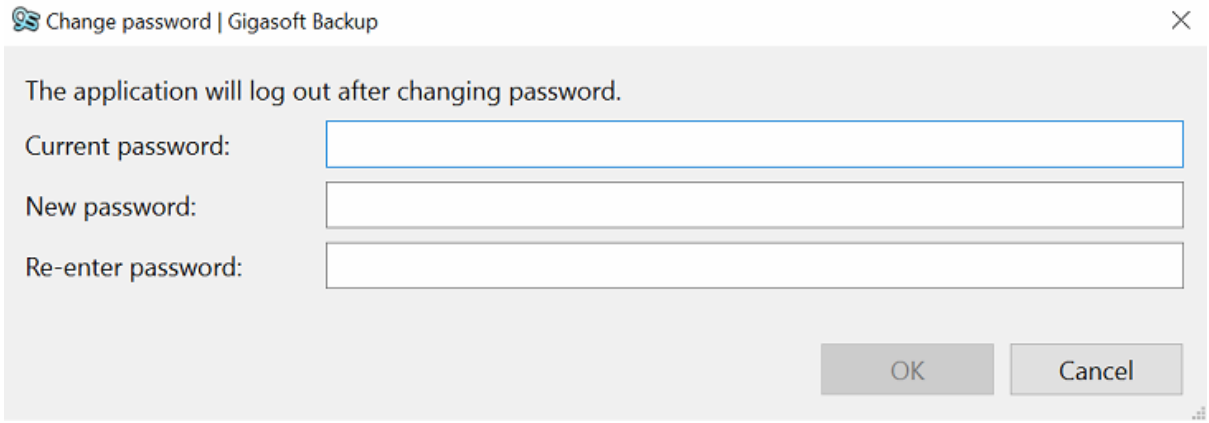
Right clicking on the Storage vault allows you to perform some administration tasks if needed, here we can apply retention rules now, this allows us to clear up the retention area and clear out any jobs that are no longer needed that have not yet been cleared by the retention pass after each backup job. We can also remove lock files should the storage vault become locked by a process (caution this can cause data loss if incorrectly run so please speak to support before using)



You can also edit some of the vault details (it's not recommended to make changes here as this can cause issues to your protected item schedules.)



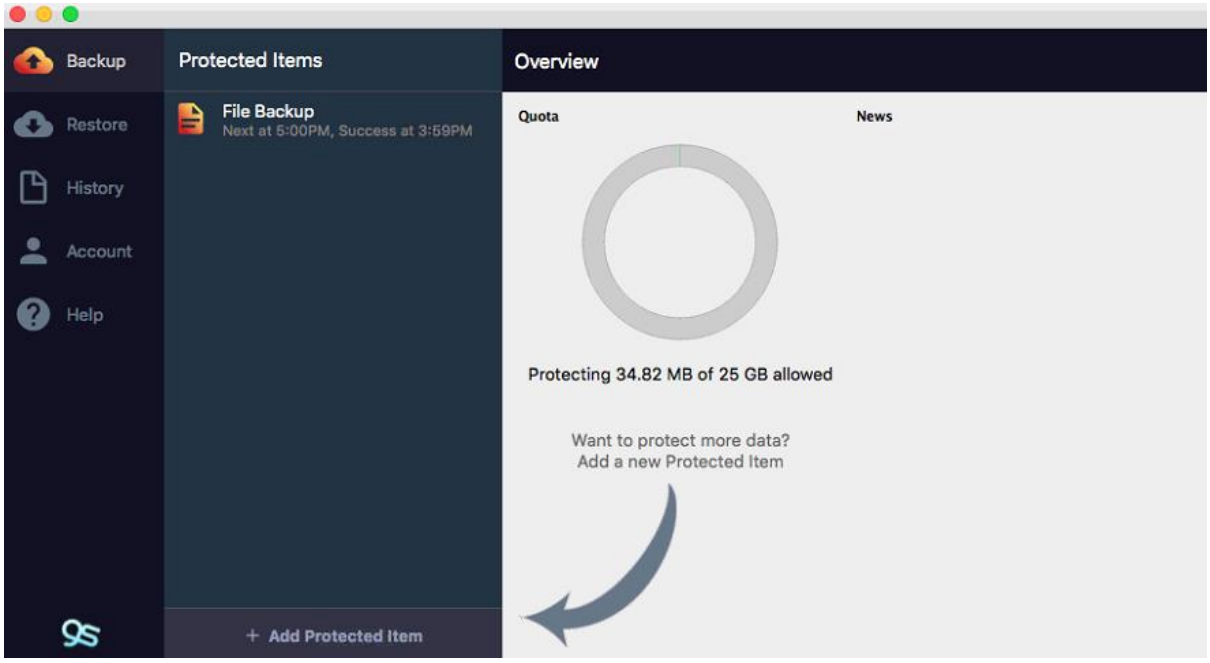
Here you can change the email address that receives the backup reports (1) you can also change your password (2 see below) and allow us to change your password should you forget it (3) in the event you do forget your password and the software is not logged in please contact support and we can generate a new password for you which you can then change once you log back in (2)



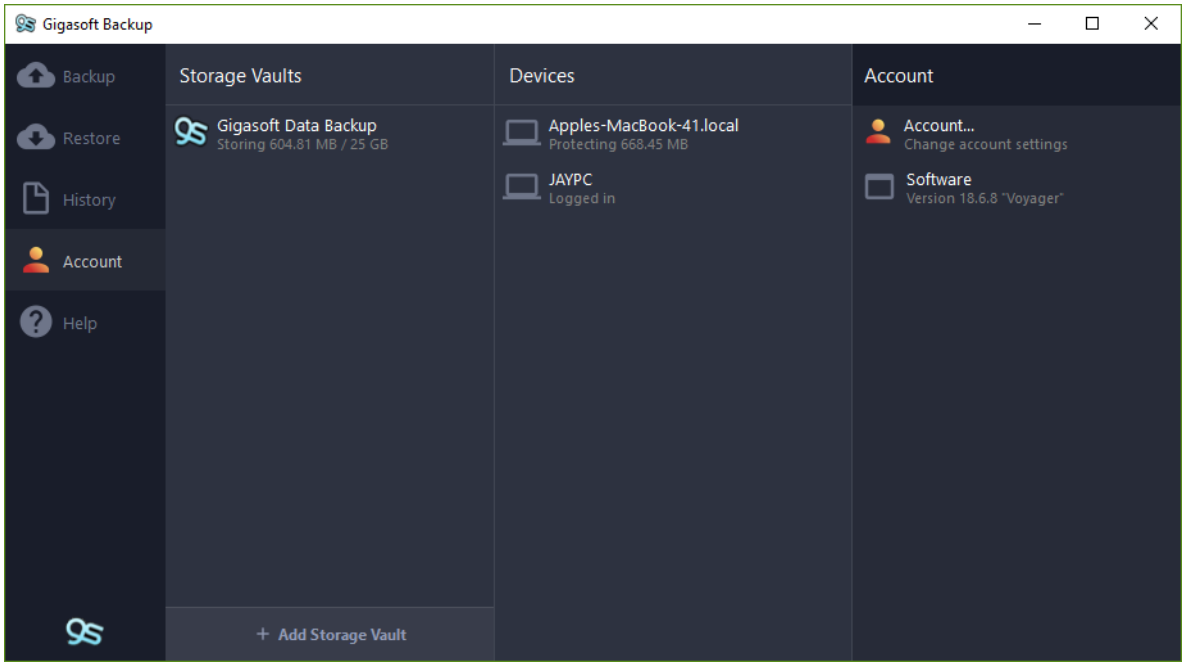
Clicking **[Change]** next to the password allows you to change the password for the account, this does not change the Encryption key

10.2 Account tab (MacOS)

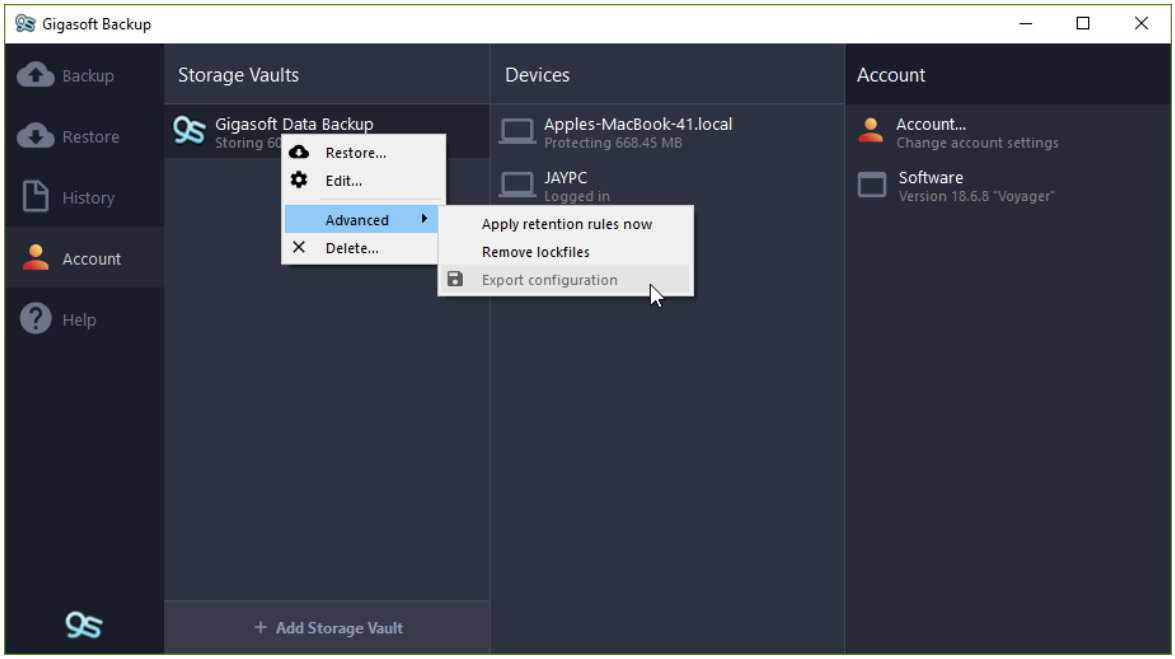
This section of the guide explains what the Account tab is used for. From here we can perform tasks on the storage vaults as well as change the account password and report email address.



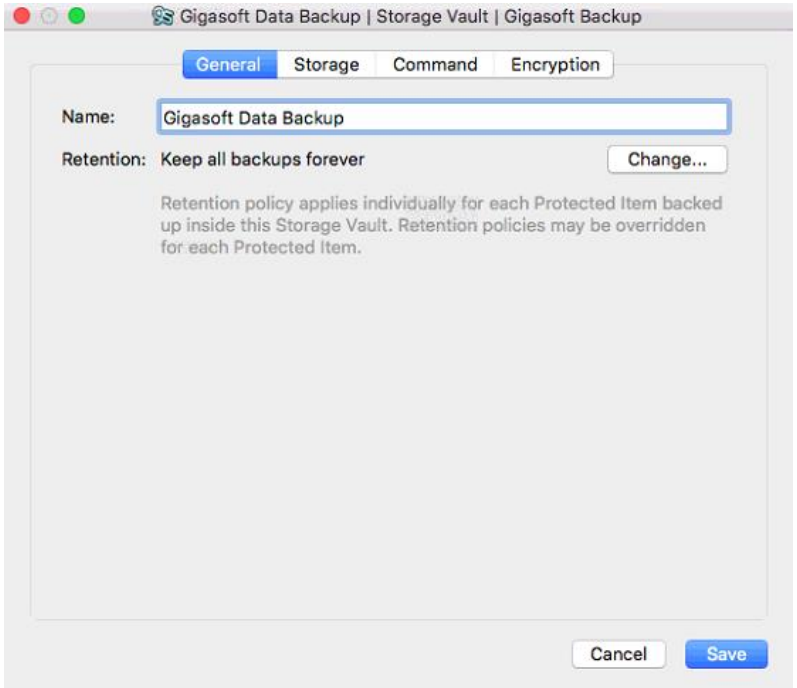
Log into the client



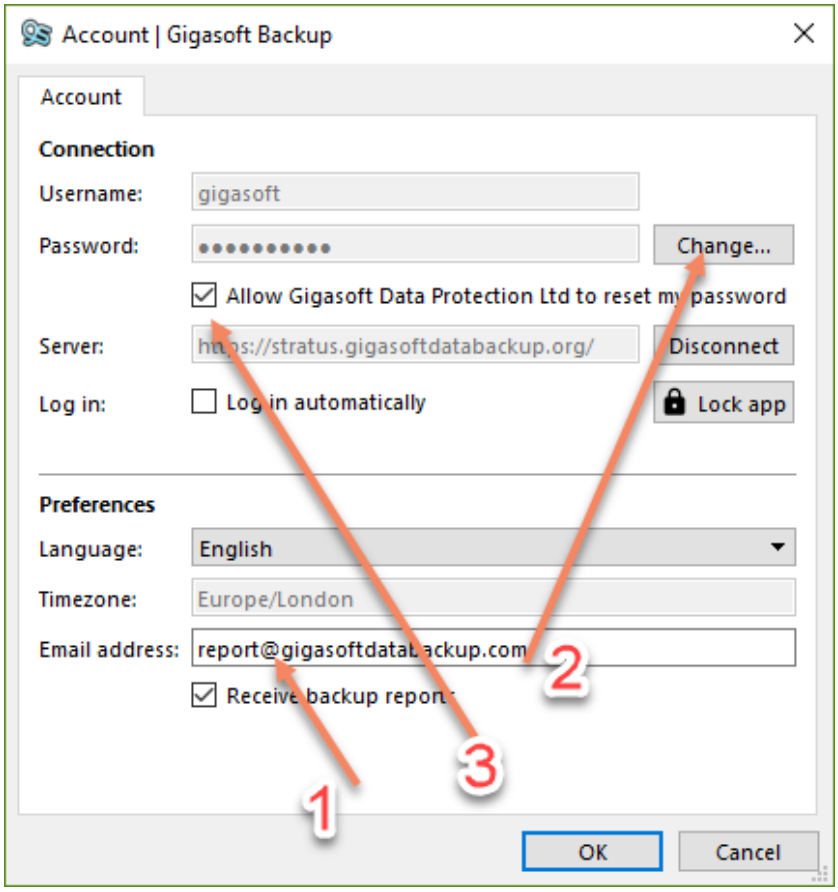
Select the **[Account]** tab



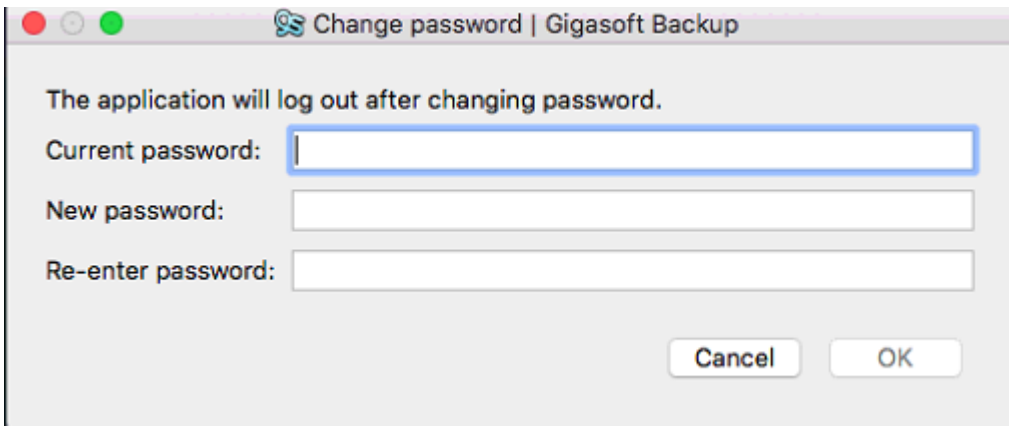
Right clicking on the Storage vault allows you to perform some administration tasks if needed, here we can apply retention rules now, this allows us to clear up the retention area and clear out any jobs that are no longer needed that have not yet been cleared by the retention pass after each backup job. We can also remove lock files should the storage vault become locked by a process (caution this can cause data loss if incorrectly run so please speak to support before using)



You can also edit some of the vault details (it's not recommended to make changes here as this can cause issues to your protected item schedules.)



Here you can change the email address that receives the backup reports (1) you can also change your password (2 see below) and allow us to change your password should you forget it (3) in the event you do forget your password and the software is not logged in please contact support and we can generate a new password for you which you can then change once you log back in (2)



Clicking **[Change]** next to the password allows you to change the password for the account, this does not change the Encryption key

10.2 Account tab (Linux Command Line)

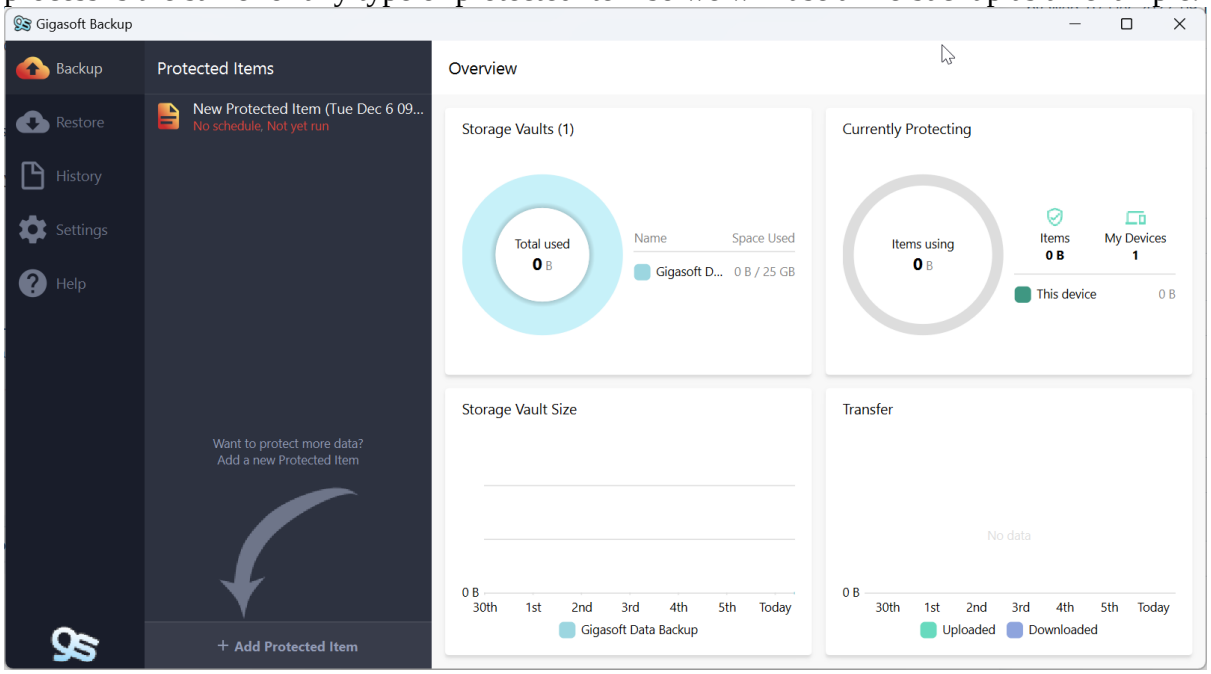
There is no account tab option in the command line version, you can find this information via the customer portal.

11 Running a backup manually

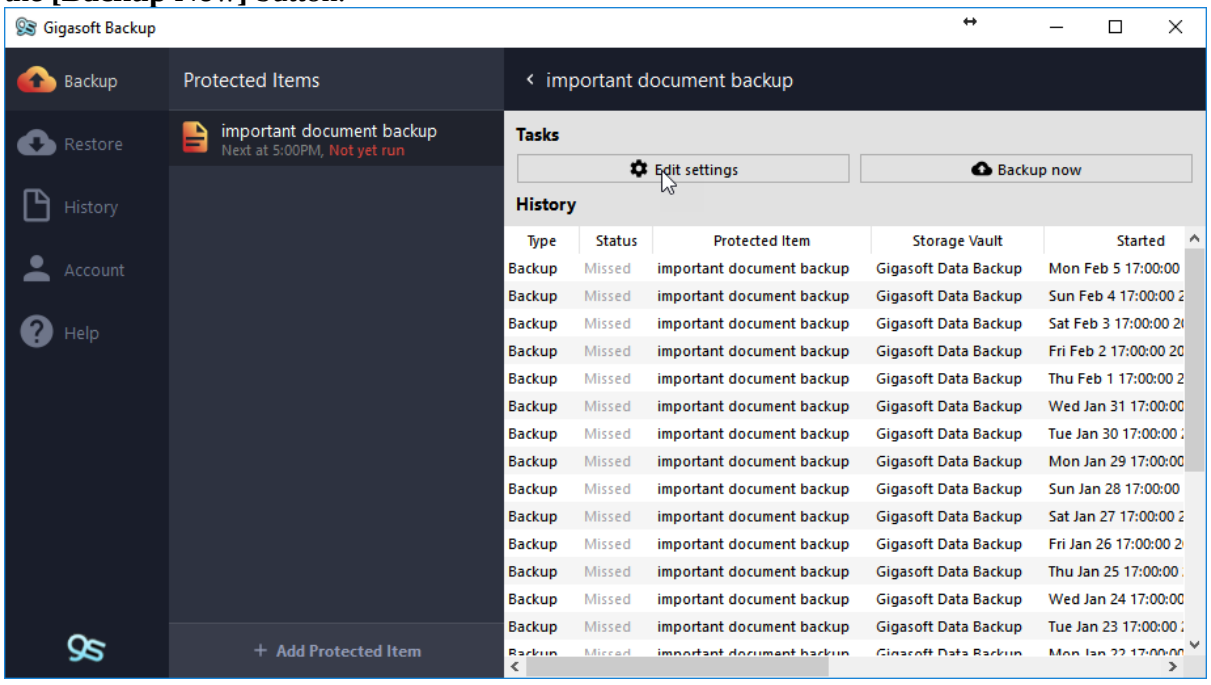
In this section we will walk you through the process of running a manual file backup should you need to on the different versions of the client, the process is similar for other types of protected items.

11.1 Running a backup manually (Windows)

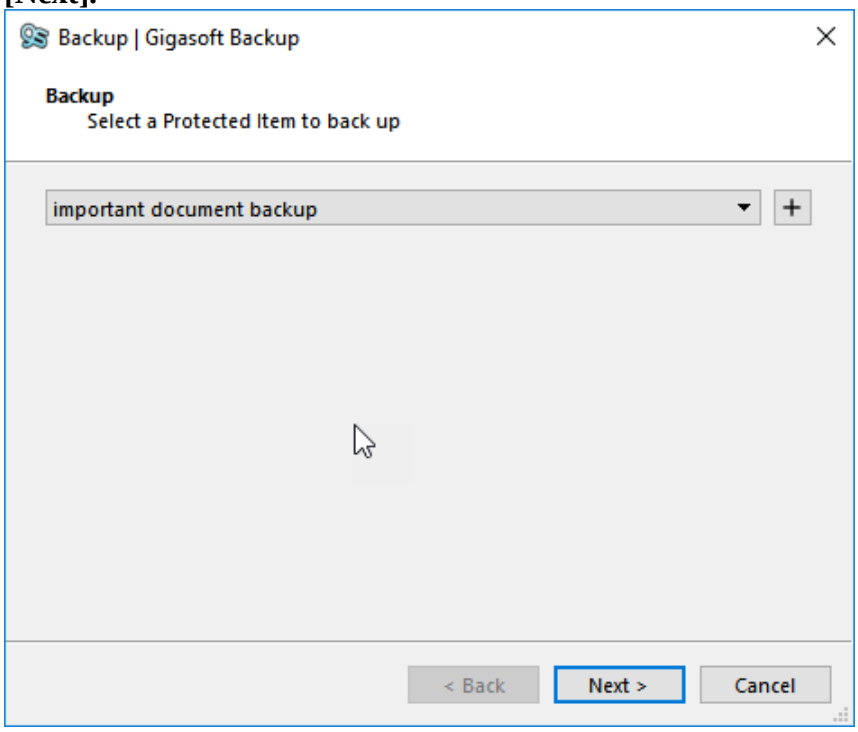
In this section we will guide you through the process of running a backup manually, the process is the same for any type of protected item so we will use a file backup as an example.



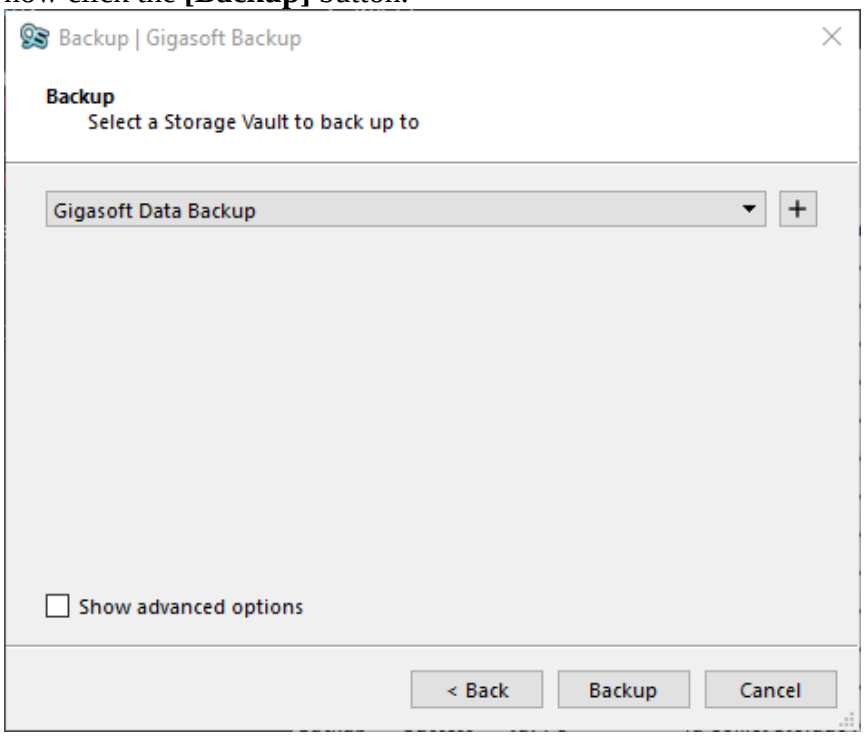
Firstly, login to the Gigasoft Backup software on the client machine and then click on a protected item name, this will open the tasks page, on the Right-hand side of the screen click the **[Backup Now]** button.

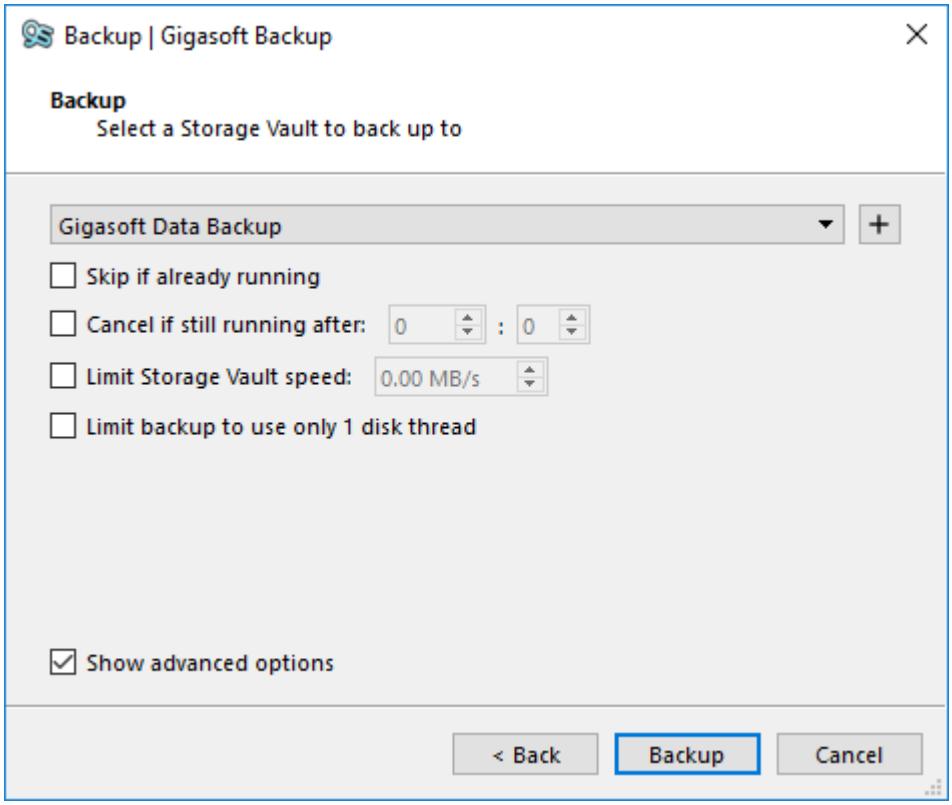


On the next screen select the name of the protected item you wish to backup now and click **[Next].**



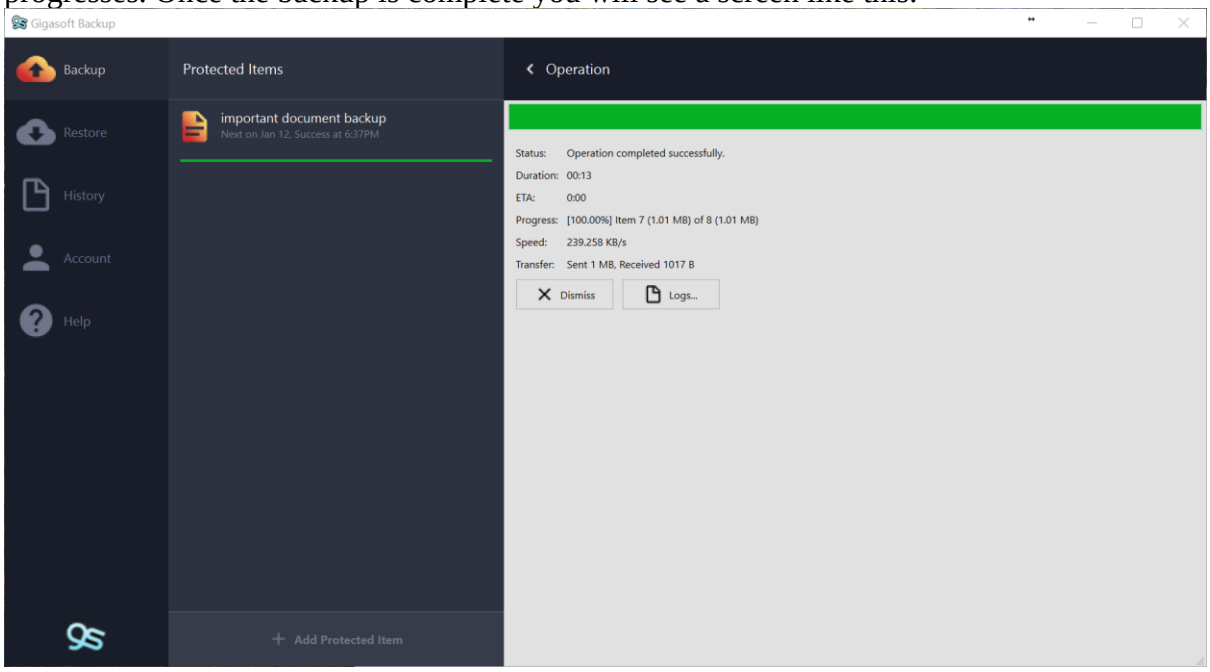
This screen will ask you where you would like to store this backup, if this is an offsite backup select **[Gigasoft Data Backup]** if this is a local backup select the name of your local vault, now click the **[Backup]** button.





If you click on the **[Show advanced options]** you get some advanced features for controlling the backup, these include cancelling the backup after X amount of time, limiting the upload speed and also allowing the client to only use a single disk thread which is ideal for busy machines.

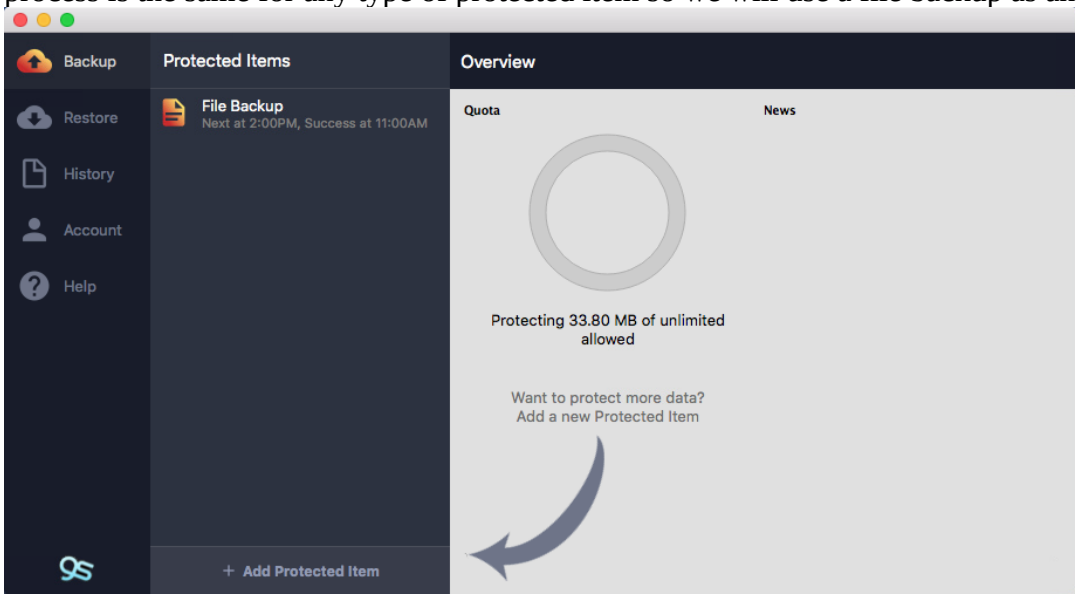
Your backup will now start and you will see the green progress bar increase as the backup progresses. Once the backup is complete you will see a screen like this.



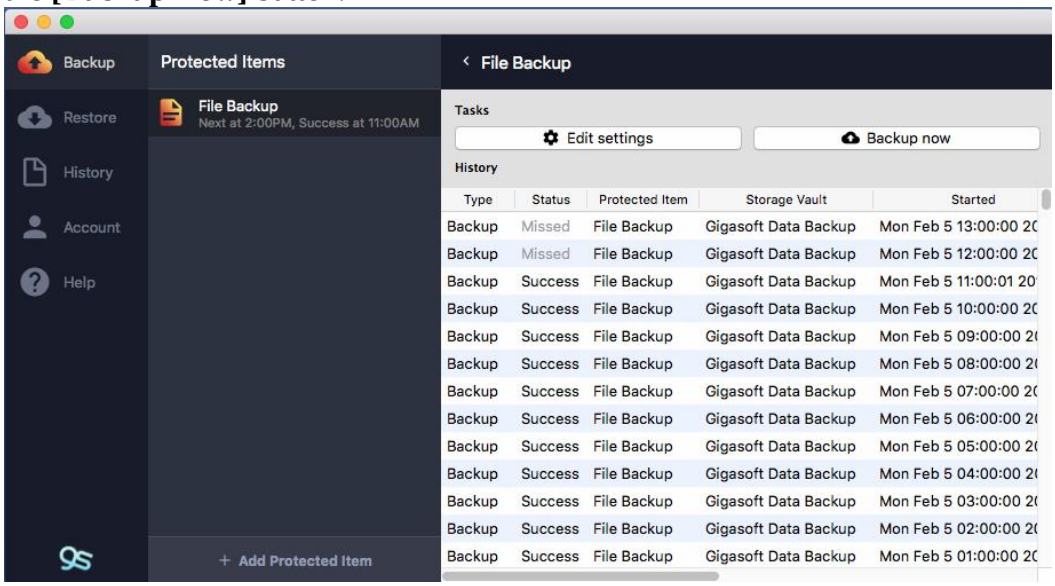
To finish click the **[Dismiss]** button and you will be returned to the main dashboard.

11.2 Running a backup manually (MacOS)

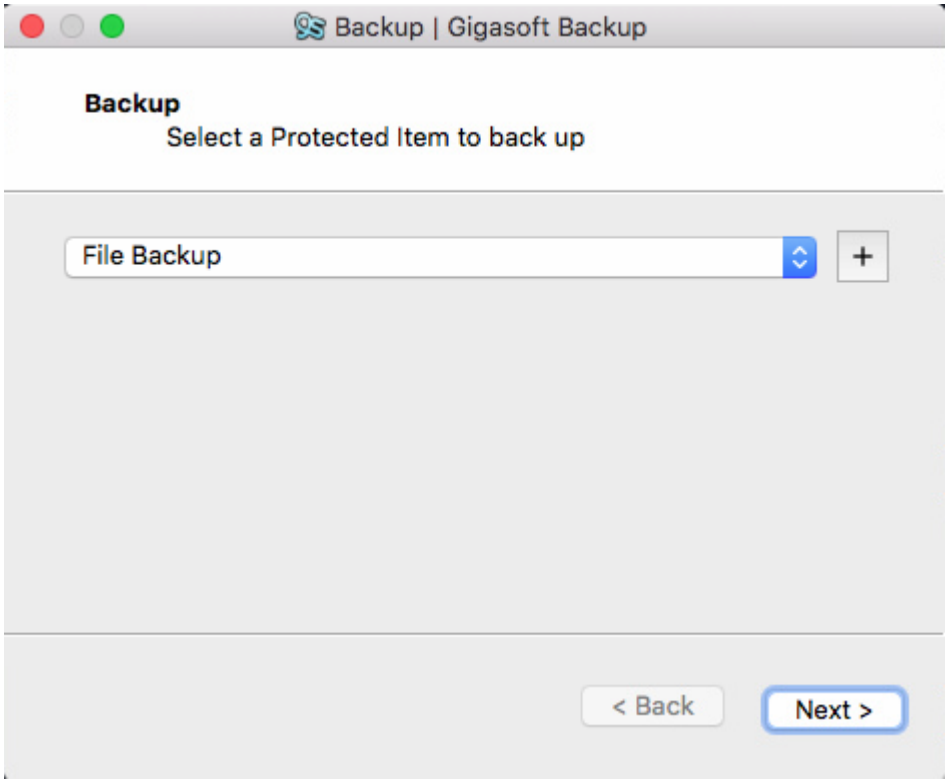
In this section we will guide you through the process of running a backup manually, the process is the same for any type of protected item so we will use a file backup as an example.



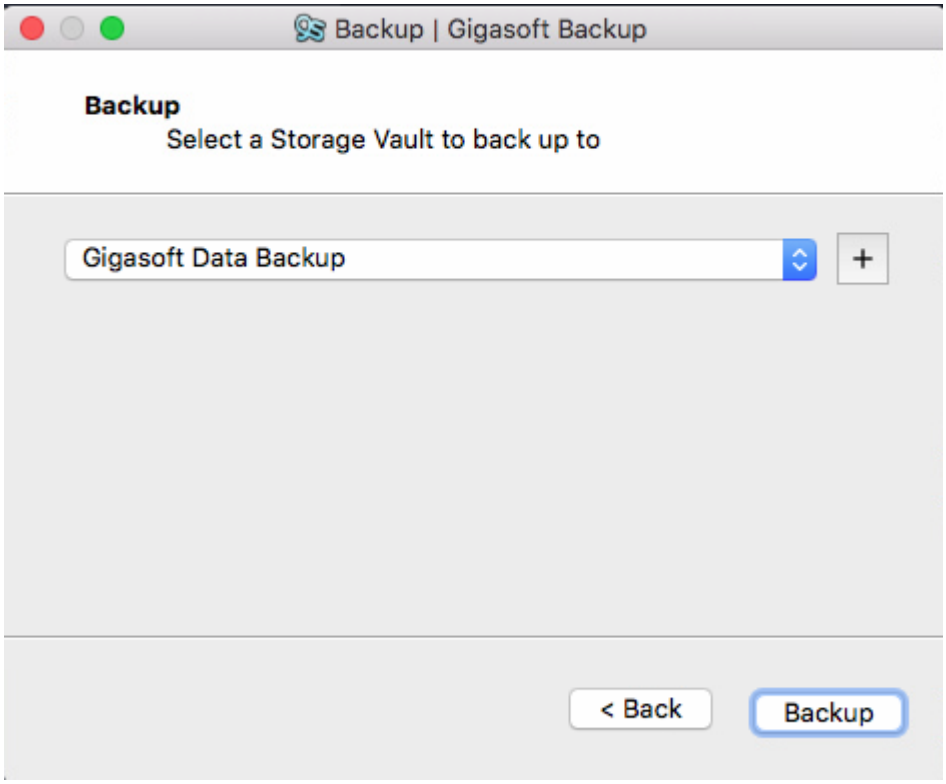
Firstly, login to the Gigasoft Backup software on the client machine and then click on a protected item name, this will open the tasks page, on the Right-hand side of the screen click the **[Backup Now]** button.



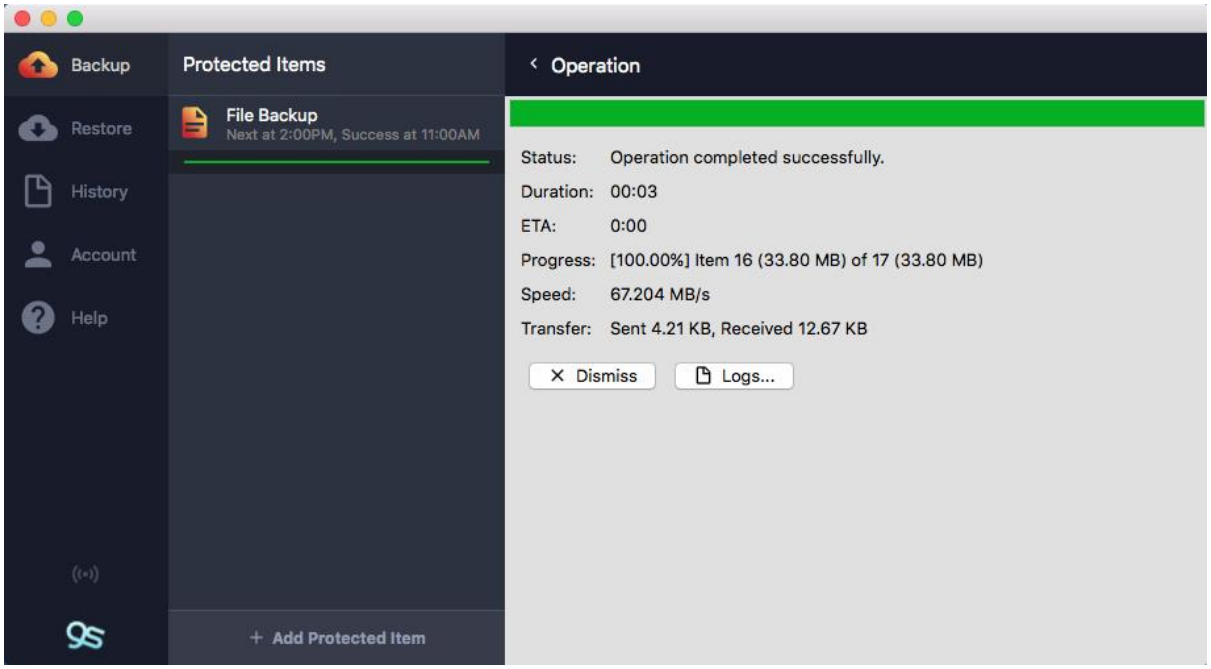
On the next screen select the name of the protected item you wish to backup now and click **[Next].**



This screen will ask you where you would like to store this backup, if this is an offsite backup select **[Gigasoft Data Backup]** if this is a local backup select the name of your local vault, now click the **[Backup]** button.



Your backup will now start, and you will see the green progress bar increase as the backup progresses. Once the backup is complete you will see a screen like this.



To finish click the **[Dismiss]** button and you will be returned to the main dashboard.

11.3 Running a backup manually (Linux)

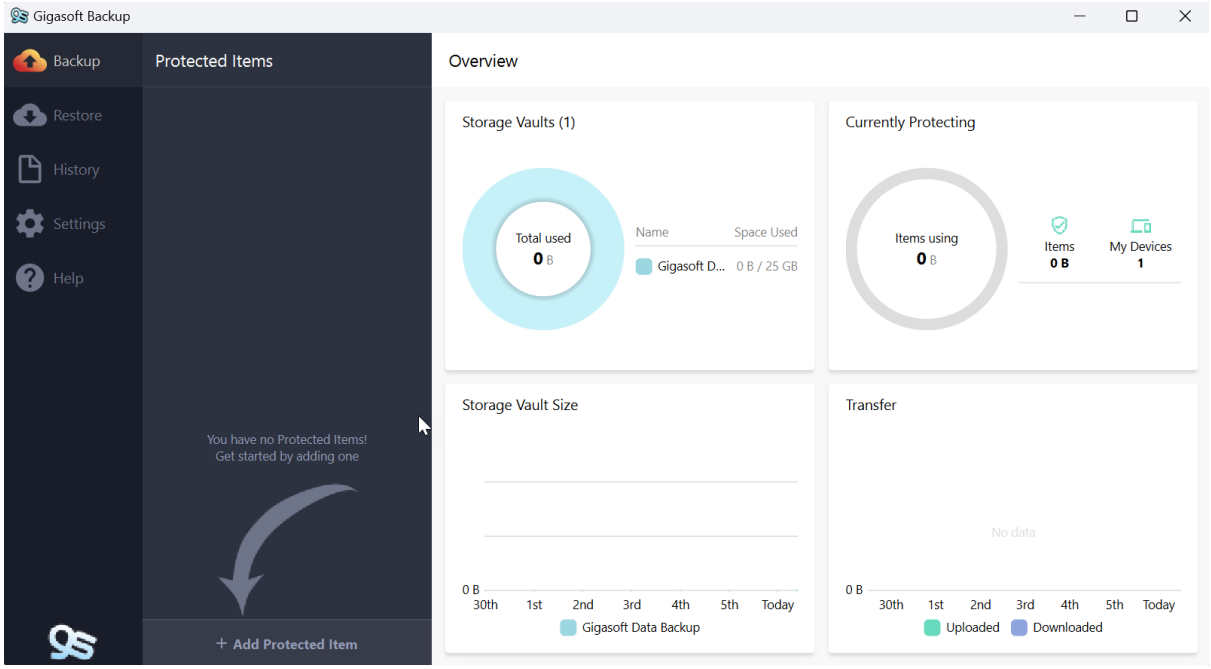
Currently this is not possible to do from the client, but it can be done remotely via the customer portal.

12 Local backups

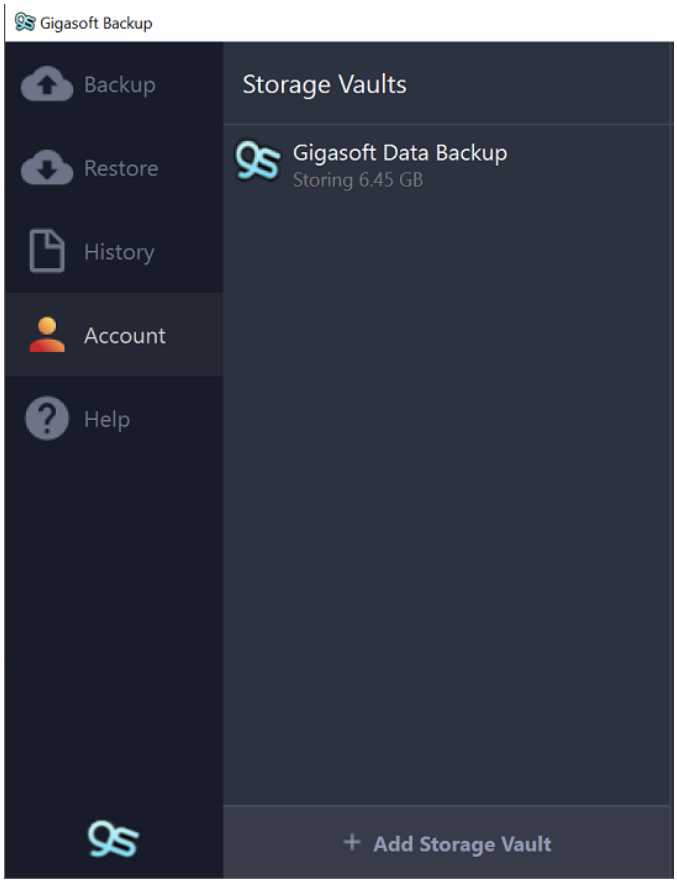
In this section we will cover the basics of creating a local backup, the local backup is useful for storing data locally for fast retrieval or for non-critical data that you do not need to store offsite.
The process is very similar to an offsite backup but we need to change the storage vault to a local drive or network share.

12.1 Windows

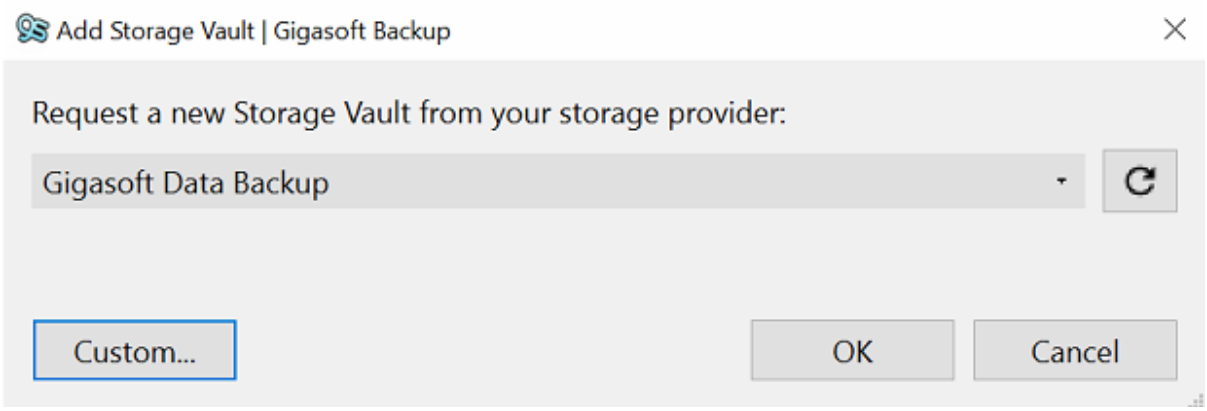
Performing a local backup is very similar to an offsite backup but first we need to create the local vault.



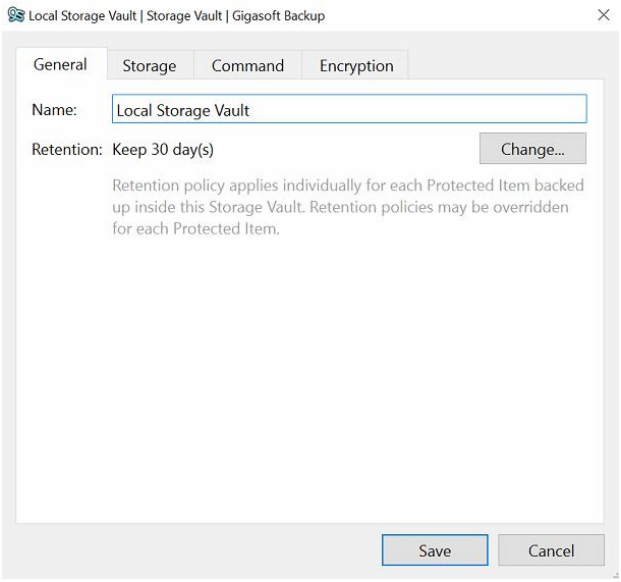
Firstly, log into the Gigasoft Backup Manager.



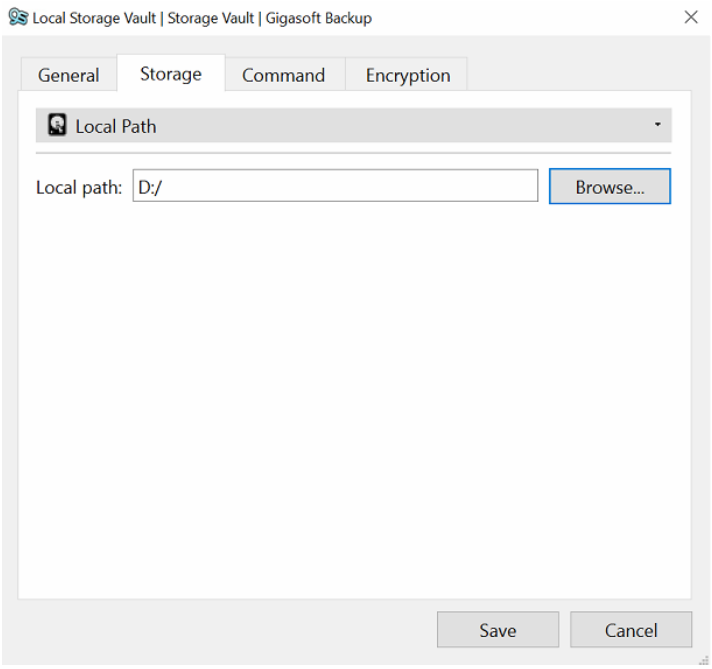
Now click on the **[Account tab]** and select **[+ Add Storage Vault]** button at the bottom of the page.



On this screen you will be presented with an option to request a new vault from the storage provider, in this case please click the **[Custom]** button.



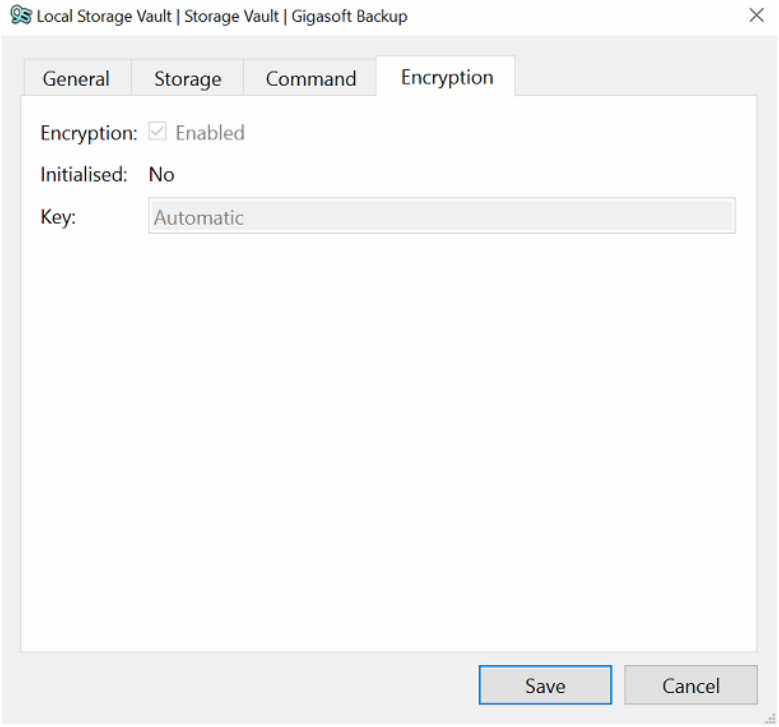
In the Name field give your local storage vault a memorable name to help identify it, in our example we have used *Local Storage Vault*, click **[Change]** to change the default retention policy if you wish, this is overridden by the protected item policy so it's not important at this stage. Click on the **[Storage]** tab.



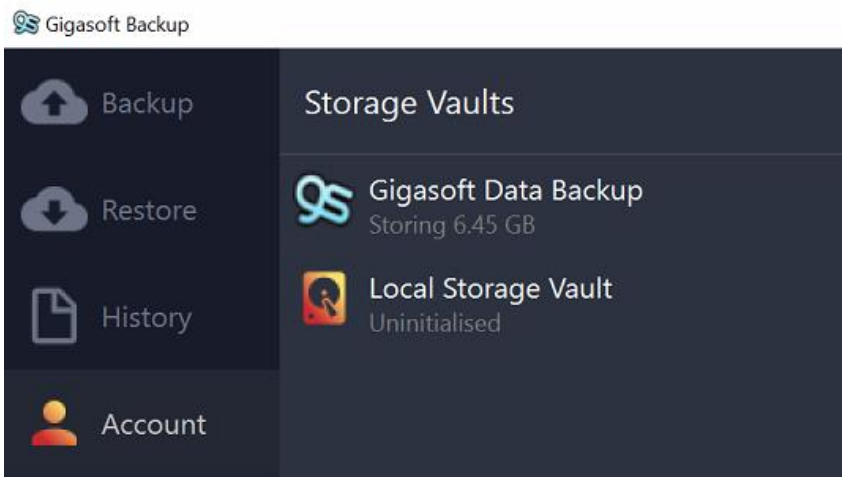
From the drop-down list select ***Local Path*** and then click the **[Browse]** button to open an explorer window to help choose where you would like to store your data locally, this would ideally be a locally attached disk, removable hard drive or a network storage device. In our example we have selected a removable drive **D:**

You can run commands at the storage level if needed but these are not normally needed.

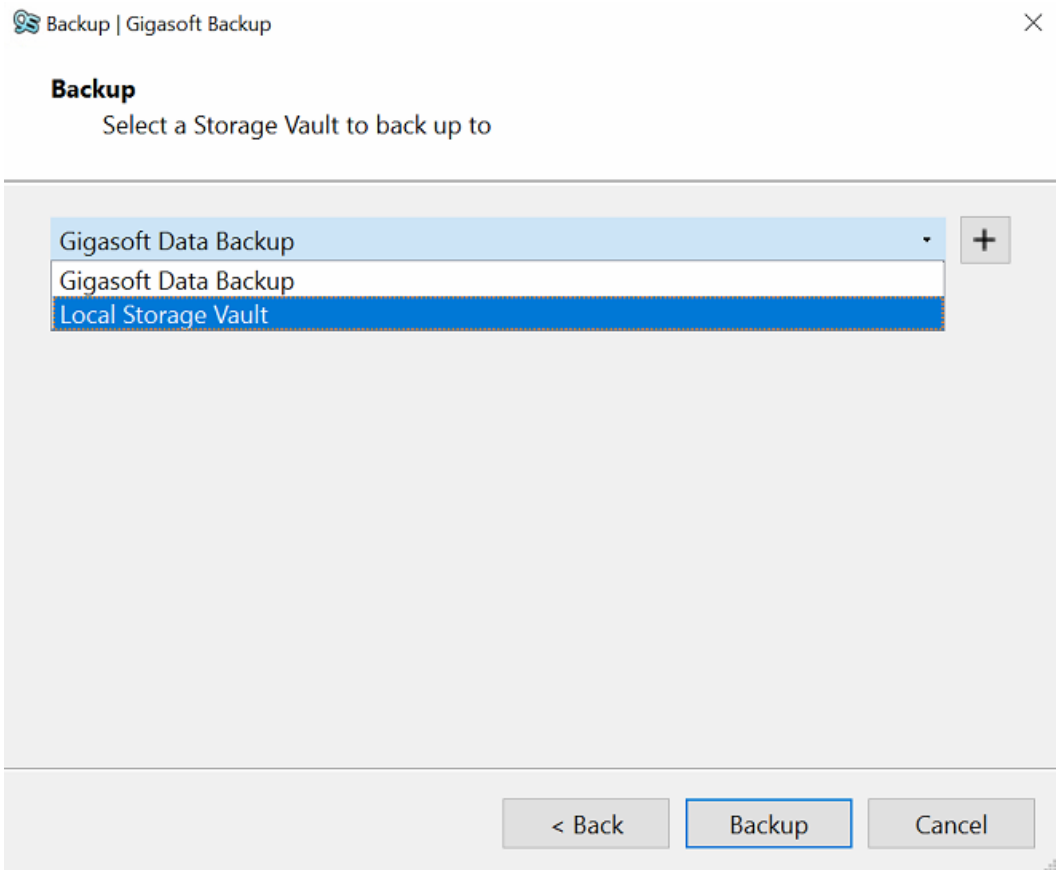
On the Encryption tab you can see the encryption key is set to automatic, the system takes care of this for you so there is no need to try and remember a complex encryption key, the encryption key is different to your password and is only know by the client software.



Click on the **[Save]** button to create the Local vault.



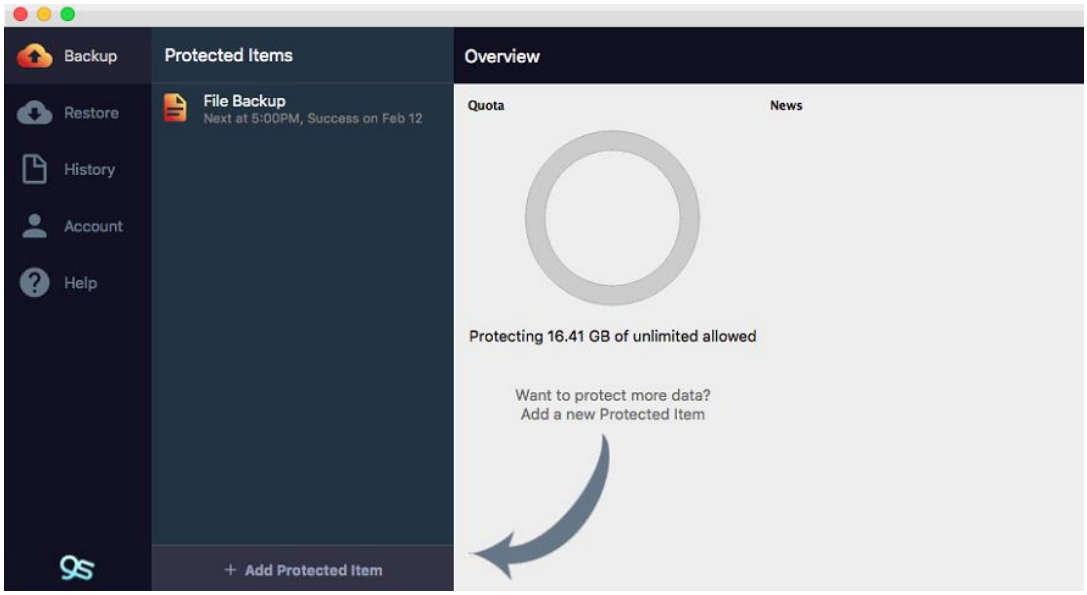
You will now see that you have two vaults, one is offsite and one is your local vault, you can store data to either device.



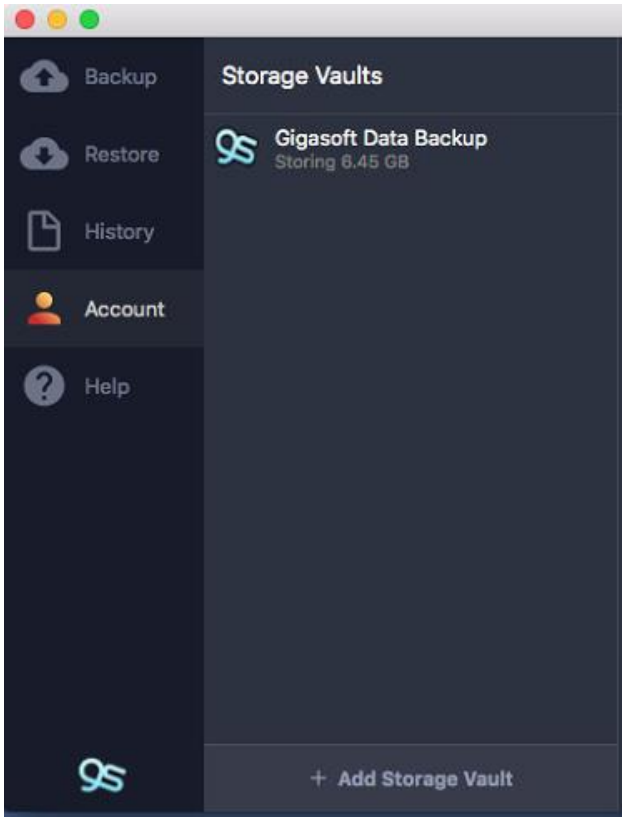
When creating protected items, you will be able to choose from the drop down which vault you would like the data to be stored on or you can create multiple schedules so that your data is backed up in both locations if you wish, you are also able to select the local vault from the manual backup wizard as well.

12.2 MacOS

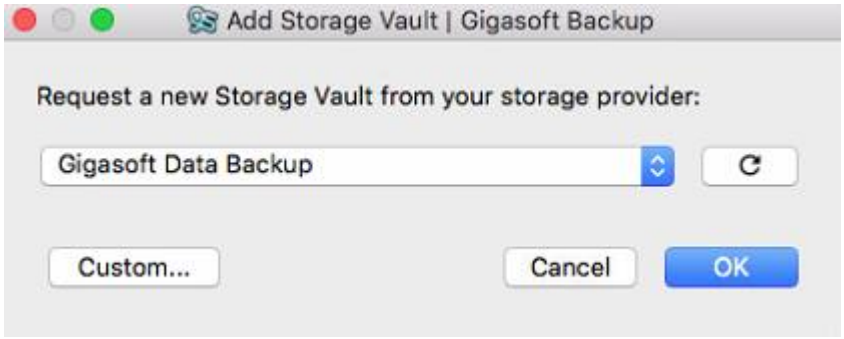
Performing a local backup is very similar to an offsite backup but first we need to create the local vault.



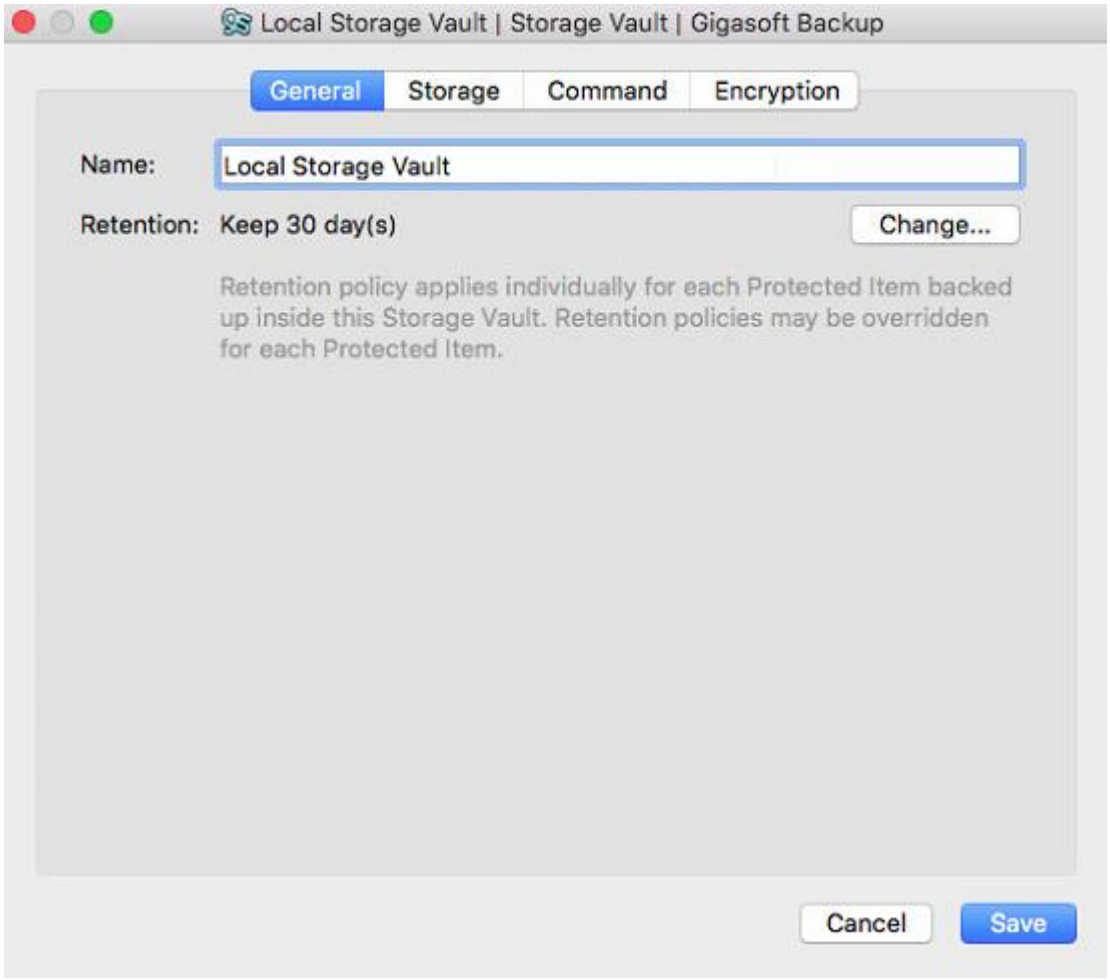
Firstly, log into the Gigasoft Backup Manager.



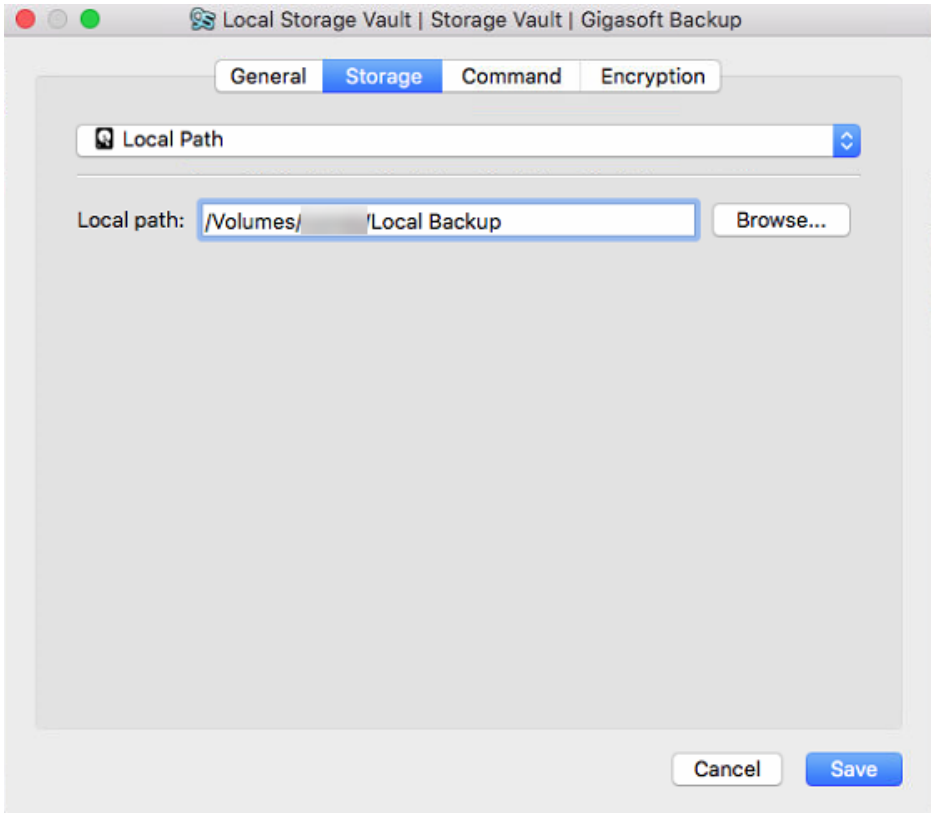
Now click on the **[Account tab]** and select **[+ Add Storage Vault]** button at the bottom of the page.



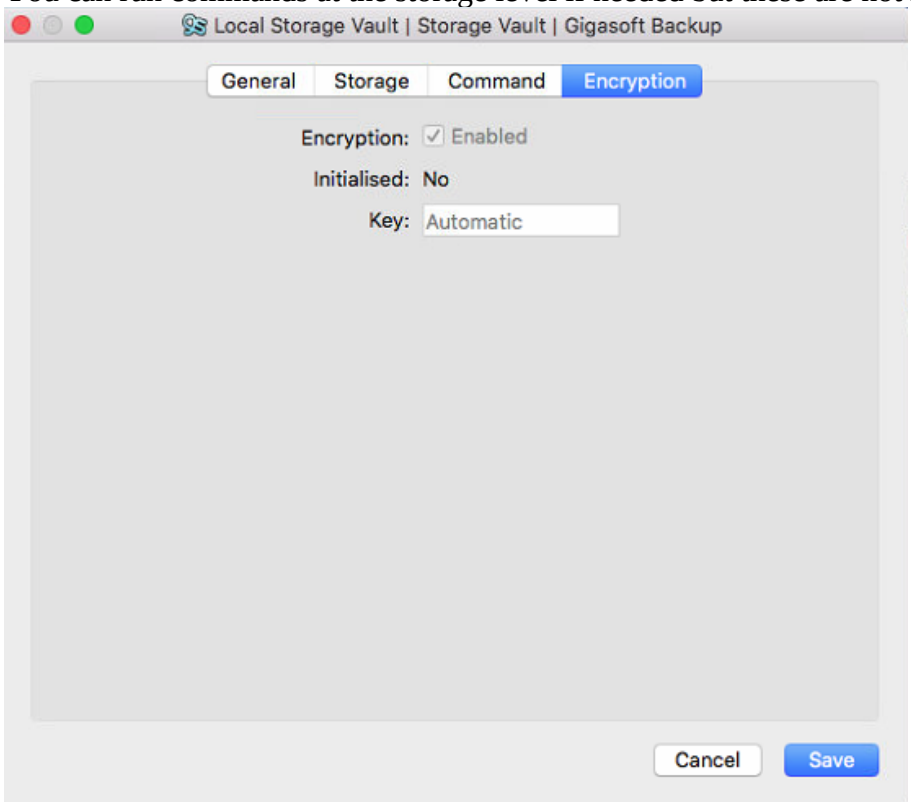
On this screen you will be presented with an option to request a new vault from the storage provider, in this case please click the **[Custom]** button.



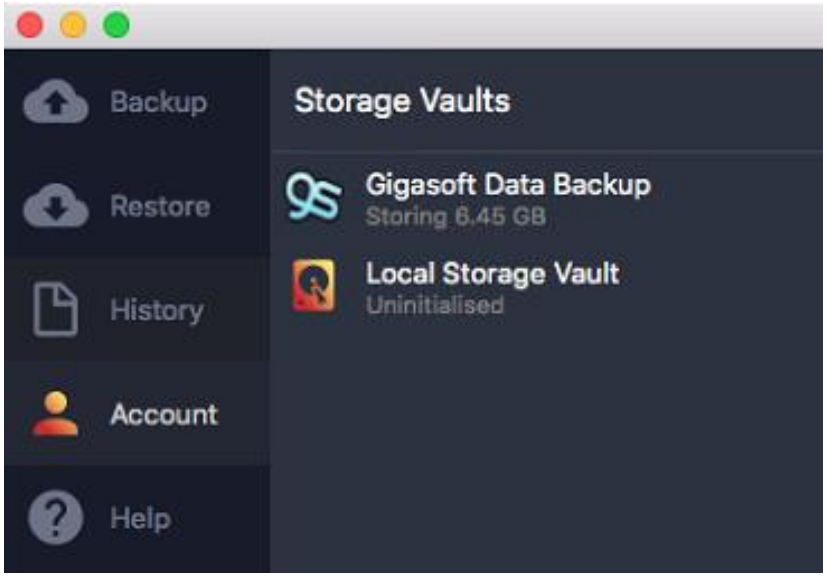
In the Name field give your local storage vault a memorable name to help identify it, in our example we have used *Local Storage Vault*, click **[Change]** to change the default retention policy if you wish, this is overridden by the protected item policy so it's not important at this stage. Click on the **[Storage]** tab.



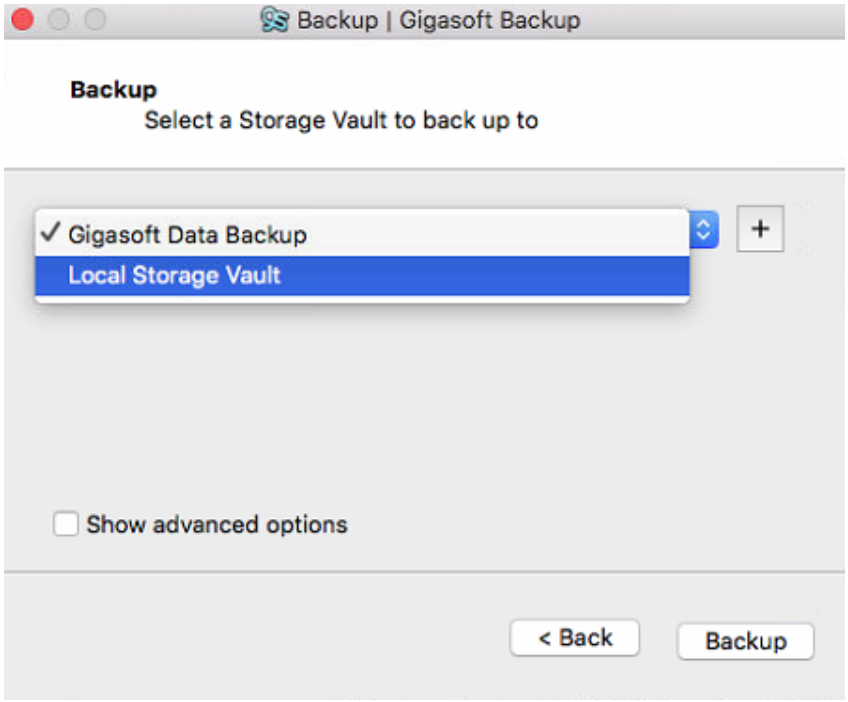
From the drop-down list select ***Local Path*** and then click the **[Browse]** button to open an explorer window to help choose where you would like to store your data locally, this would ideally be a locally attached disk, removable hard drive or a network storage device.
You can run commands at the storage level if needed but these are not normally needed.



On the Encryption tab you can see the encryption key is set to automatic, the system takes care of this for you so there is no need to try and remember a complex encryption key, the encryption key is different to your password and is only know by the client software.
Click on the **[Save]** button to create the Local vault.



You will now see that you have two vaults, one is offsite and one is your local vault, you can store data to either device.



When creating protected items, you will be able to choose from the drop down which vault you would like the data to be stored on or you can create multiple schedules so that your data is backed up in both locations if you wish, you are also able to select the local vault from the manual backup wizard as well.

13 Seed loading data to Gigasoft

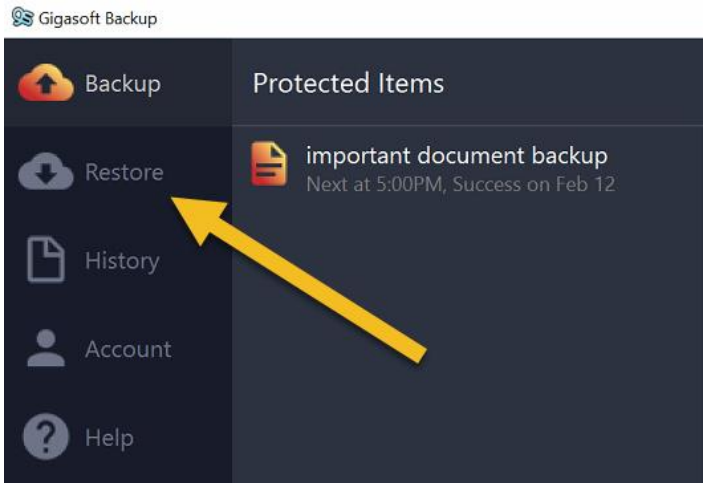
If you have a lot of data that will take too long to upload it is possible to seed the data to our servers, this involves backing up the data locally to one of our seed drives and then shipping this drive to us so we can copy the data over to the servers, this is not something that can currently be done by the end user so please call Gigasoft who can arrange this on your behalf, we will be able to send out the required drive and then with your help remote in to perform the seedload

14 Bulk restore via a Gigasoft Restore Drive

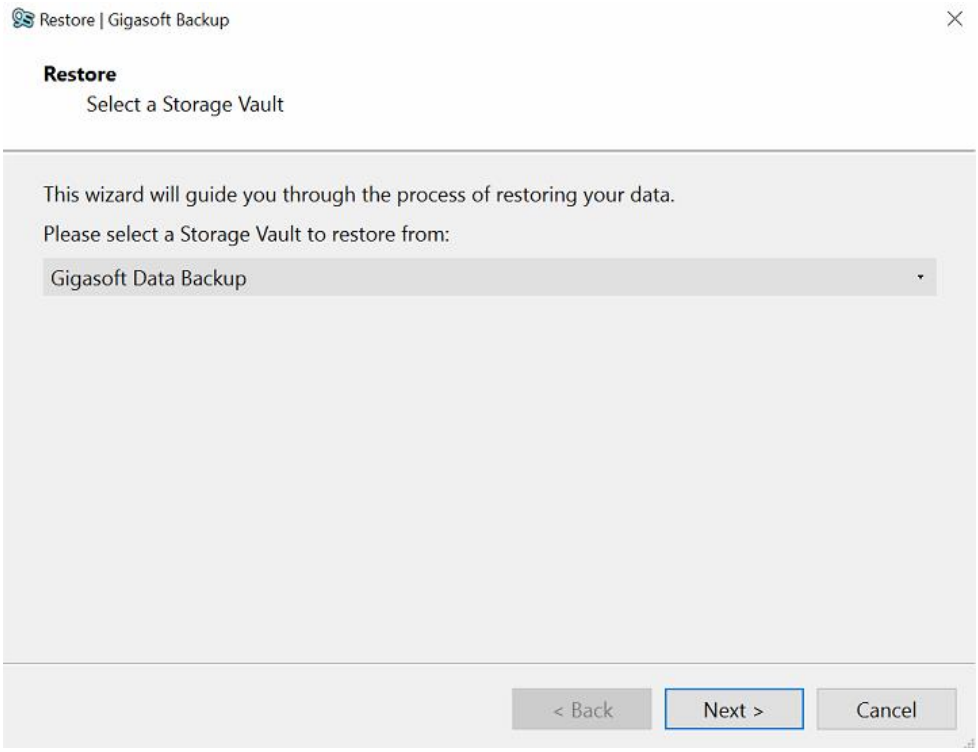
If you have had a total data loss and require a large portion of your data back you can opt for a restore drive. Please call Gigasoft who can arrange this and then ship the encrypted data back to you. Once you receive the drive please call in again for an engineer to start the restore process, this is not something that can currently be done by the end user.

15 Remove a single backup snapshot

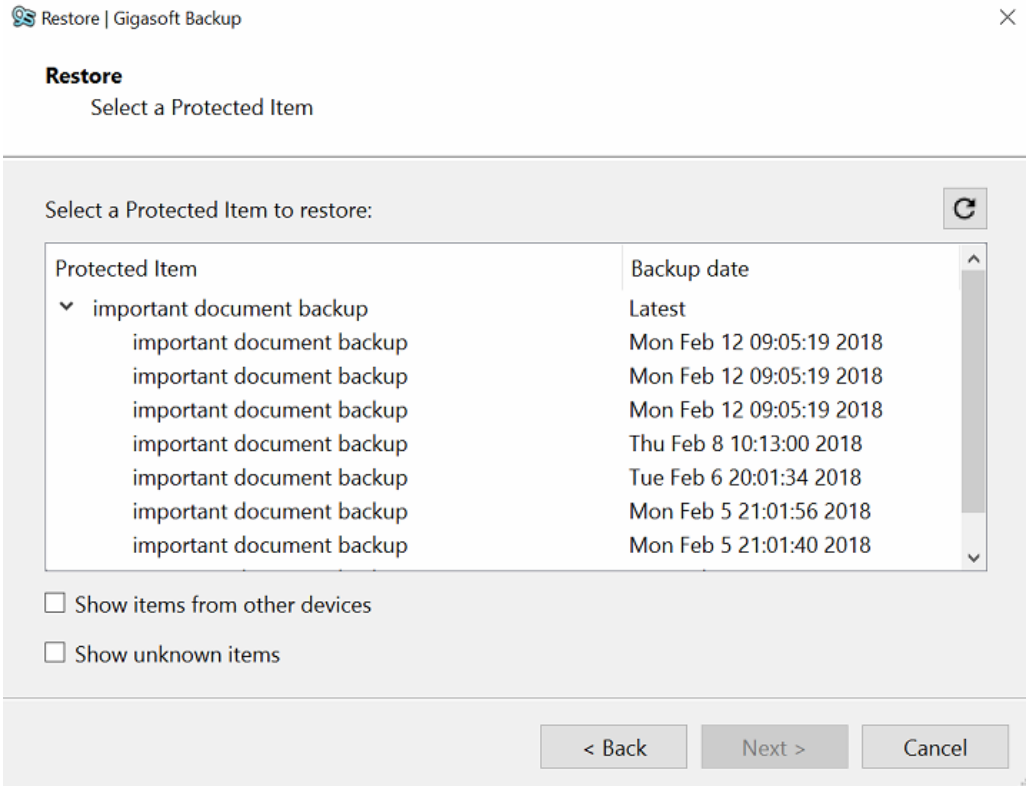
You can remove a single snapshot from within a Storage Vault as follows:



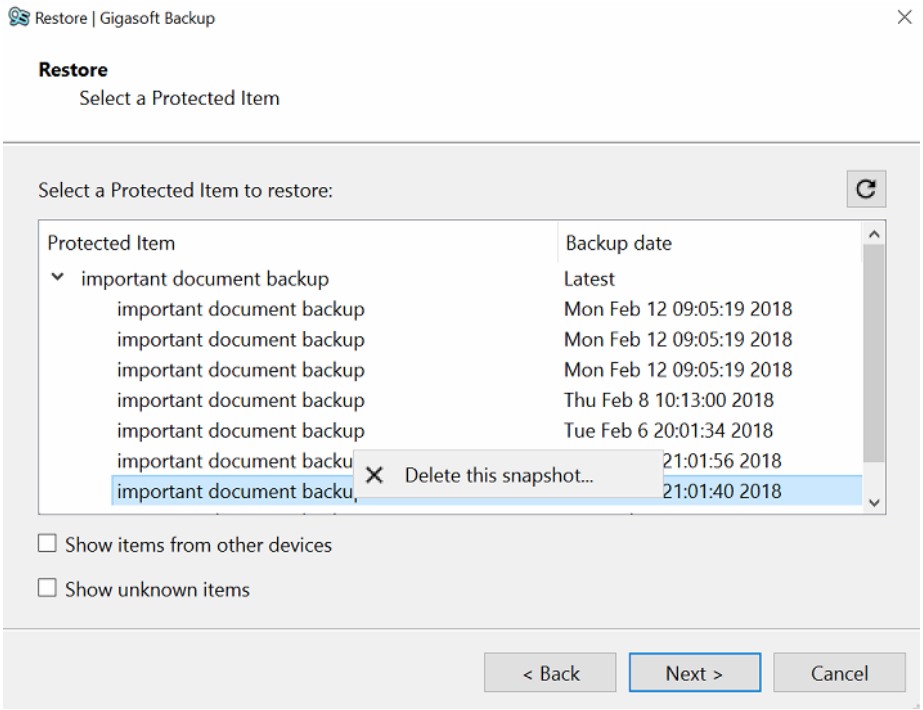
Click the Restore button in the left-hand menu bar



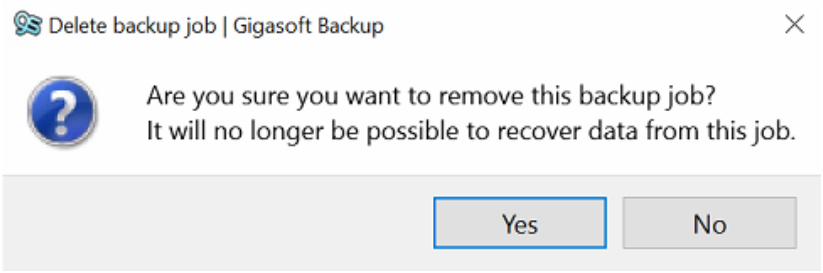
Select the Storage Vault containing the backed-up data, and click Next



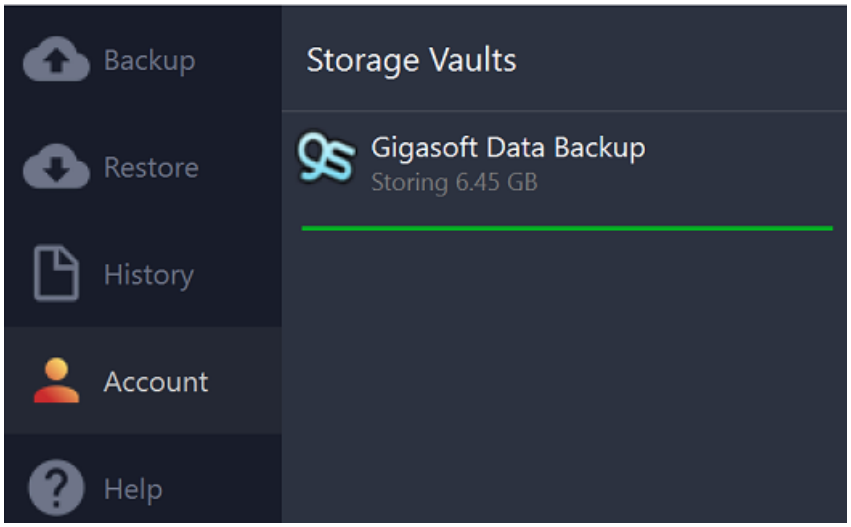
Identify the Protected Item snapshot that you want to remove from the Storage Vault, unfolding if necessary



Right click the Protected Item snapshot and choose "Delete this snapshot"



Click yes to remove the backup job



Gigasoft Backup Manager will remove the snapshot from the Storage Vault, and then immediately clean up unused data within the Storage Vault to save on disk space.