MSP360 Best Practices for Backups and Restores

Content

Notation

Best practices. Consider implementing these recommendations.

Caveats or warning information.

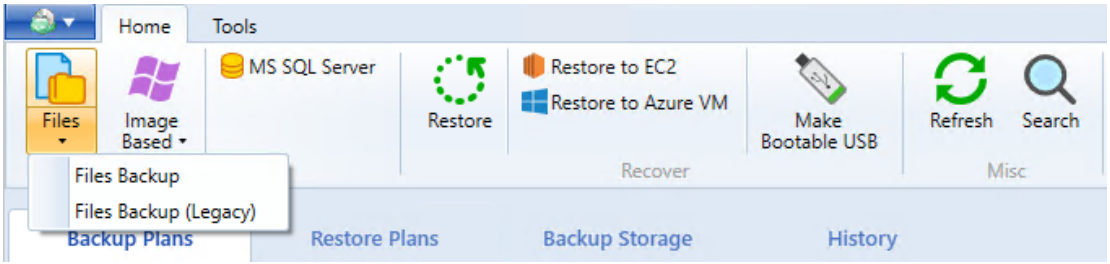
Misuse or incorrect configuration.

```
Code block
```

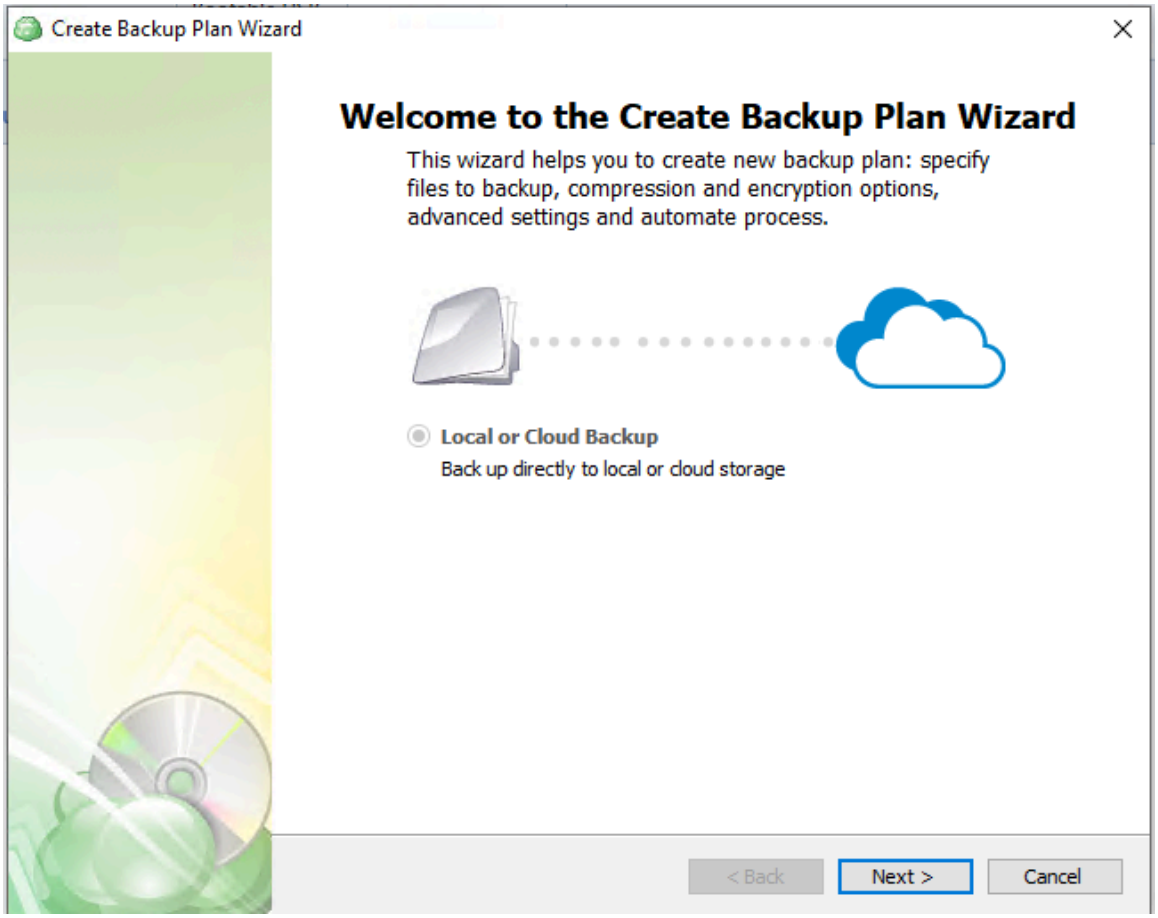
File-Level Backup Plans

Backup for Windows using the Agent

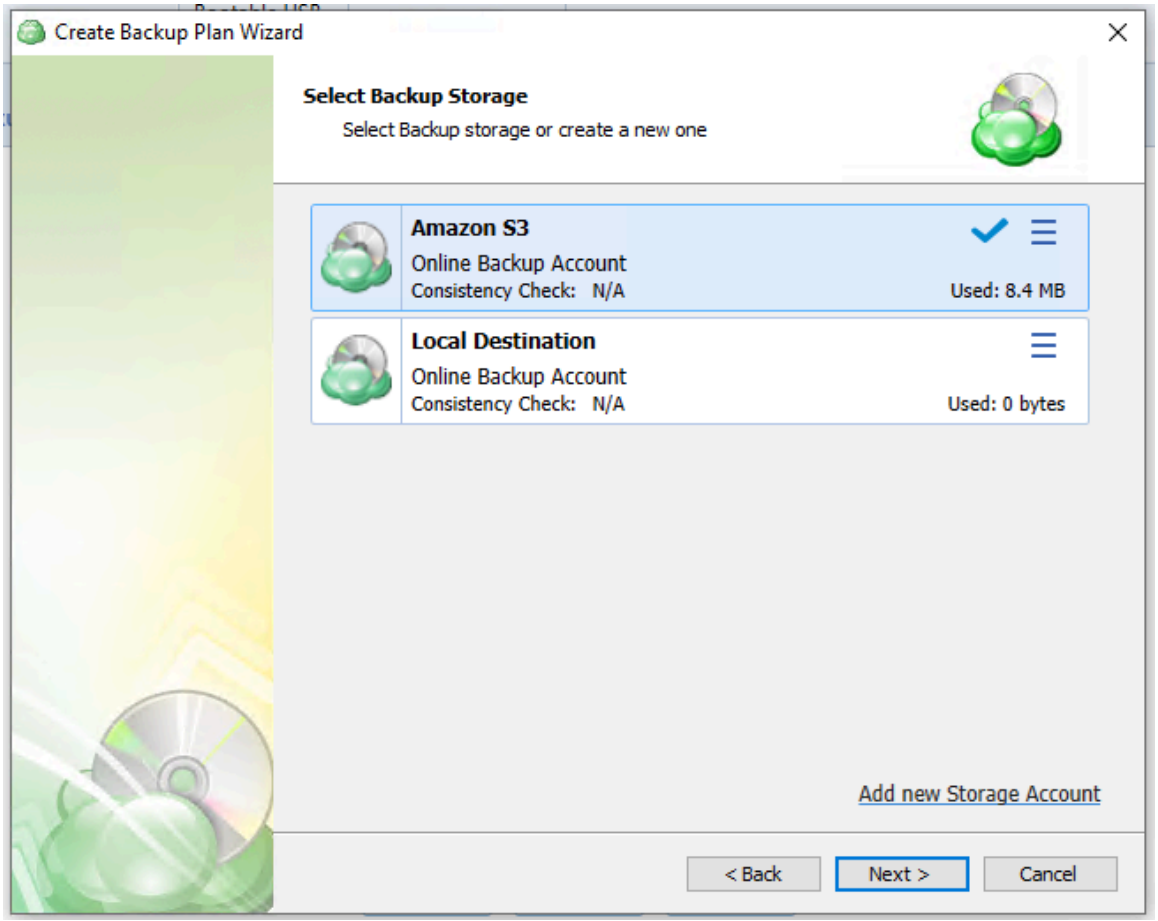
Step 1. After launching the Online Backup, you can run the Backup Wizard by clicking “Files” on the “Home” tab of the application's main toolbar, then clicking “Files Backup”.



Step 2. Only “Local or Cloud Backup” is currently supported for this backup type, click “Next” to continue.

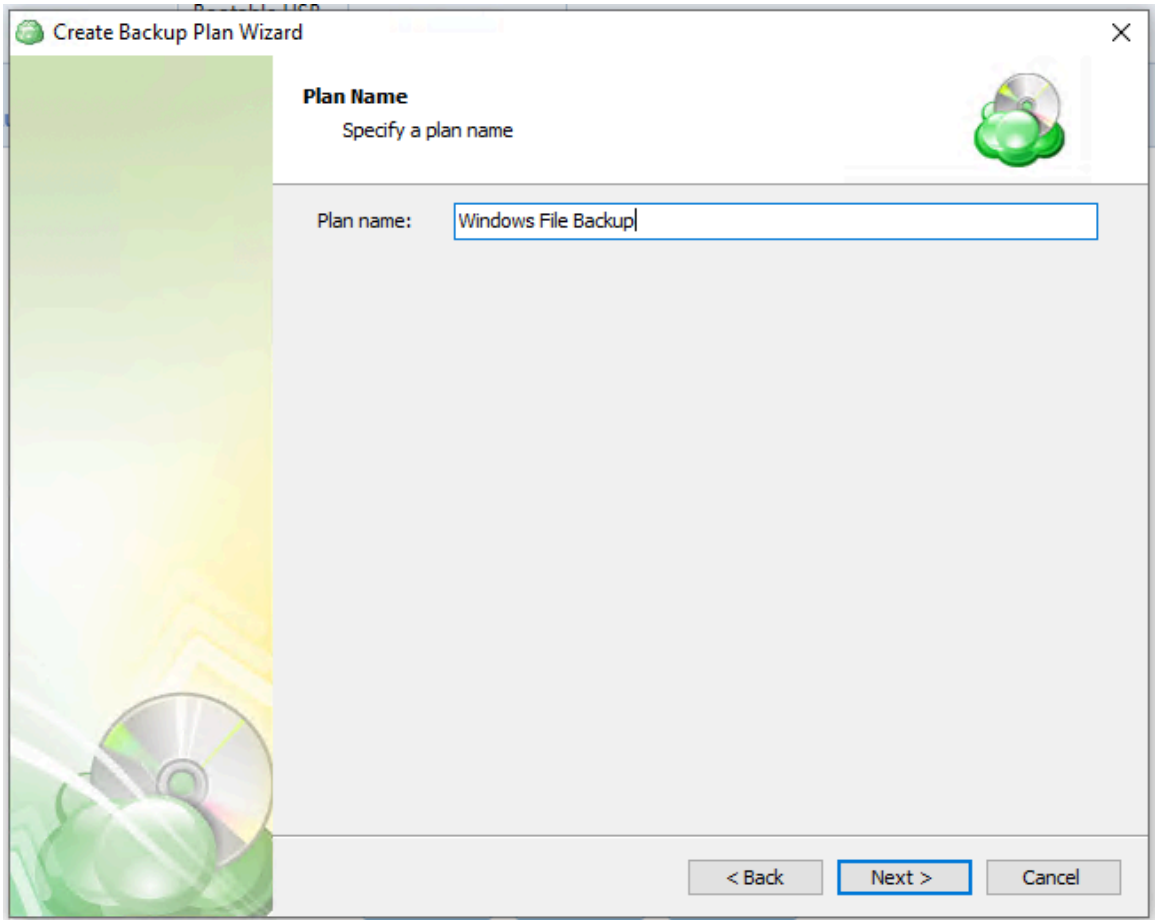


Step 3. The next step will prompt you to select the destination for the backup.



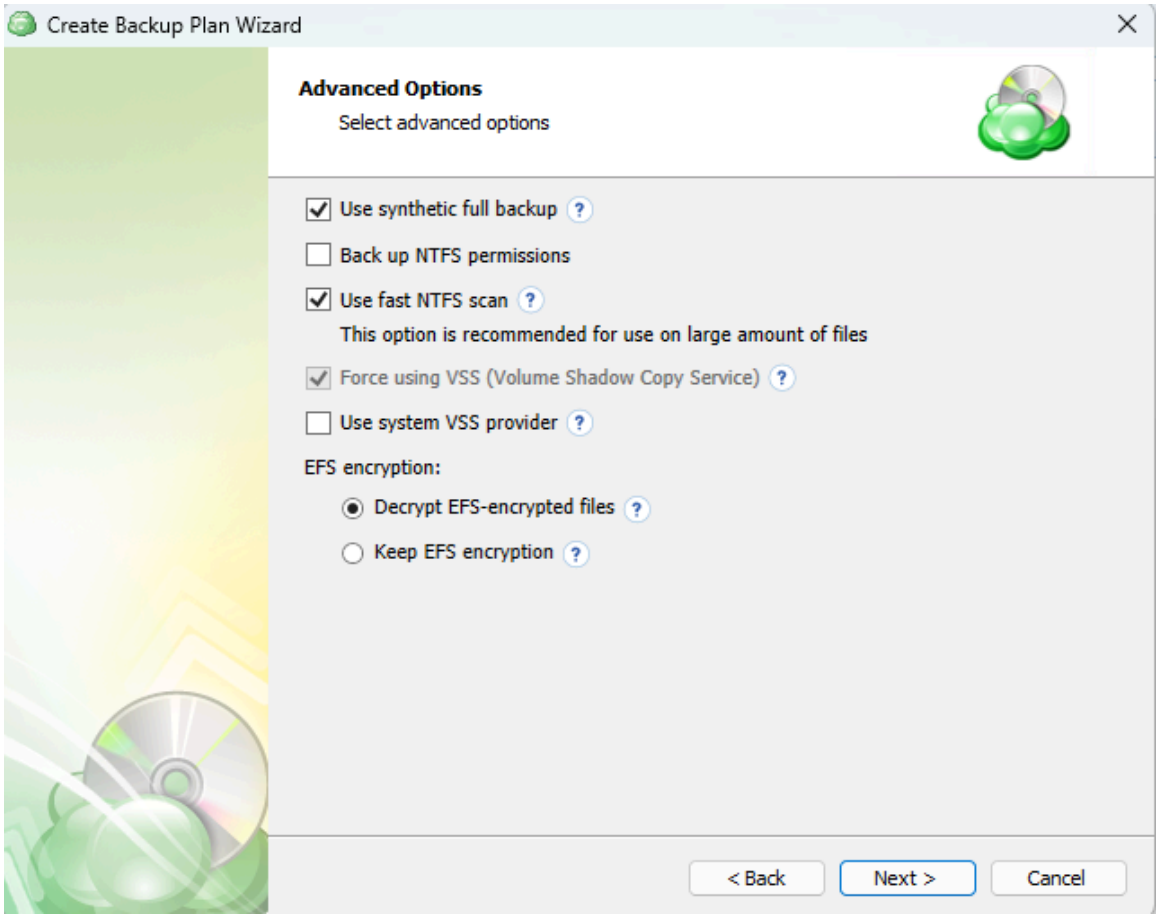
If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

Step 4. Once the destination has been selected, the next screen will prompt you for a plan name.



It is recommended that you select a name which helps you clearly identify the computer as well as the type of backup.

Step 5. The following step will prompt you for several options.

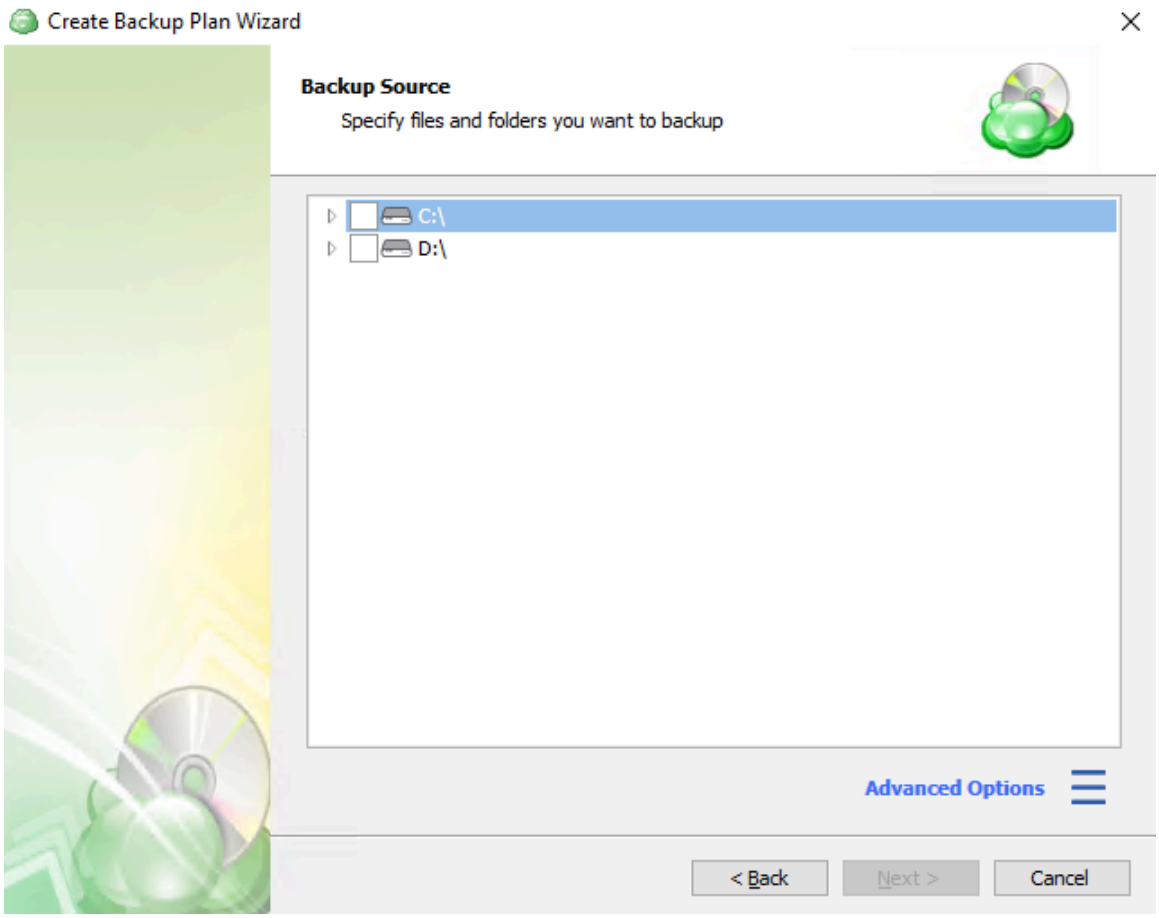


- **Use synthetic full backup:** This option is available only for backups to cloud destinations and improves performance of Full Backups by enabling the use of synthetic full backup technology.
- **Backup NTFS permissions:** Enable this option to retain all NTFS permissions assigned to your files, folders, and network shares. You may still choose whether or not to include these when restoring the files.
- **Use fast NTFS scan:** Enabling this allows the application to more quickly scan the NTFS file system for changes by using a low-level API, at the expense of increased local resource usage. The performance increase will likely only be noticeable when backing up a considerably large number of files and is also dependent on the type of device being backed up. The setting will not impact the speed of the initial full backup and will only be noticeable on subsequent backups.

- **Force using Volume Shadow Copy Service (VSS):** Select this check box to back up objects from a snapshot created by the VSS service in order to avoid any access conflicts. This option is enabled by default.
- **Use system VSS provider:** Using this option will force the application to use the native Windows VSS provider. If an error occurs while using the native provider, this option can be deselected to allow the application to scan for and use other 3rd party VSS providers. It is recommended that this option is selected by default.
- **EFS encryption:** Choose whether to keep EFS encryption intact or to decrypt the data during the backup plan execution then reenabling it.

> Before choosing whether to keep EFS encryption, refer to EFS-encrypted File Backup to determine which is the best option for your use case.

Step 6. The next step is to select the data to be backed up.

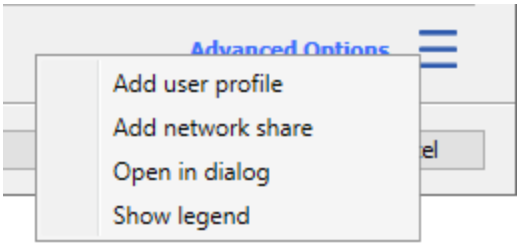


On Windows system partitions it is recommended to only back up \Users\ folder. An Image backup is better suited to back up Windows and any other installed applications.

Databases cannot be backed up at the file level while in use. A Pre and Post action to stop and start the database should be used prior to backing up at the file level. MSP360 MS SQL Server edition offers a robust solution for backing up active MS SQL databases.

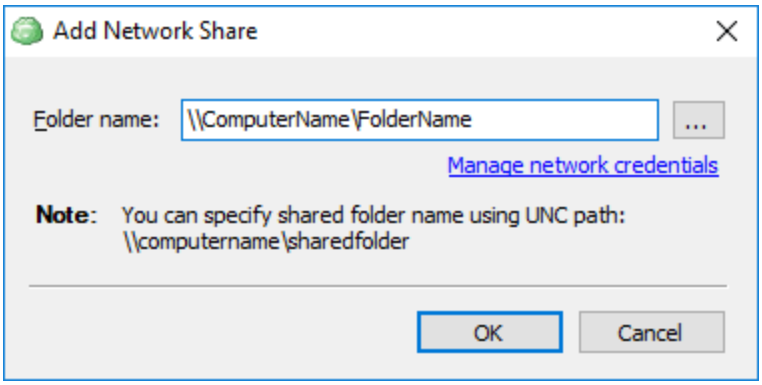
> Files and folders which are not accessible to the service account used by the backup plan will not be backed up and may cause the plan to fail. See information for more options.

For more advanced selection or the inclusion of a network share in the backup plan, click on the three-line (“hamburger”) icon on the lower right corner of the window.

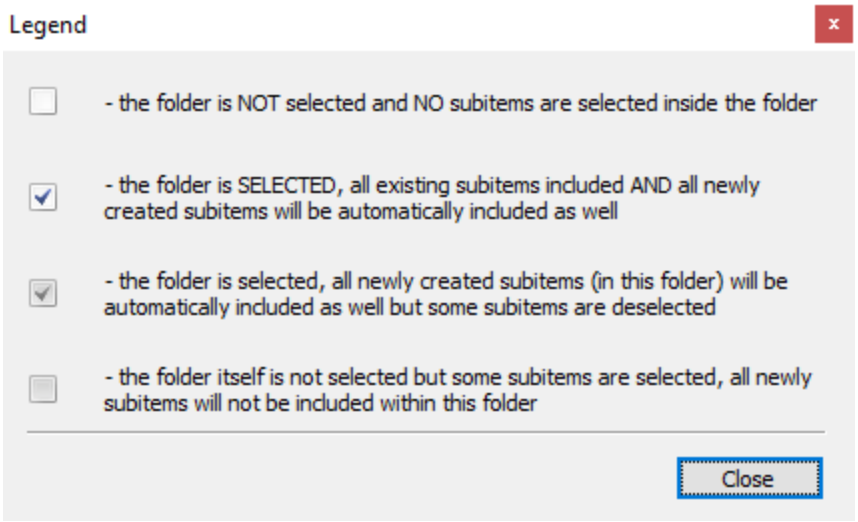


The following options are available on this menu:

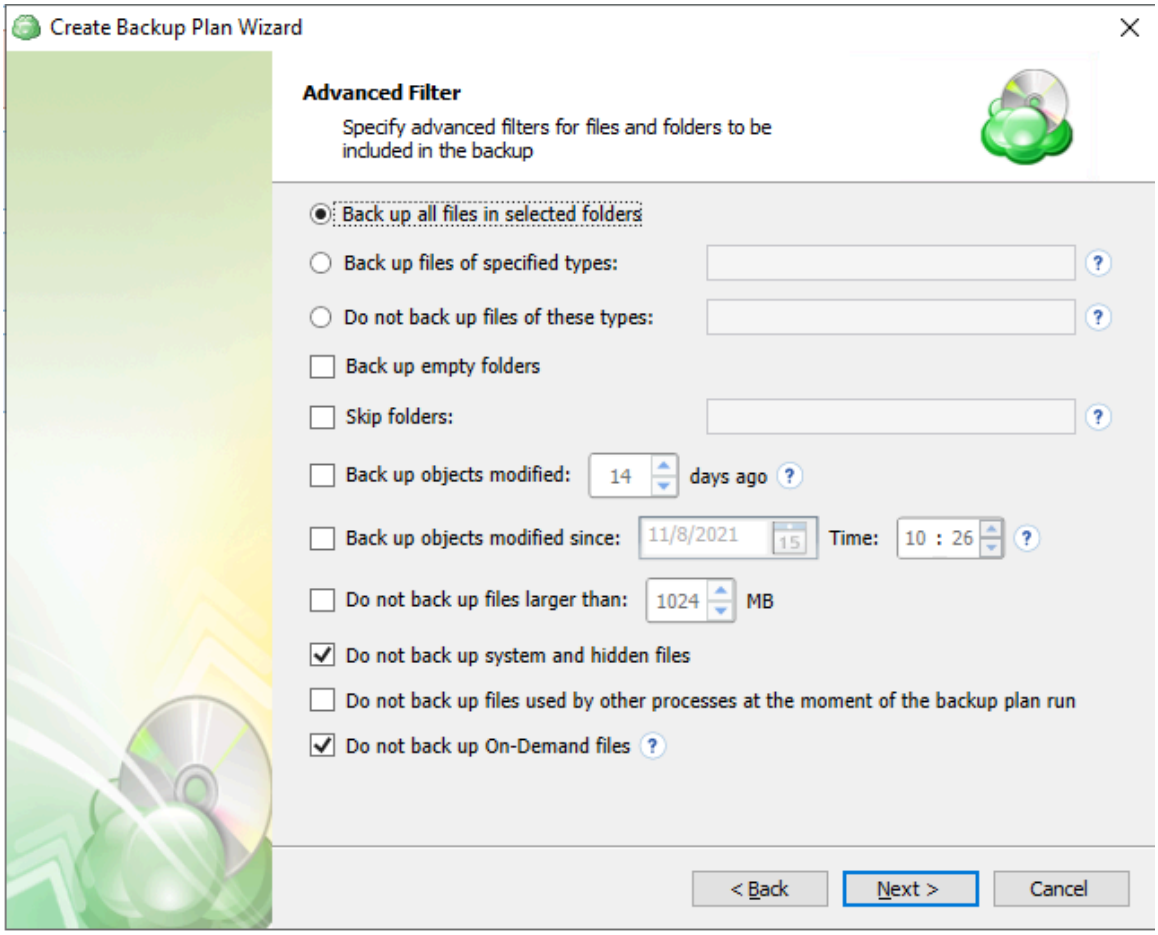
- **Add user profile.** Use this option to explicitly include user folders in your backup (such as *"Documents"*, *"Downloads"*, or *"Favorites"*).
- **Add network share.** Opens a dialog window where you can specify the path to a network share containing files that you wish to include in the backup. You may also enter alternate user credentials required to access the network share.



- **Open in dialog.** Invokes a new dialog window displaying a larger view of the file tree.
- **Show legend.** Invokes a dialog window explaining how to interpret the different states of the checkboxes in the file tree, as follows.



Step 7. On this step, you are presented with the “Advanced Filter” page, where you can define the various criteria that the backup service should use when determining which files should be backed up based on more advanced filtering than is available through the check boxes on the previous step.

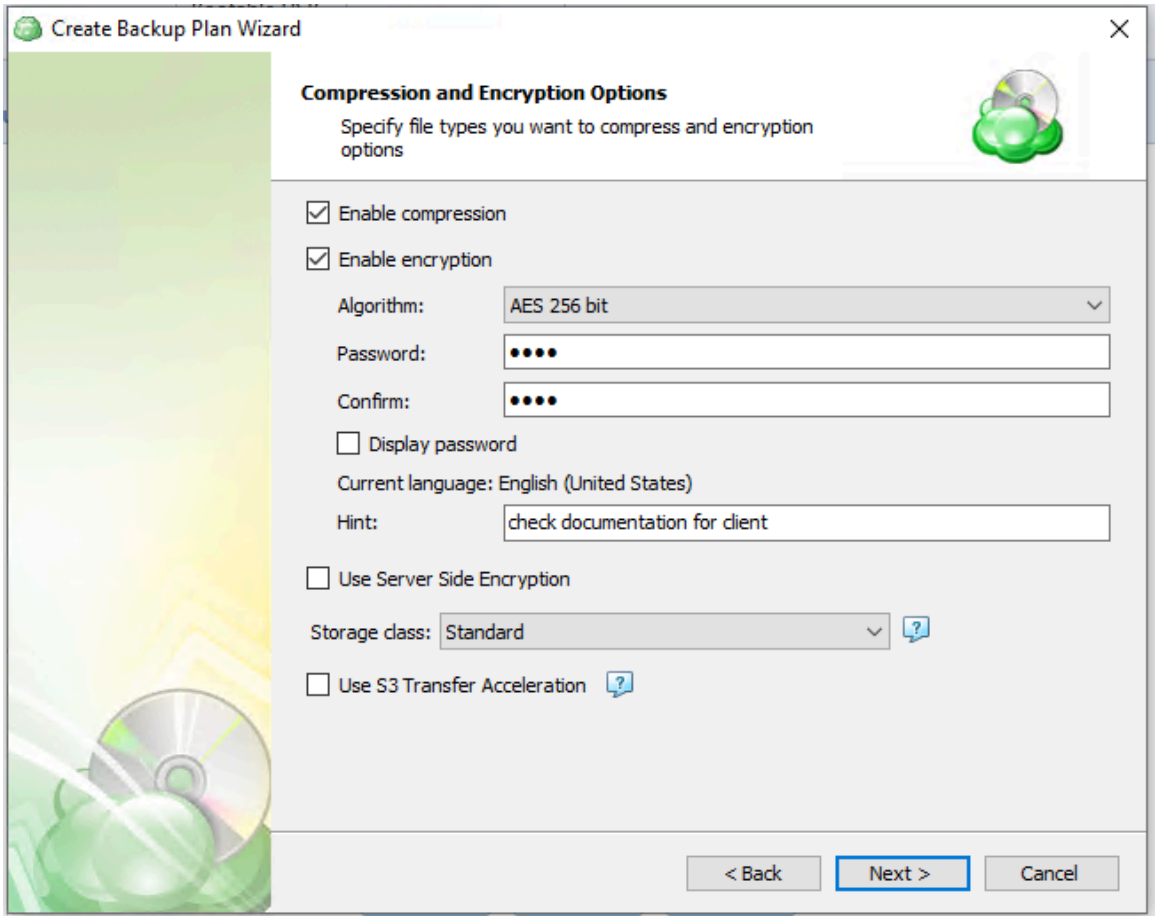


> When using the Advanced Filters, the number of files actually uploaded can differ from the number of files that are calculated in the local folder Properties.

> “Skip Folders” will exclude any folders that contain the specified partial name. For example, “temp” will exclude all folders with “temp” in the name in all sources.

Step 8. With all the selections for what data should be backed up and where the backup should be stored, you are now presented with options for compression, encryption, storage class, and

transfer options of the backed up data. The options presented here may vary depending on the features supported by your selected backup destination.



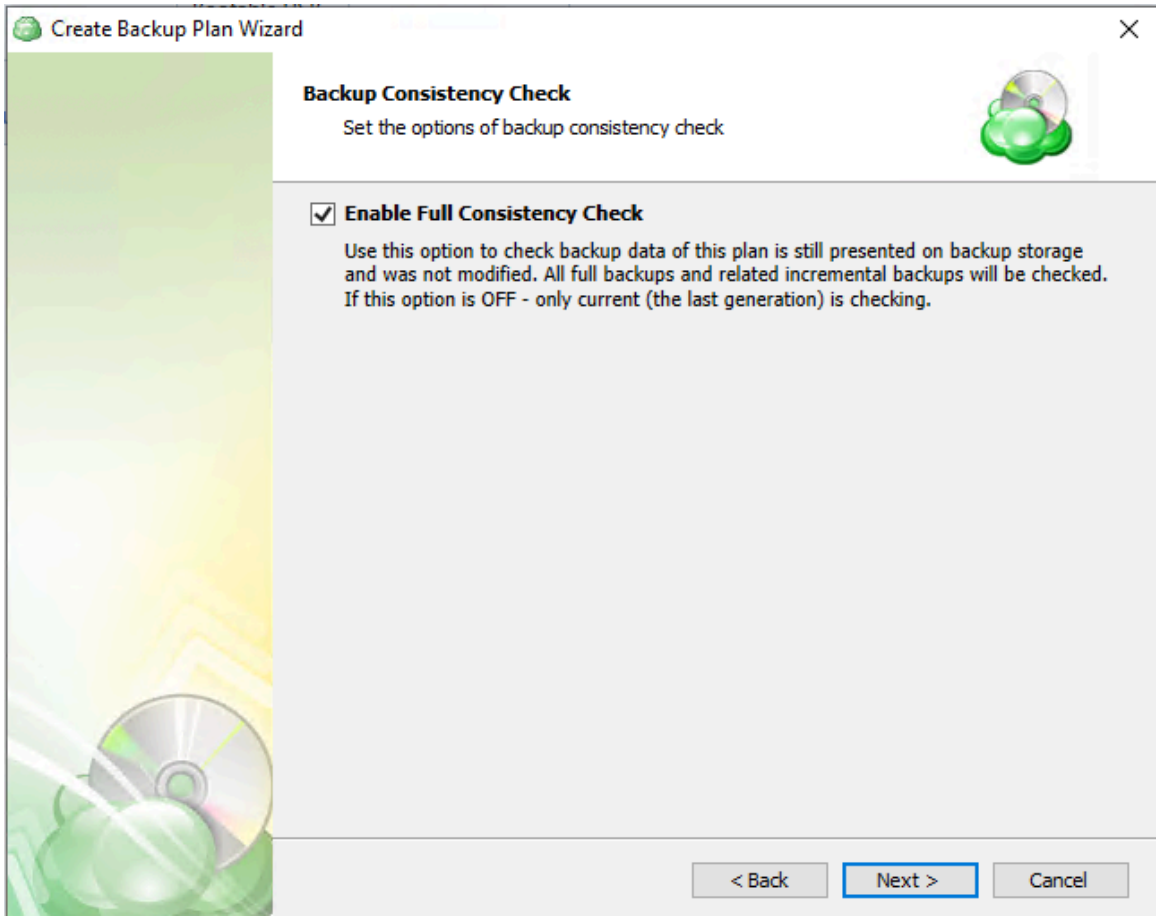
Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

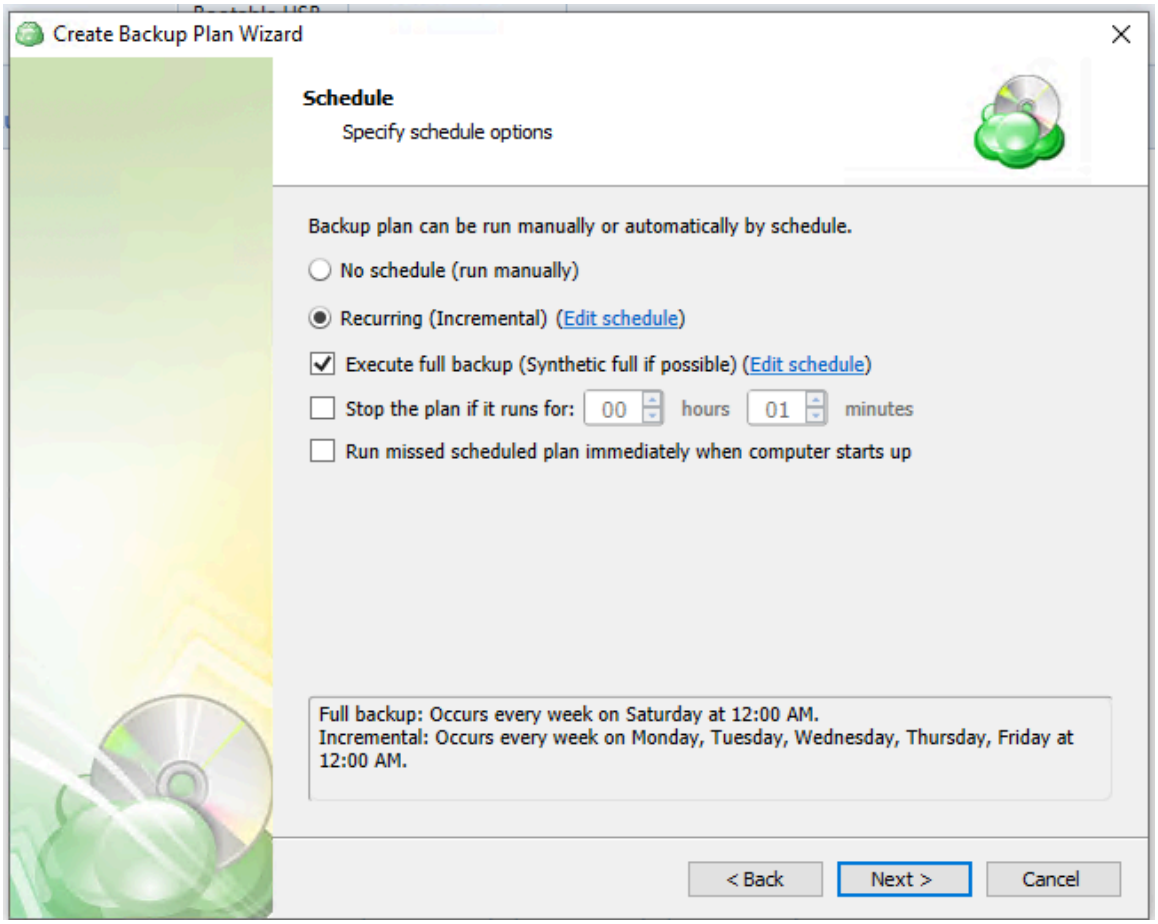
It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a

secure place and enable the Password Recovery Service.

Step 9. Next you are presented with an option for the type of Backup Consistency Check to use with the plan. It is recommended that you leave “Enable Full Consistency Check” enabled.



Step 10. Next you are prompted to set the schedule for your backup plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.



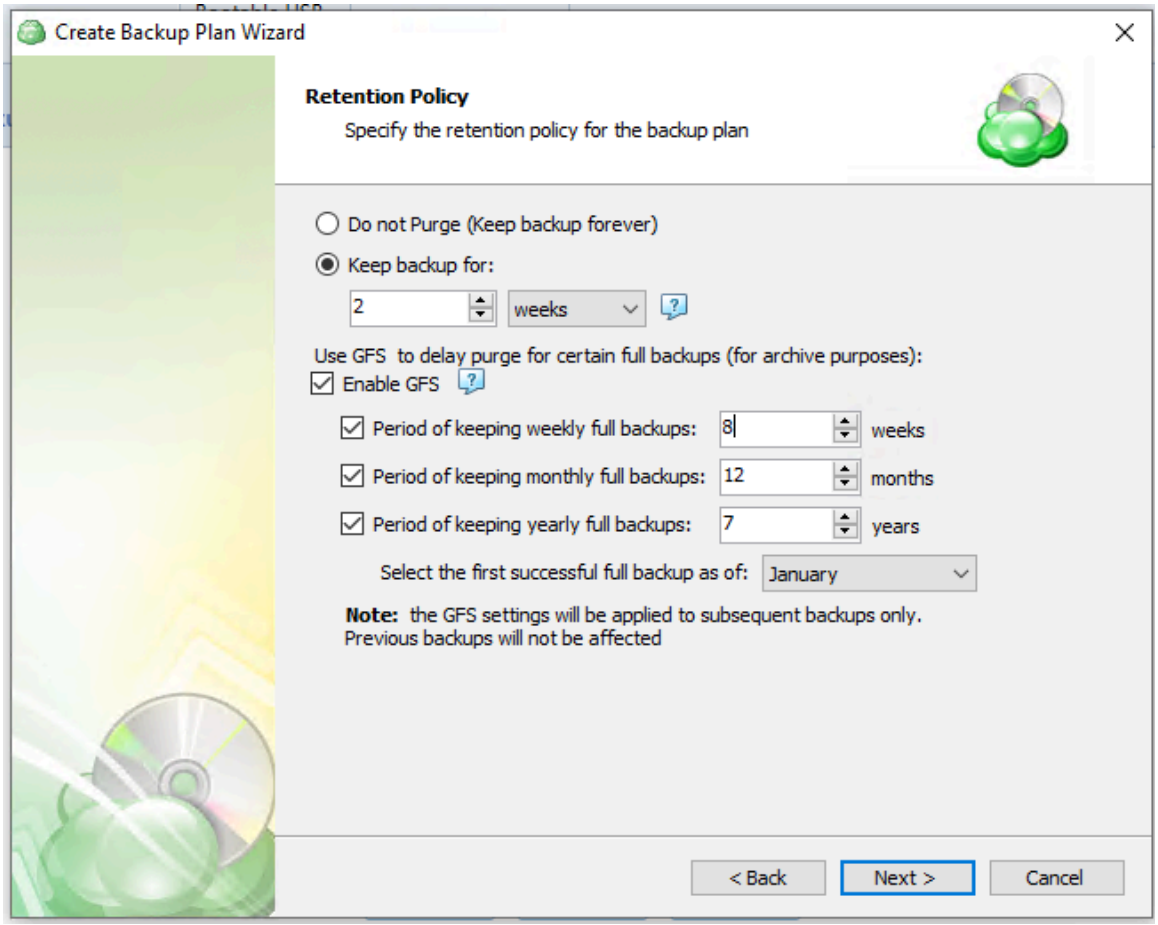
Schedule a “Full Backup” at regular periods, once a week will be suitable in most circumstances.

The retention policy will only perform properly with regular scheduled full backups.

Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

> Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

Step 11. On the “Retention Policy" step, you can set the policies the application will use to determine which data to purge at regular intervals and define the multigenerational Grandfather-Father-Son (GFS) parameters if required.



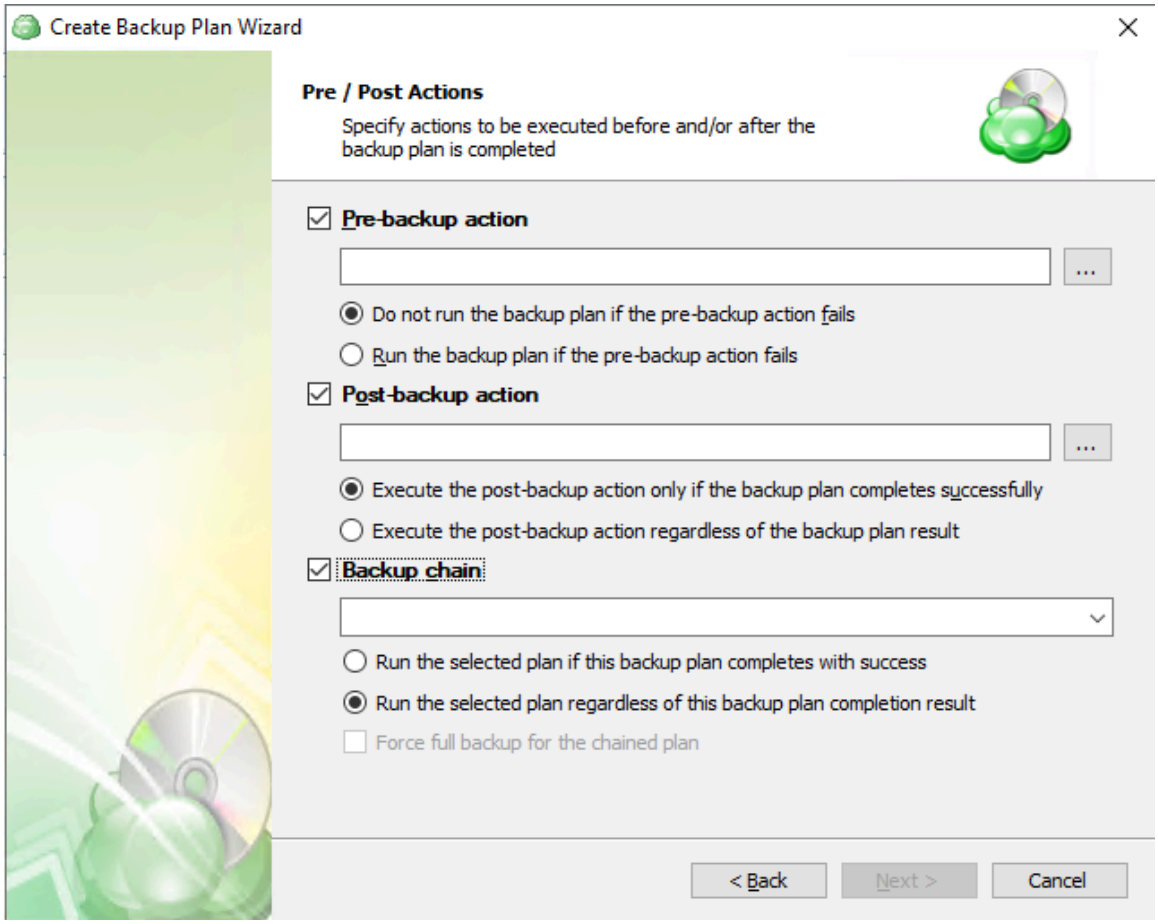
- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.
- **Enable GFS**: Select this option if you want to keep Full Backups for archival purposes at the selected intervals.

- **Period of keeping weekly full backups**: Set the number of Weekly Full Backups to retain. This is determined separately from the “Keep backup for” value and relies on Full Backups to be scheduled on at least a weekly basis in the previous step.
- **Period of keeping monthly full backups:** Number of Monthly Full Backups to retain. A Full Backup can be flagged as both a Weekly and Monthly backup, but once the number of Weekly Full Backups has exceeded their retention setting, only those also flagged as a Monthly will be retained.
- **Period of keeping yearly full backups:** Set the number of Yearly Full Backups to retain. A Full Backup can be flagged as a Weekly, Monthly, and Yearly Backup. Once the number of Monthly Full Backups has exceeded their retention setting, only those also flagged as a Yearly will be retained.
    - **Select the first successful full backup as of**: Select the first Monthly Full Backup you would like to flag and retain as the first Yearly Full Backup.

Restore Points will not be deleted until the youngest point in the chain has met the retention criteria.

GFS Retention provides an excellent way to efficiently archive data for compliance. Additional information can be found in GFS Policy topics in the MBS Documentation

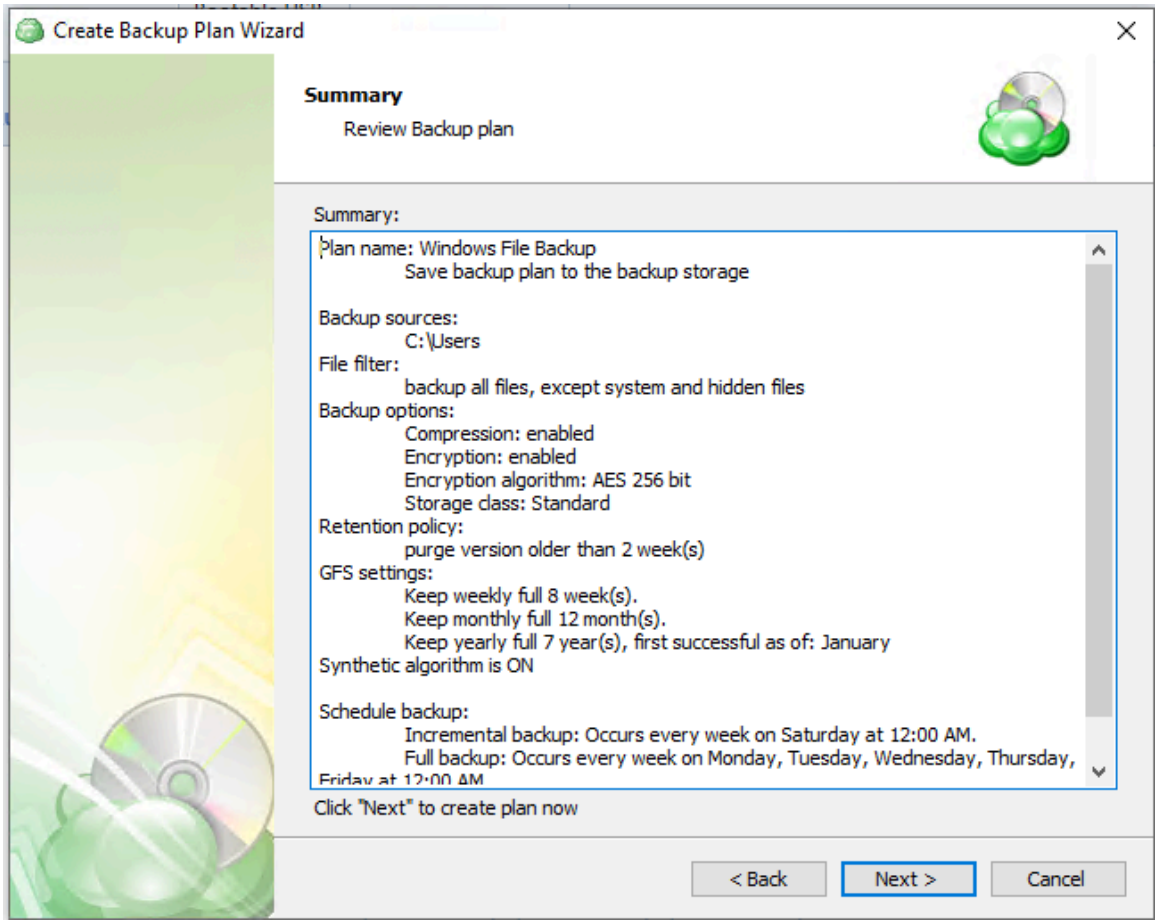
Step 12. The “Pre/Post Actions” page allows the execution of custom scripts before and/or after the running of a backup task, and can chain multiple backup tasks together for sequential execution.



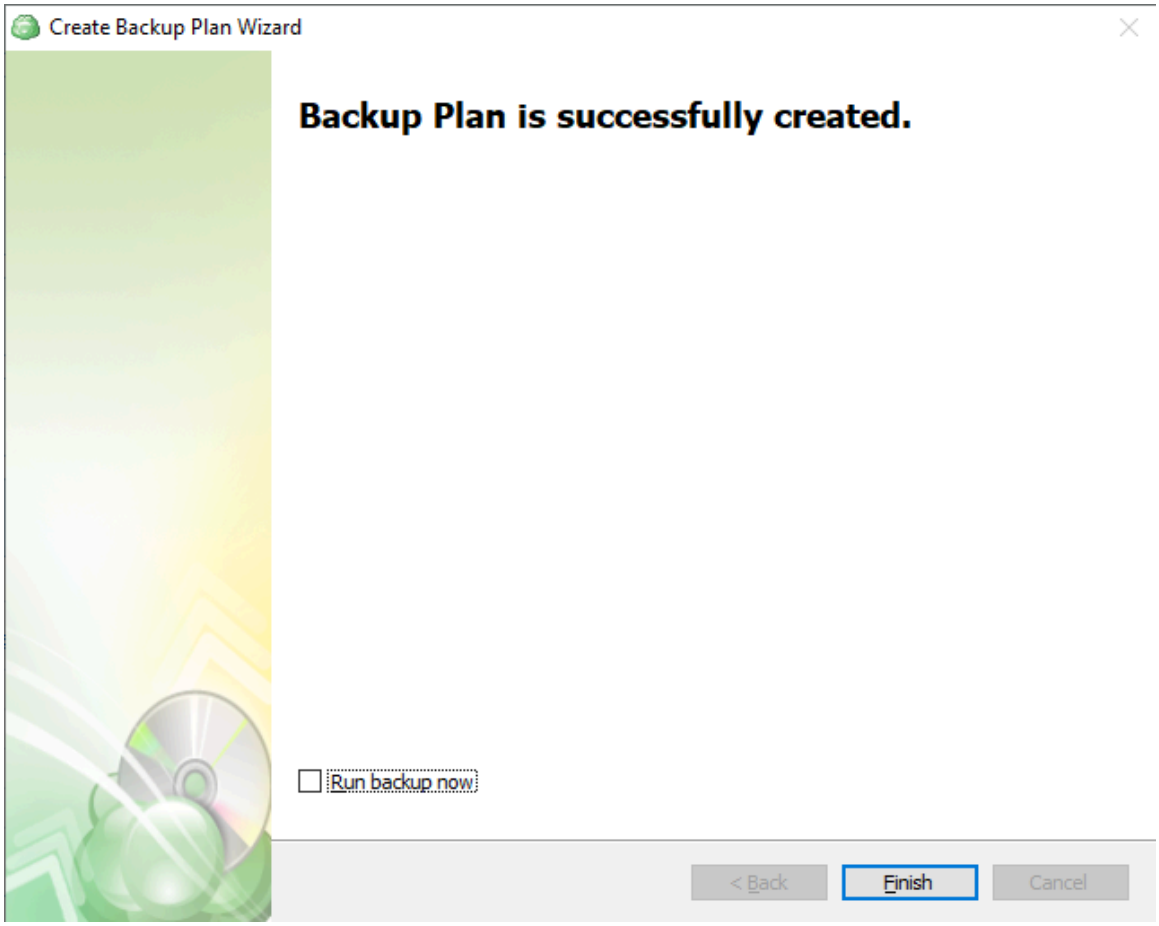
Common scenarios for using Pre/Post actions:

- How to Back Up MySQL Database using CloudBerry Backup
- How to Back Up Oracle Database using CloudBerry Backup
- How to Use Rotating Drives Strategy with MBS

Step 13. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.

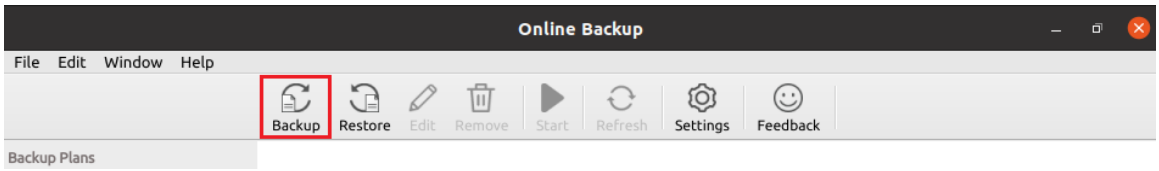


Step 14. The final step of the process is to select when the Backup Plan will start running. To have it start the initial full backup immediately, select the “Run Backup Now” option and click “Finish”. Otherwise, click “Finish” and the backup will begin at the next scheduled time.



Backup for Mac / Linux using the Agent

Step 1. After launching Online Backup, you can start the Backup Wizard by clicking on the "Backup" button on the top menu.

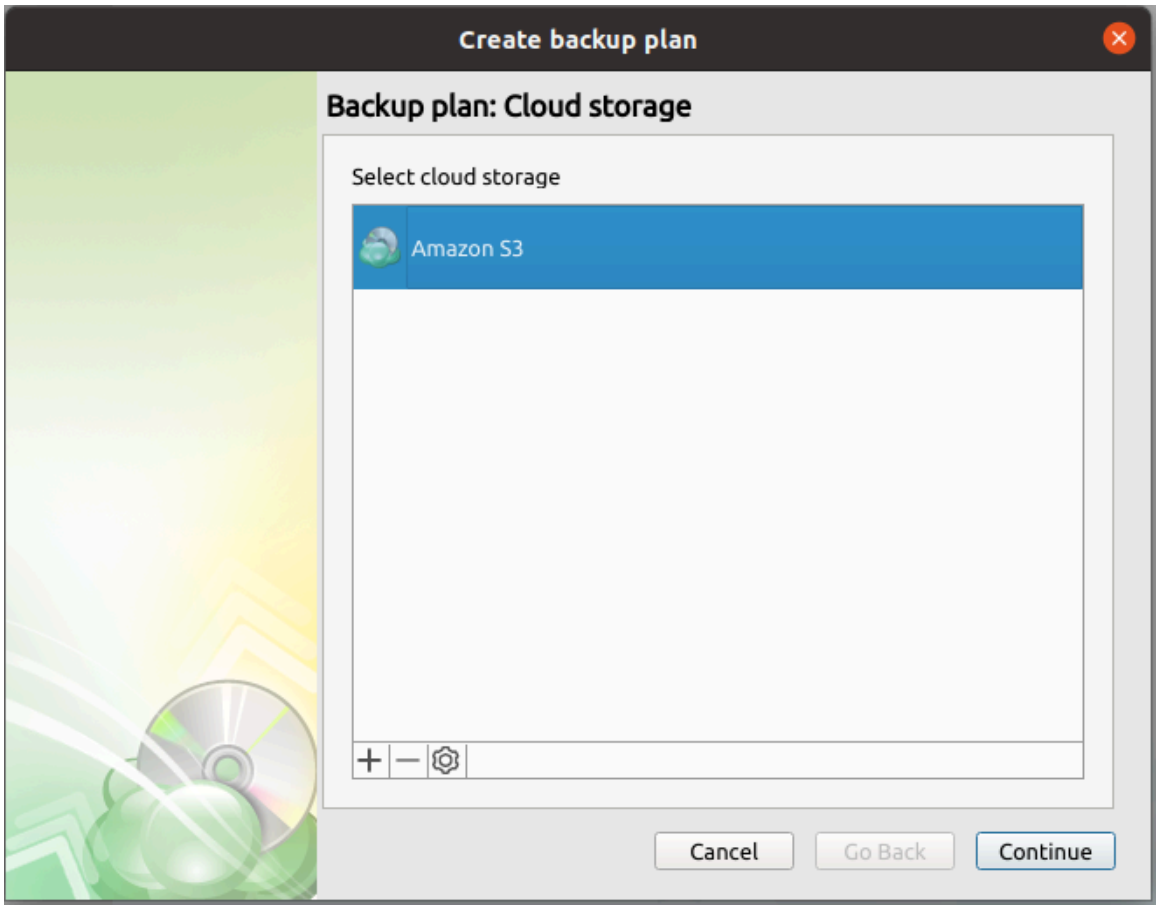


Step 2. After clicking on the Backup button, you will be prompted to choose between the New Backup Format, and the Current Backup Format. Click on "Try New Backup Format (BETA)" to continue.

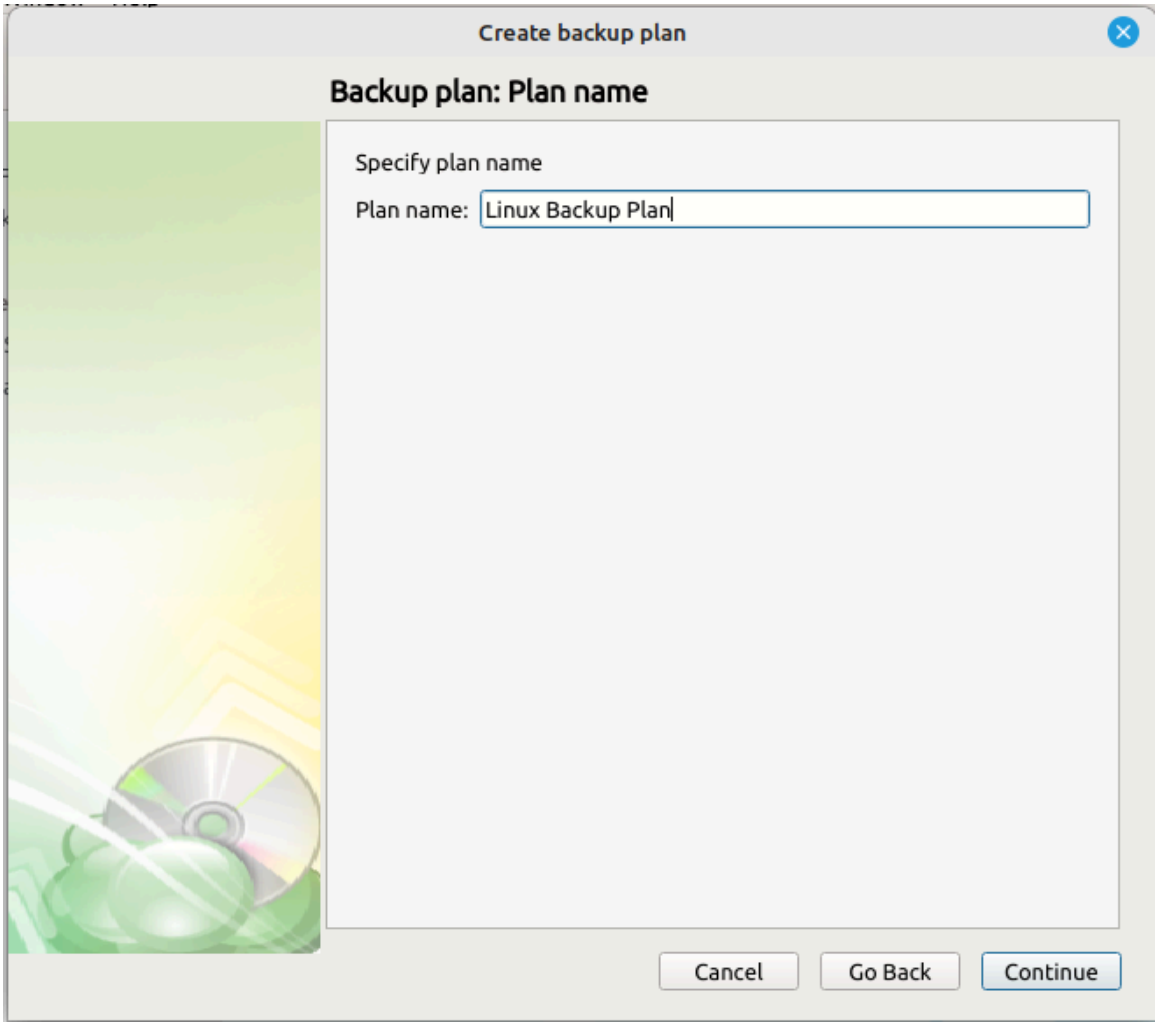
New backup format features for macOS and Linux backup (BETA) are:

- Client-Side Deduplication
- Automatic Consistency Checks
- Restore on Restore Points
- Improved incremental backup performance.

Step 3. At the "Cloud Storage" step, select the storage destination for the backup.

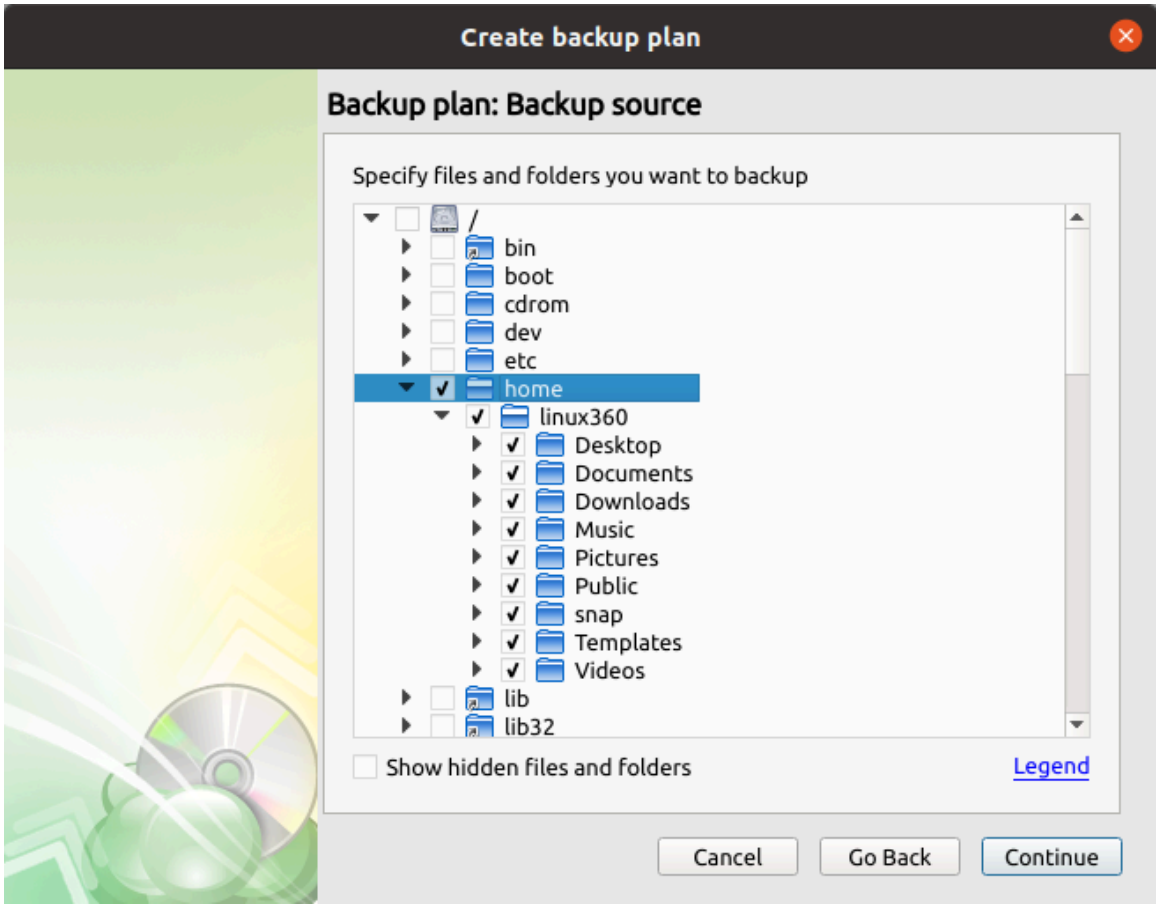


Step 4. Once the destination has been selected, the next screen will prompt you for a plan name.



It is recommended that you select a name which helps you clearly identify the computer as well as the type of backup.

Step 5. At the "Backup Source" step, select all the files and folders that are required to be backed up.



We generally recommend backing up the contents of:

/home (user files)
/etc (daemons configuration files)
/var/* (only the subdirectories that are needed, like /var/mail, /var/mysql, /var/www etc.)

In some cases, you might also need to backup data from:

/media or **/mnt** (if there's a mount point containing important info)
/root (if there is any important information or settings stored in the

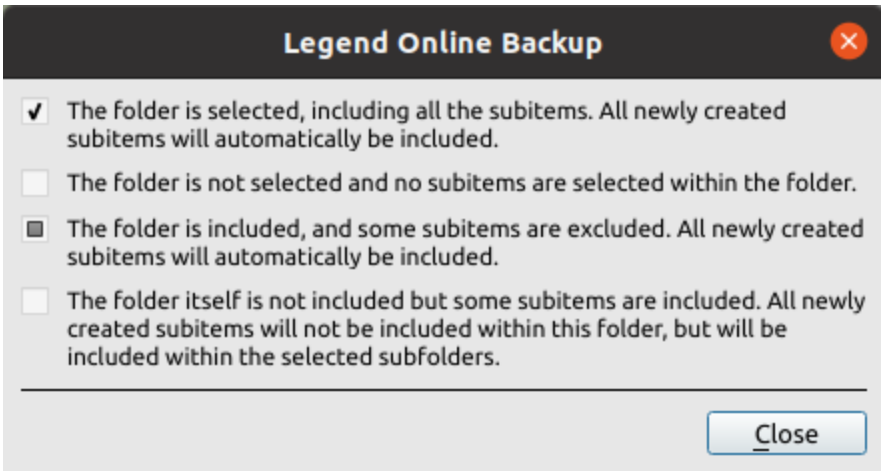
home directory of the root user)

It is essential that these locations should not be included in the backup:
/boot
/dev
/var/run
/tmp
/sys
/Applications - MacOS only
/Library - MacOS only

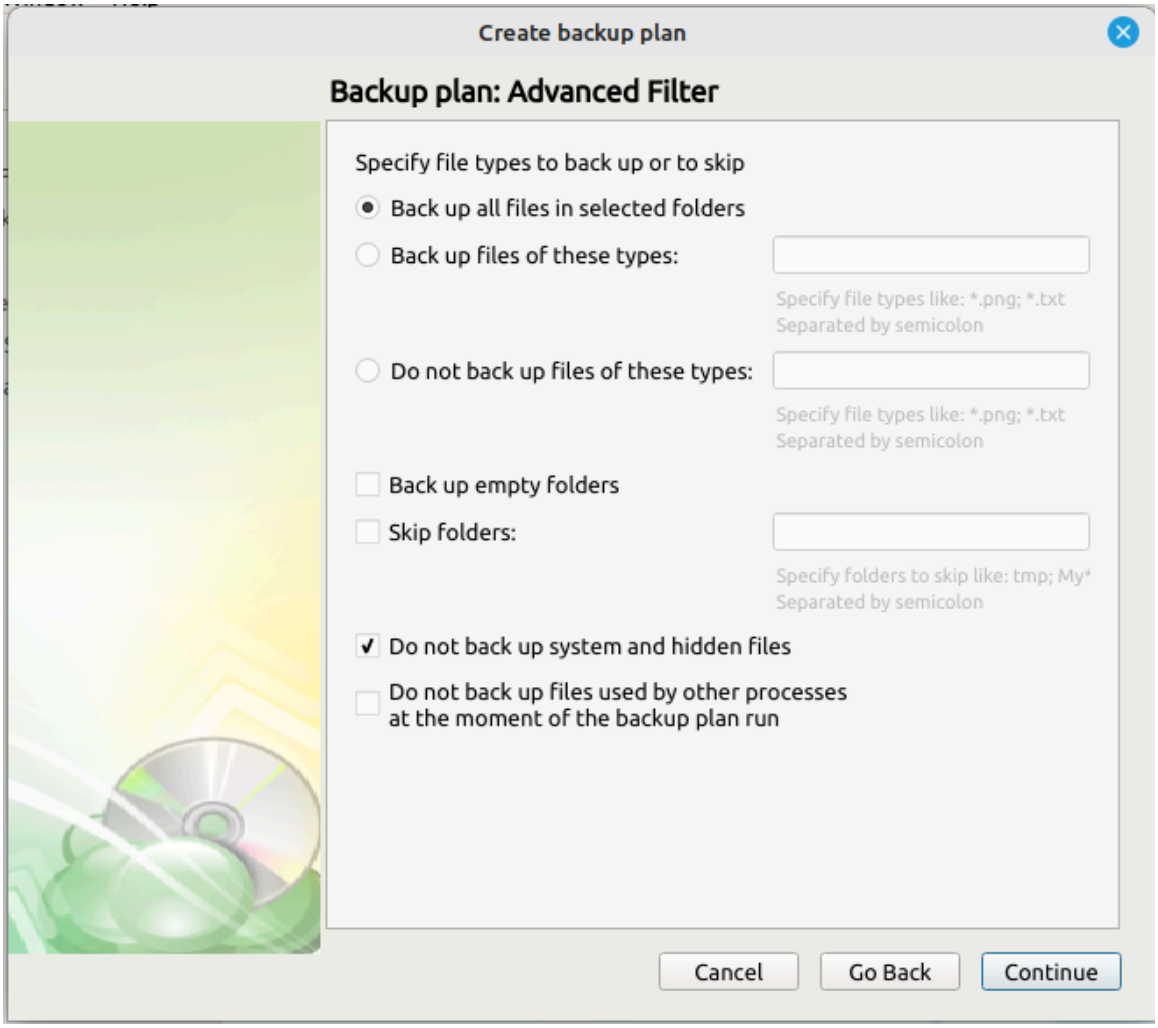
Databases cannot be backed up at the file level while in use. A Pre and Post action to stop and start the database should be used prior to backing up at the file level.

Files and folders which are not accessible to the service account used by the backup plan will not be backed up and may cause the plan to fail. Ensure all necessary rights are granted prior to starting the backup.

- **Legend.** Invokes a dialog window explaining how to interpret the different states of the checkboxes in the file tree, as follows.



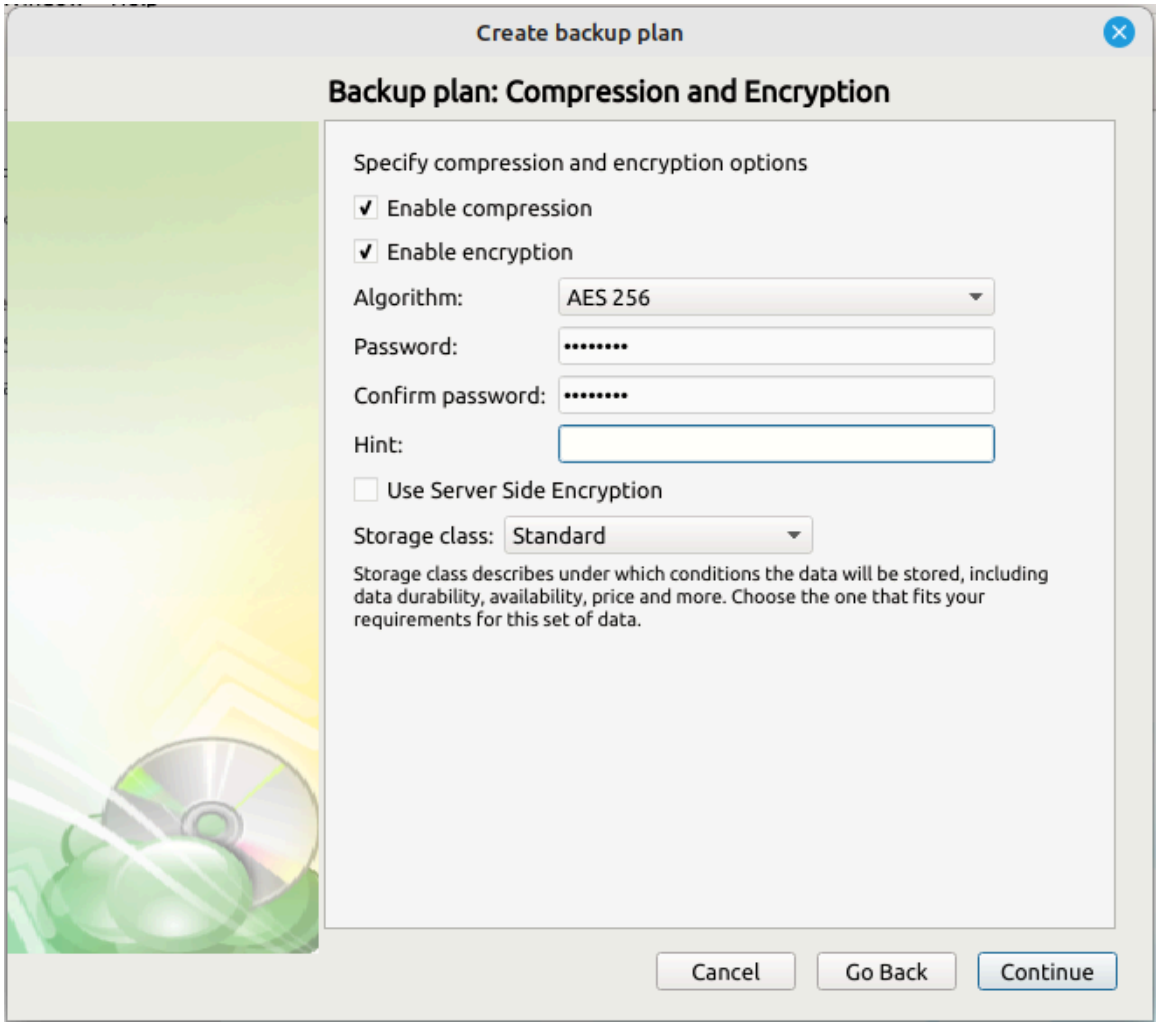
Step 6. Next you will be prompted with the "Advanced Filter" selections, which will allow you specify which files or folders in the selection locations should be skipped.



When using the Advanced Filters, the number of files actually uploaded can differ from the number of files that are calculated in the local folder Properties.

“Skip Folders” will exclude any folders that contain the specified partial name. For example, “temp” will exclude all folders with “temp” in the name in all sources.

Step 7. Once all data to backup has been selected, the next step is to determine whether compression or encryption should be applied. Other options in this step may change depending on the capabilities of the selected Backup Destination.



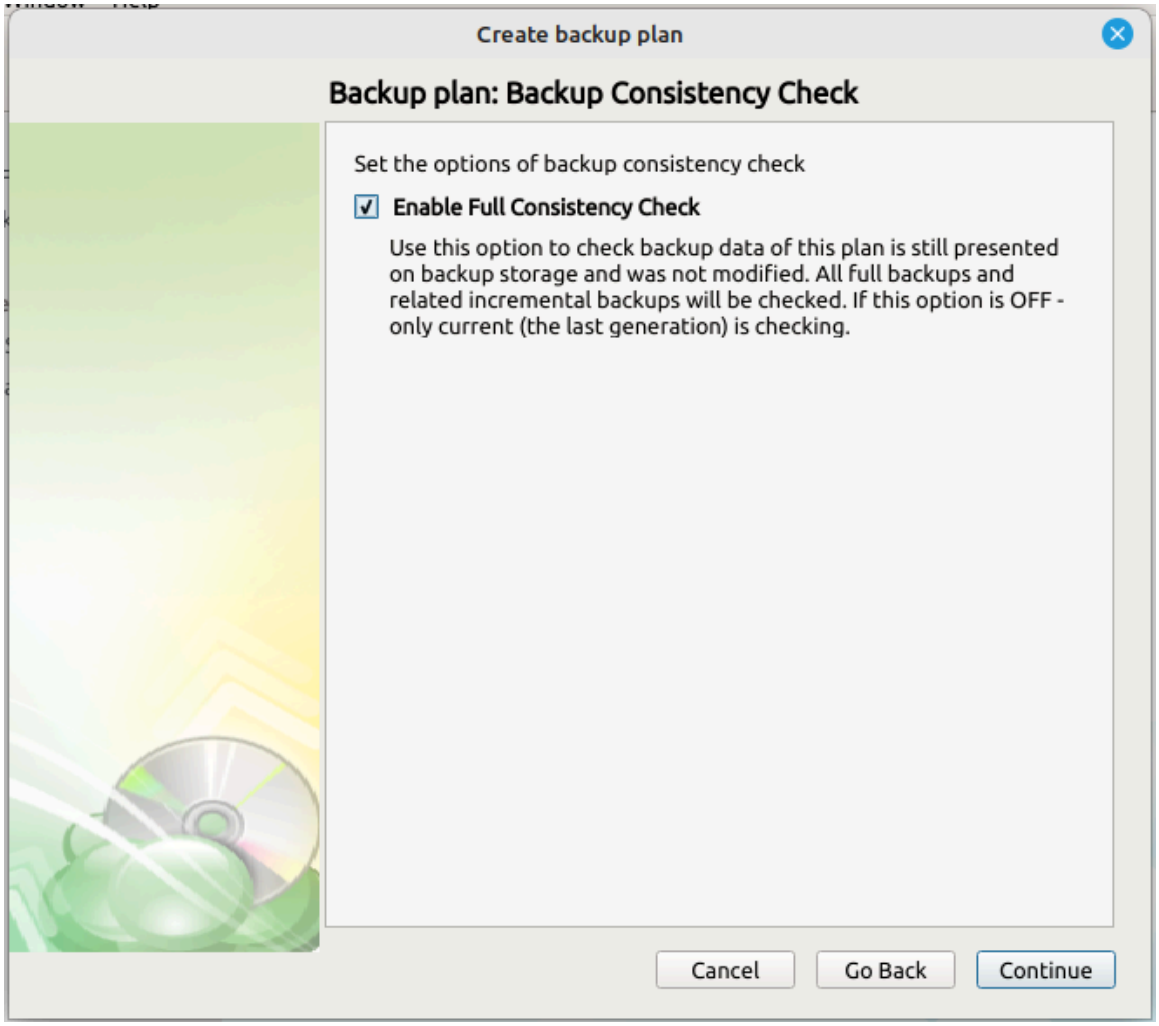
Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place.

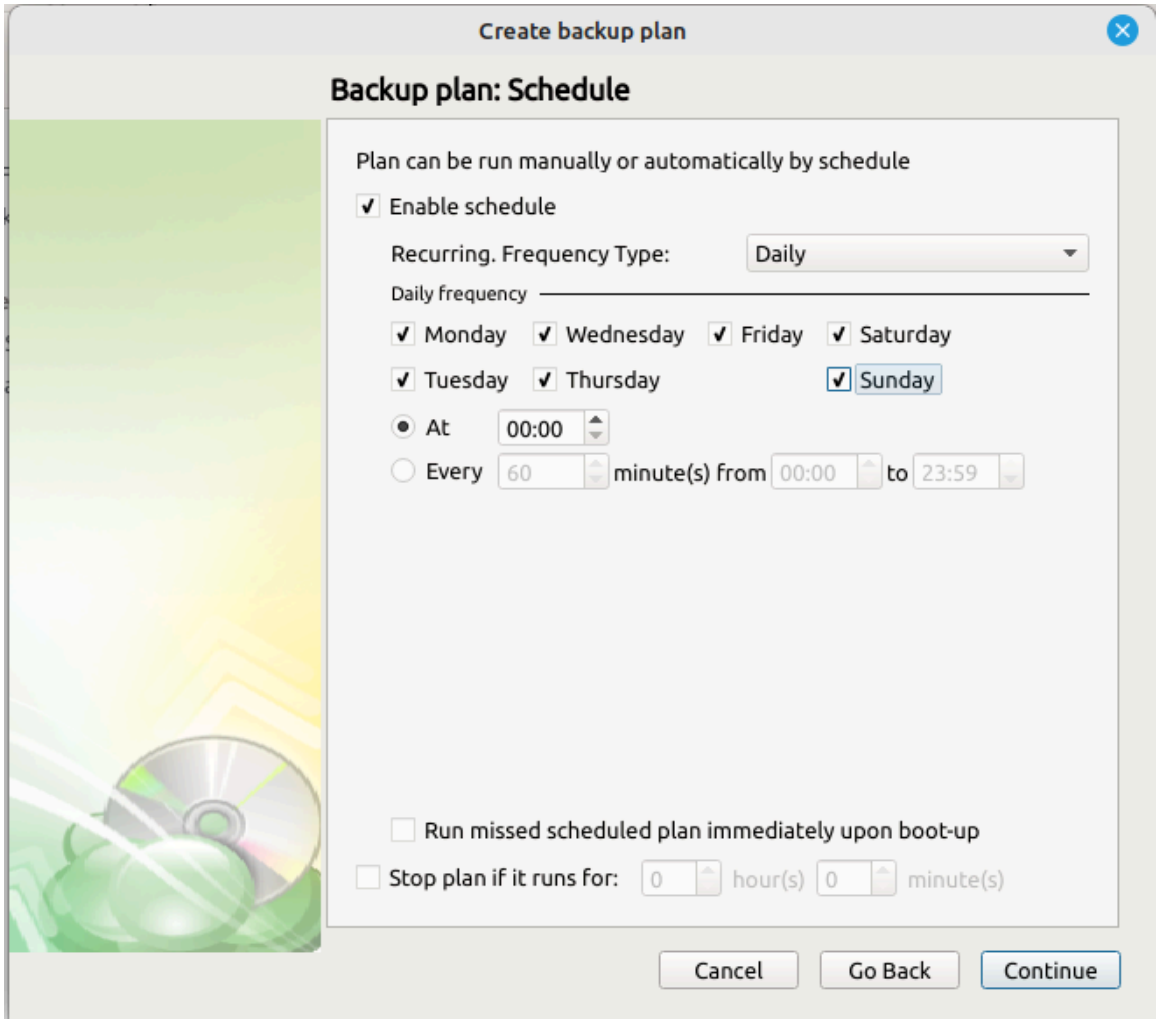
"Server Side Encryption" is only available on certain cloud providers and is separate from the MSP360 encryption. The native encryption applies only to the data the application backs up, while the server side encryption refers to encrypting the bucket on the cloud service itself.

Step 8. Next you are presented with an option for the type of Backup Consistency Check to use with the plan. It is recommended that you leave “Enable Full Consistency Check” enabled.



We strongly recommend leaving the Full Consistency Check enabled. This feature checks all full backups and their related incremental backups, instead of only the last backup generation.

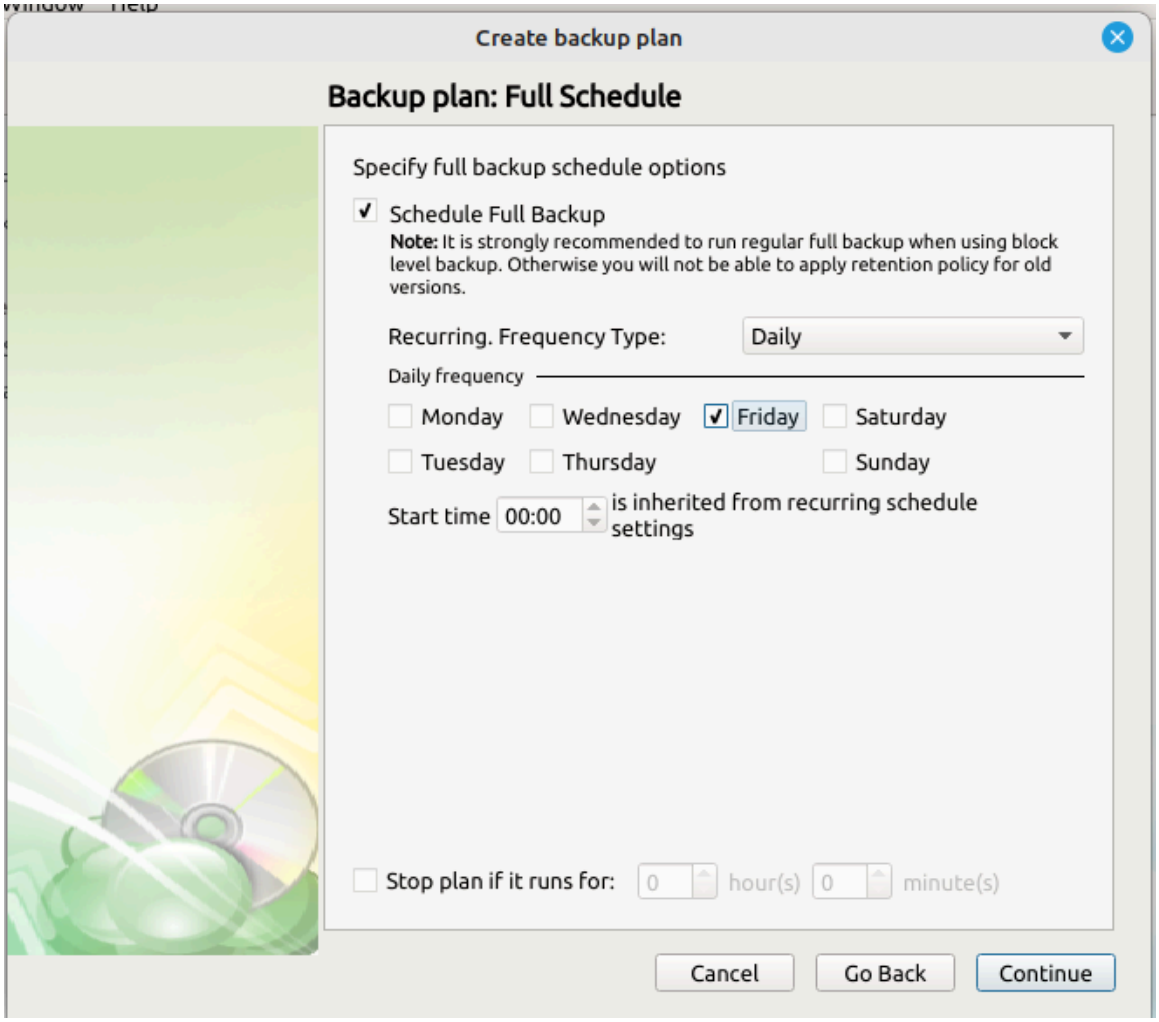
Step 9. Next, you can configure the frequency which Incremental Backups will run, or choose not to create a schedule and instead run the plan manually.



Enabling the "**Run missed scheduled backup immediately upon boot-up"** option will ensure that the backup process will begin automatically after your computer starts up if the last backup was not able to start at the scheduled time for any reason. This is the recommended option for Desktops and Laptops.

Do not use the "Stop the plan if it runs for:" option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

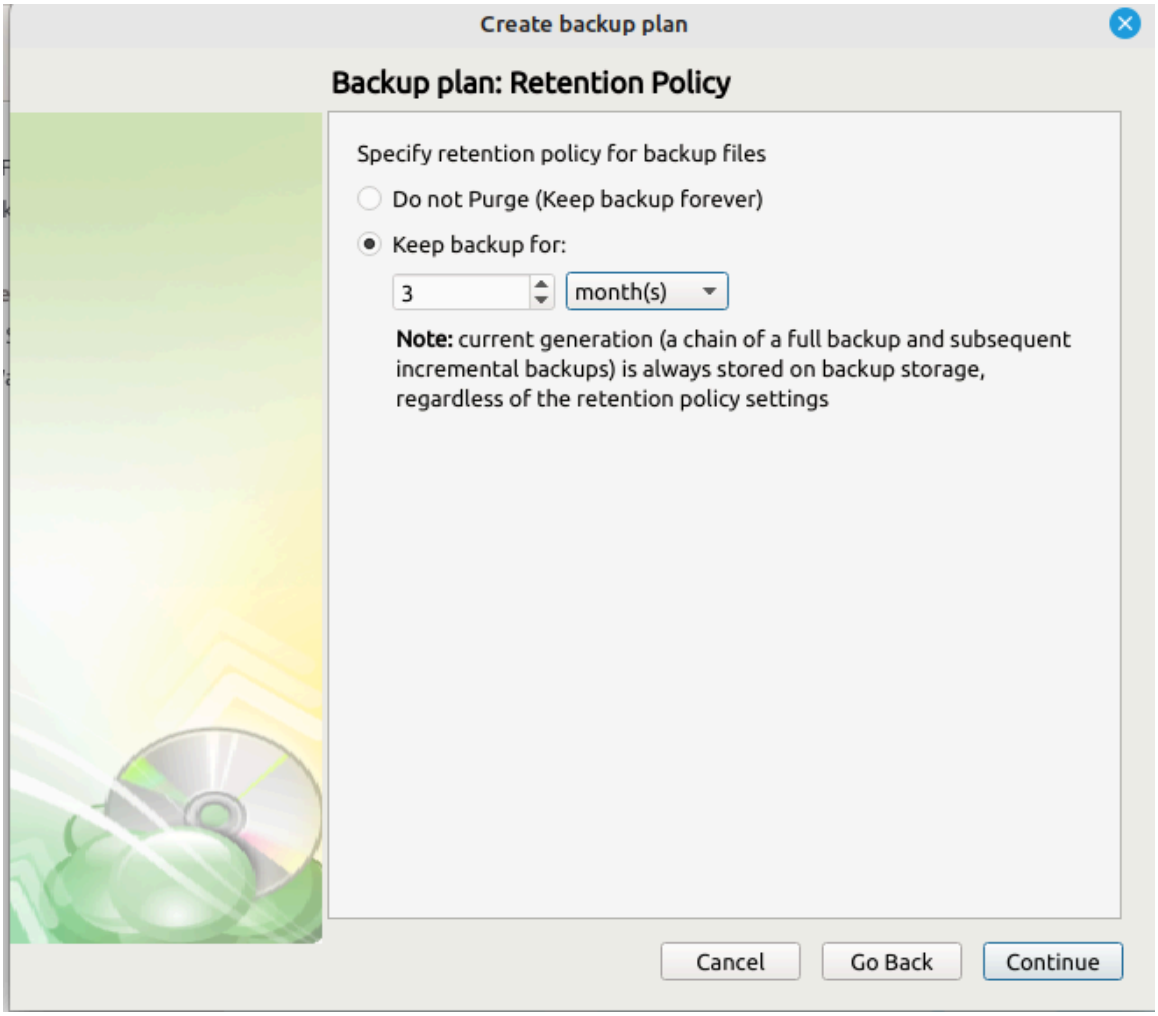
Step 10. After scheduling the Incremental Backups, the next step is to schedule how often a Full Backup will run. Full Backups are required to create backup generations and for the Retention rules to apply.



Failure to schedule Full backups will prevent the retention rules from applying. This will result in high storage costs and slower restorations.

Schedule a “Full Backup” at regular periods, once a week will be suitable in most circumstances.

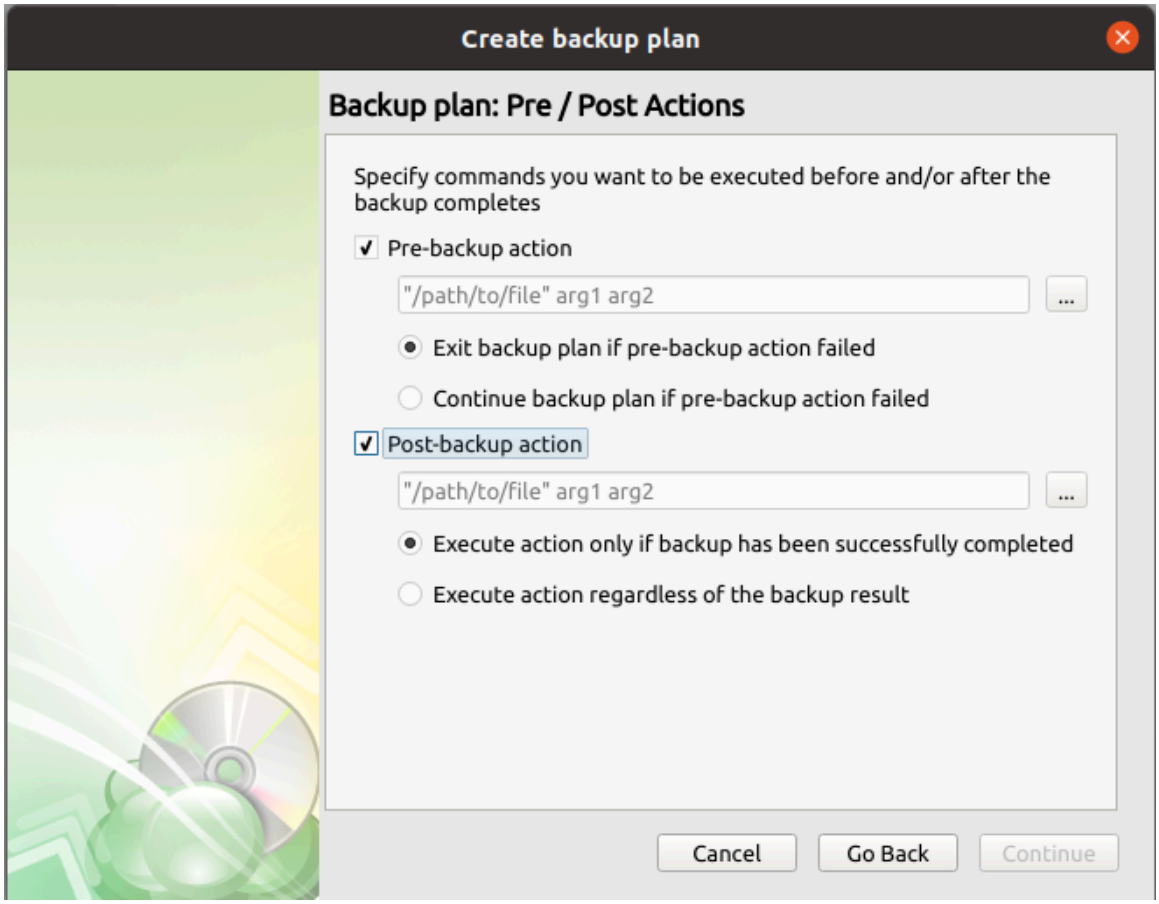
Step 11. Next, you can specify the retention policy - these are the rules that specify how data is deleted from the cloud. The process is automatically performed at the end of every successful run of the backup plan.



- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.

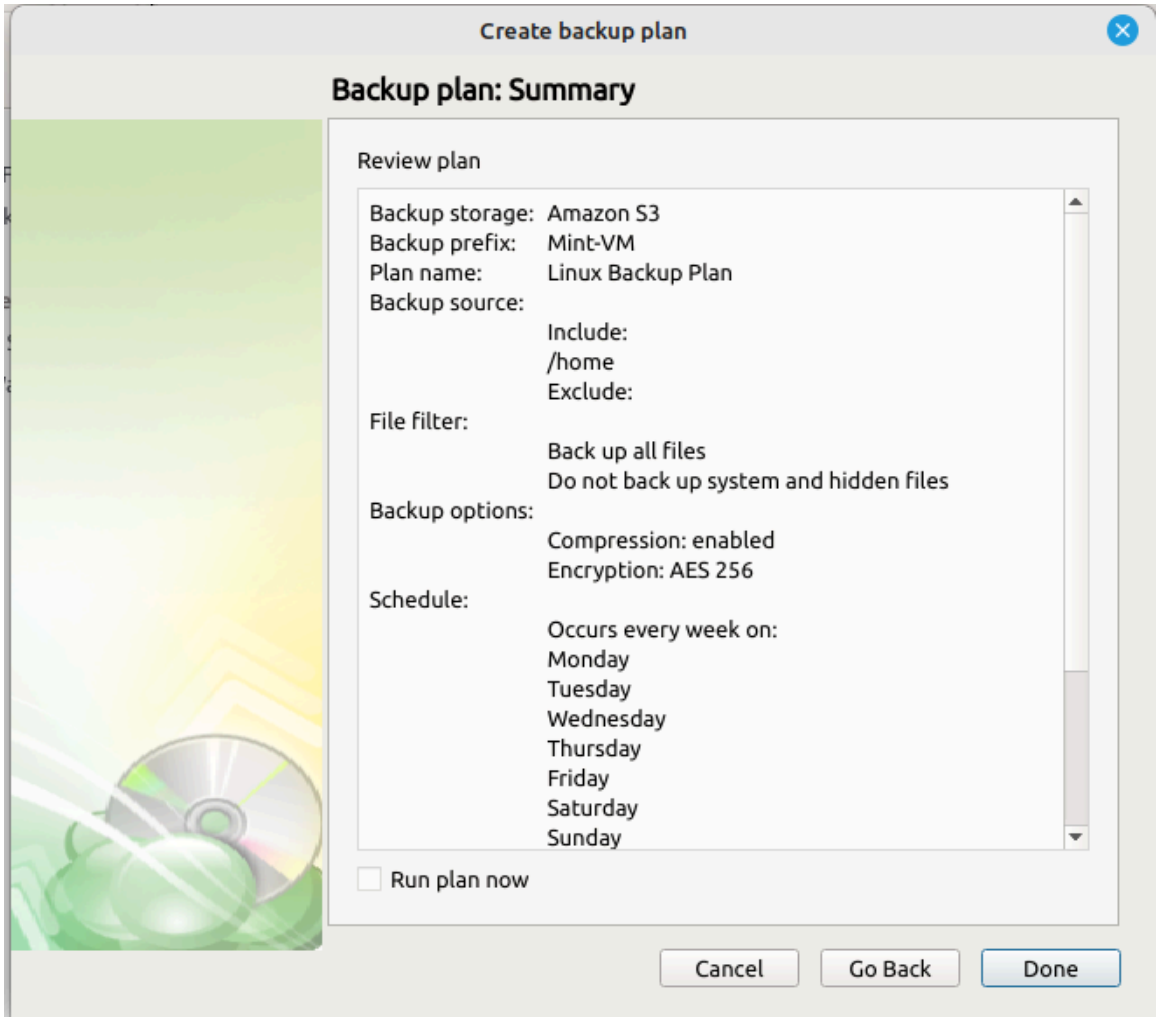
> The retention policy will only perform with regular scheduled full backups.

Step 12. The “Pre/Post Actions” page allows the execution of custom scripts before and/or after the running of a backup task.



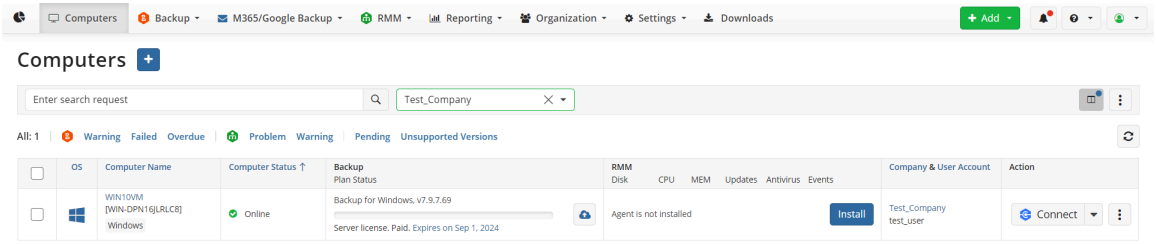
Common scenarios for using Pre/Post actions:
- How to Back Up MySQL Database using CloudBerry Backup
- How to Back Up Oracle Database using CloudBerry Backup
- How to Use Rotating Drives Strategy with MBS

Step 13. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Done”. If you select “Run plan now” the backup will start immediately, otherwise it will start at the next scheduled time.

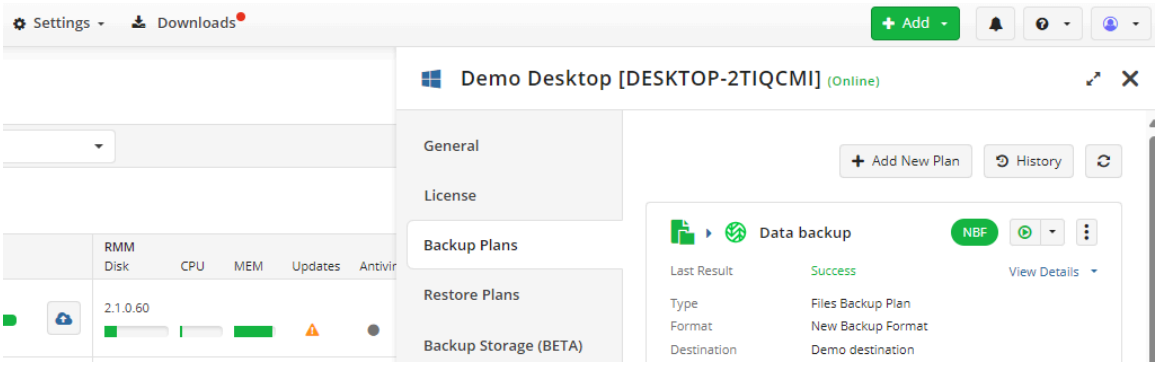


File Backup Plans using MBS

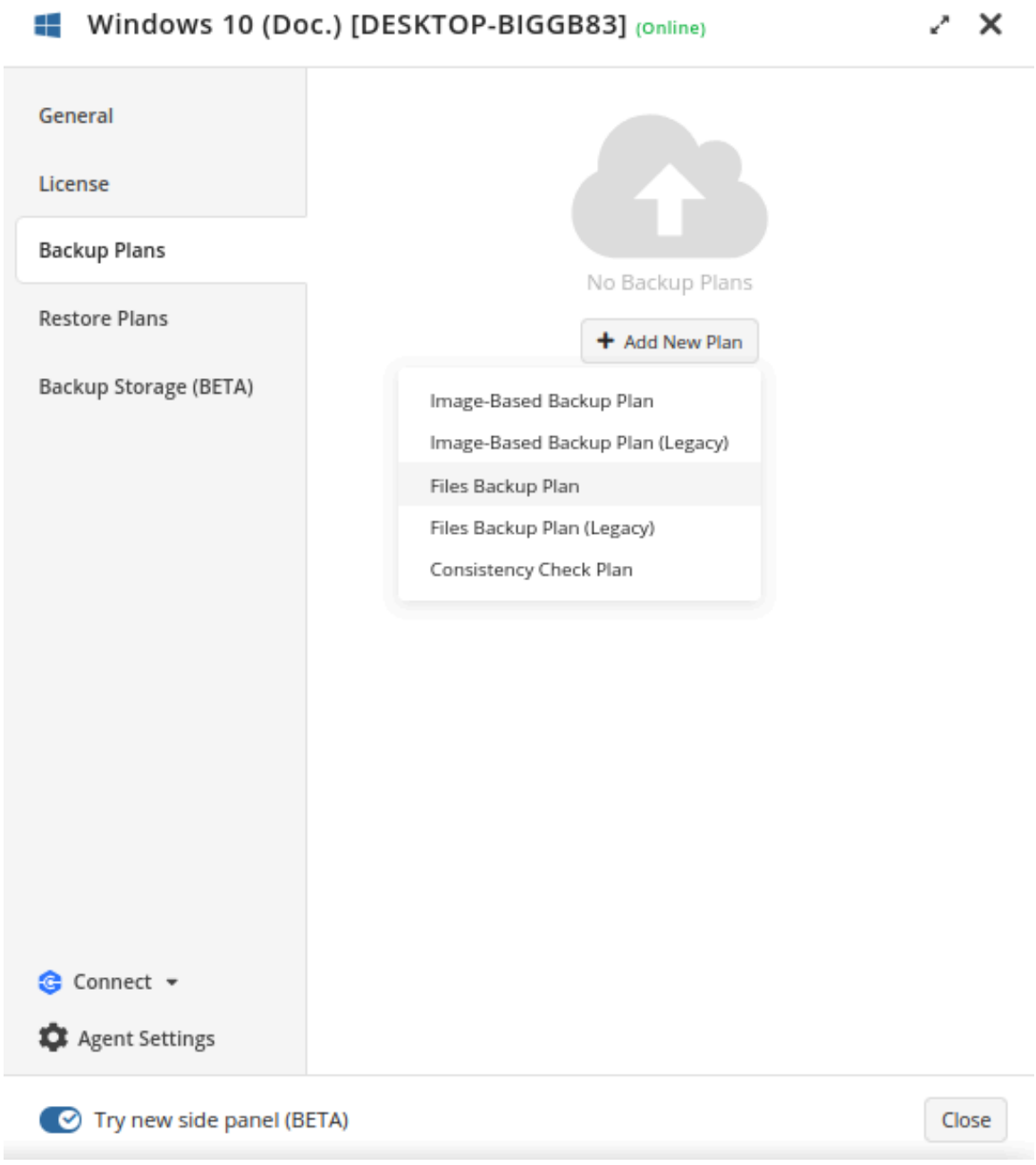
Step 1. In the MBS Console, click on Computers, or Backup > Computers, to display a list of computers available in your account.



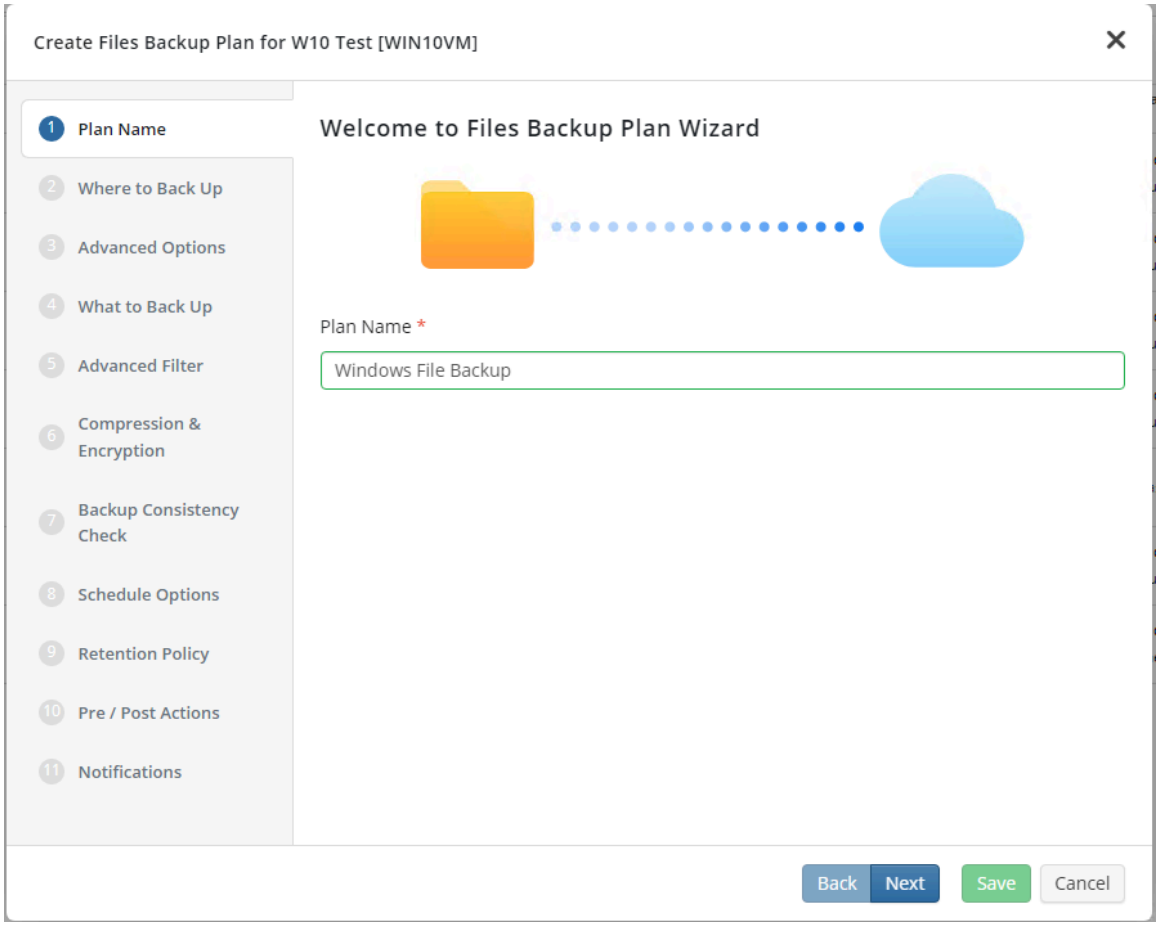
Step 2. Locate the computer you wish to backup from the list and open the current list of plans by either clicking on the name of the computer, or by selecting “Show Plans” from the gear menu.



Step 3. If it is either a newly deployed computer or a computer that already has plans, you will be printed to the backup plans tab and you'll find the 'Add New Plan' button, after this, left click on 'Files Backup Plan'

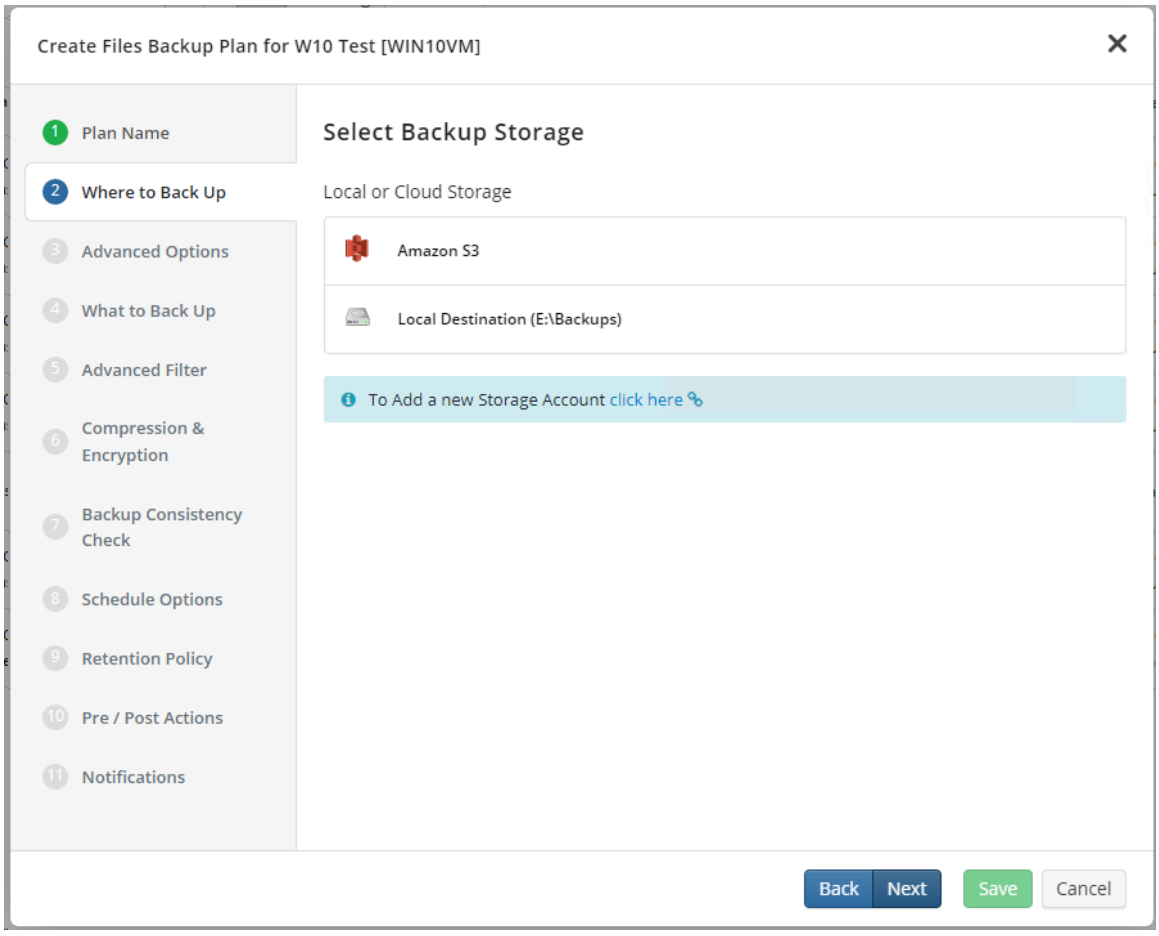


Step 4. The step in creating a new backup plan is to give it a name. Once you have entered a name, click “Next”

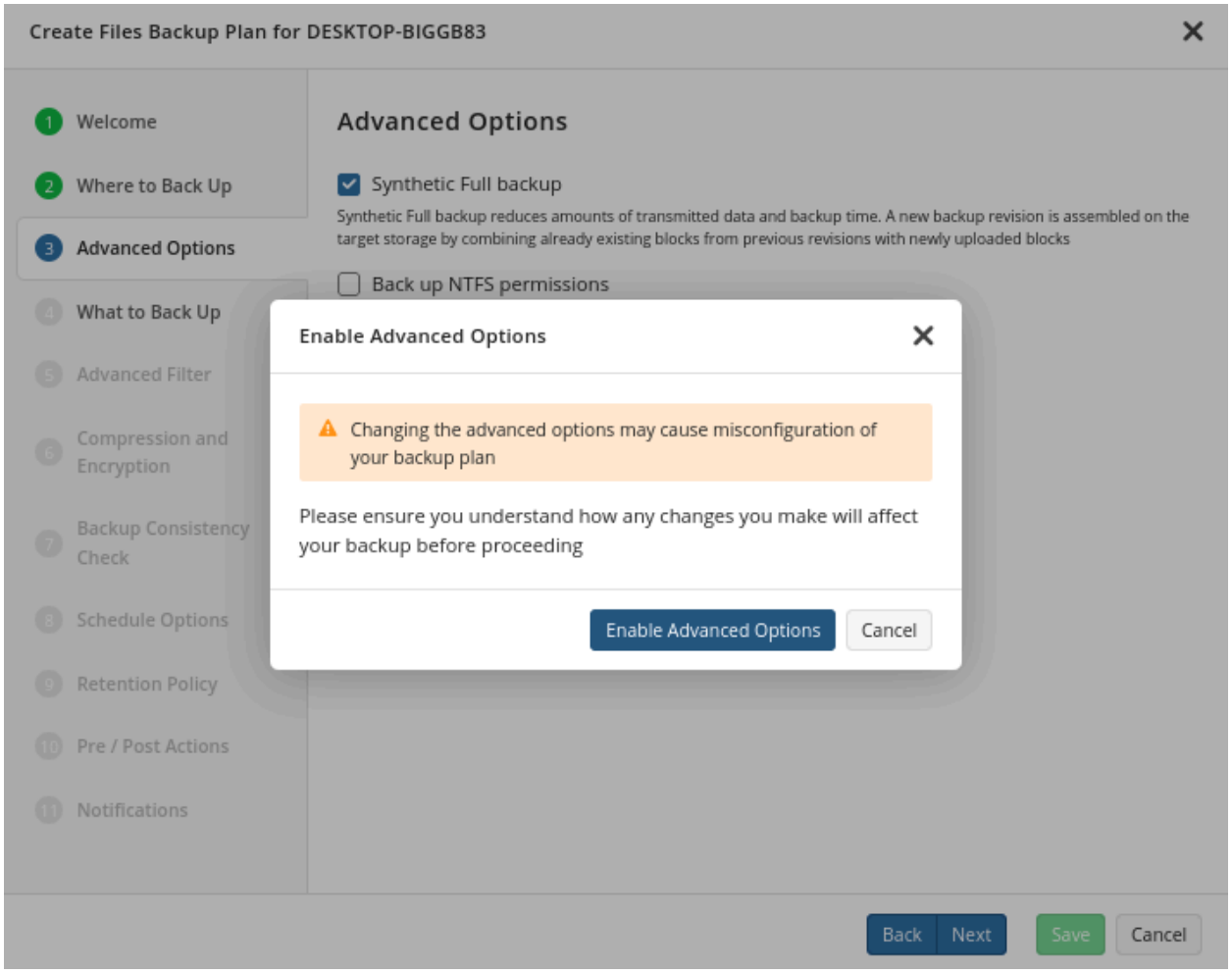


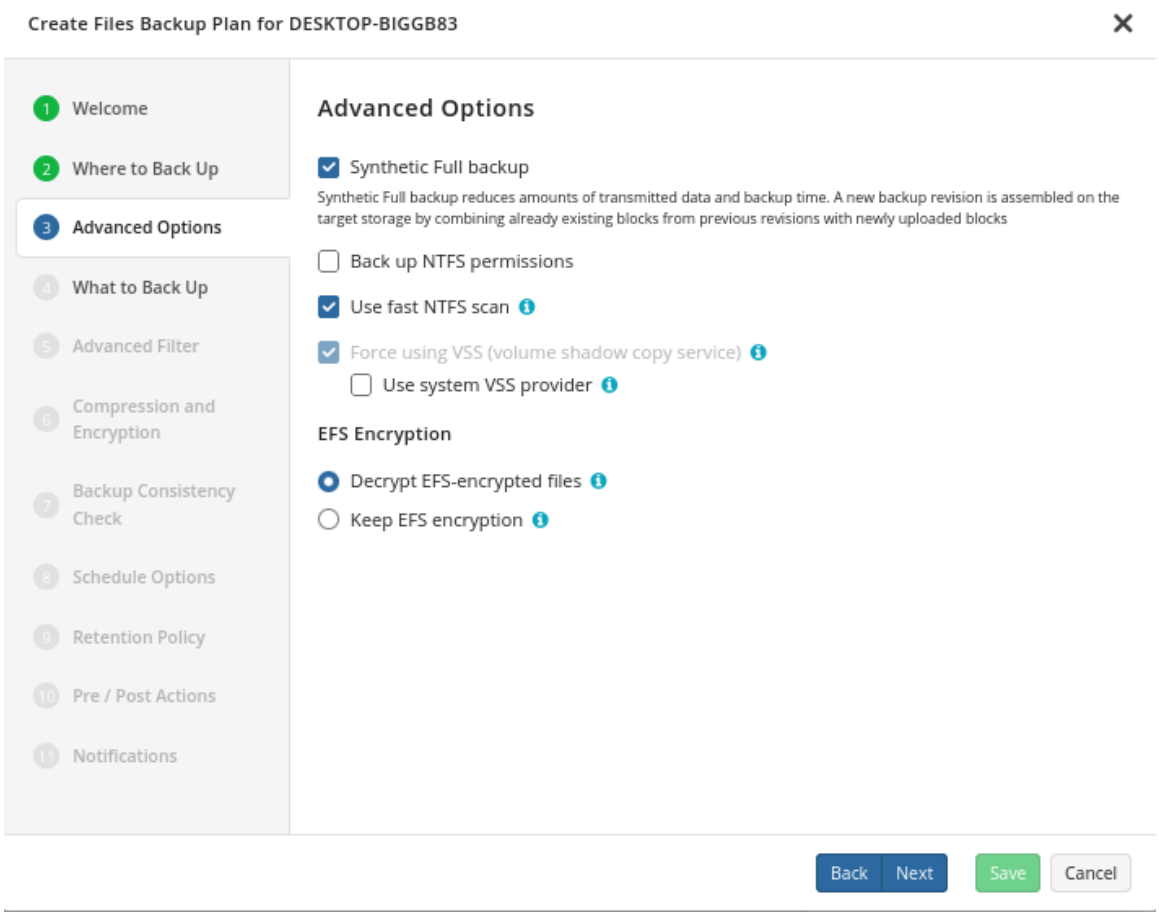
It is recommended that you select a name which helps you clearly identify the computer as well as the type of backup.

Step 5. The second step in the wizard allows you to select the backup destination. Once it is selected, click “Next”.



Step 6. By default ‘Advanced Options’ will be skipped. Click ‘Advanced Options’ and then ‘Enable Advanced Options’ to edit them



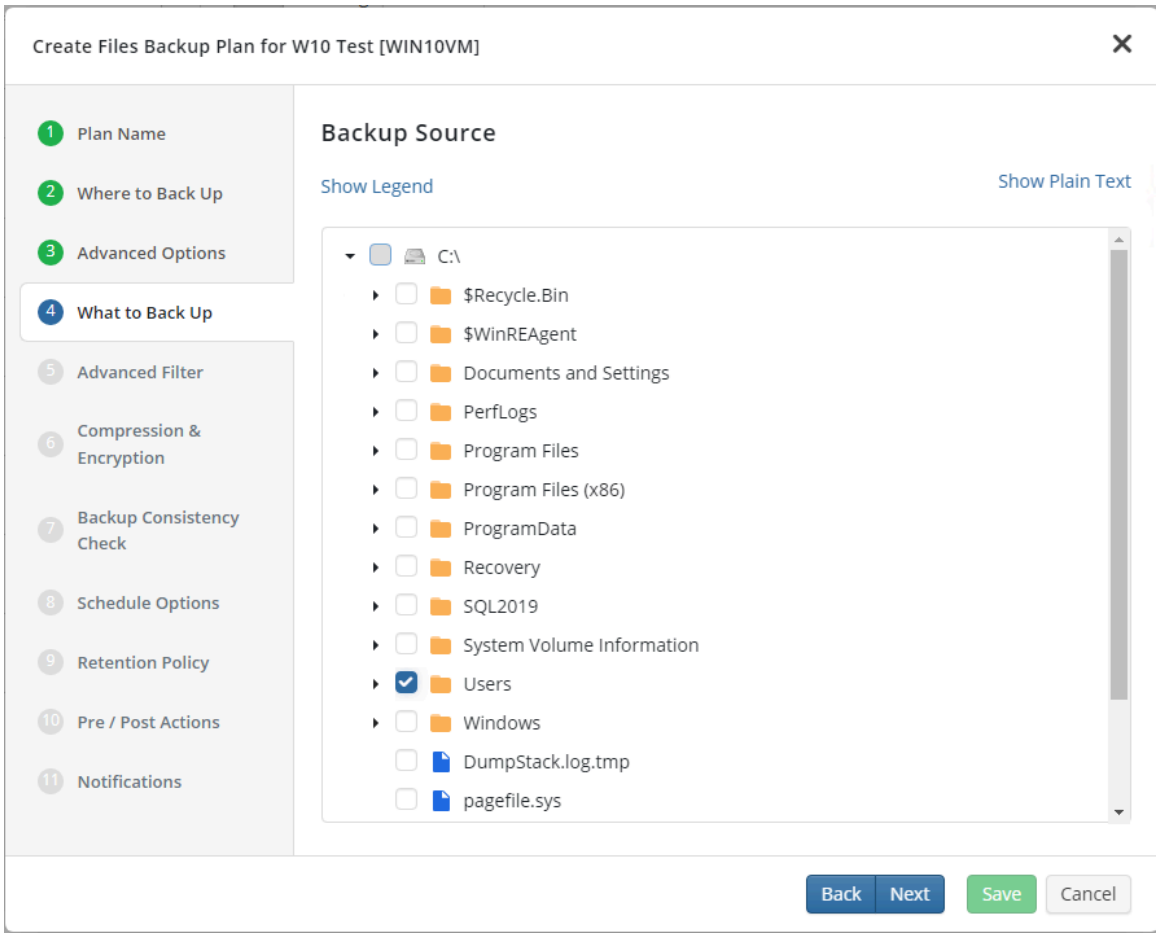


- **Use synthetic full backup:** This option is available only for backups to cloud destinations and improves performance of Full Backups by enabling the use of synthetic full backup technology.
- **Backup NTFS permissions:** Enable this option to retain all NTFS permissions assigned to your files, folders, and network shares. You may still choose whether or not to include these when restoring the files.
- **Use fast NTFS scan:** Enabling this allows the application to more quickly scan the NTFS file system for changes by using a low-level API, at the expense of increased local resource usage. The performance increase will likely only be noticeable when backing up a considerably large number of files and is also dependent on the type of device being backed up. The setting will not impact the speed of the initial full backup and will only be noticeable on subsequent backups.
- **Force using Volume Shadow Copy Service (VSS):** Select this check box to back up objects from a snapshot created by the VSS service in order to avoid any access conflicts. This option is enabled by default.

- **Use system VSS provider:** Using this option will force the application to use the native Windows VSS provider. If an error occurs while using the native provider, this option can be deselected to allow the application to scan for and use other 3rd party VSS providers. It is recommended that this option is selected by default.
- **EFS encryption:** Choose whether to keep EFS encryption intact or to decrypt the data during the backup plan execution then reenabling it.

> Before choosing whether to keep EFS encryption, refer to EFS-encrypted File Backup to determine which is the best option for your use case.

Step 7. The next step is to select the data to be backed up.

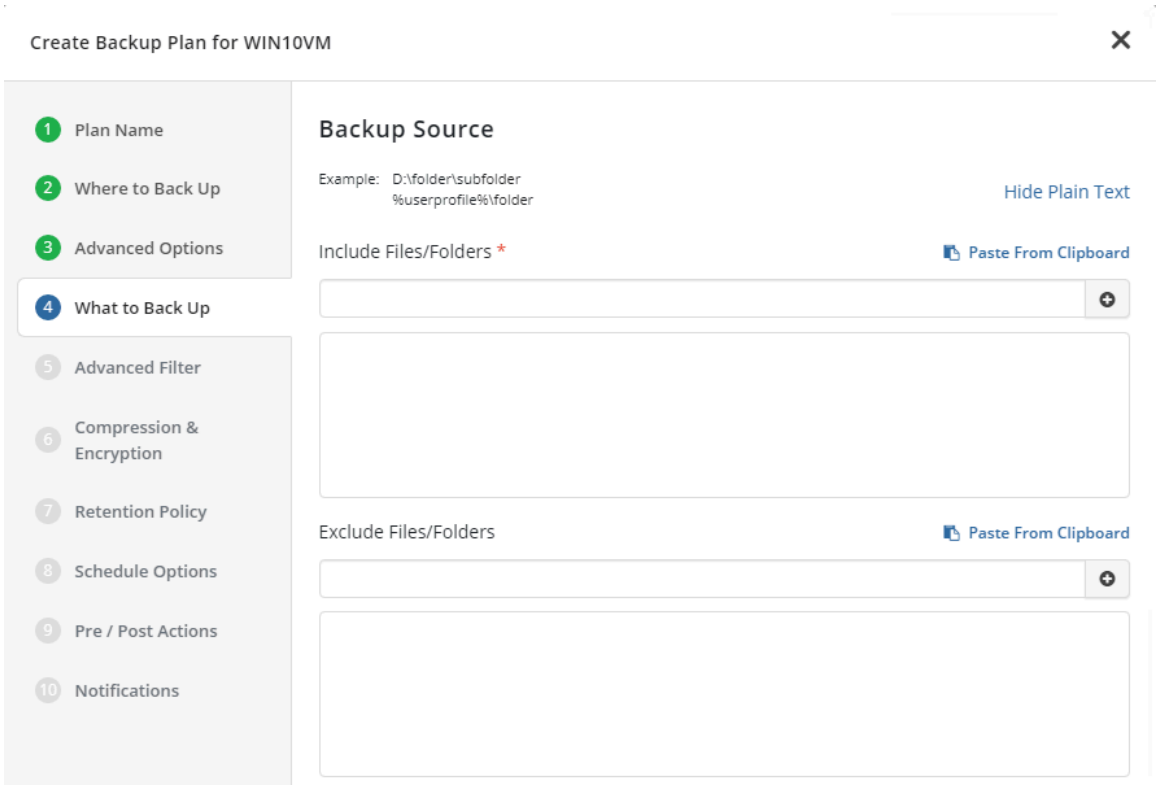


On Windows system partitions it is recommended to only back up \Users\ folder. An Image backup is better suited to back up Windows and any other installed applications.

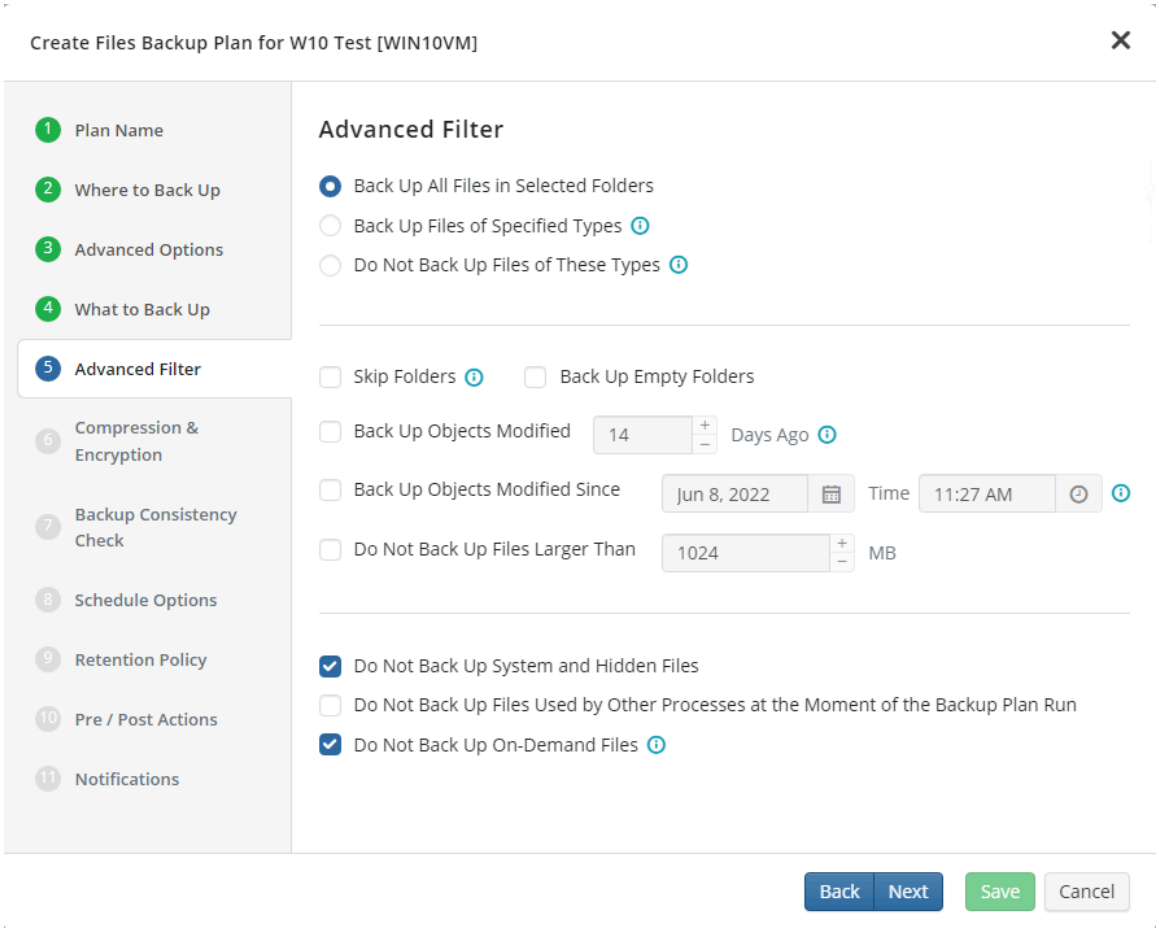
Databases cannot be backed up at the file level while in use. MSP360 MS SQL Server edition offers a robust solution for backing up active MS SQL databases.

Files and folders which are not accessible to the service account used by the backup plan will not be backed up and may cause the plan to fail.

For more advanced selection or the inclusion of a network share in the backup plan, click on the “Show Plain Text” hyperlink on the right side. This will change the file browser window to a format which allows specific paths to be included or excluded by typing or pasting in the full path:



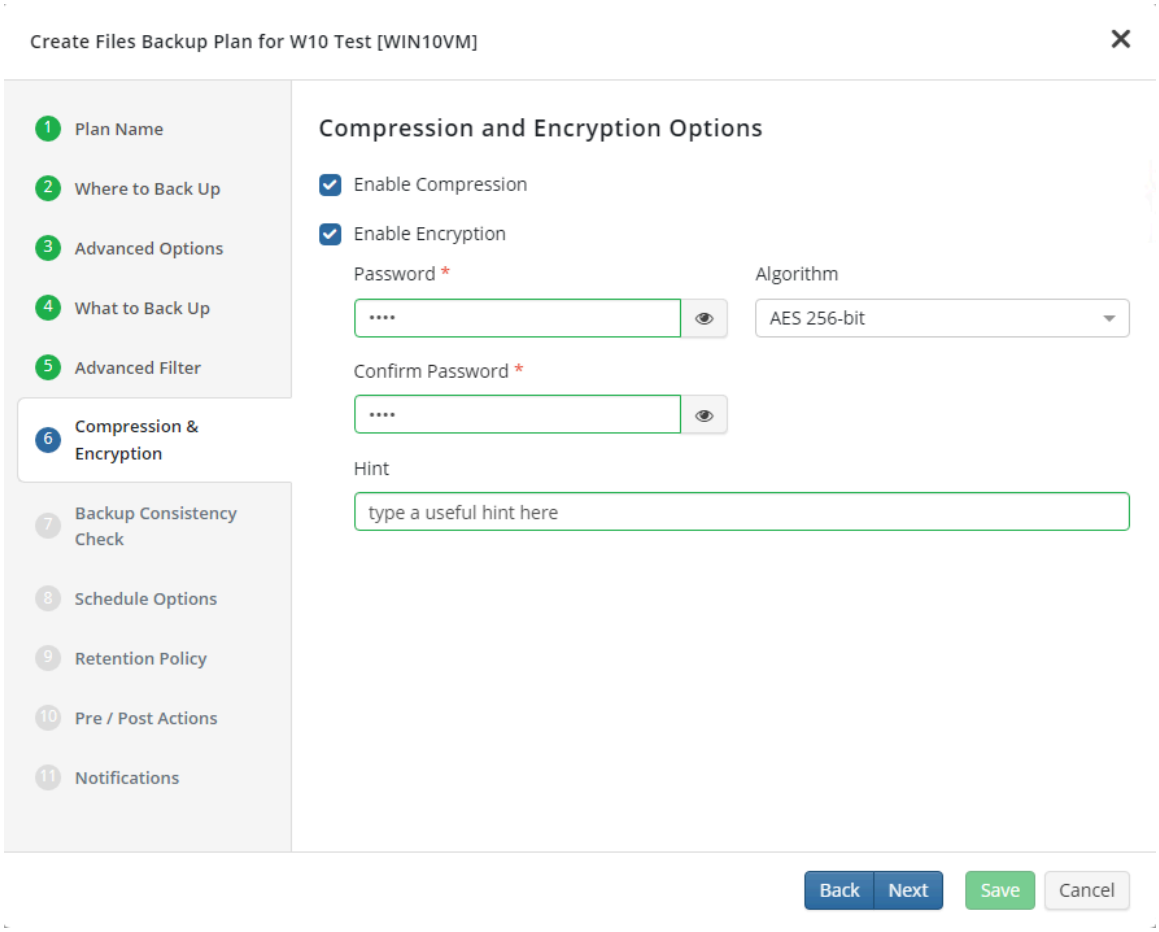
Step 8. On this step, you are presented with the “Advanced Filter” page, where you can define the various criteria that the backup service should use when determining which files should be backed up based on more advanced filtering than is available through the check boxes on the previous step.



When using the Advanced Filters, the number of files actually uploaded can differ from the number of files that are calculated in the local folder Properties.

“Skip Folders” will exclude any folders that contain the specified partial name. For example, “temp” will exclude all folders with “temp” in the name in all sources.

Step 9. Once the source data is selected, you can now choose whether to compress or encrypt the data.

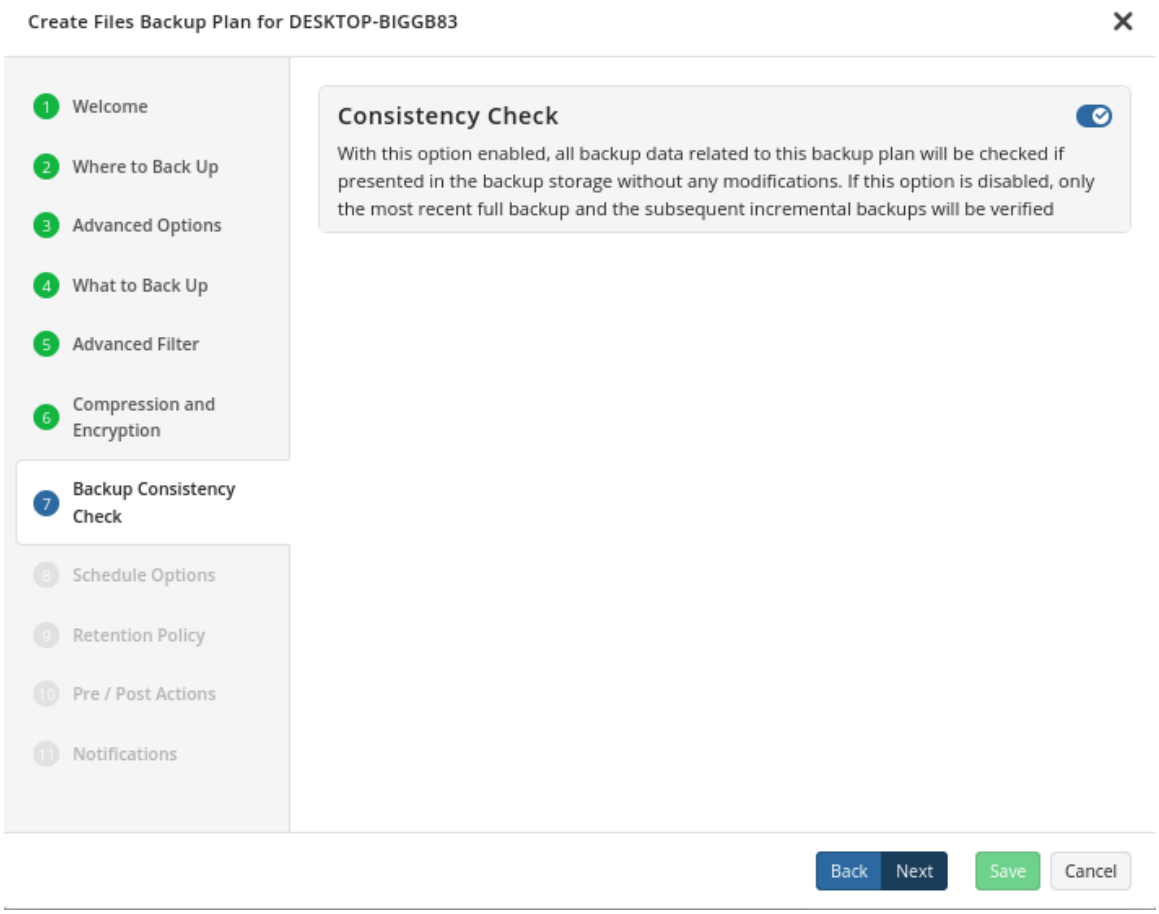


Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

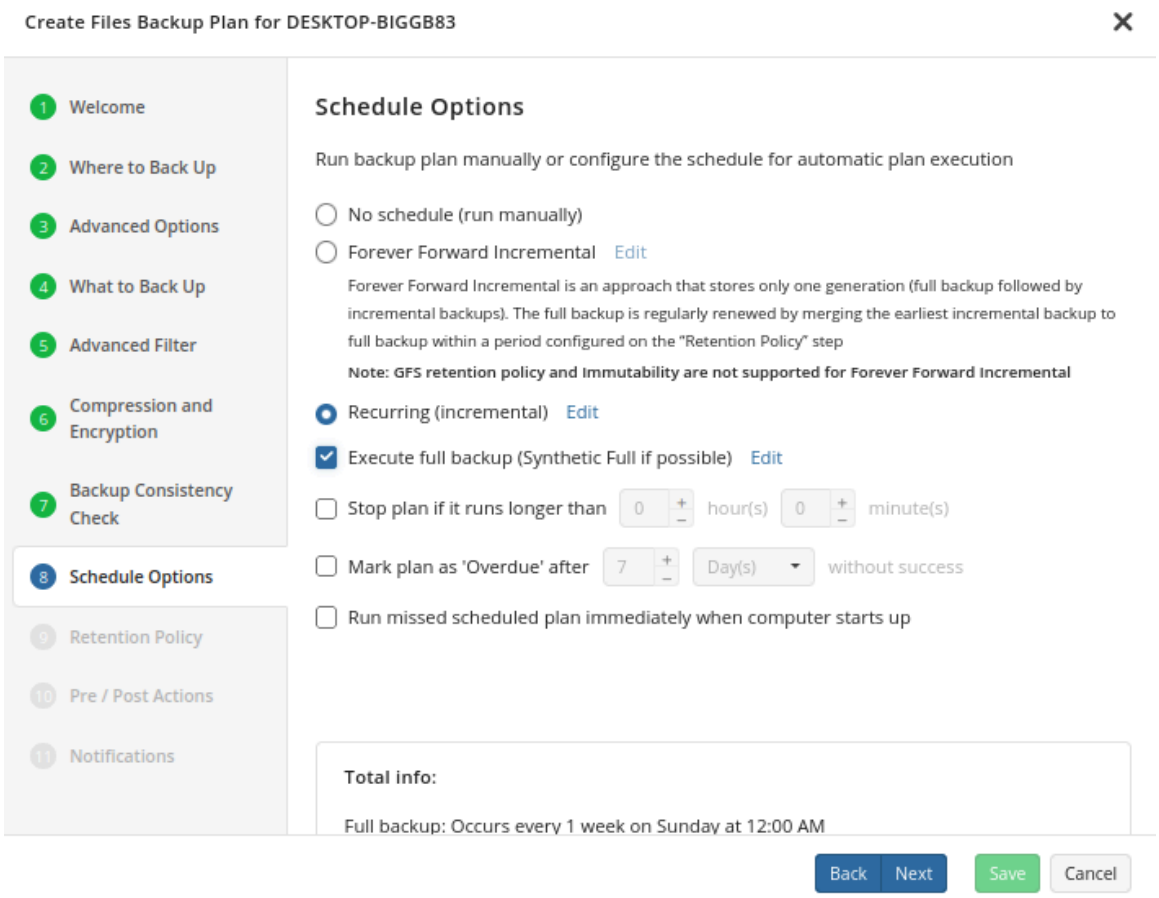
Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place and enable the Password Recovery Service.

Step 10. Next you are presented with an option for the type of Backup Consistency Check to use with the plan. It is recommended that you leave “Enable Full Consistency Check” enabled.



Step 11. Next you are prompted to set the schedule for your backup plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.



The Forever Forward Incremental (FFI) backup schedule minimizes storage usage by retaining only one full backup. Subsequent backups store only incremental changes. The number of restore points depends on the backup frequency and retention policy.

Schedule a “Full Backup” at regular periods, once a week will be suitable in most circumstances.

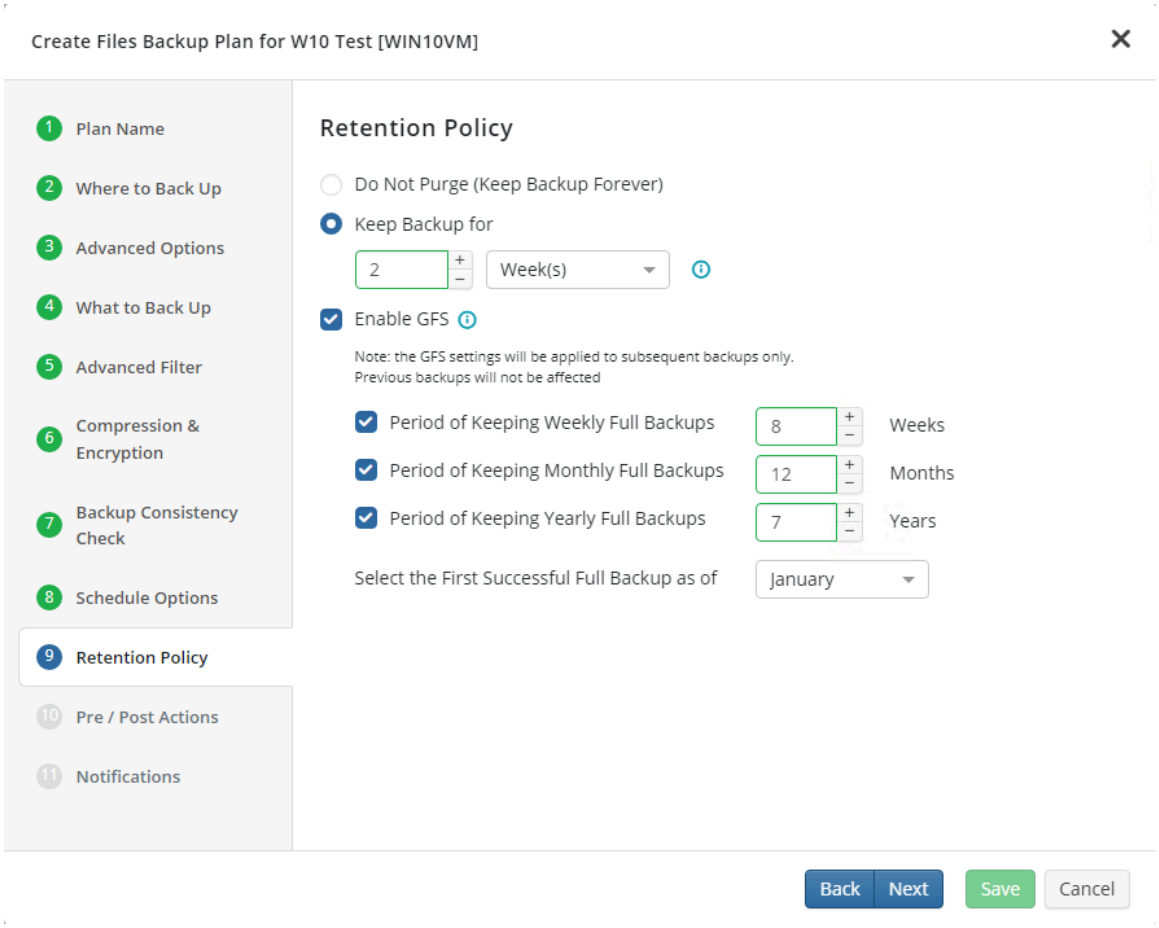
The retention policy will only perform properly with regular scheduled full backups.

- Block Level Backup and Full Backup Explained

Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

Step 12. On the “Retention Policy" step, you can set the policies the application will use to determine which data to purge at regular intervals and define the multigenerational Grandfather-Father-Son (GFS) parameters if required.



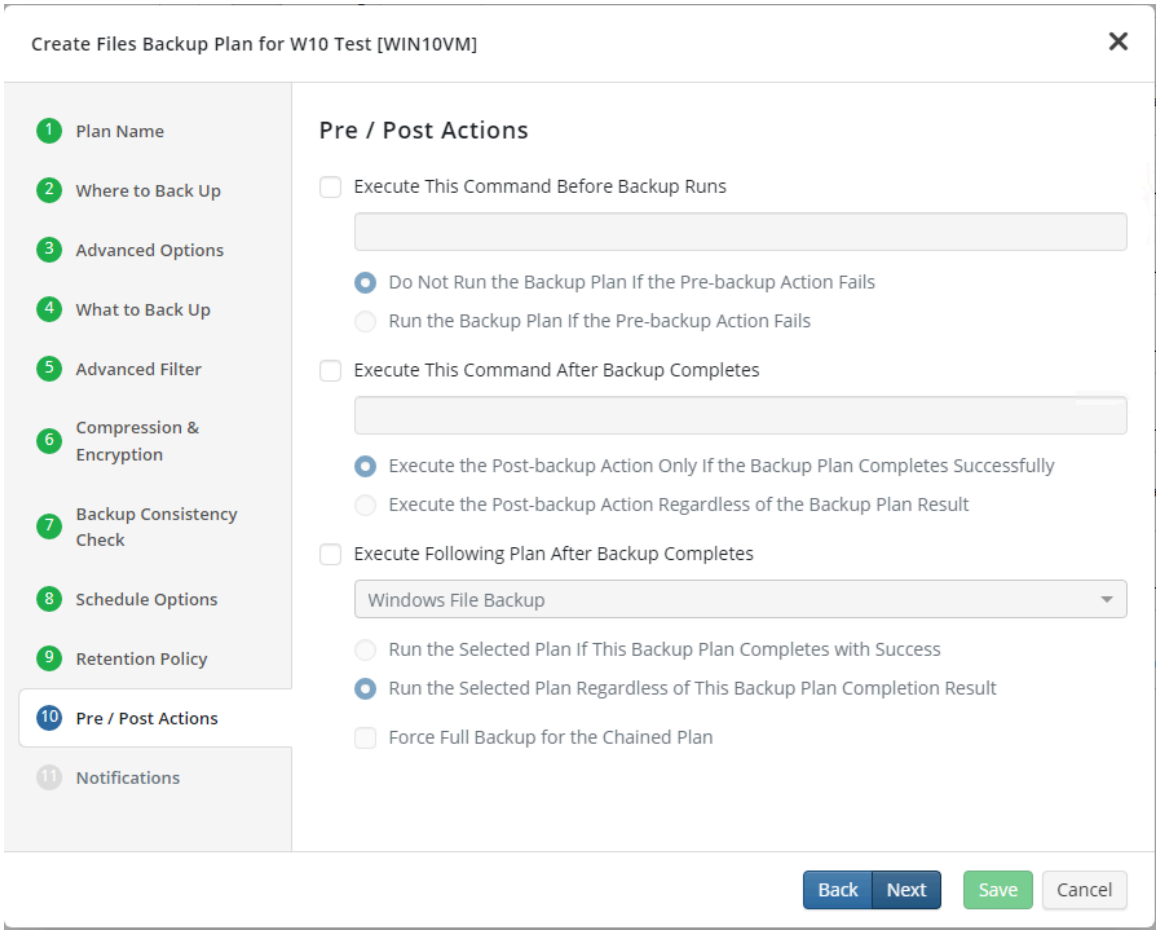
- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.
- **Enable GFS**: Select this option if you want to keep Full Backups for archival purposes at the selected intervals.
- **Period of keeping weekly full backups**: Set the number of Weekly Full Backups to retain. This is determined separately from the “Keep backup for” value and relies on Full Backups to be scheduled on at least a weekly basis in the previous step.
- **Period of keeping monthly full backups:** Number of Monthly Full Backups to retain. A Full Backup can be flagged as both a Weekly and Monthly backup, but once the number of Weekly Full Backups has exceeded their retention setting, only those also flagged as a Monthly will be retained.

- **Period of keeping yearly full backups:** Set the number of Yearly Full Backups to retain. A Full Backup can be flagged as a Weekly, Monthly, and Yearly Backup. Once the number of Monthly Full Backups has exceeded their retention setting, only those also flagged as a Yearly will be retained.
    - **Select the first successful full backup as of**: Select the first Monthly Full Backup you would like to flag and retain as the first Yearly Full Backup.

Restore Points will not be deleted until the youngest point in the chain has met the retention criteria.

GFS Retention provides an excellent way to efficiently archive data for compliance. Additional information can be found in GFS Policy topics in the MBS Documentation

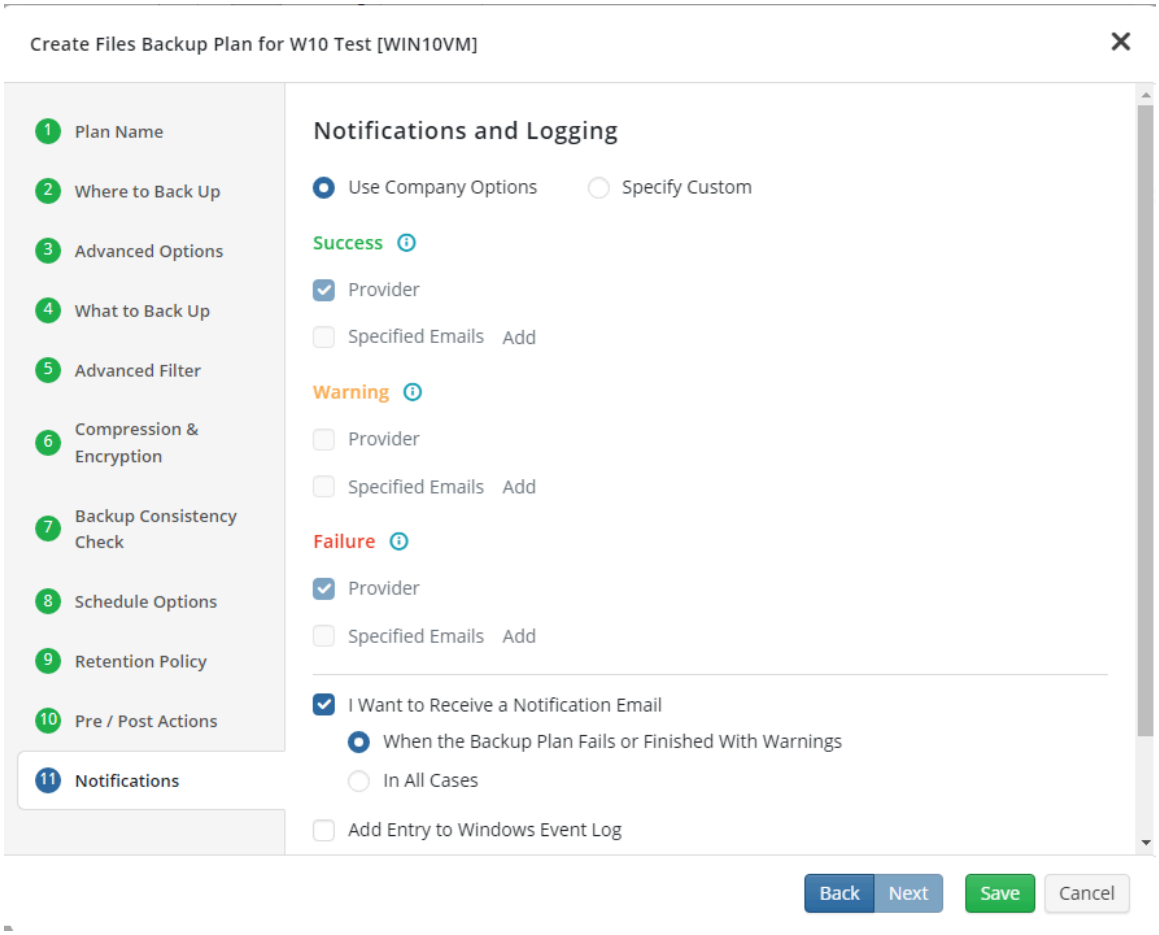
Step 13. The “Pre/Post Actions” page allows the execution of custom scripts before and/or after the running of a backup task, and can chain multiple backup tasks together for sequential execution.



Common scenarios for using Pre/Post actions:

- How to Back Up MySQL Database using CloudBerry Backup
- How to Back Up Oracle Database using CloudBerry Backup
- How to Use Rotating Drives Strategy with MBS

Step 14. The final step when creating a Backup Plan is to review the Notifications and Logging. The default settings applied at the Company level are selected by default, however you are also able to specify custom options per plan.

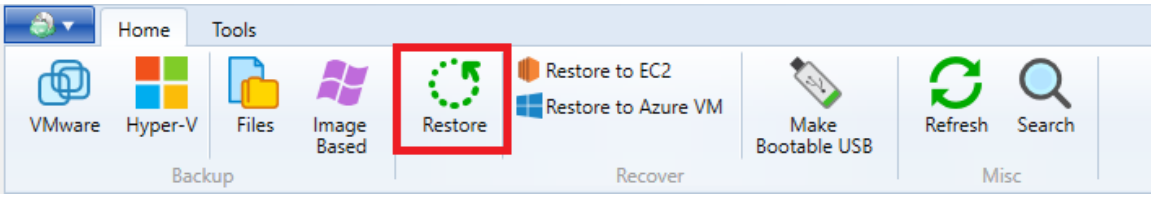


Once you are satisfied with the selected notifications and logging, clicking “Save” will create the new plan and close the wizard.

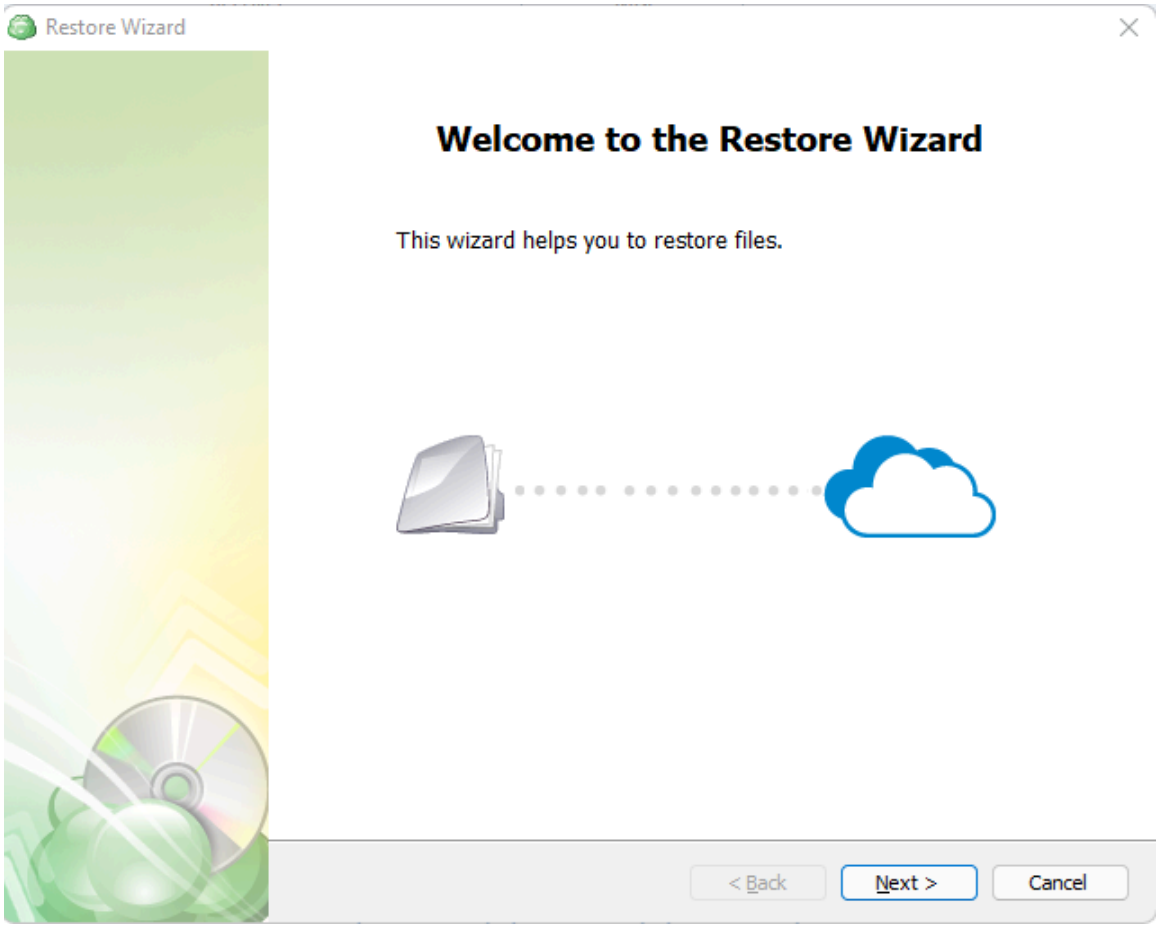
File-Level Restore Plans

Restore for Windows using the Agent

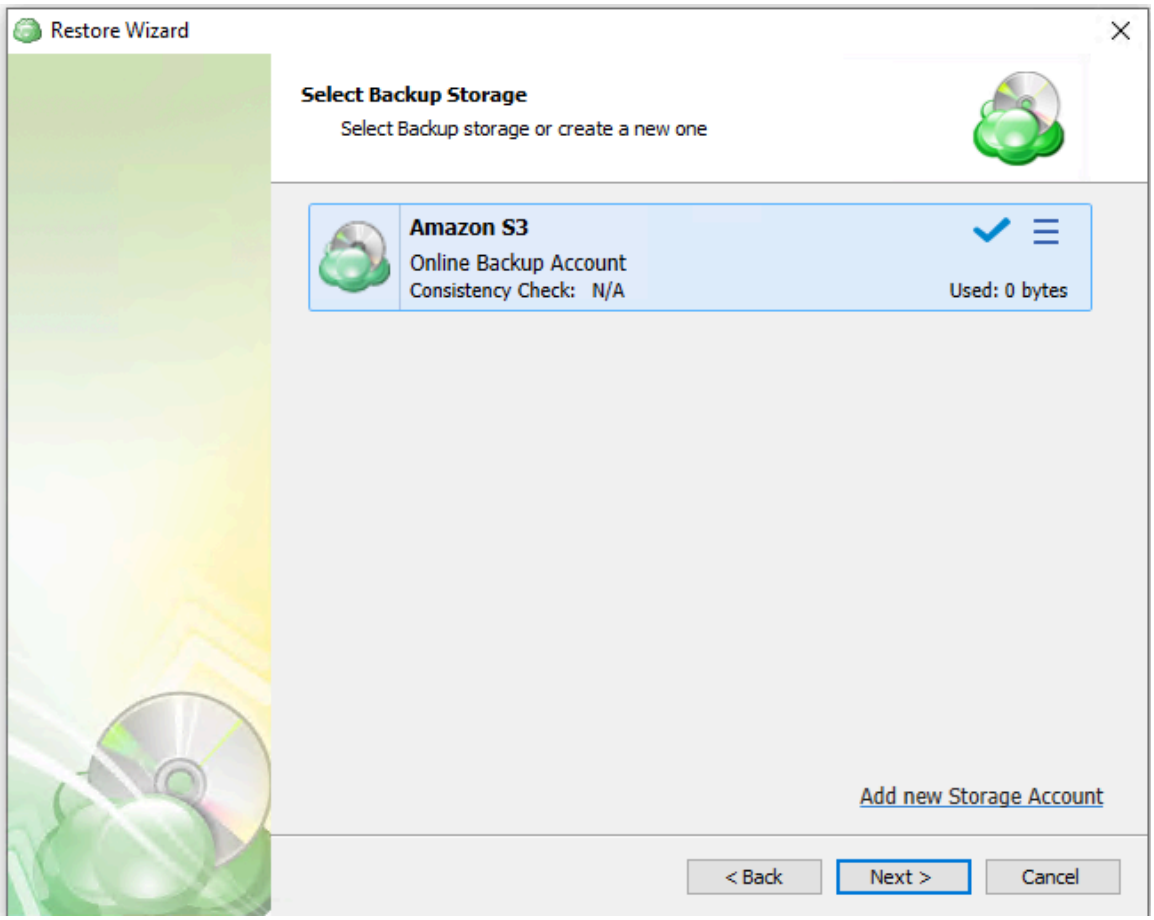
Step 1. After launching the Online Backup, you can run the Restore Wizard by clicking on “Restore” main toolbar.



Step 2. Click on “Next” to advance past the welcome screen for the wizard

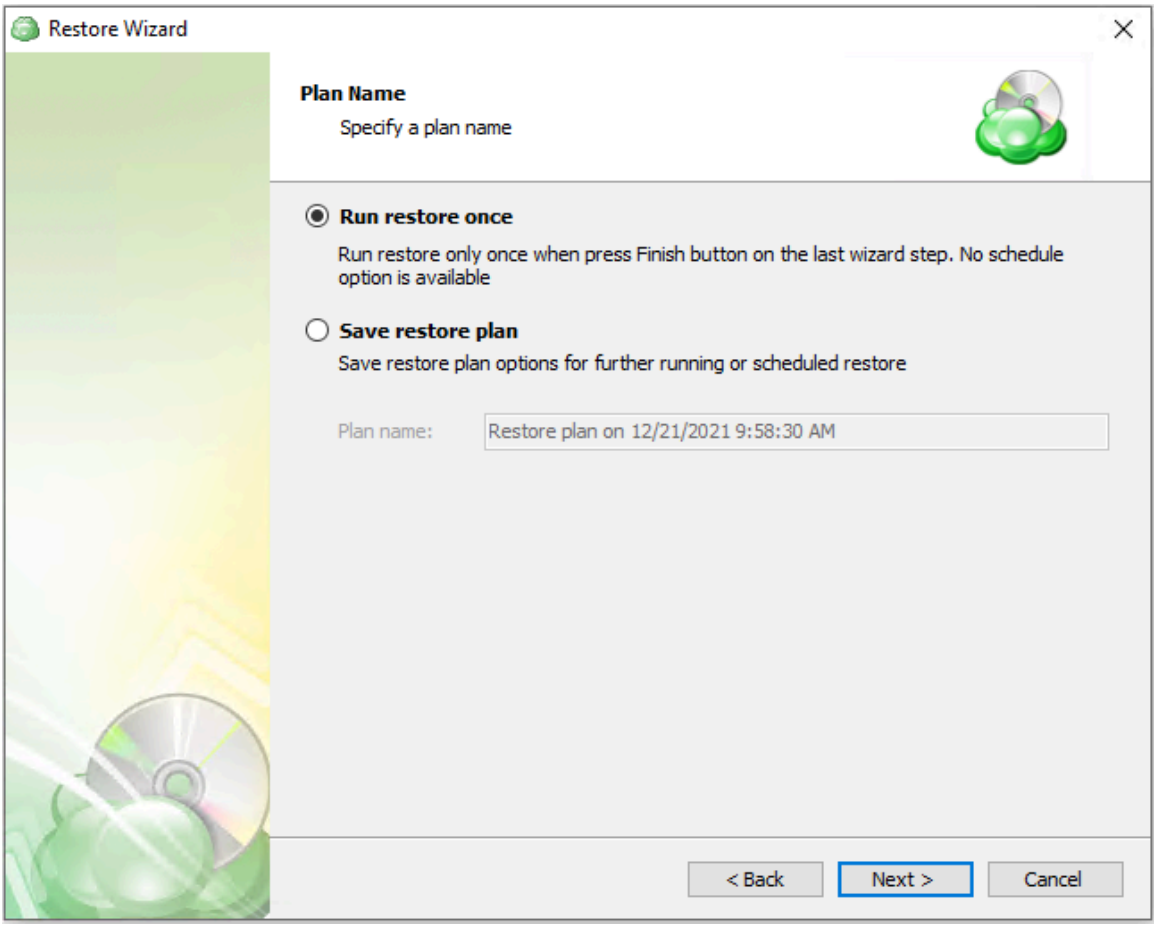


Step 3. The next step will prompt you to select the source for the restore.



If the desired source is not in the list, you can click “Add new Storage Account” to add it.

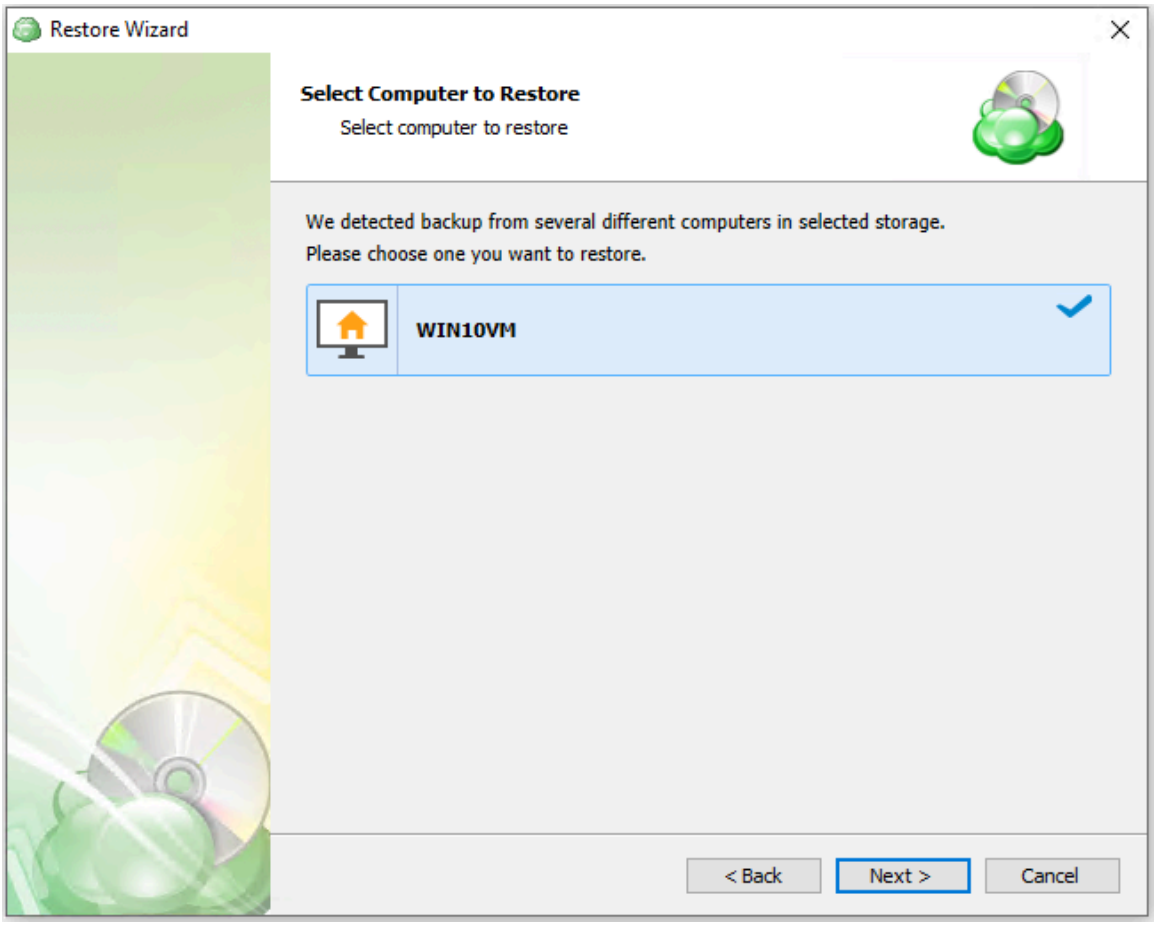
Step 4. Once the source has been selected, the next screen allows you to choose between running the plan a single time or saving it for later use.



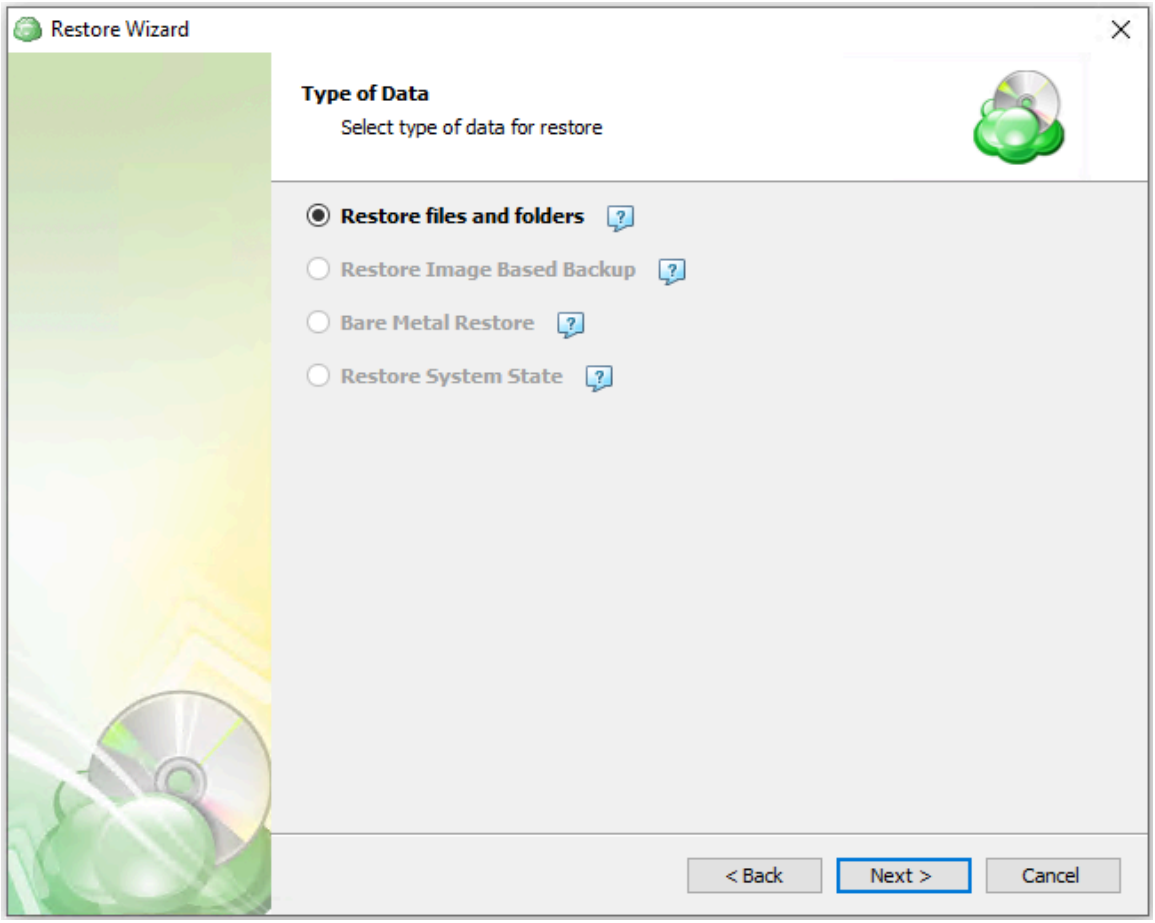
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

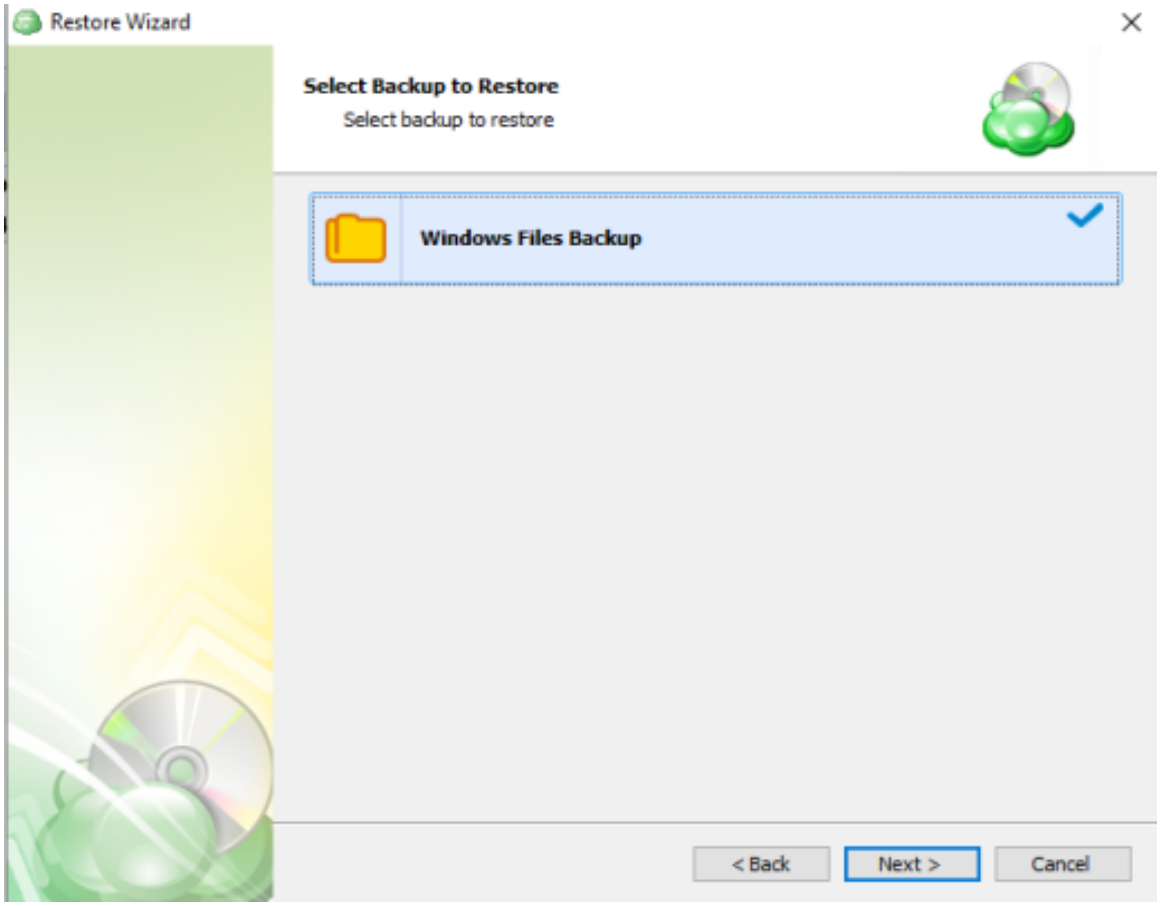
Step 5. With the type of restore selected, the next step is to select the correct computer to be restored.



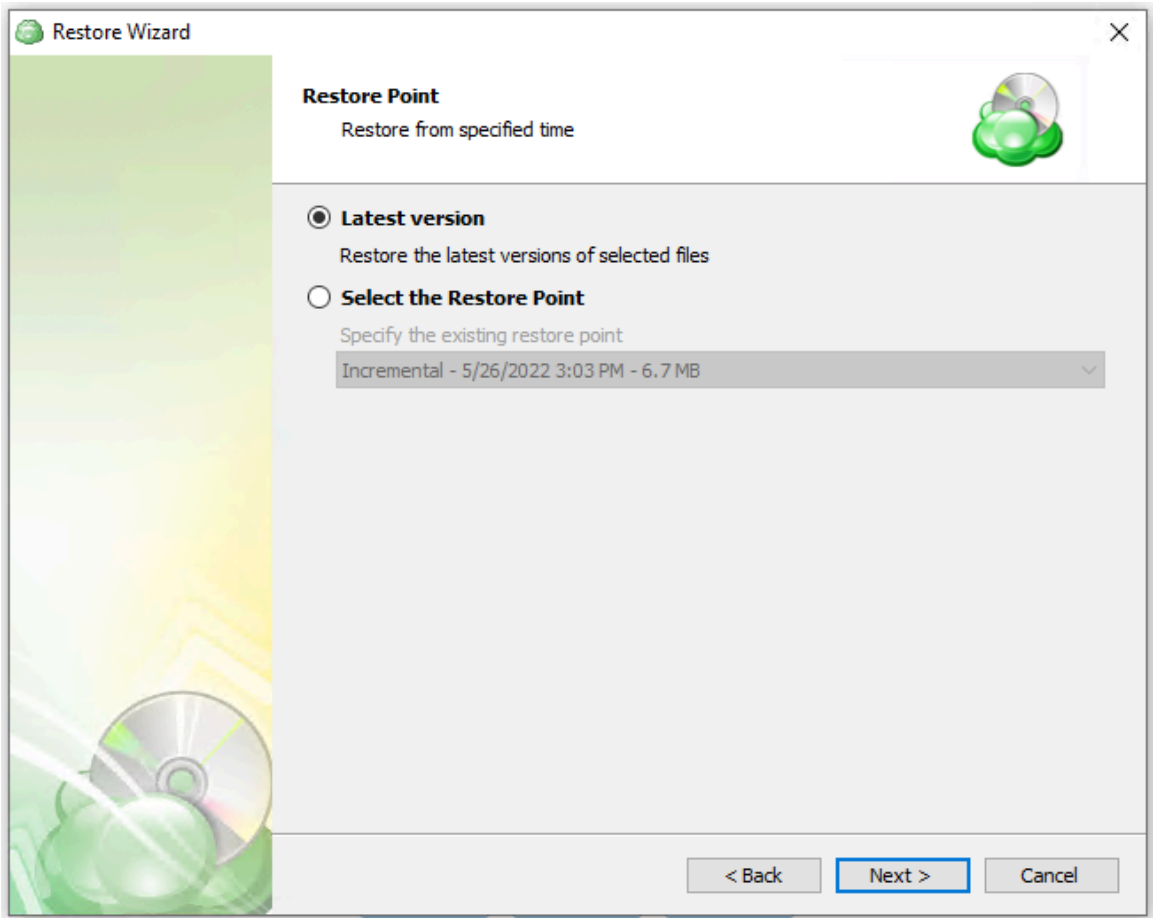
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore files and folders” option to continue.



Step 7. With the correct type of restore selected, the application will generate a list of available backup plans.



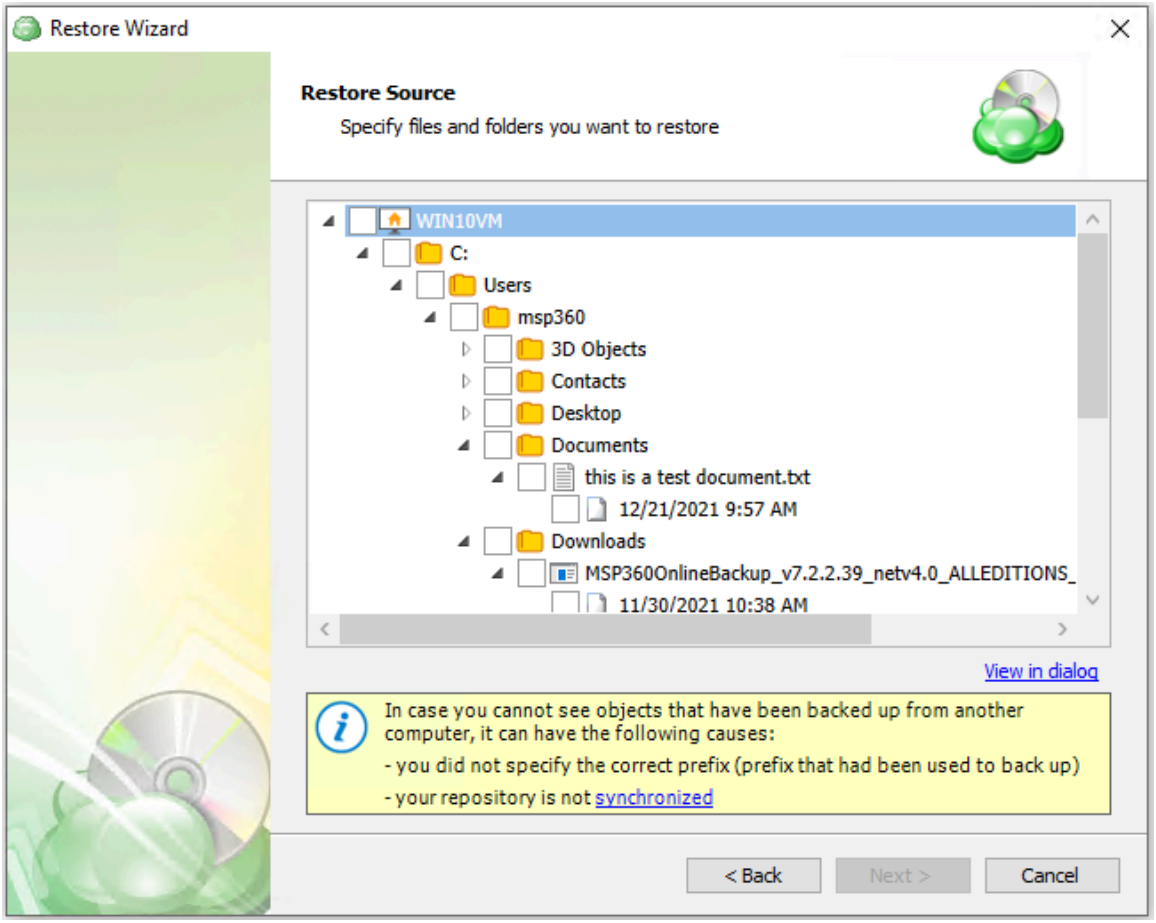
Step 8. Next you will be given a choice for what point in time you would like to restore the files to.



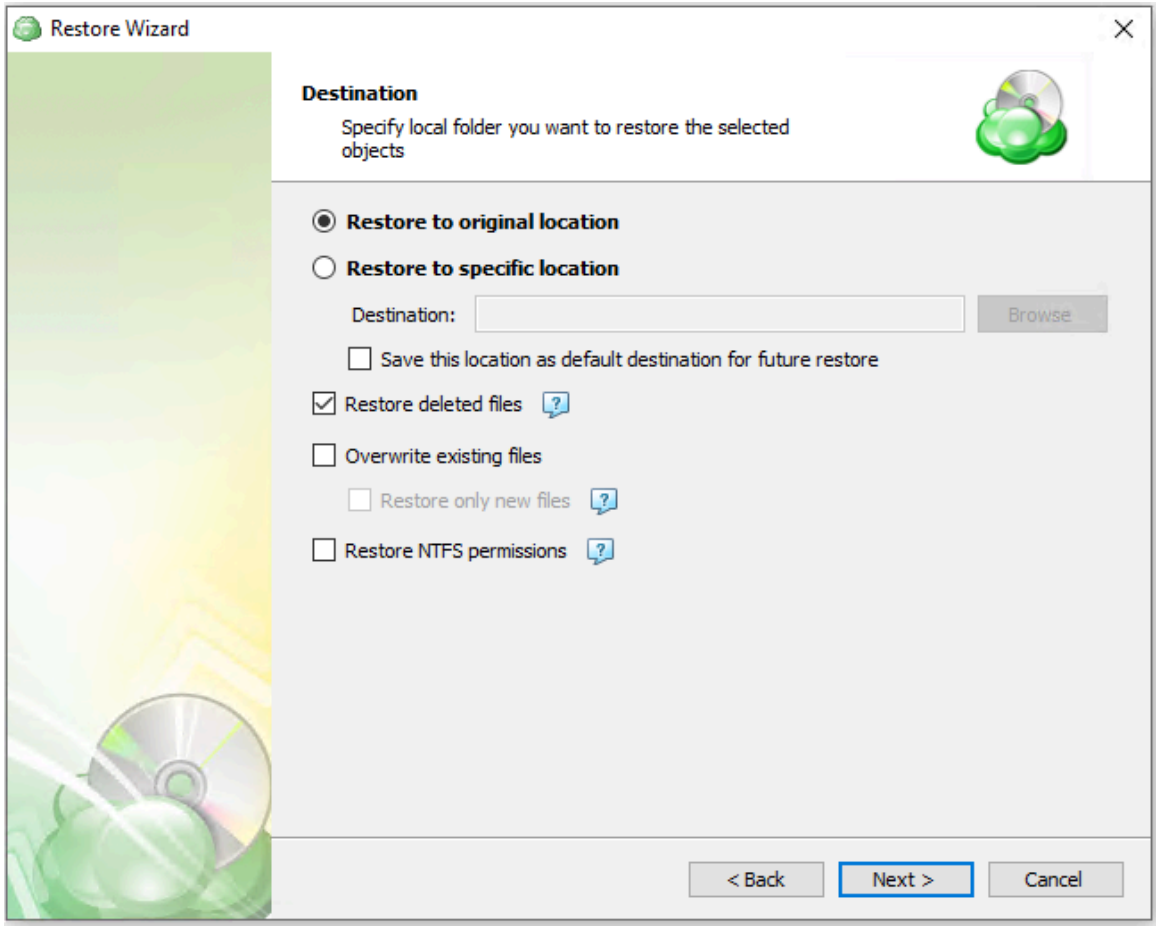
- **Latest Version:** Automatically restores the newest version of each file in the source regardless of which restore point it belongs to.
- **Select the Restore Point:** Restores the files as they existed at the specified restore point.

> If there is no copy of a specific file at the selected restore point, the application will automatically select the newest version from previous restore points.

Step 9. Next, you will be able to expand the restore source and browse through the available files and folders. If “Manually” was selected on the previous step you will also be able to expand each individual file to select which version to restore.



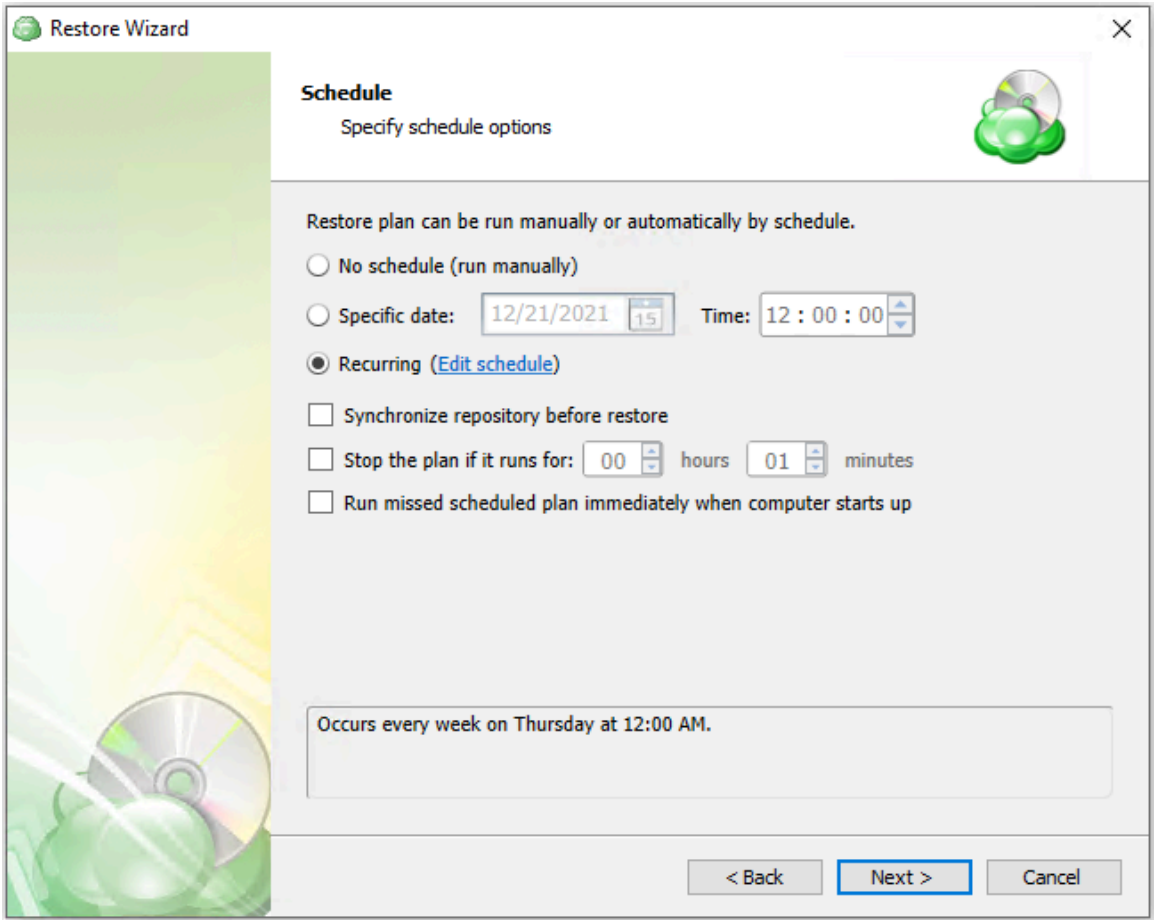
Step 10. After selecting the files or folders to restore, you are able to select the location they should be restored to.



- **Restore to original location:** Automatically restores all files to their original location but does not overwrite existing files unless otherwise specified.
- **Restore to specific location:** Allows you to choose the path to where the files should be restored. Any files or folder structure needed will be created within the designated path.
- **Restore deleted files:** The application will restore files currently marked as having been deleted in the source but which were present at the point in time selected for the restore. Only applies if the backup plan was configured to track deleted files.
- **Overwrite existing files:** Allows existing files to be overwritten by the restore process.
- **Restore only new files:** The plan will intelligently detect the files currently in the destination and only files for which the version in the backup is newer than the destination.
- **Restore NTFS permissions:** Any NTFS permissions will be reapplied to the restored

files. If this is left unchecked the restored files will inherit the permissions of the parent folder. Only applies if the backup plan was configured to backup the NTFS permissions.

Step 11. If “Save restore plan” was selected at the start of the wizard then the next step is to set the schedule for the restore plan. Otherwise this step will be omitted.

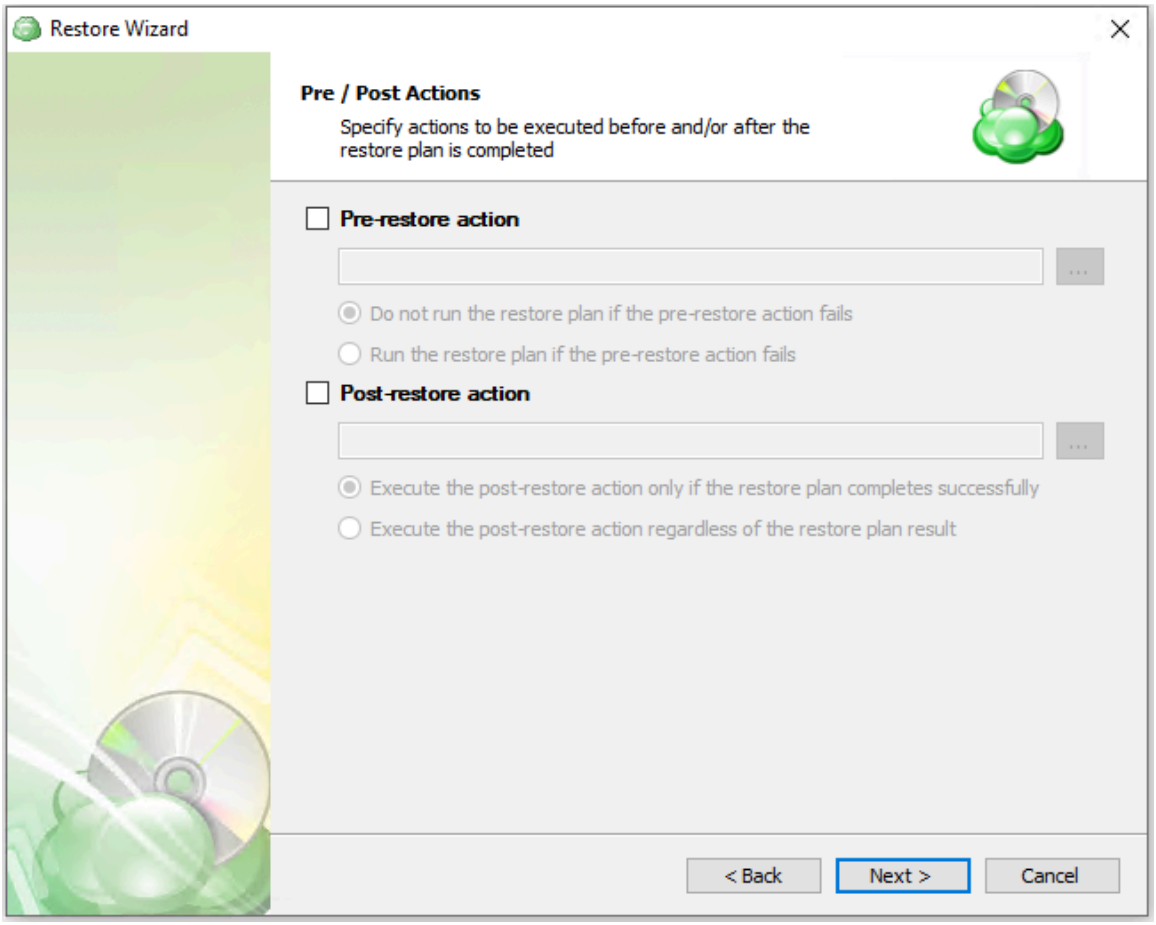


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.
- **Synchronize Repository Before Run:** Enable this option to ensure the file tree reflects the latest modifications made to your storage. It is a good practice to use it when you restore to a different computer

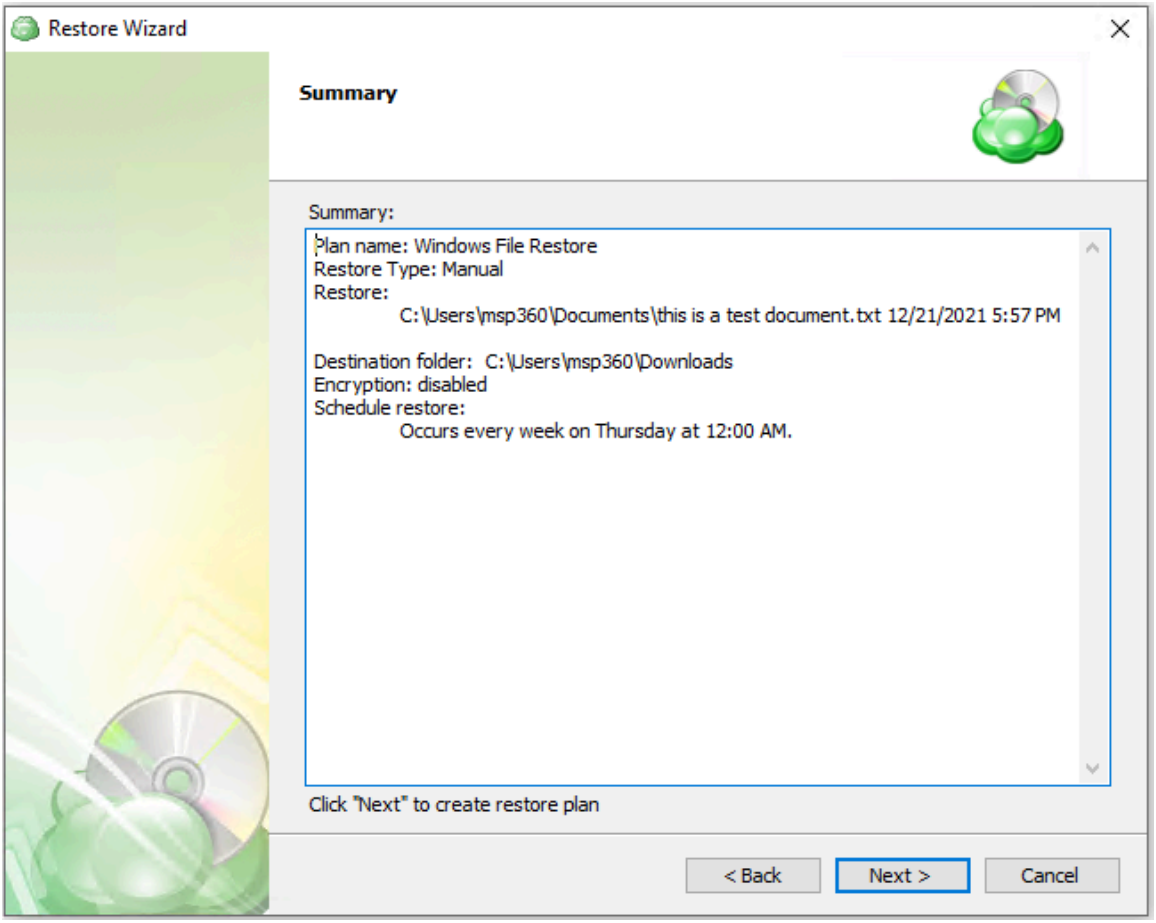
Do not use the “**Stop the plan if it runs for:**” option if you have a slow or unstable internet connection.

Enabling the “**Run missed scheduled restore immediately when computer starts up”** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

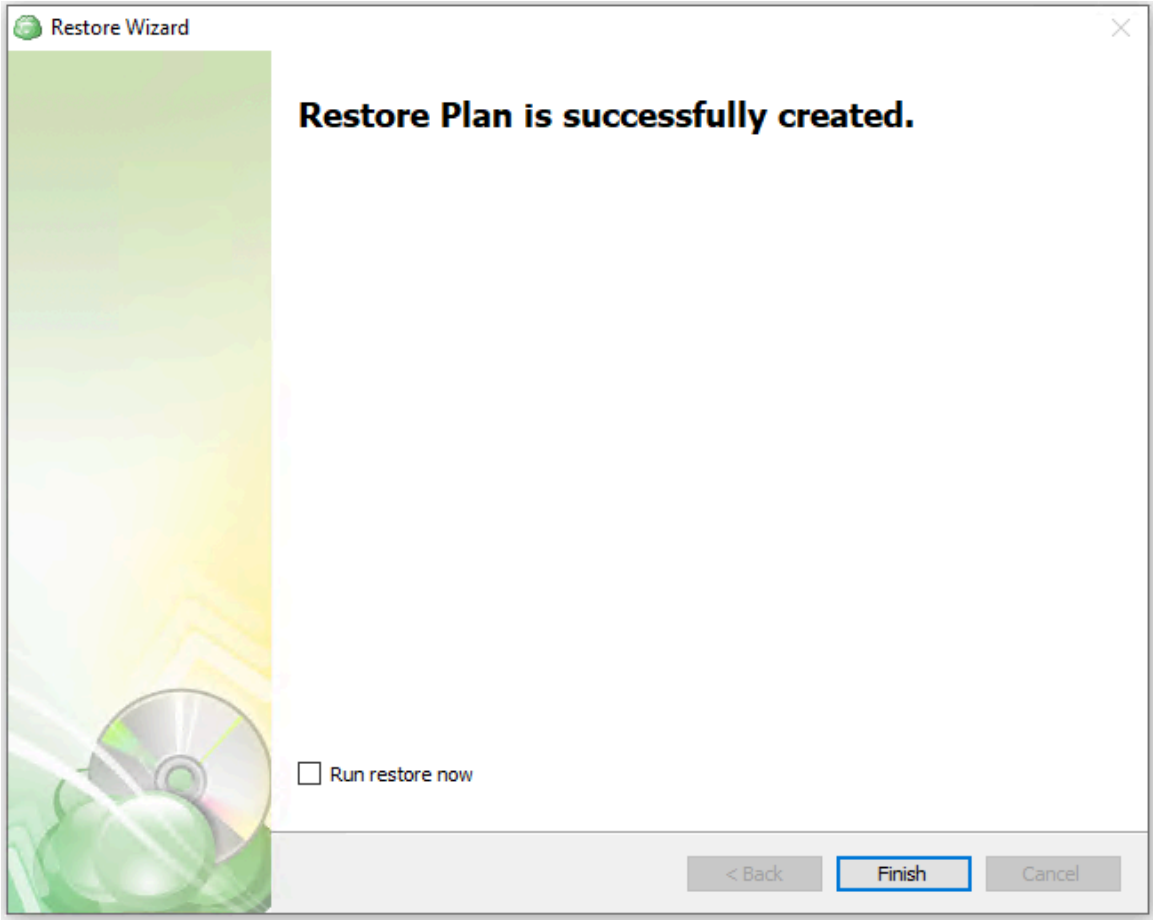
Step 12. The next step is to set any custom scripts which should execute before and/or after the restore plan runs.



Step 13. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.

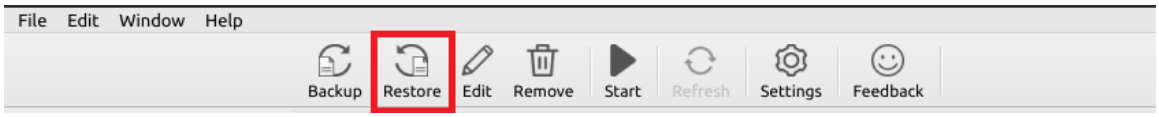


Step 14. The final step in the wizard will confirm that the Restore Plan has been created successfully. If the plan was scheduled, you can opt to run it immediately by checking the “Run restore now” box and clicking Finish. Otherwise, the plan will be set to run at the next scheduled time.

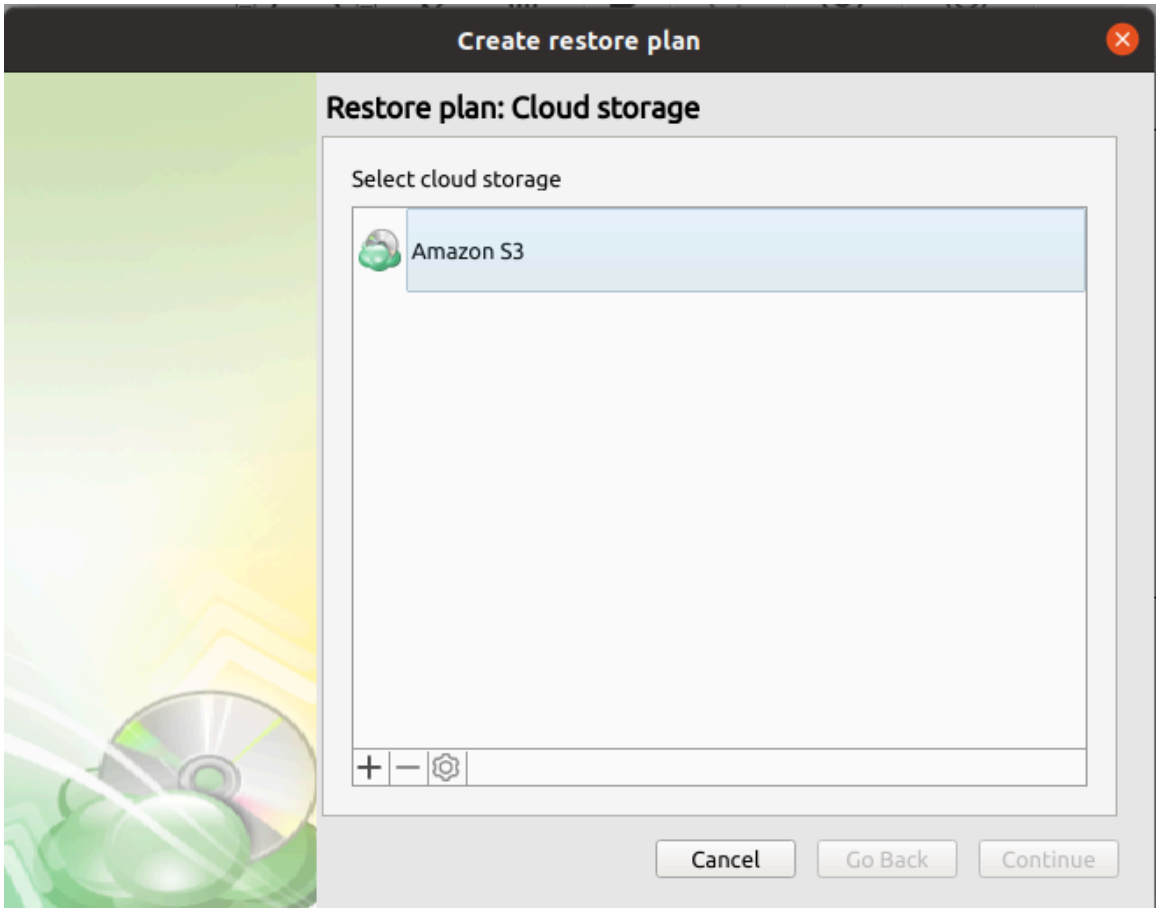


Restore for Mac / Linux using the Agent

Step 1. After launching the Online Backup, you can run the Restore Wizard by clicking on “Restore” main toolbar.

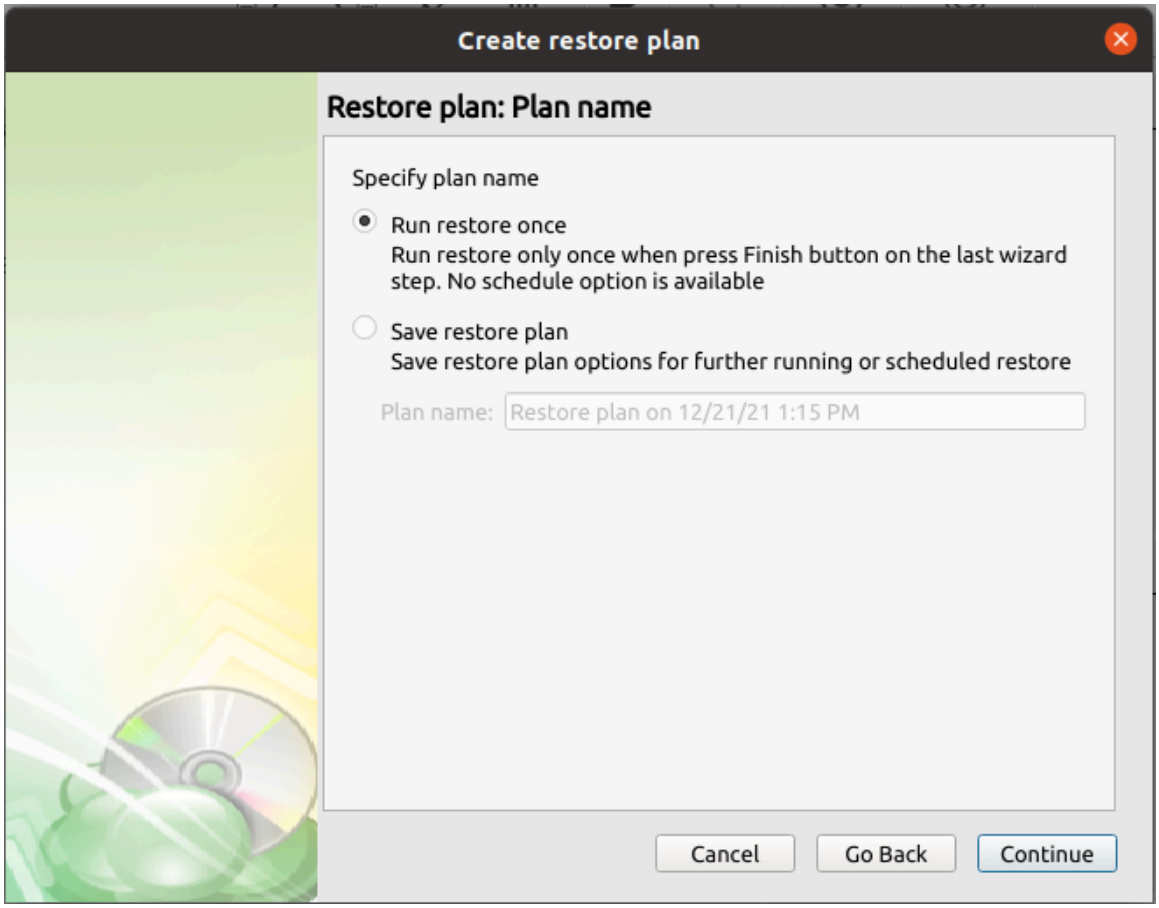


Step 2. The next step will prompt you to select the source for the restore.



If the desired source is not in the list, you can click on the “plus” to add it.

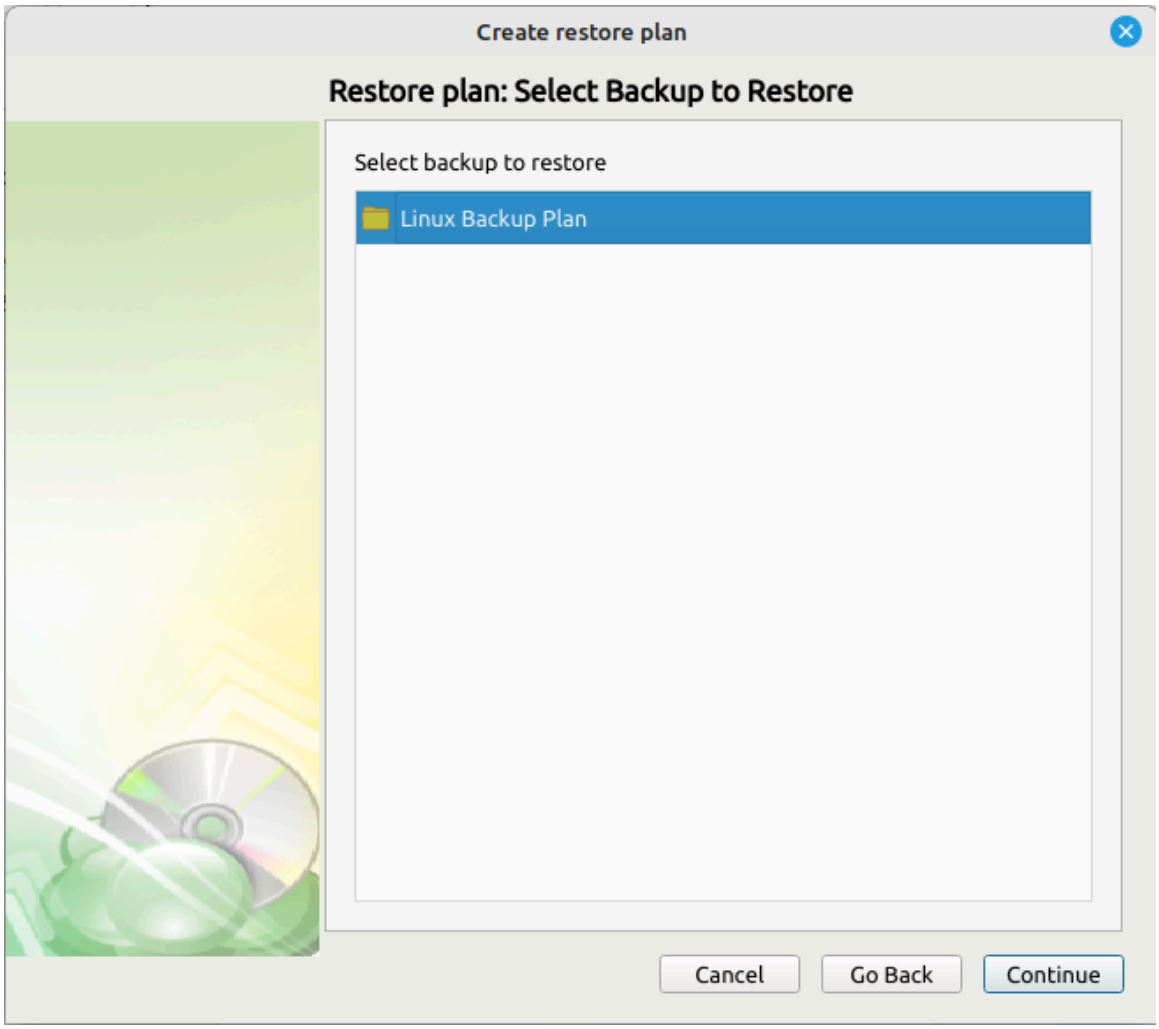
Step 3. Once the source has been selected, the next screen allows you to choose between running the plan a single time or saving it for later use.



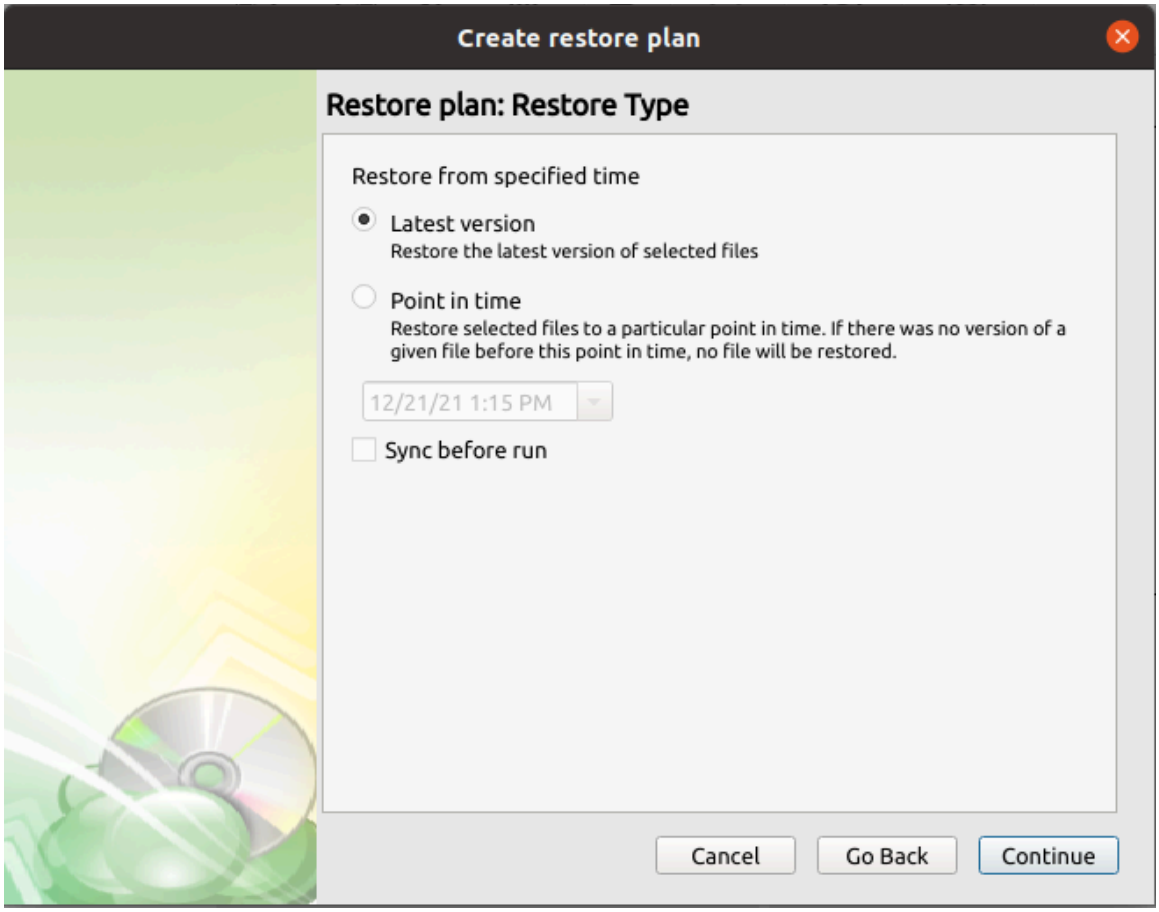
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

Step 4. Next you will have to select which backup you are going to restore.



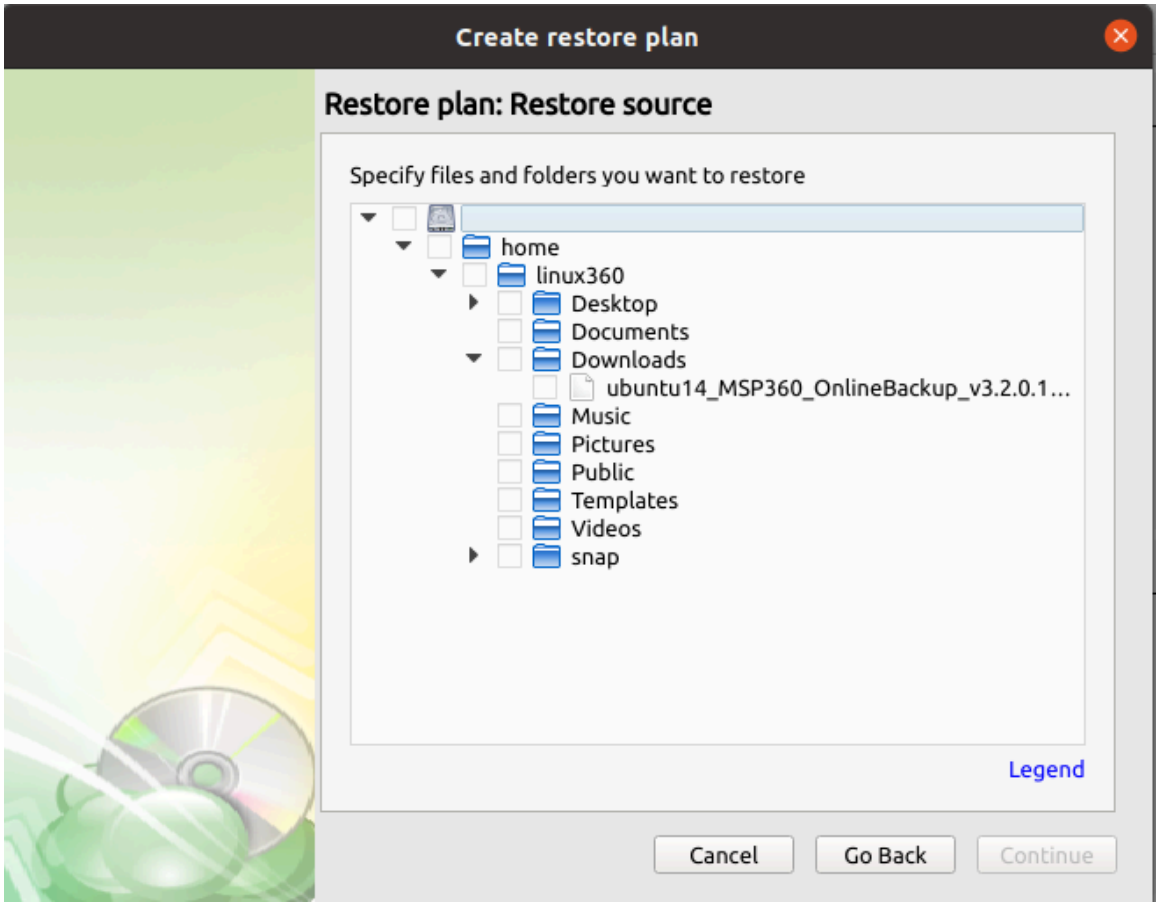
Step 5. Next you will be given a choice for what point in time you would like to restore the VM to.



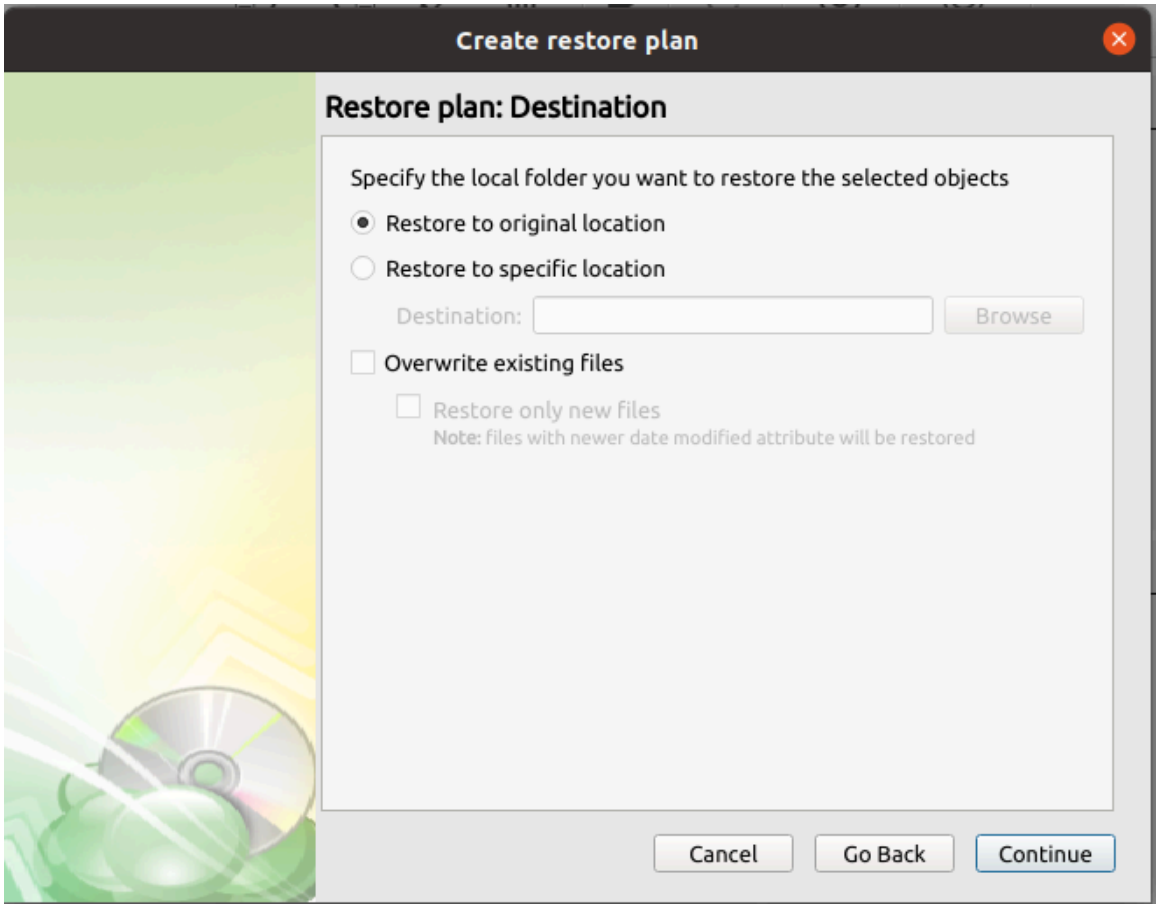
- **Latest Version:** Automatically restores the newest version of each file in the source regardless of which restore point it belongs to.
- **Point in time:** Restores the files as they existed at the specified time.

> If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

Step 6. Next, you will be able to expand the restore source and browse through the available files and folders.

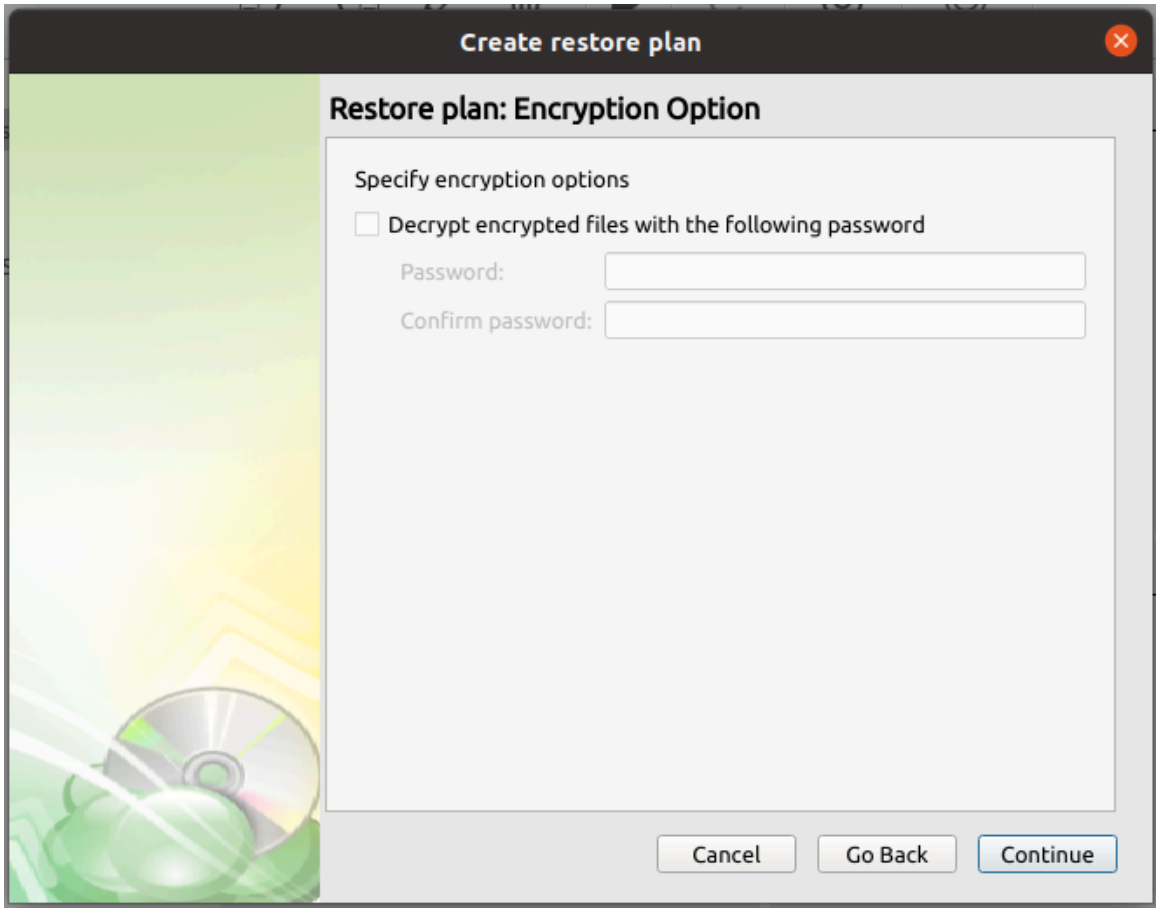


Step 7. After selecting the files or folders to restore, you are able to select the location they should be restored to.

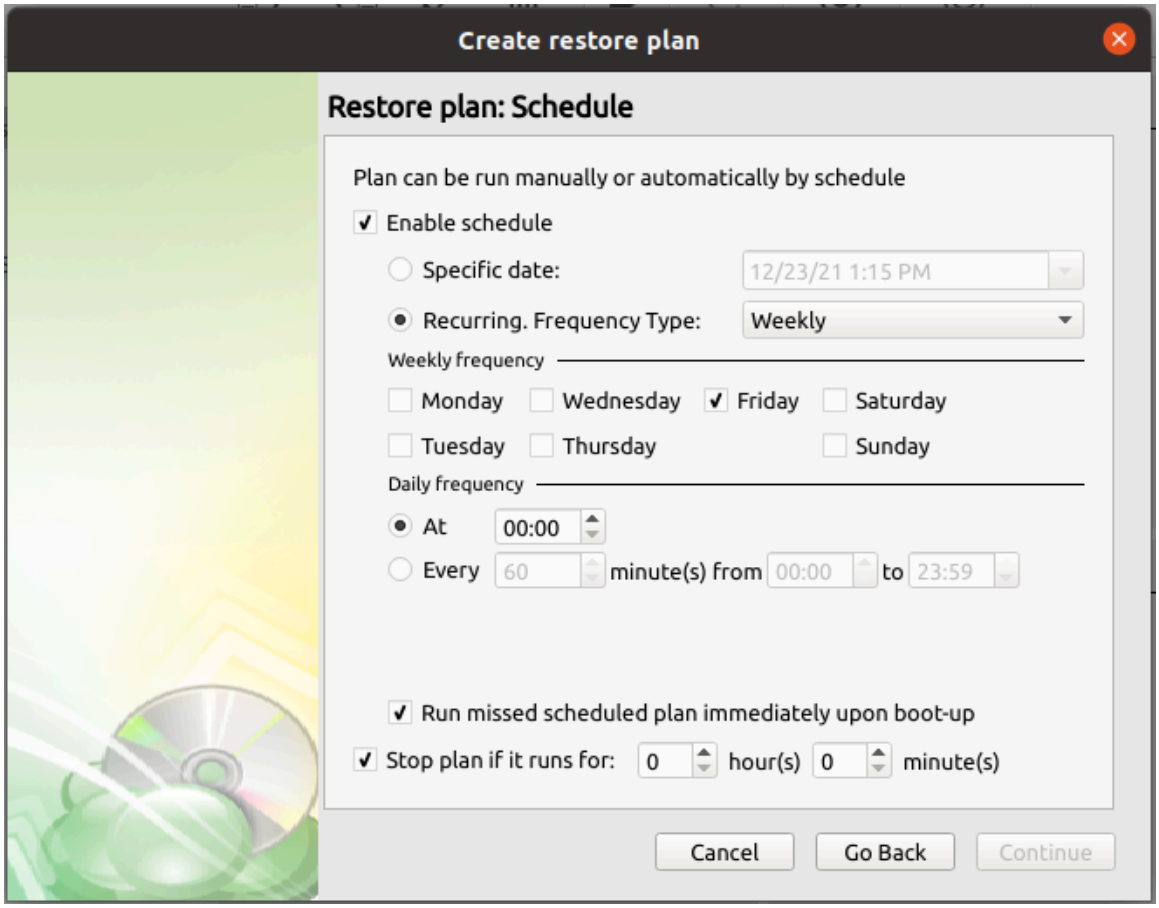


- **Restore to original location:** Automatically restores all files to their original location but does not overwrite existing files unless otherwise specified.
- **Restore to specific location:** Allows you to choose the path to where the files should be restored. Any files or folder structure needed will be created within the designated path.
- **Overwrite existing files:** Allows existing files to be overwritten by the restore process.
- **Restore only new files:** The plan will intelligently detect the files currently in the destination and only files for which the version in the backup is newer than the destination.

Step 8. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the restored data.



Step 9. If “Save restore plan” was selected at the start of the wizard then the next step is to set the schedule for the restore plan. Otherwise this step will be omitted.



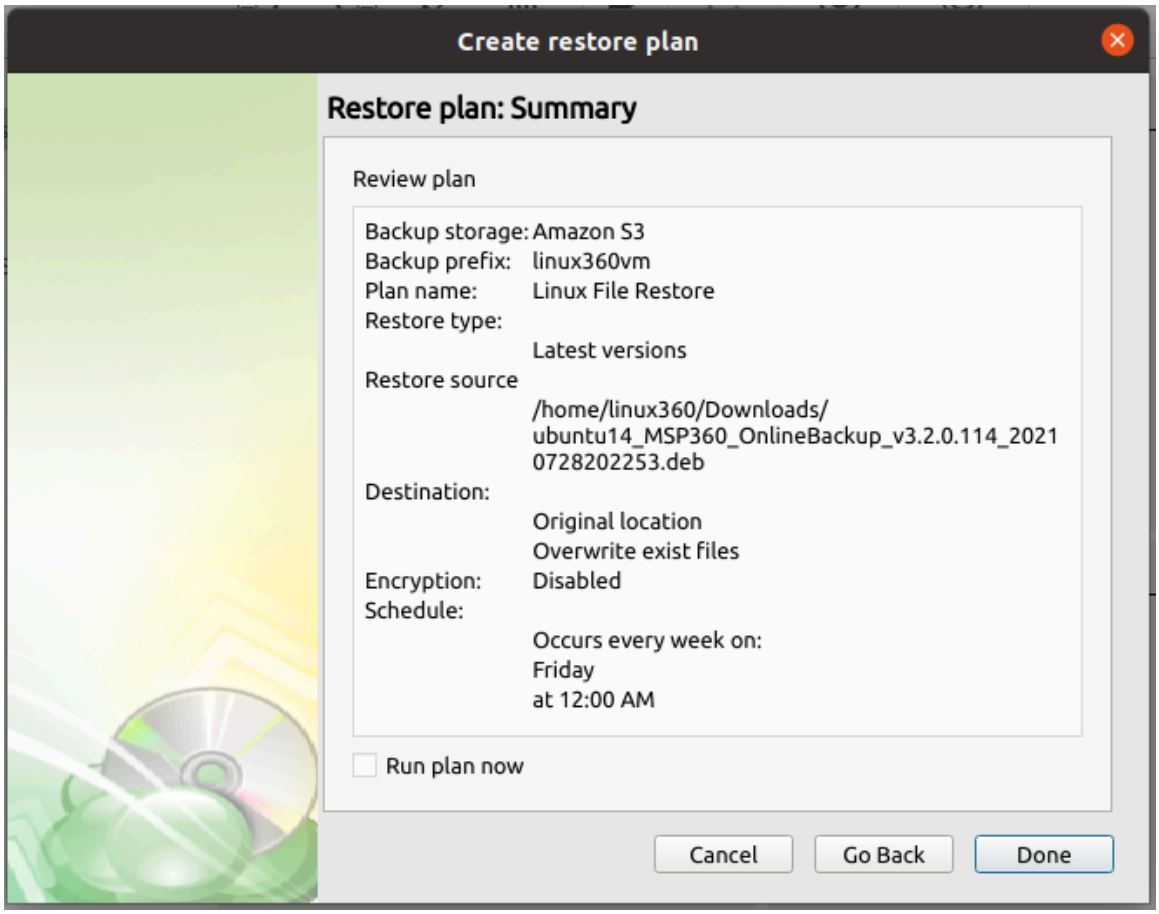
- **Enable schedule:** Leave this unchecked if you want to execute the Restore manually. Otherwise check it to enable the scheduling options.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

Do not use the “**Stop the plan if it runs for:**” option if you have a slow or unstable internet connection.

Enabling the “**Run missed scheduled restore immediately when computer starts up”** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only

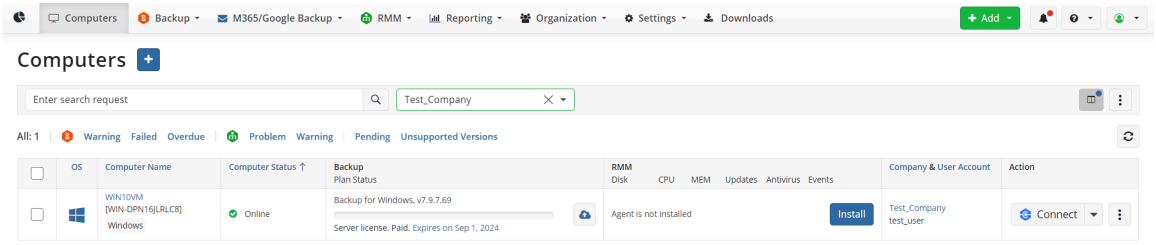
recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 9. The final step in the wizard will provide you with a summary of all previously selected options. If the plan was scheduled, you can opt to run it immediately by checking the “Run plan now” box and clicking “Done”. Otherwise, the plan will be set to run at the next scheduled time.

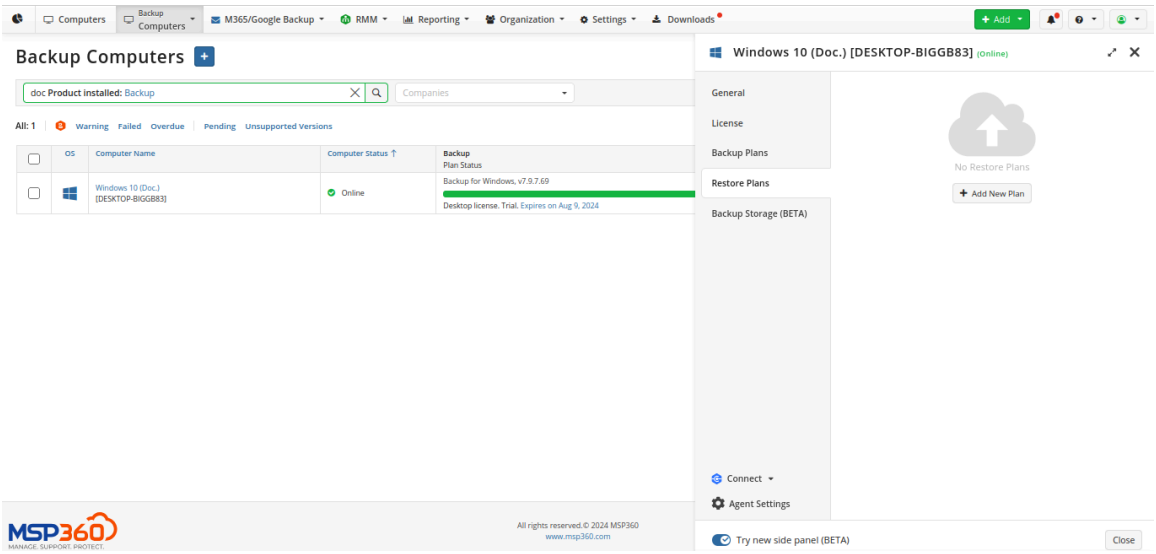


File Restore Plans using MBS

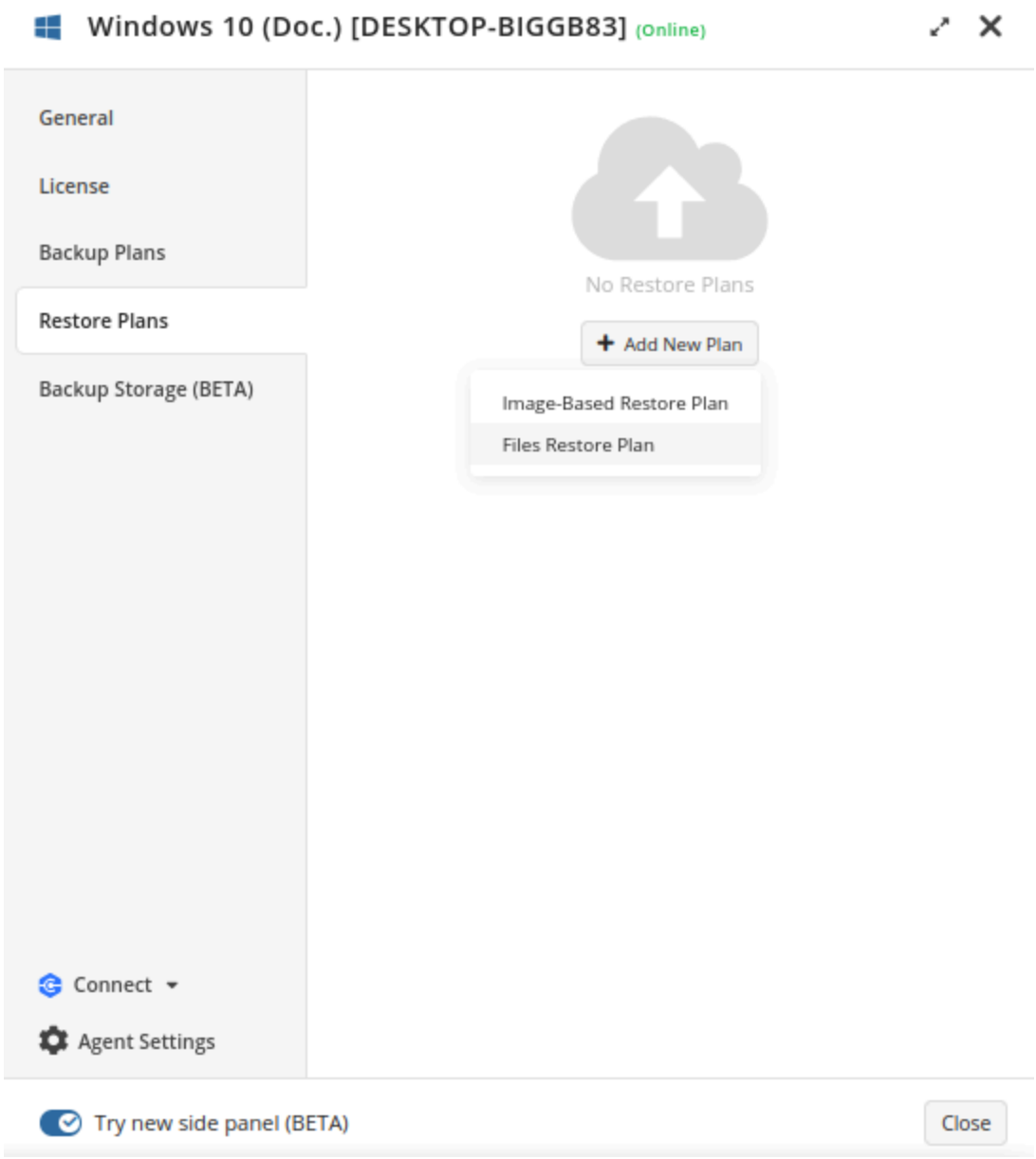
Step 1. From the MBS Portal, left-click Computers, or click on Backup > Computers



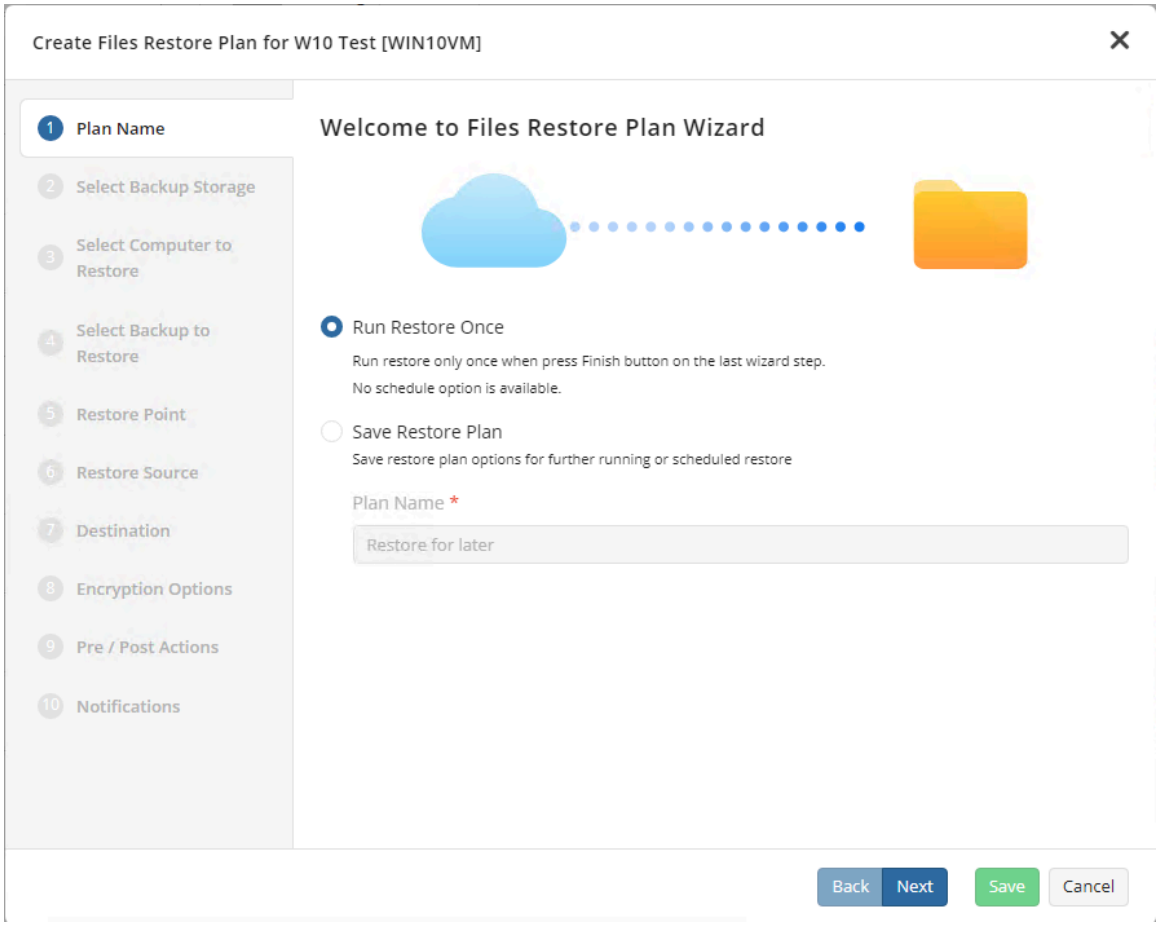
Step 2. Locate the computer you wish to restore from the list and open the current list of plans by either clicking on the name of the computer, or by selecting “Show Plans” from the gear menu. Then navigate to the Restore Plans tab.



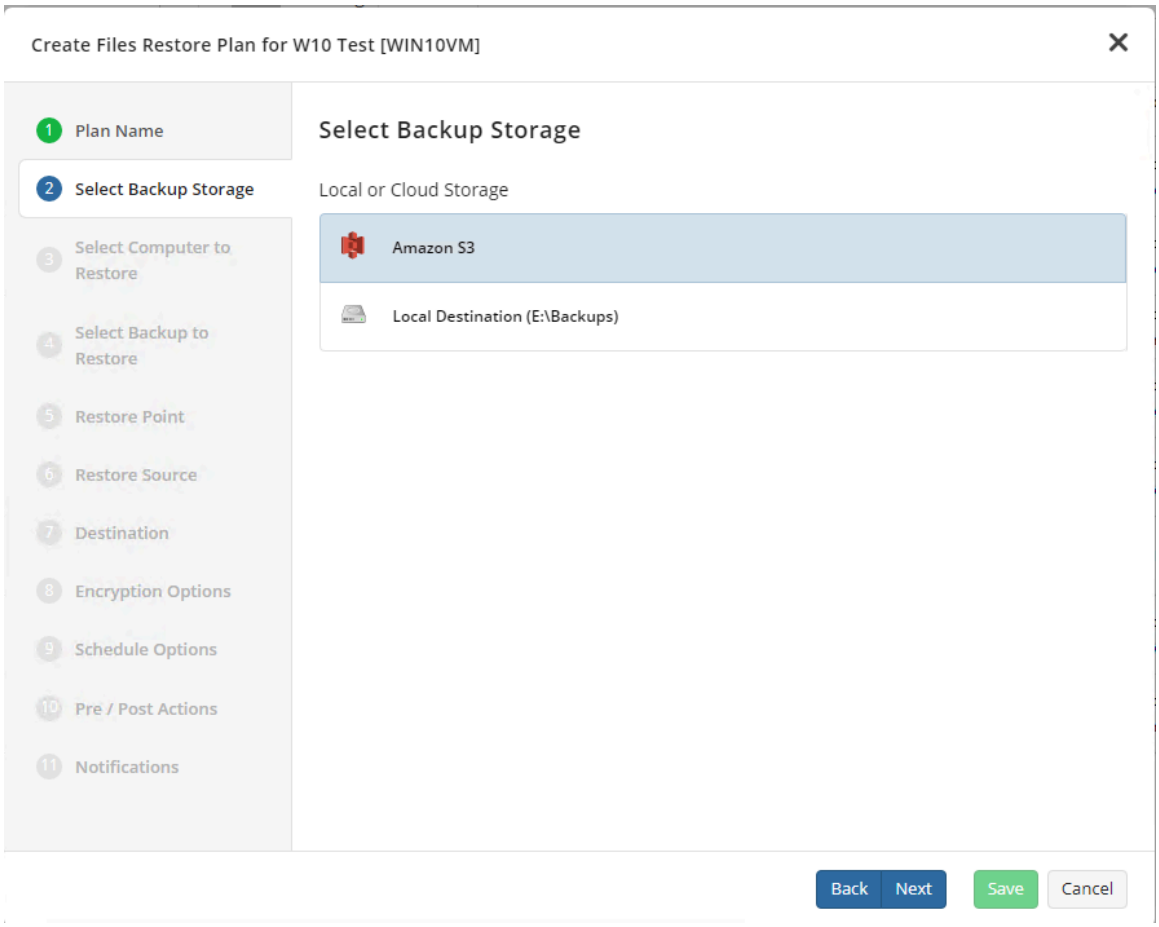
Step 3. If it is a newly deployed computer, you will be prompted with a list of options to create new plans, otherwise, click on the “plus” icon and then under “Restore” header click “Files”



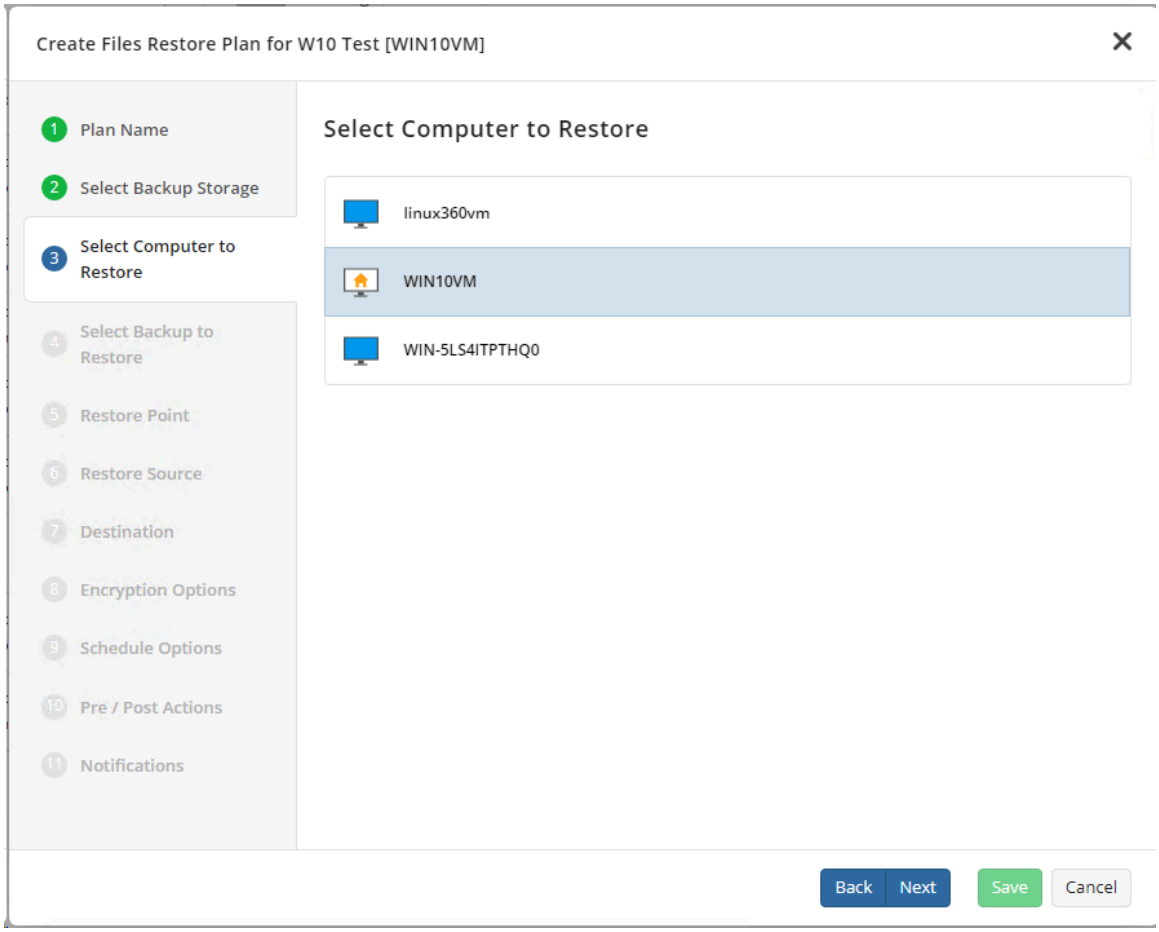
Step 4. The first step when making a Restore Plan is to select if it should run only once, or if it should be saved for future or scheduled use. The latter will allow you to name the plan.



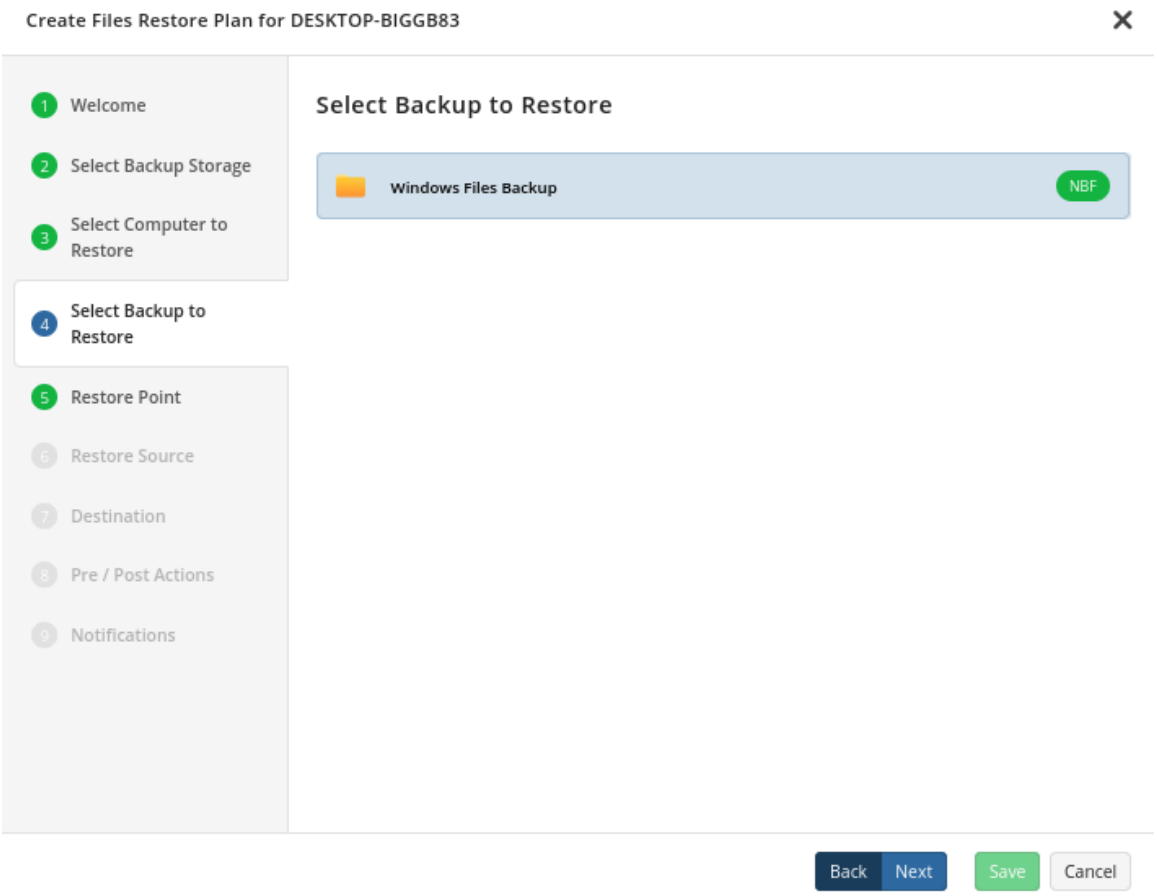
Step 5. Next, select the Restore Source.



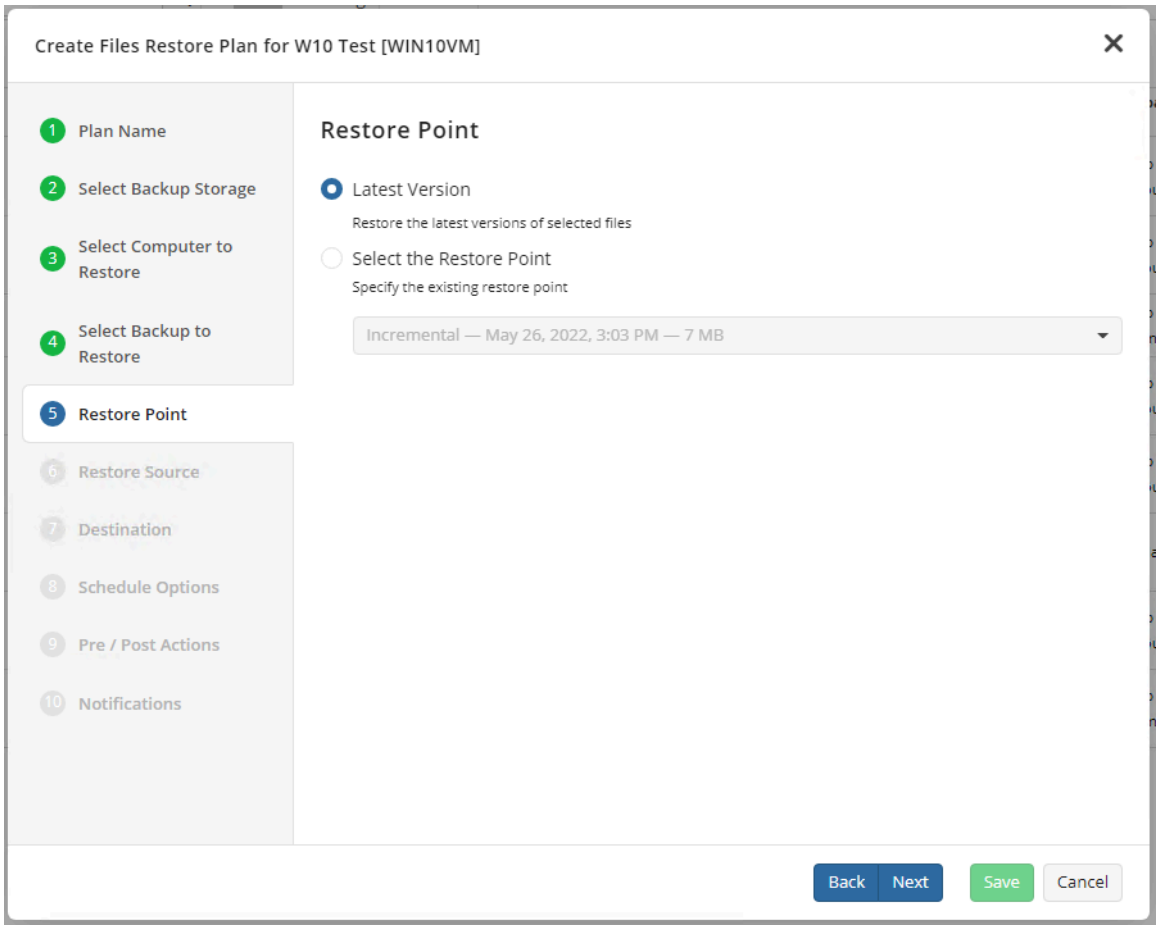
Step 6. The next step is to select the computer to restore. The computer for which the restore plan is being created will have a different icon than other computers.



Step 7. Next, you are presented with a list of backup plans available to be restored for the selected computer on the selected storage. Select the desired plan and click on Next.



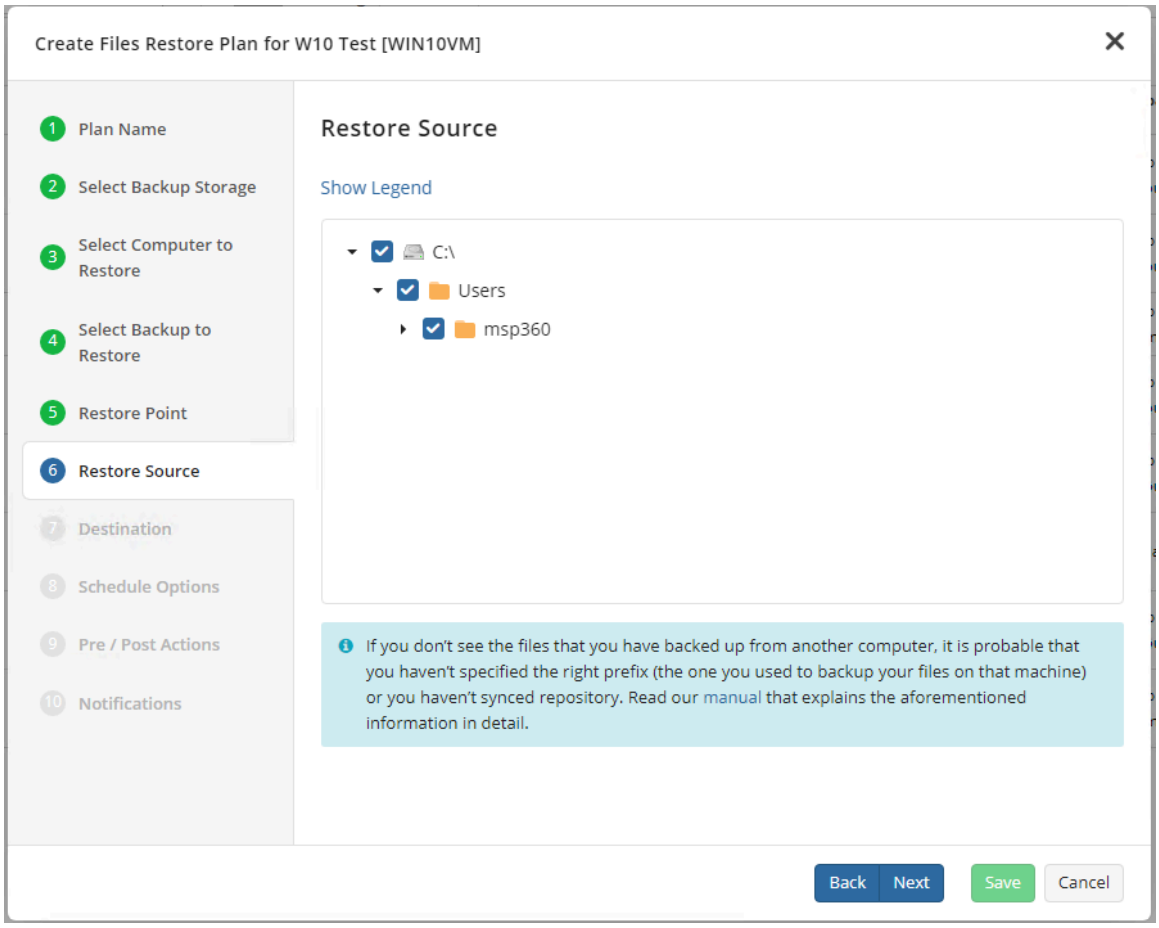
Step 8. The next step is to select the desired point in time to restore to.



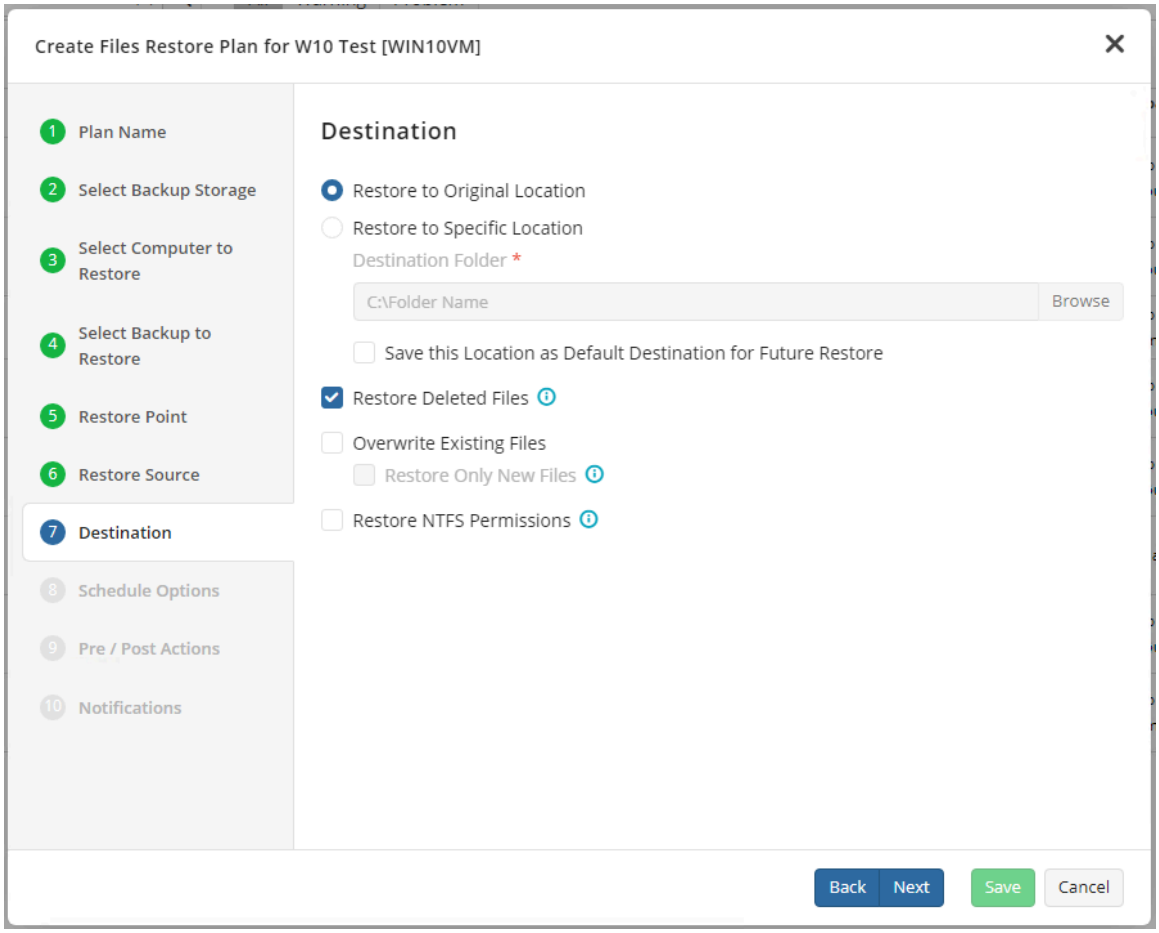
- **Latest Version:** Automatically restores the newest version of each file in the source regardless of which restore point it belongs to.
- **Select the Restore Point:** Restores the files as they existed at the specified restore point.

> If there is no copy of a specific file at the selected restore point, the application will automatically select the newest version from previous restore points.

Step 9. Next, select the files and folders to restore from the selected restore point.



Step 10. Next, choose a destination for the restored file(s) or folder(s).

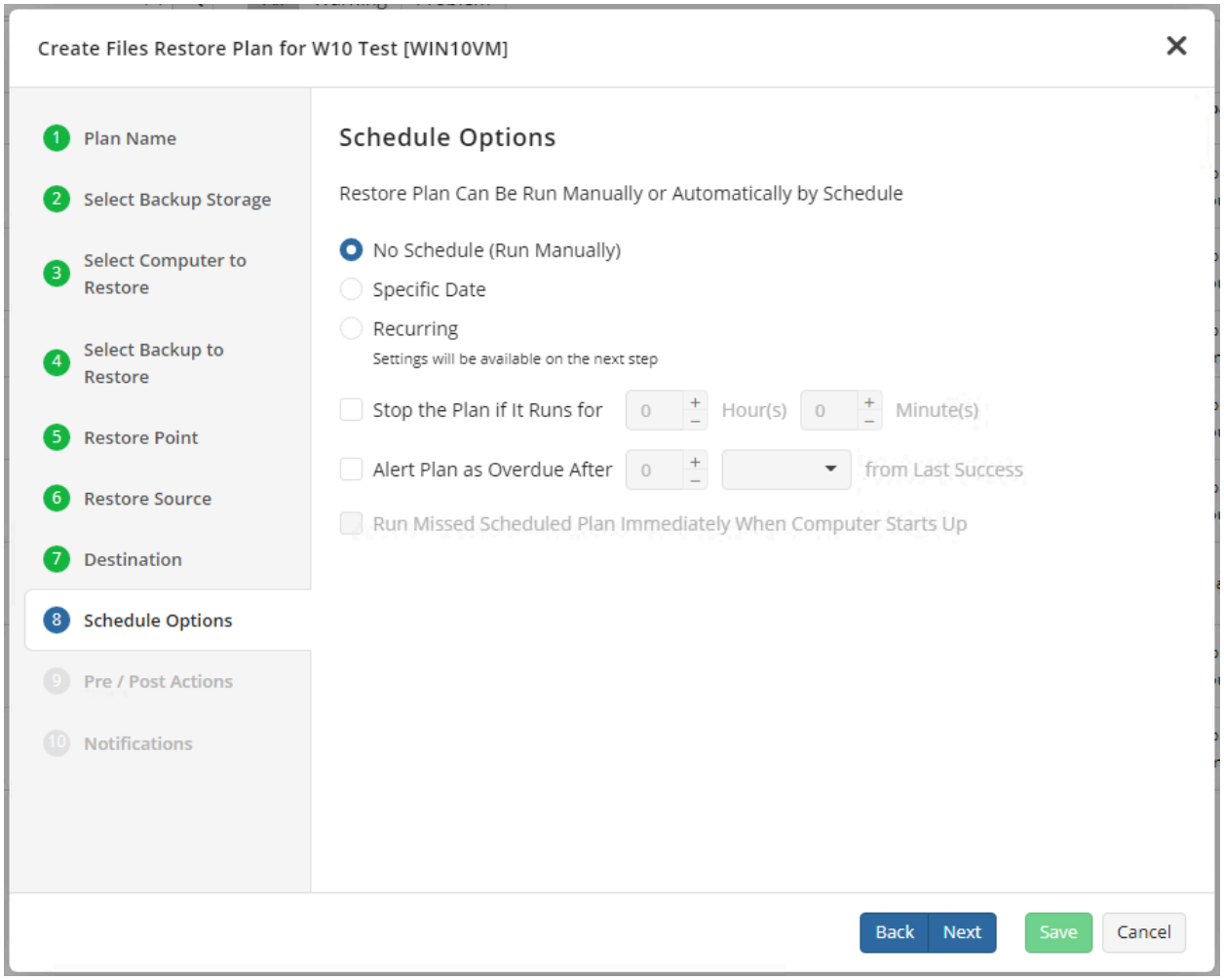


- **Restore to original location:** Automatically restores all files to their original location but does not overwrite existing files unless otherwise specified.
- **Restore to specific location:** Allows you to choose the path to where the files should be restored. Any files or folder structure needed will be created within the designated path.
- **Restore deleted files:** The application will restore files currently marked as having been deleted in the source but which were present at the point in time selected for the restore. Only applies if the backup plan was configured to track deleted files.
- **Overwrite existing files:** Allows existing files to be overwritten by the restore process.
- **Restore only new files:** The plan will intelligently detect the files currently in the destination and only files for which the version in the backup is newer than the destination.
- **Restore NTFS permissions:** Any NTFS permissions will be reapplied to the restored files. If this is left unchecked the restored files will inherit the permissions of the parent

folder. Only applies if the backup plan was configured to backup the NTFS permissions.

> Selecting the **"Overwrite the existing files"** option will overwrite all files that have the same names as those in the destination path.

Step 11. Next, set the schedule for the plan.

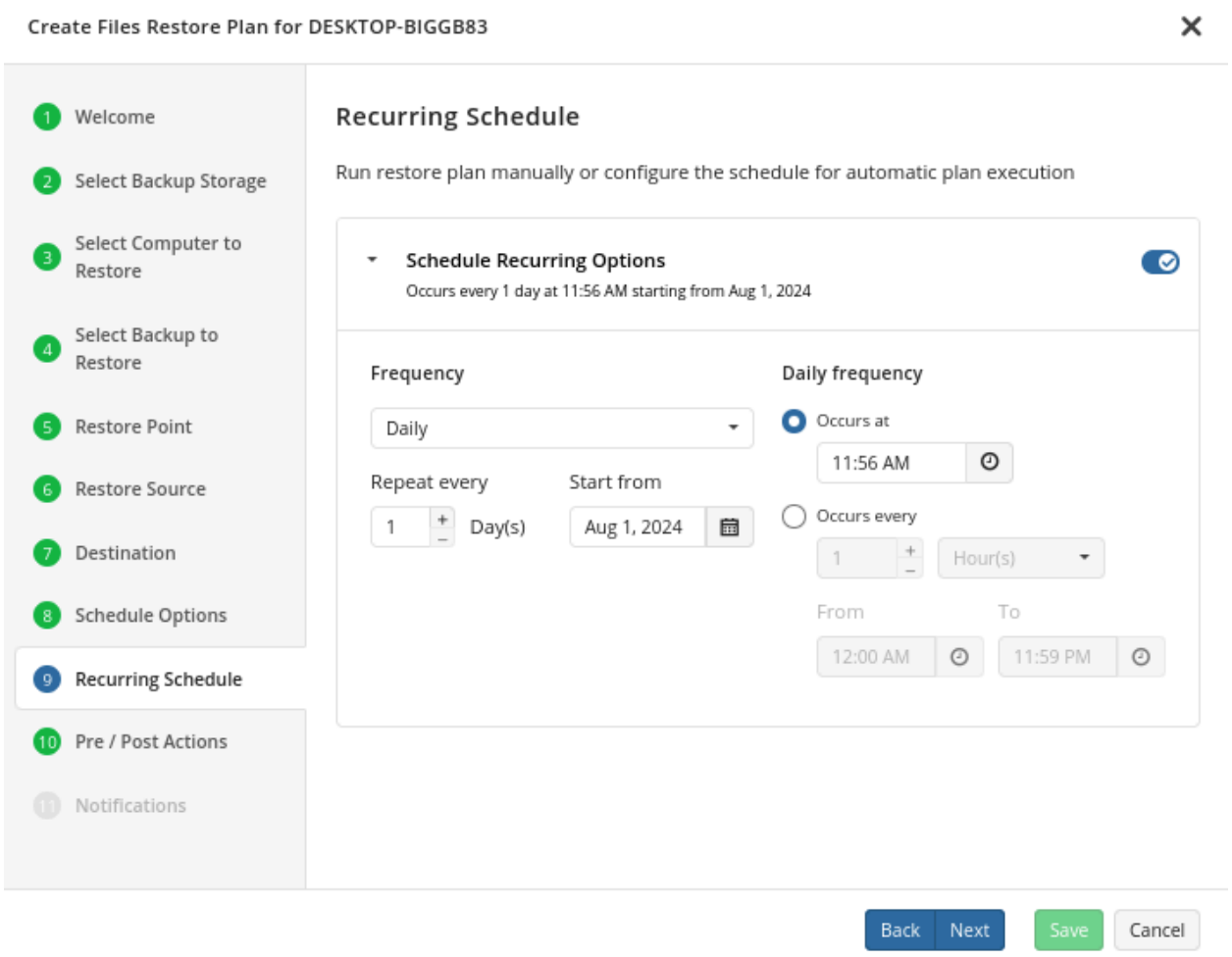


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option will add an additional step to the wizard which enables you to schedule recurring Restorations at custom intervals

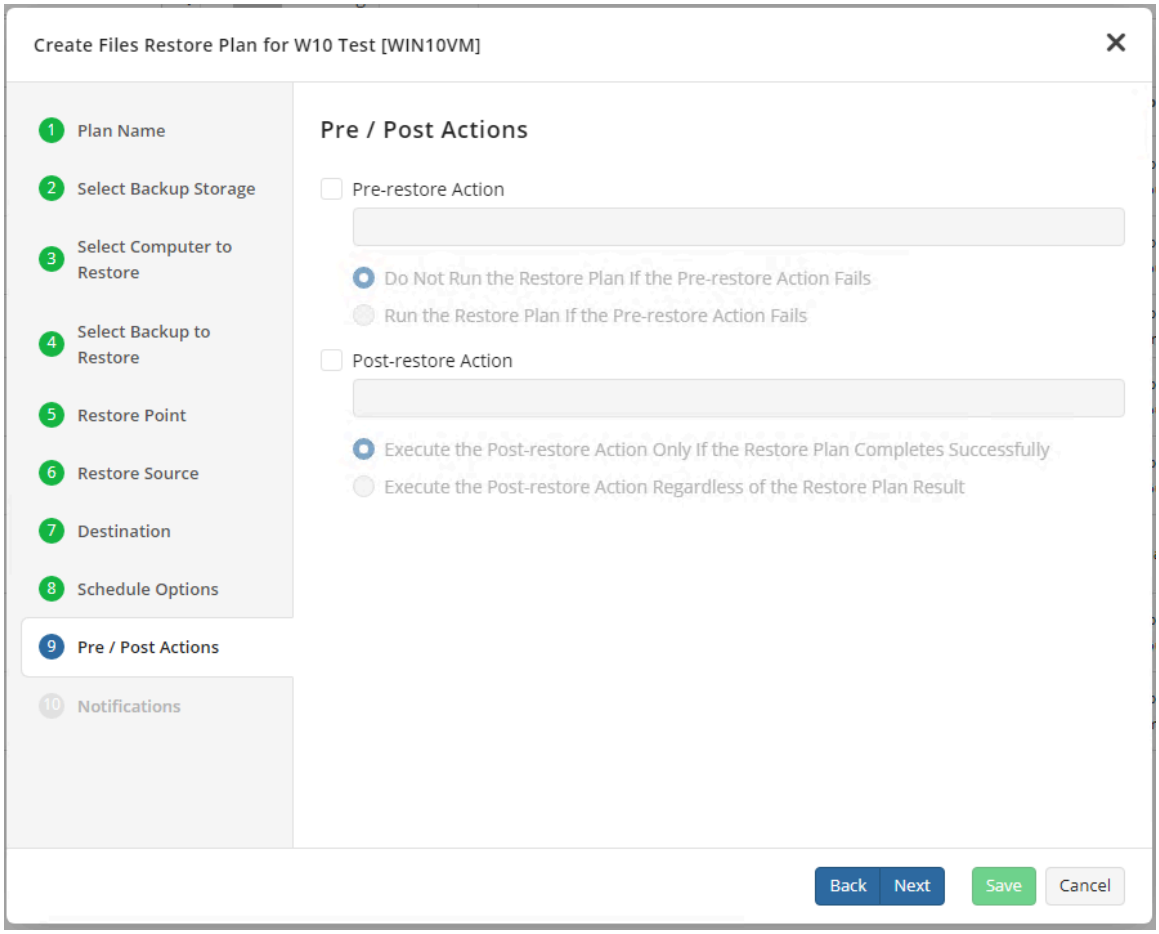
Do not use the “**Stop the plan if it runs for:**” option if you have a slow or unstable internet connection.

Enabling the “**Run missed scheduled restore immediately when computer starts up”** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

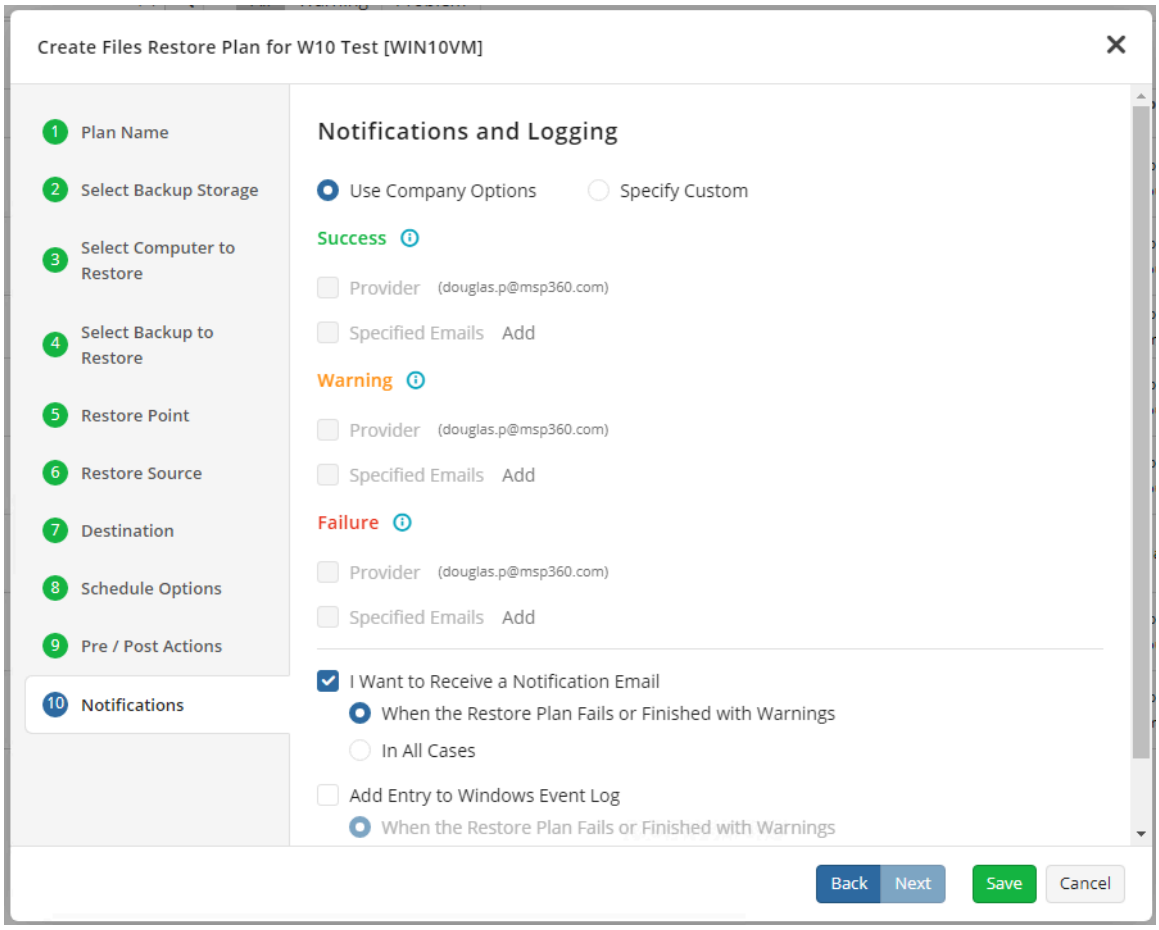
Step 12. If 'Recurring Schedule' is selected, the next step is to set up the schedule for restorations.



Step 13. The next step is to specify any Pre or Post Actions which should be triggered by the Restore Plan.



Step 14. Finally, specify any notifications you would like to receive when the plan runs.

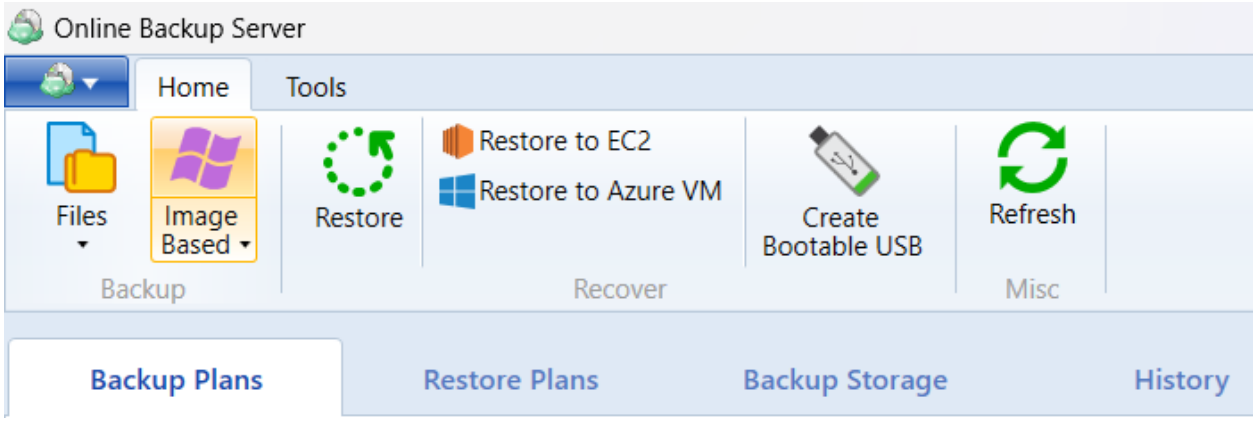


Step 15. Click on Save when you are happy with your selections. If the plan is set to run only a single time and has no set schedule, it will automatically start. Otherwise, if it is set to run only once and is scheduled, it will display in the list of plans until the scheduled time. If it is only set to run once, then when it completes successfully it will remove itself from the list of plans. Only Restore Plans which are saved will remain in the list for future use.

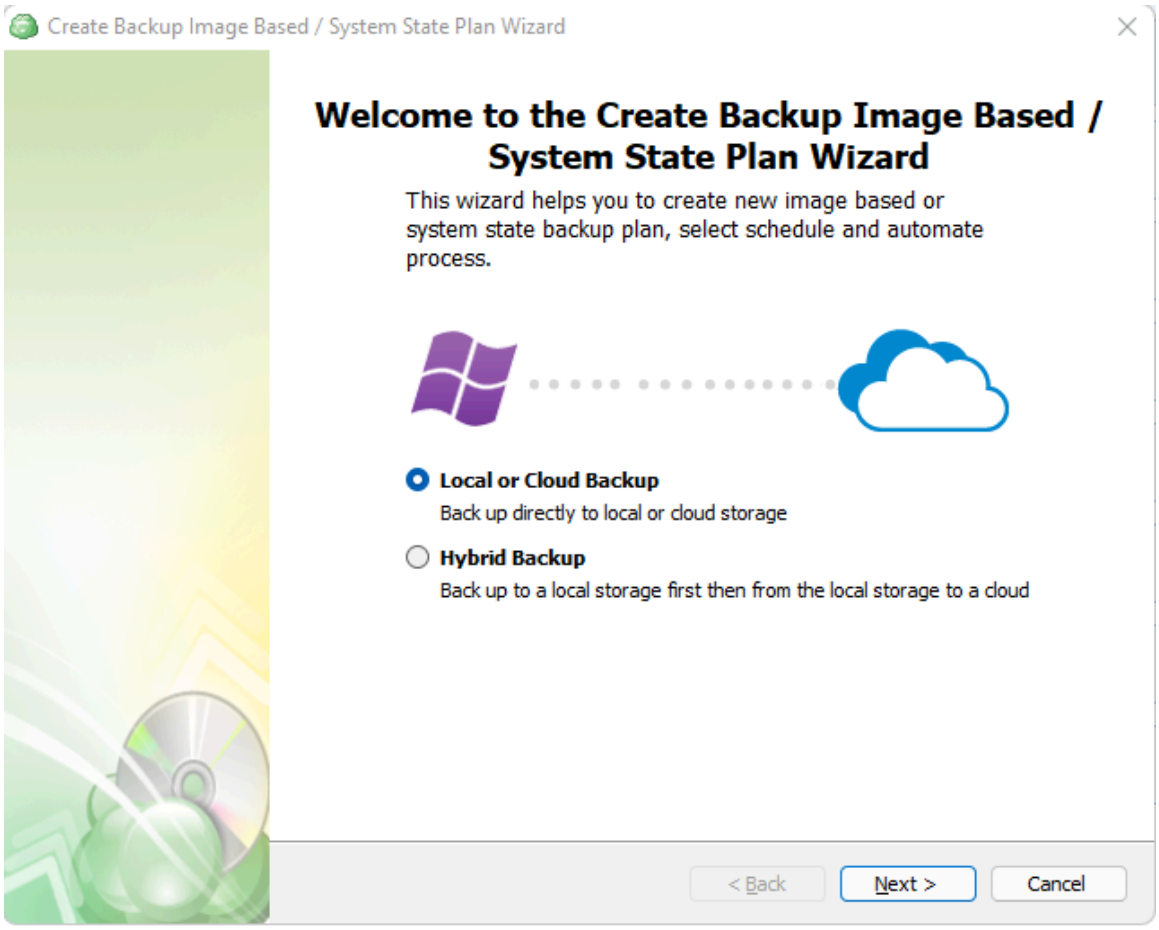
Image-Based Backup Plans

Backup for Windows using the Agent

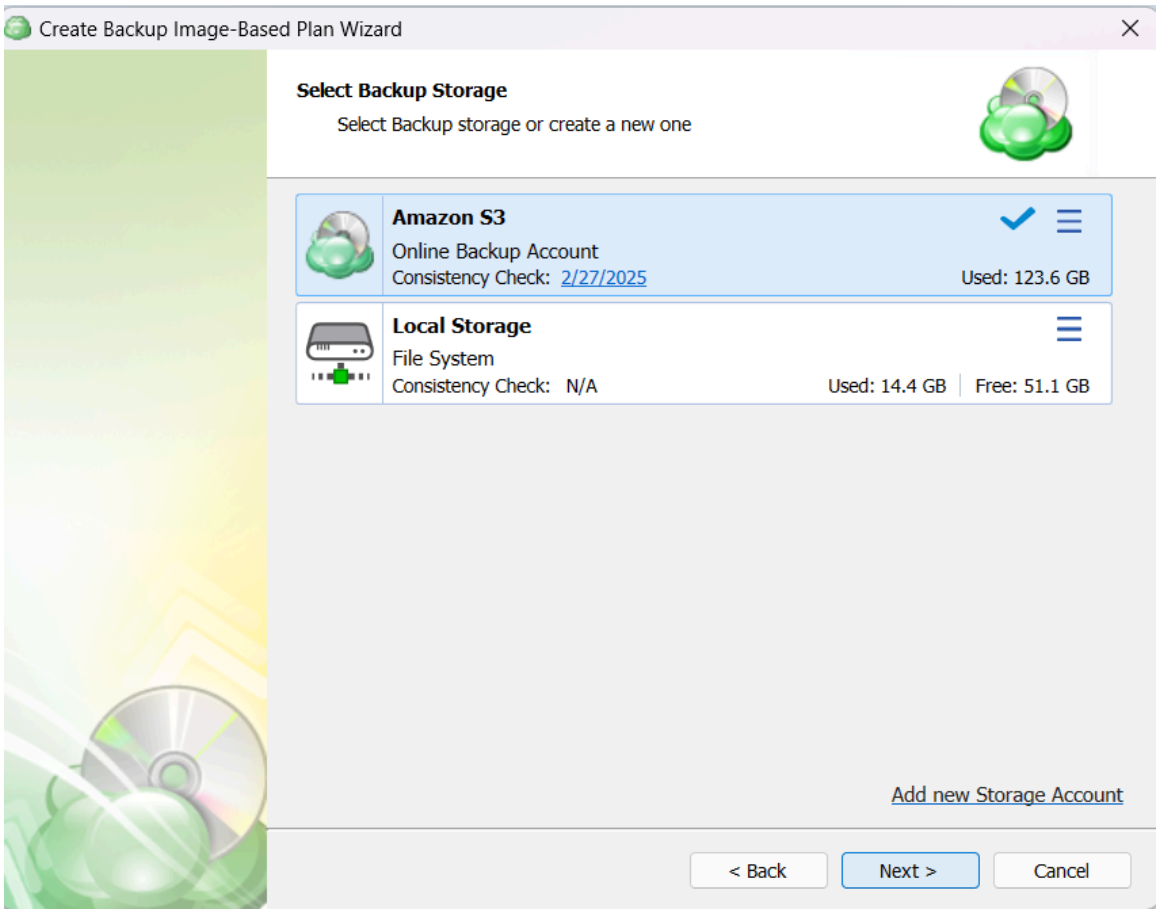
Step 1. After launching Online Backup, you can run the Backup Wizard by clicking “Image Based” on the “Home” tab of the application's main toolbar.



Step 2. Select the desired type of backup, local or cloud.

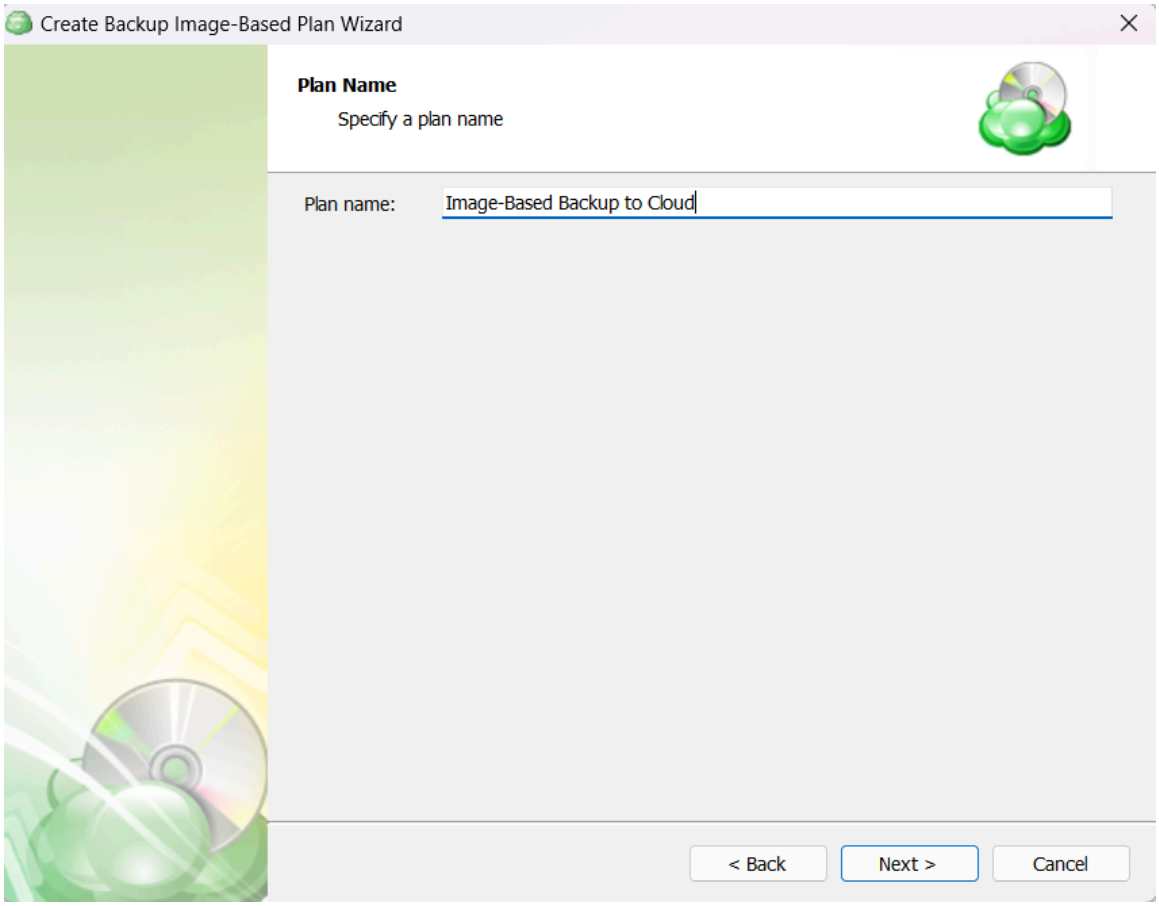


Step 3. The next step will prompt you to select the destination for the backup.



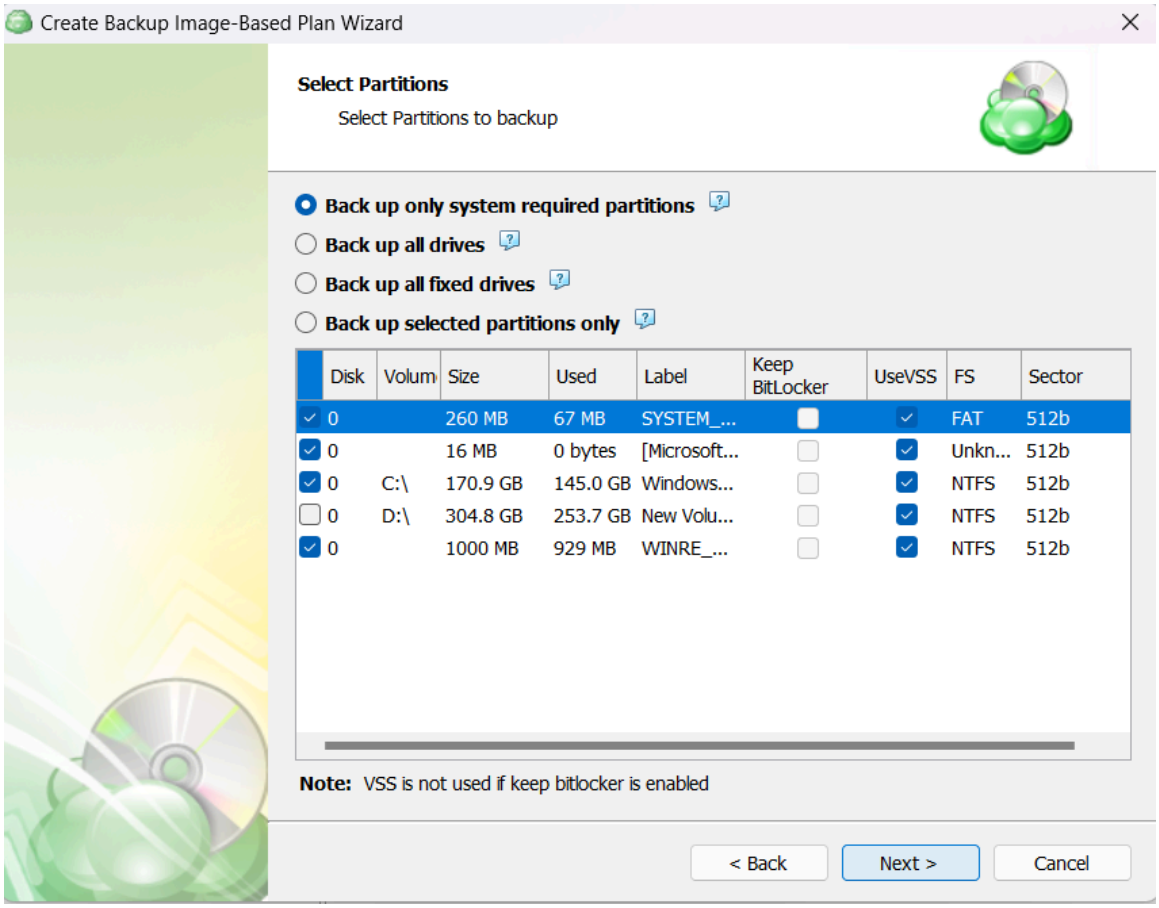
If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

Step 4. Once the destination has been selected, the next screen will prompt you for a plan name.



It is recommended that you select a name which helps you clearly identify the computer as well as the type of backup.

Step 5. On the next step, you will be able to select which partitions should be included in this plan.



- **Back up only system required partitions:** This will automatically select only those partitions required to launch the operating system.
- **Back up all drives:** Selects all available partitions.
- **Back up all fixed drives:** Selects all partitions on non-removable media (internal drives only).
- **Back up selected partitions only:** Allows you to select only the partitions you would like to back up.
- **Keep BitLocker:** Enabling this will instruct the application to backup the data in the current encrypted state. This will prevent the Incremental backups from functioning as intended.

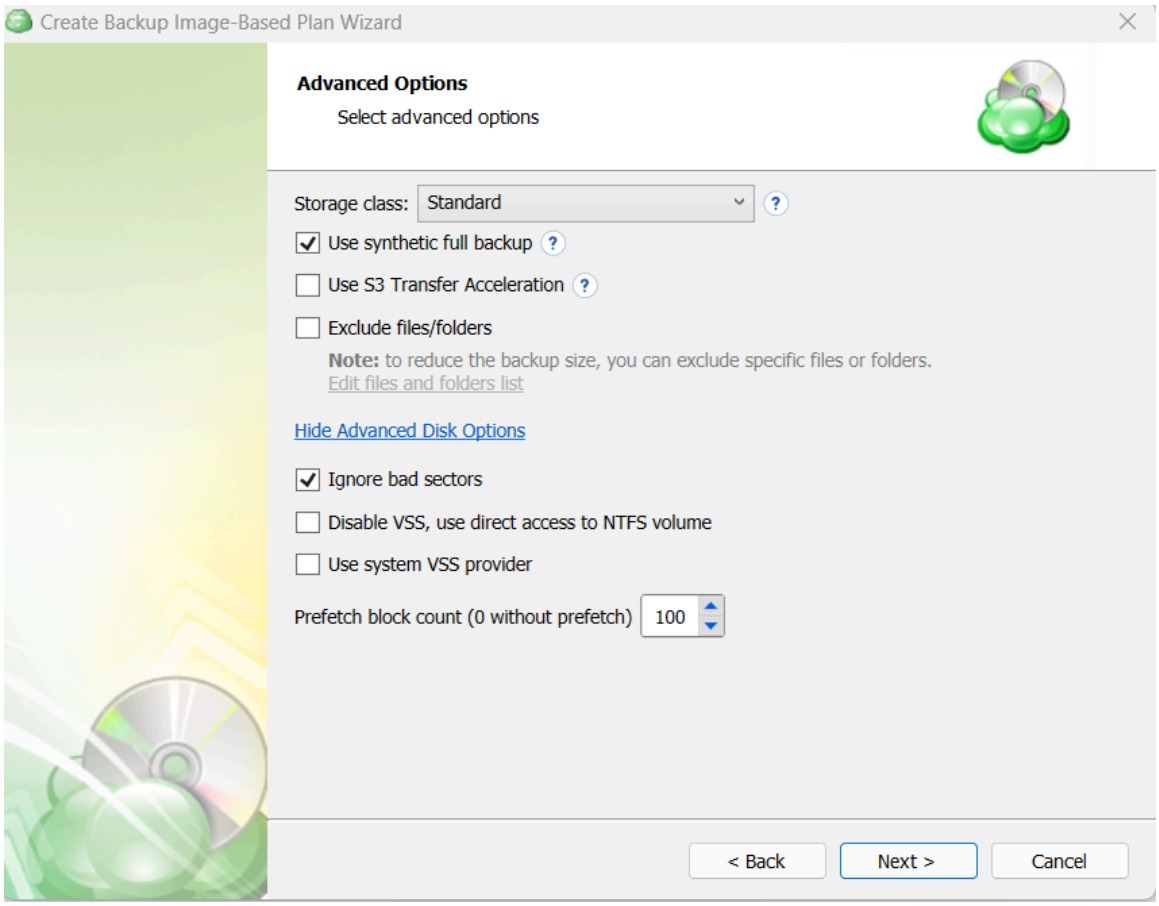
It is strongly recommended to leave the “Keep BitLocker” option disabled. The application will automatically disable BitLocker for the duration of the backup process and then re-enable it afterwards. This will ensure the integrity of the backup cannot be compromised from changes in the BitLocker encrypted data.

Enabling “Keep BitLocker” will prevent Incremental backups from functioning as intended, thus each backup will be considered a full backup.

- **UseVSS:** Enabled by default, this allows the system to be fully backed up including any files or partitions which are currently locked in use by another process.

“VSS” will automatically be disabled if keeping BitLocker

Step 6. The next step shows some “Advanced Options” which can be used to control what data within the selected partitions is excluded as well as some additional control over backup parameters.



- **Use synthetic full backup:** A synthetic full backup is a type of backup that creates a full backup using in-cloud data copying, significantly improving speed and efficiency by saving time and reducing network traffic.

> Synthetic Full Backups greatly reduce the time and bandwidth needed to perform full backups after the initial full.

> Synthetic full backup usage for long-term (cold) storage tiers can result in high storage costs. You can find more information about the supported cloud providers and storage classes in this article.

- **Exclude files/folders:** Selecting this will open a file browser similar to the one used in the File-Based Backup which will allow you to select specific paths or files to be excluded from the image backup.

> On Windows system partitions it is recommended to exclude the \Users\ folder from the image, and set up a separate File backup for that folder.

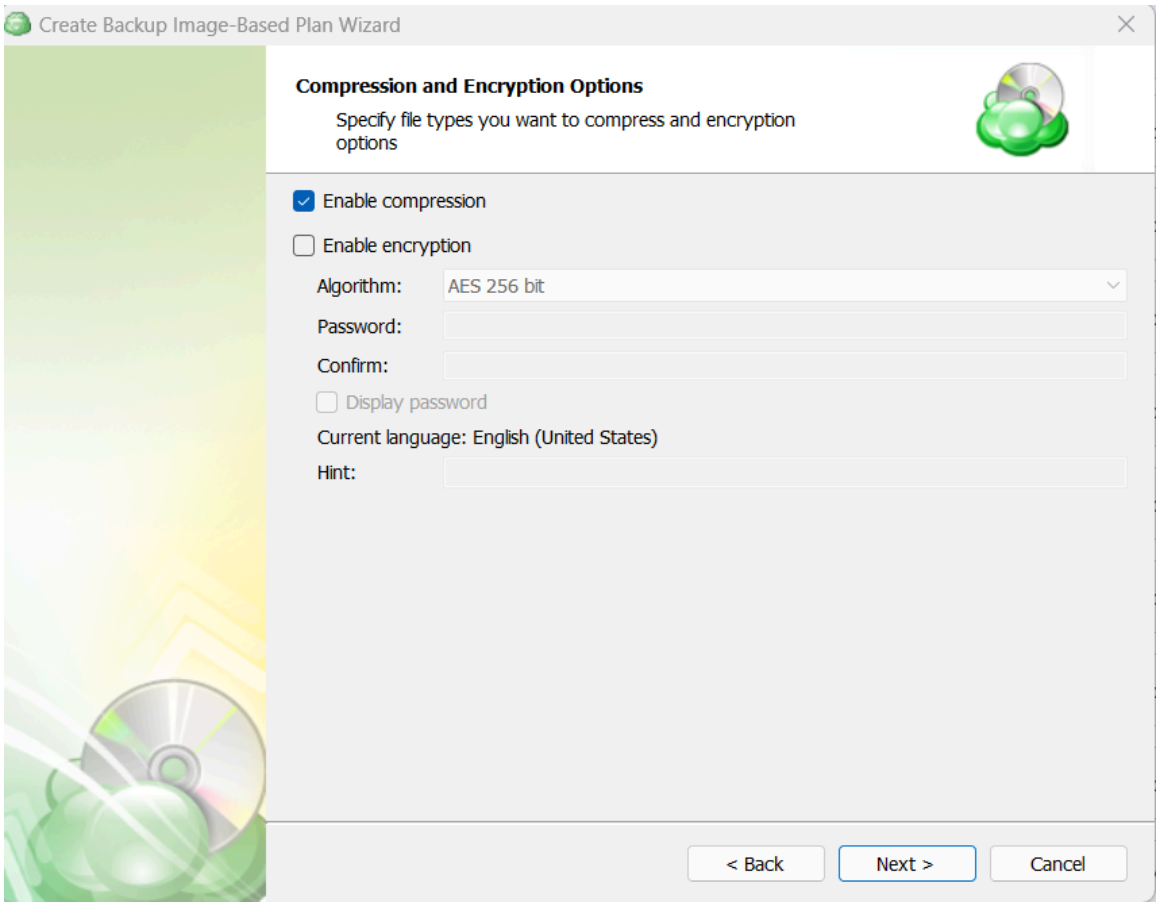
- **Ignore bad sectors:** Enabled by default, this allows the backup to skip any bad sectors found on the disk. It is recommended to leave this enabled unless there is a specific requirement to backup the bad sectors.
- **Disable VSS, use direct access to NTFS volume:** Disabled by default, this option should only be enabled in the event that VSS continues to fail after using the “Use system VSS provider” option.
- **Use system VSS provider:** Disabled by default, this will force the application to use the native VSS provider for the operating system in the event that another provider has been installed by another application which is causing the backup to fail.

> If VSS is failing continuously, consider enabling the “Disable VSS, use direct access to NTFS volume” option.

- **Prefetch block count:** Determines the number of individual blocks the application will simultaneously cache for uploading.

> Changing the prefetch block count is not recommended except as a reaction to extreme system performance degradation during backup.

Step 7. Next, you will choose whether to enable compression and encryption of the backup, as well as the storage class. Other options may appear depending on the features supported by your selected backup destination.

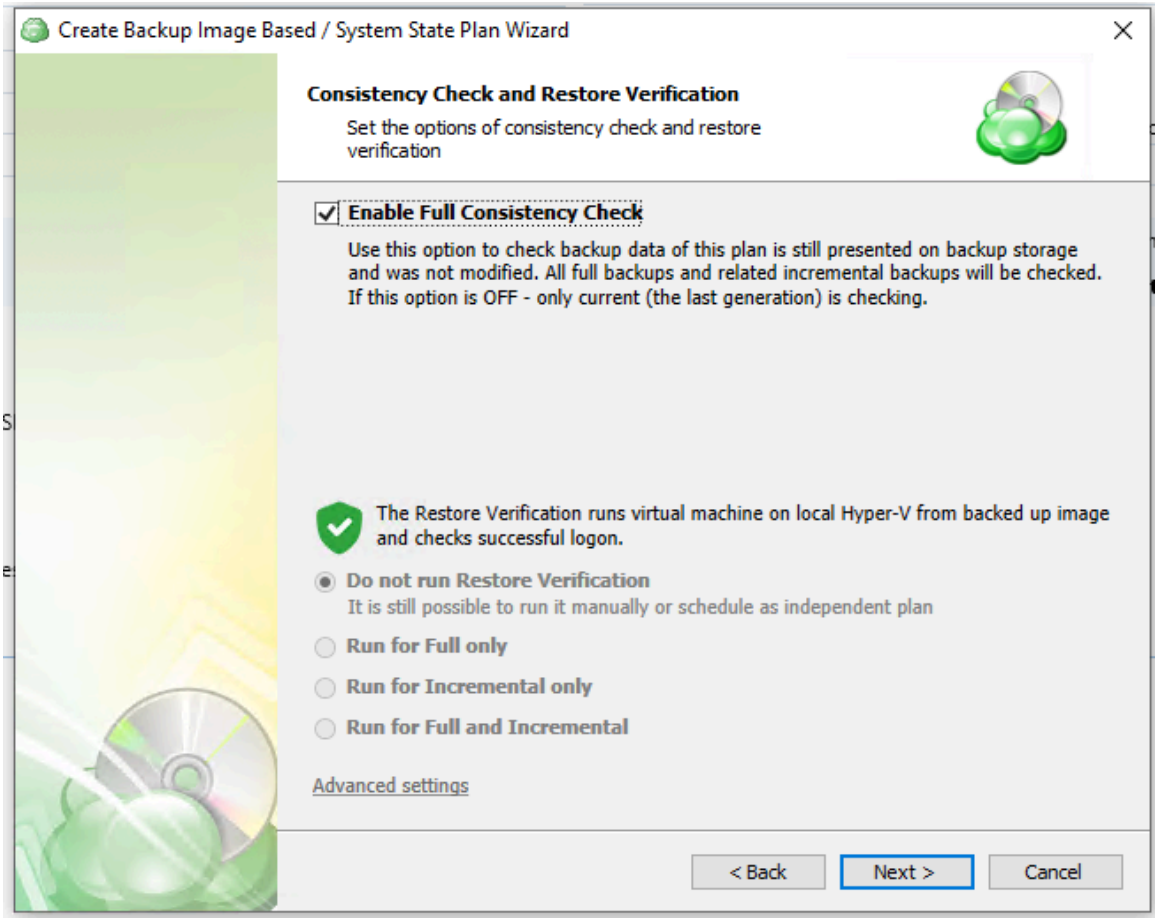


Enabling compression will reduce the size of the backup and reduce the time to upload it, both of which may decrease the cost of the backup.

Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place and enable the Password Recovery Service.

Step 8. Next you are presented with the Consistency Check and Restore Verification options.



It is recommended that you leave "**Enable Full Consistency Check**" enabled.

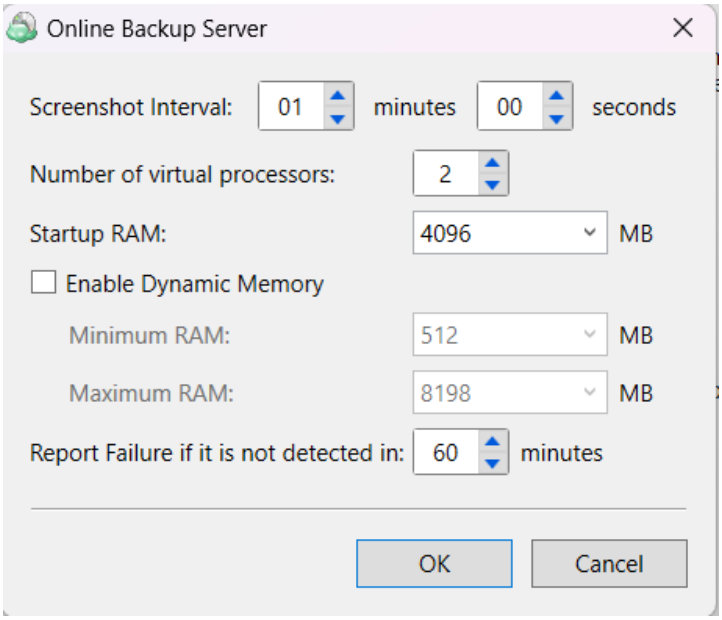
Although a successful Consistency Check ensures the backup integrity, an additional Restore Verification process can be executed as well.

This process uses a temporary Hyper-V virtual machine on the source endpoint to test Windows startup. It only retrieves the necessary backup parts from storage without the need to download the entire backup.

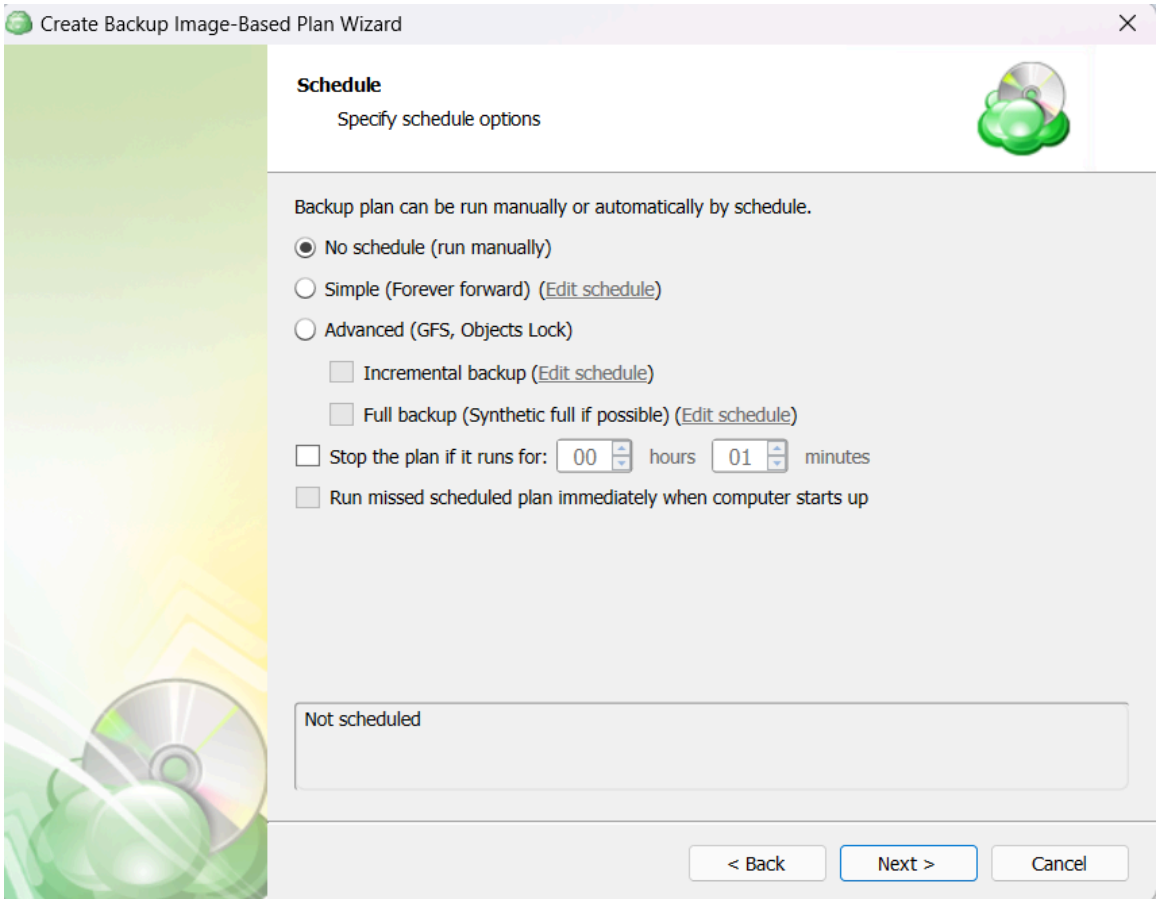
> Hyper-V is required on any endpoint utilizing Restore Verification. For more information refer to this article: Restore Verification for Image-Based Backups.

You can run the Restore Verification for incremental backups only, full backups only, for every backup, or do not run it at all.

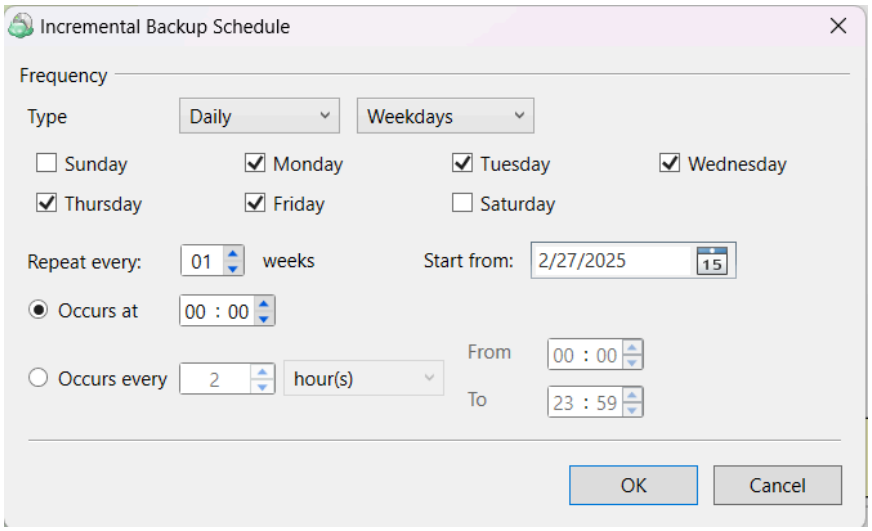
Along with the Restore Verification running mode, customize the Hyper-V auxiliary virtual machine configuration to run the Restore Verification (number of virtual processors, RAM) by clicking on Advanced Settings.



Step 9. Next you are prompted to set the schedule for your backup plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.



- **Simple (Forever forward):** Select the Simple (Forever Forward) option to use the Forever Forward Incremental (FFI). This schedule offers one full backup followed by a limited number of incrementals. Once the limit is exceeded, a new full backup is created using the synthetic full capabilities.



Forever Forward backups are only supported by a limited number of cloud storage providers. For more information, refer to Forever Forward Incremental.

The Simple (Forever forward) schedule is recommended for retention up to 100 restore points which do not require Object Lock for legal compliance.

It is not recommended to select the Simple (Forever forward) schedule for long-term storage and archival purposes. The Advanced Schedule is recommended for all storage needs over 100 restore points.

- **Advanced (GFS, Object Lock):** Select the Advanced option to set up a flexible, recurring schedule with generations. Every generation contains one full backup followed by incrementals.
    - Clicking on “Edit Schedule” next to Incremental and Full backups allow you to configure the frequency they will be created. If both a Full and Incremental are scheduled for the same day, the application will perform the Full only.

It is recommended to use the Advanced (GFS, Object Lock) option and regularly scheduled full backups for long-term storage (longer than 6 months) or backups that must comply with legal or industry requirements.

Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

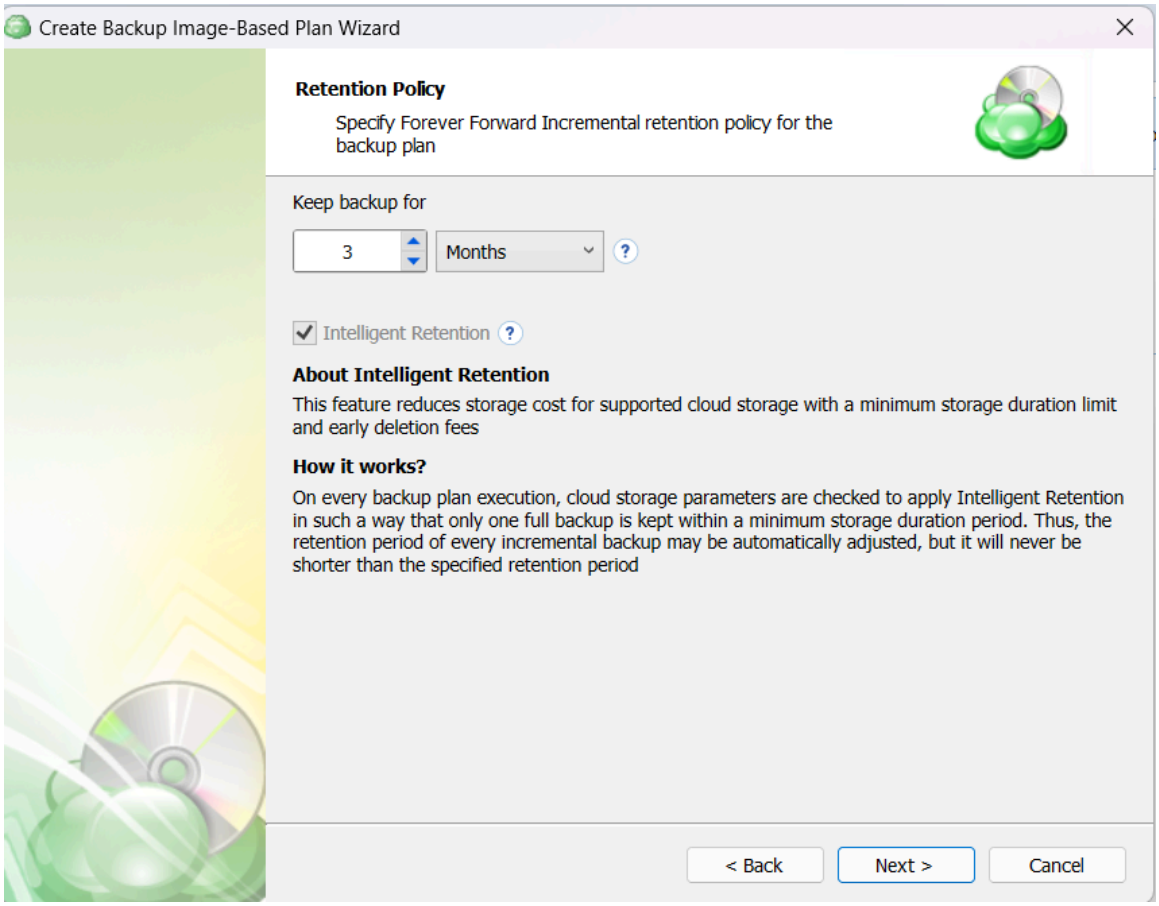
Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

Synthetic Full Backups allow the system to merge a series of incremental backups together to form a new full backup, greatly reducing the time and bandwidth needed to perform full backups after the initial full. If the storage destination does not support Synthetic full, then a traditional full will be made instead.

The Advanced Schedule and GFS retention policies will only perform properly with regularly scheduled full backups.

Step 10. On the “Retention Policy" step, you can set the policies the application will use to determine which data to purge at regular intervals.

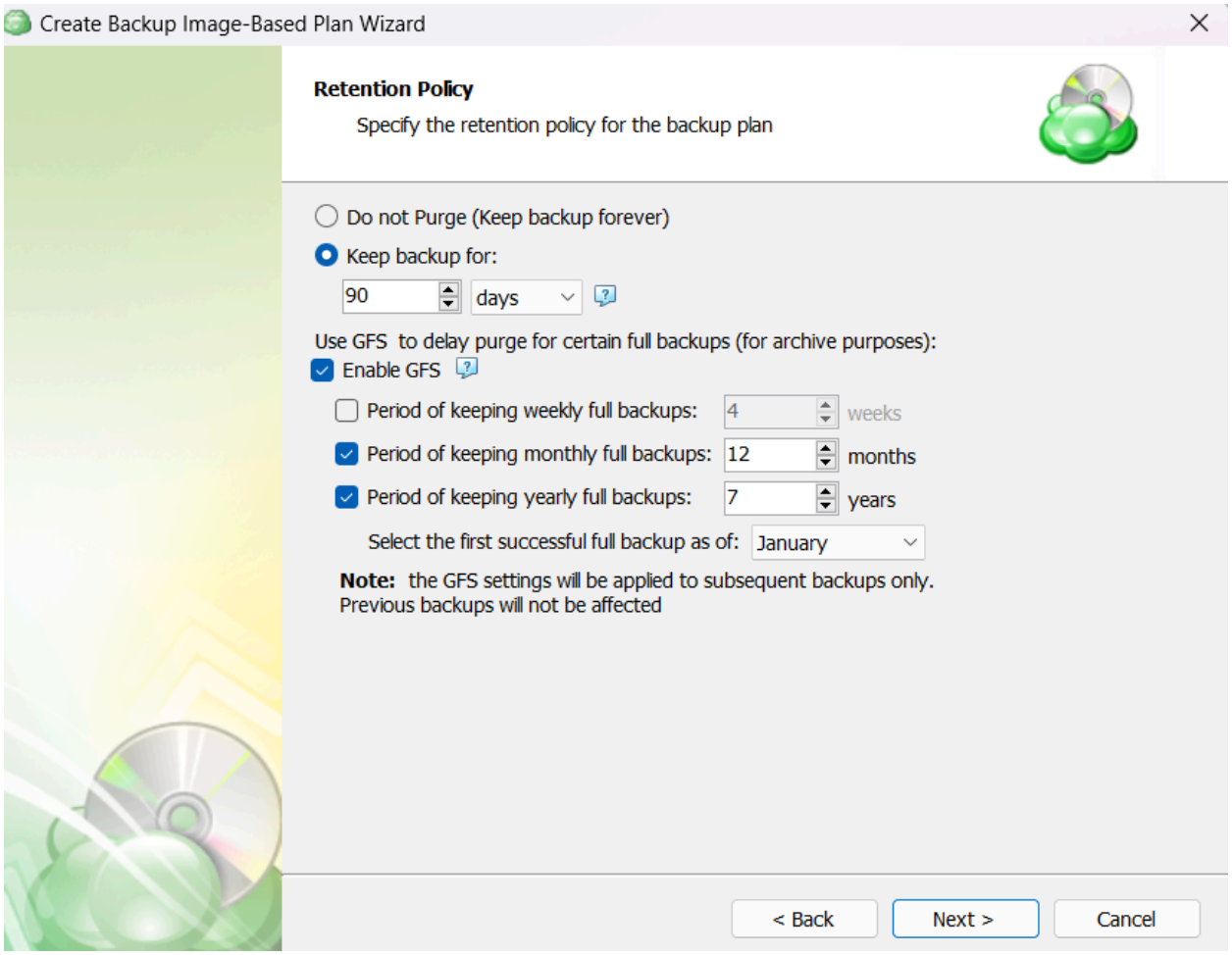
If you have selected the Simple (Forever forward) schedule you will be presented with the following options:



- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.

If you have selected the Advanced (GFS, Object Lock) schedule, you will also have an option to define the multigenerational Grandfather-Father-Son (GFS) parameters if required.

This allows you to retain full backups for longer periods while purging the incremental backups after a shorter period.

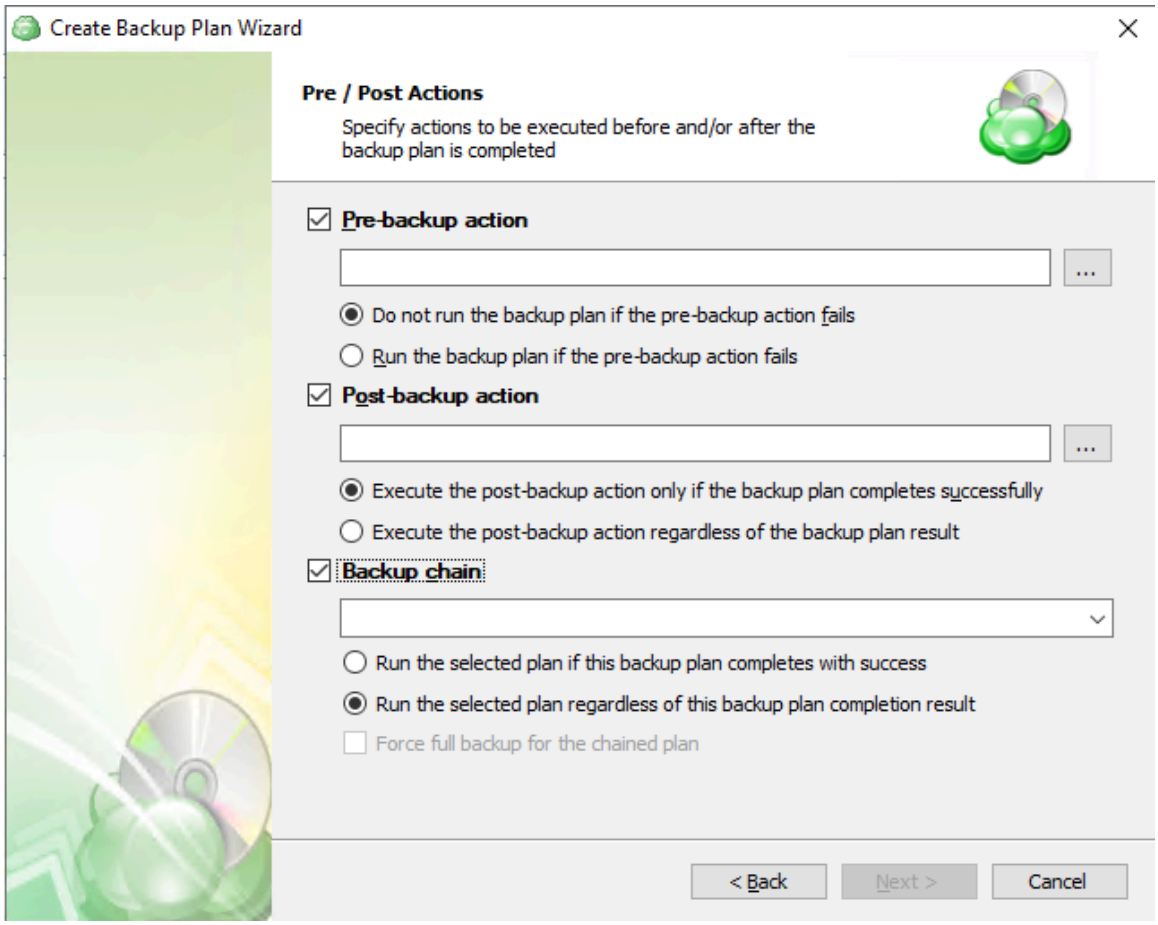


- **Enable GFS**: Select this option if you want to keep Full Backups for archival purposes at the selected intervals.
- **Period of keeping weekly full backups**: Set the number of Weekly Full Backups to retain. This is determined separately from the “Keep backup for” value and relies on Full Backups to be scheduled on at least a weekly basis in the previous step.
- **Period of keeping monthly full backups:** Number of Monthly Full Backups to retain. A Full Backup can be flagged as both a Weekly and Monthly backup, but once the number of Weekly Full Backups has exceeded their retention setting, only those also flagged as a Monthly will be retained.
- **Period of keeping yearly full backups:** Set the number of Yearly Full Backups to retain. A Full Backup can be flagged as a Weekly, Monthly, and Yearly Backup. Once the number of Monthly Full Backups has exceeded their retention setting, only those also flagged as a Yearly will be retained.
    - **Select the first successful full backup as of**: Select the first Monthly Full Backup you would like to flag and retain as the first Yearly Full Backup.

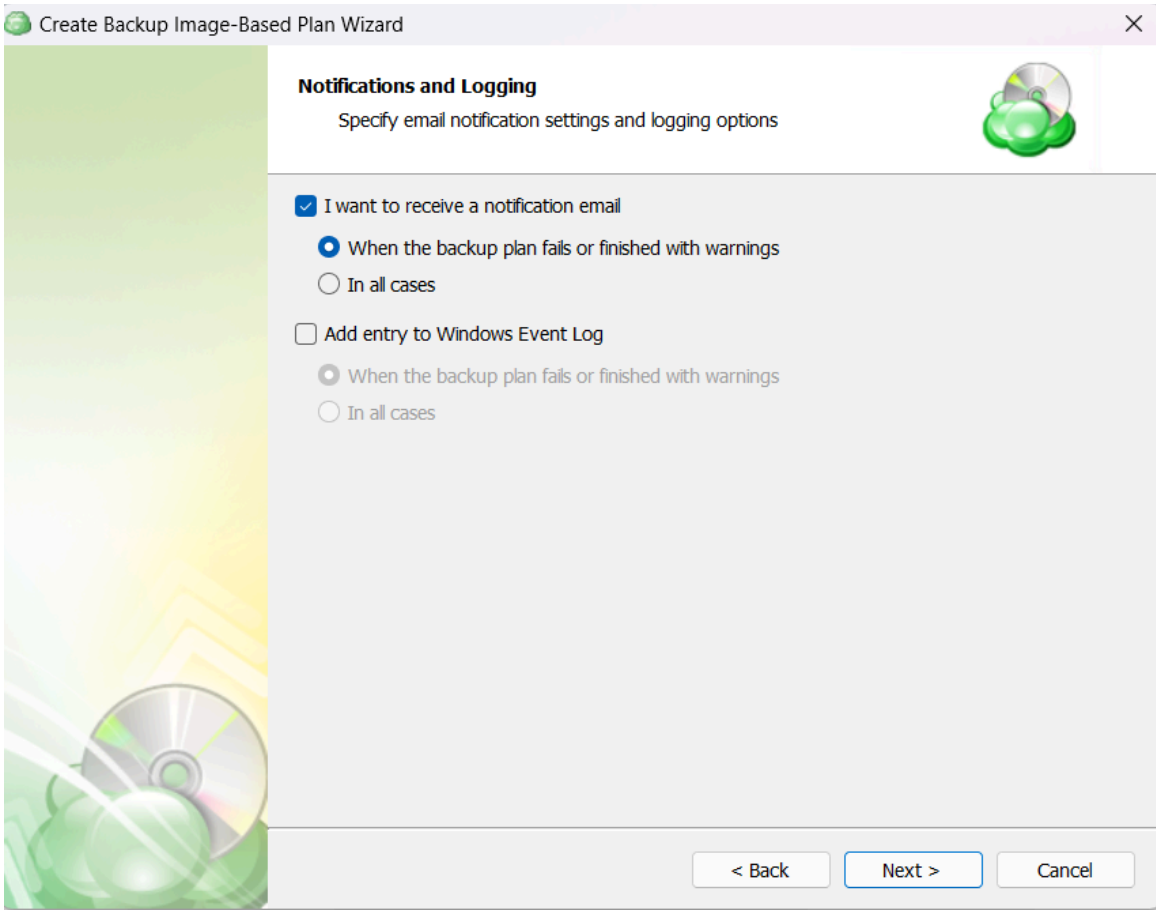
Generations will not be deleted until the youngest point in the chain has met the retention criteria.

GFS Retention provides an excellent way to efficiently archive data for compliance. Additional information can be found in GFS Policy topics in the MBS Documentation

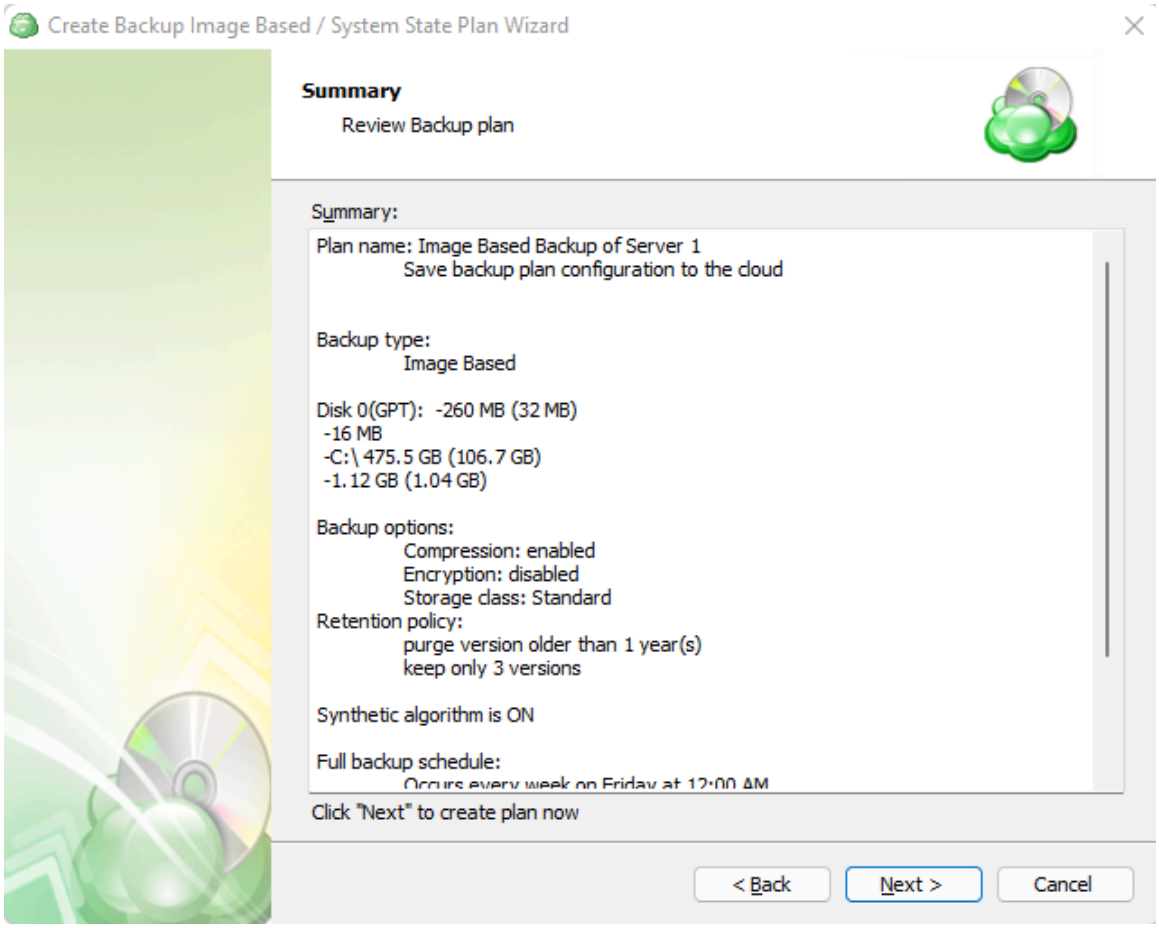
Step 11. The "Pre/Post Actions" page allows the execution of custom scripts before and/or after the running of a backup task, and can chain multiple backup tasks together for sequential execution.



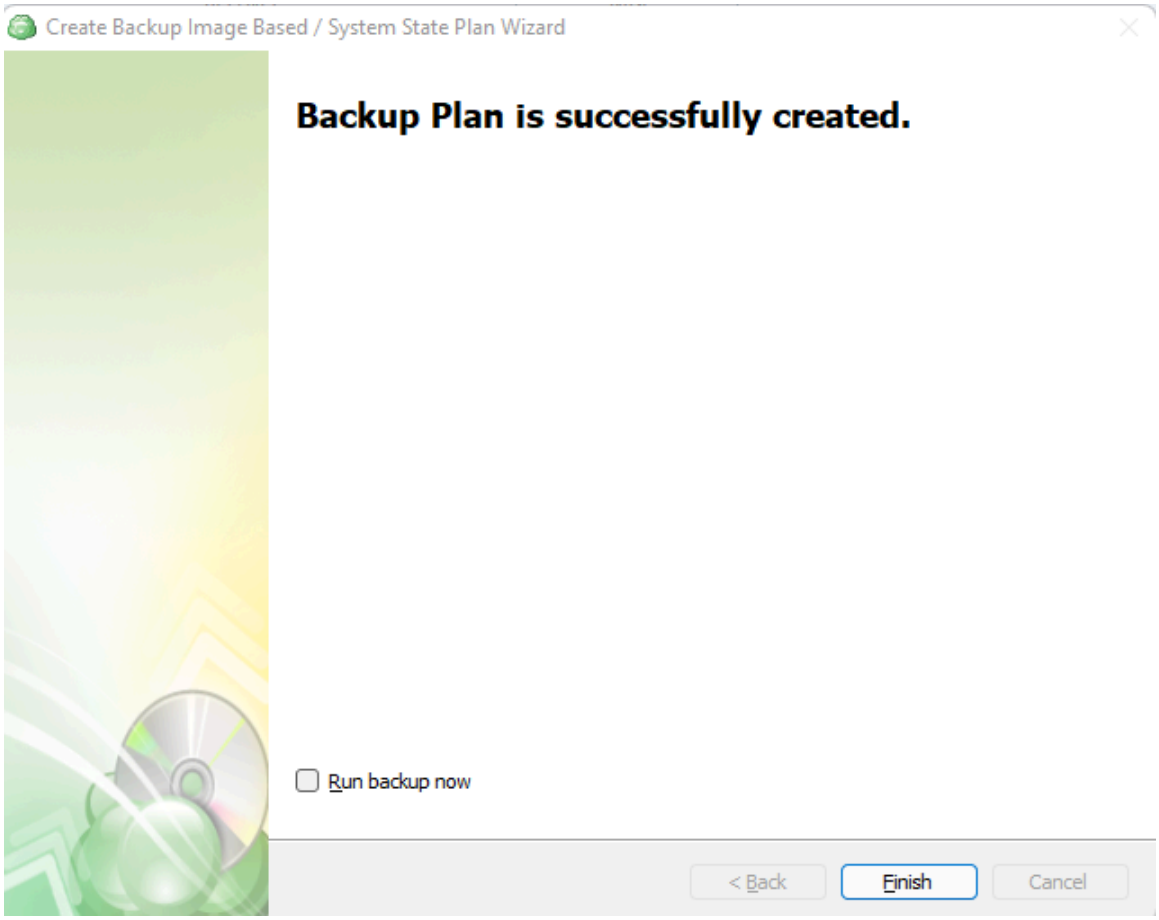
Step 12. The “Notifications and Logging” page allows you to enable notification email and add an entry to Windows Event Log upon backup plan completion or failure.



Step 13. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.

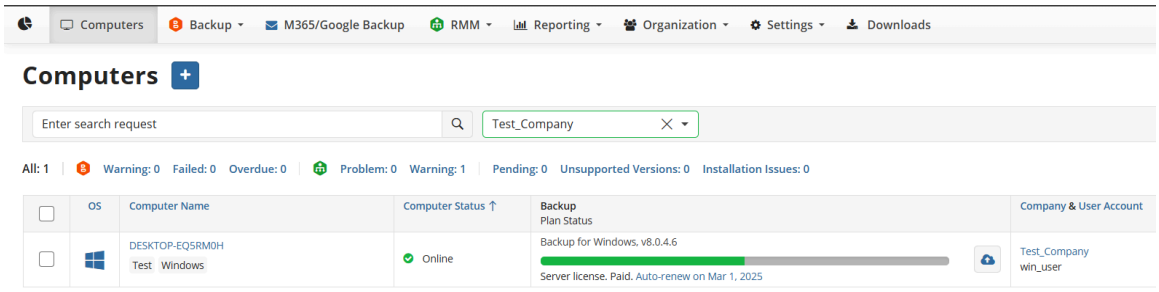


Step 14. After clicking next on the previous step, the Backup Plan is created. The final step is to acknowledge this and determine whether to run the backup immediately or for it to wait until the next scheduled occurrence.

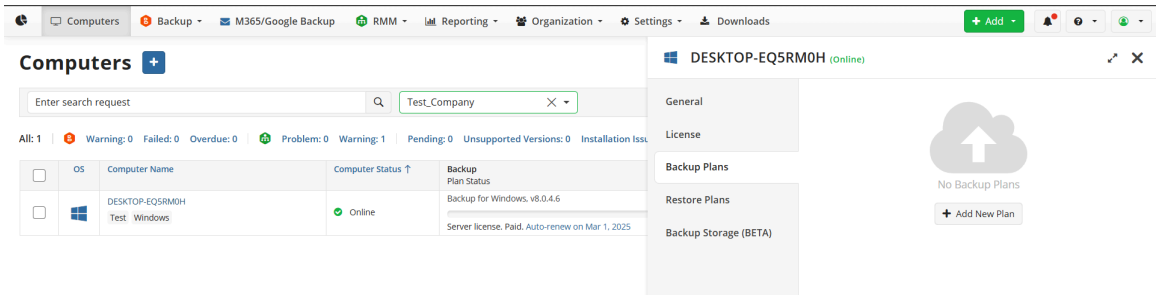


Backup for Windows using MBS

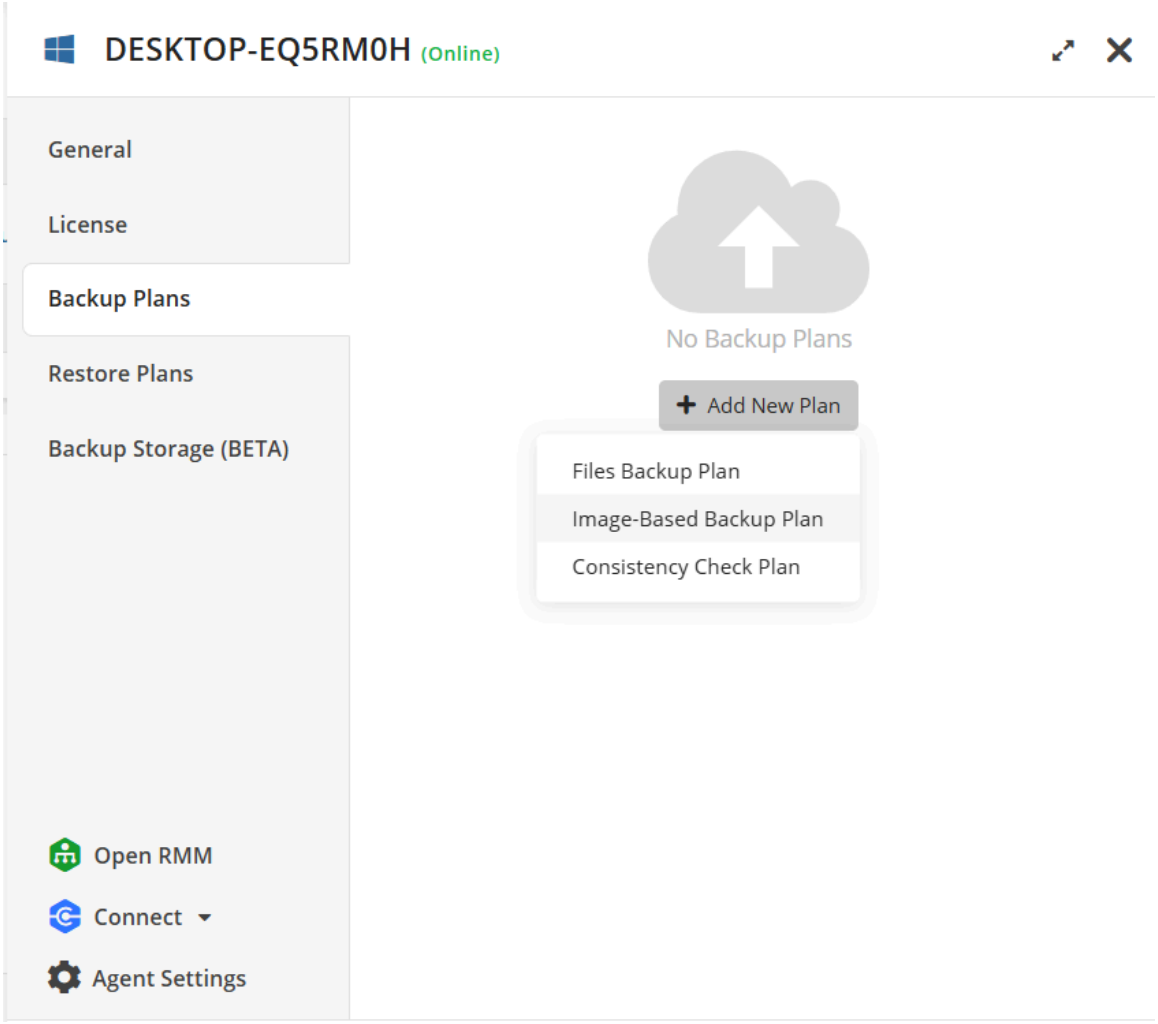
Step 1. Navigate to the MBS Portal and select the “Computers” page on the main menu.



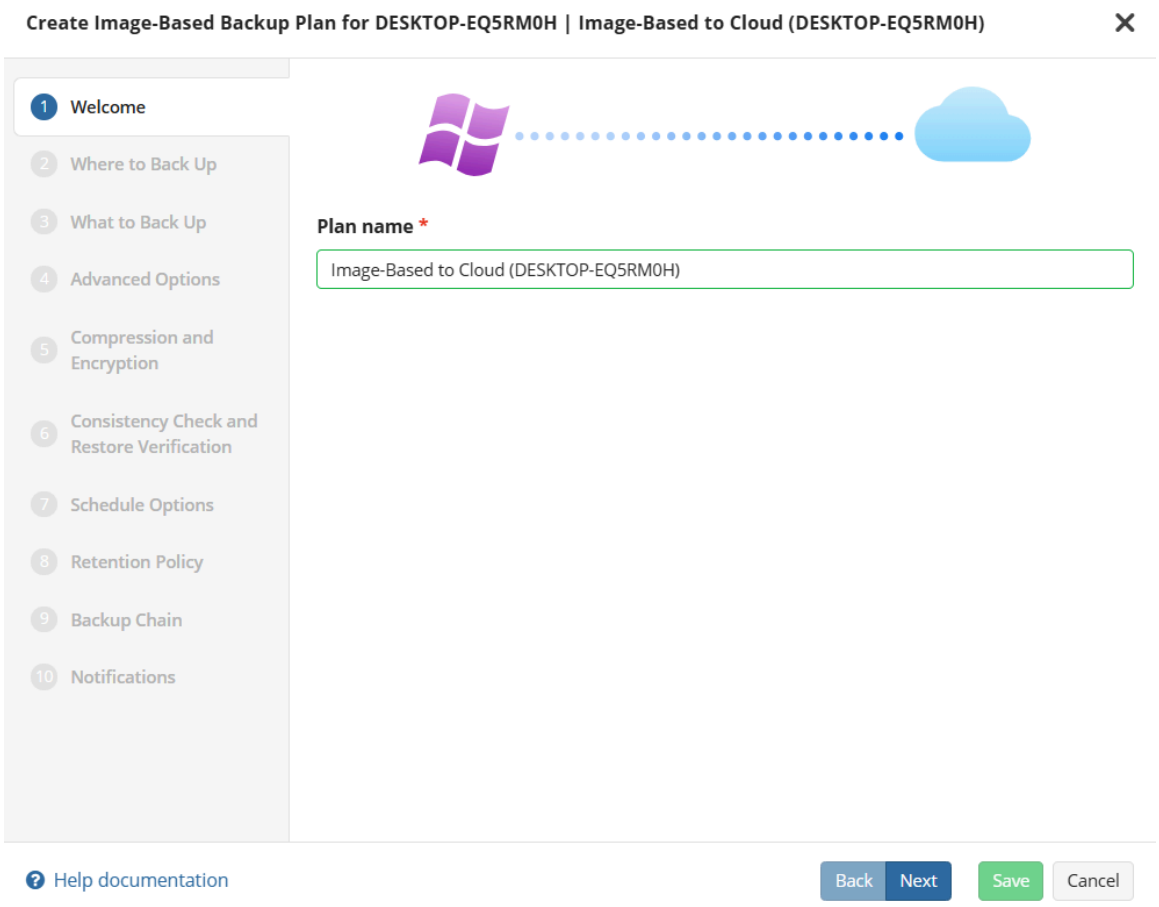
Step 2. Locate the computer you wish to backup from the list and open the current list of plans by either clicking on the name of the computer, clicking on the backup status bar, or by selecting “Show Plans” from the gear menu.



Step 3. Click on the “Add New Plan” button and select “Image-Based Backup Plan”.

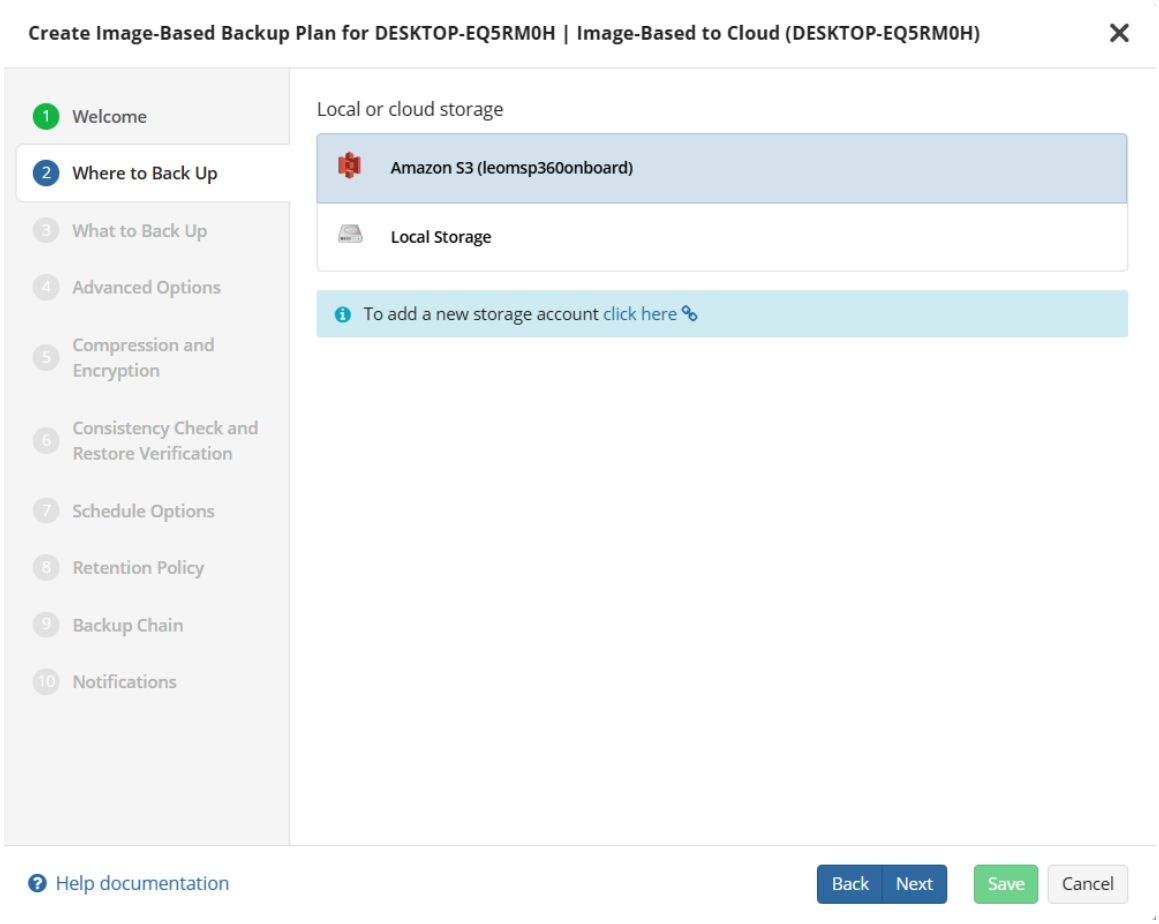


Step 4. The step in creating a new backup plan is to give it a name. Once you have entered a name, click “Next”

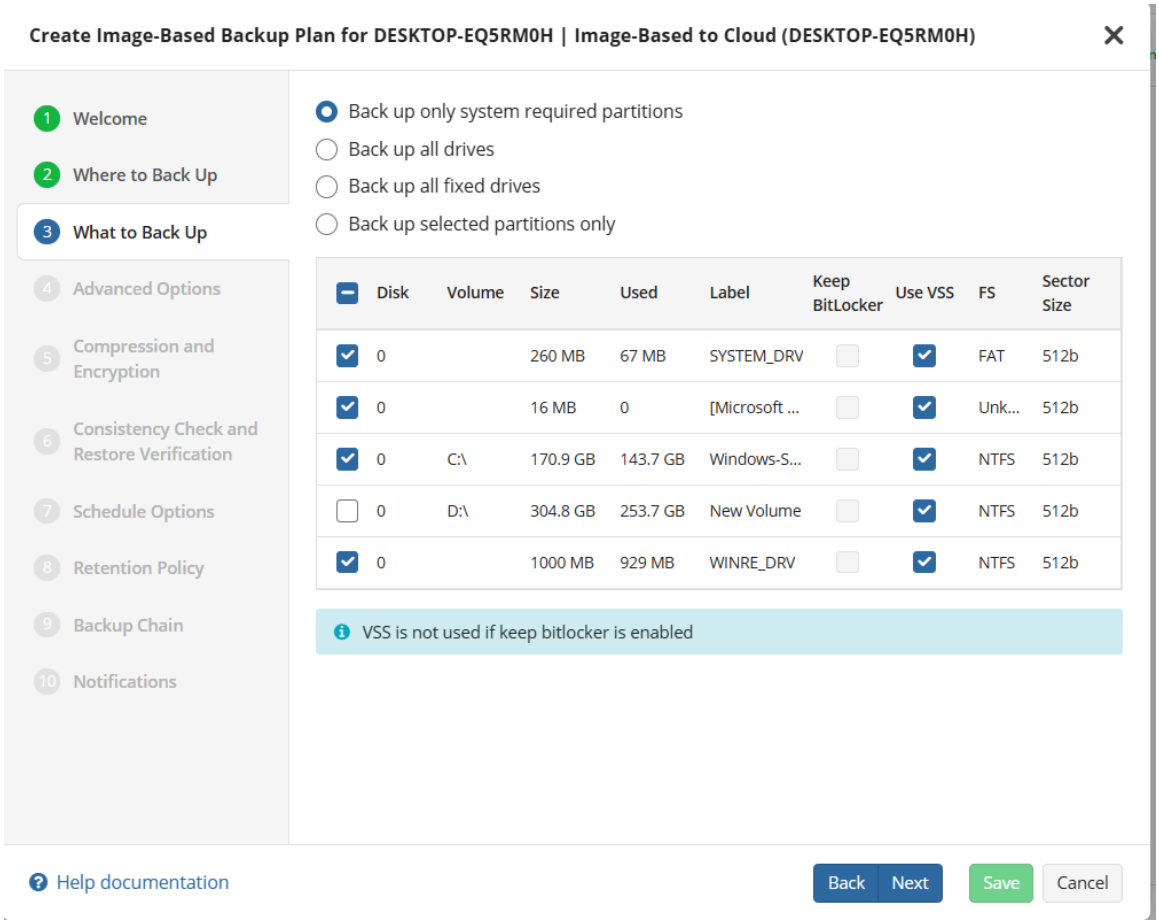


It is recommended that you select a name which helps you clearly identify the computer, company, as well as the type of backup.

Step 5. The second step in the wizard allows you to select the backup destination. Once it is selected, click “Next”.



Step 6. On the next step, you are prompted to select what partitions you would like to back up.



- **Back up only system required partitions:** This will automatically select only those partitions required to launch the operating system.
- **Back up all drives:** Selects all available partitions. This will include external media.
- **Back up all fixed drives:** Selects all partitions on non-removable media (internal drives only).
- **Back up selected partitions only:** Allows you to select only the partitions you would like to back up.
- **Keep BitLocker:** Enabling this will instruct the application to backup the data in the current encrypted state. This will prevent the Incremental backups from functioning as intended.

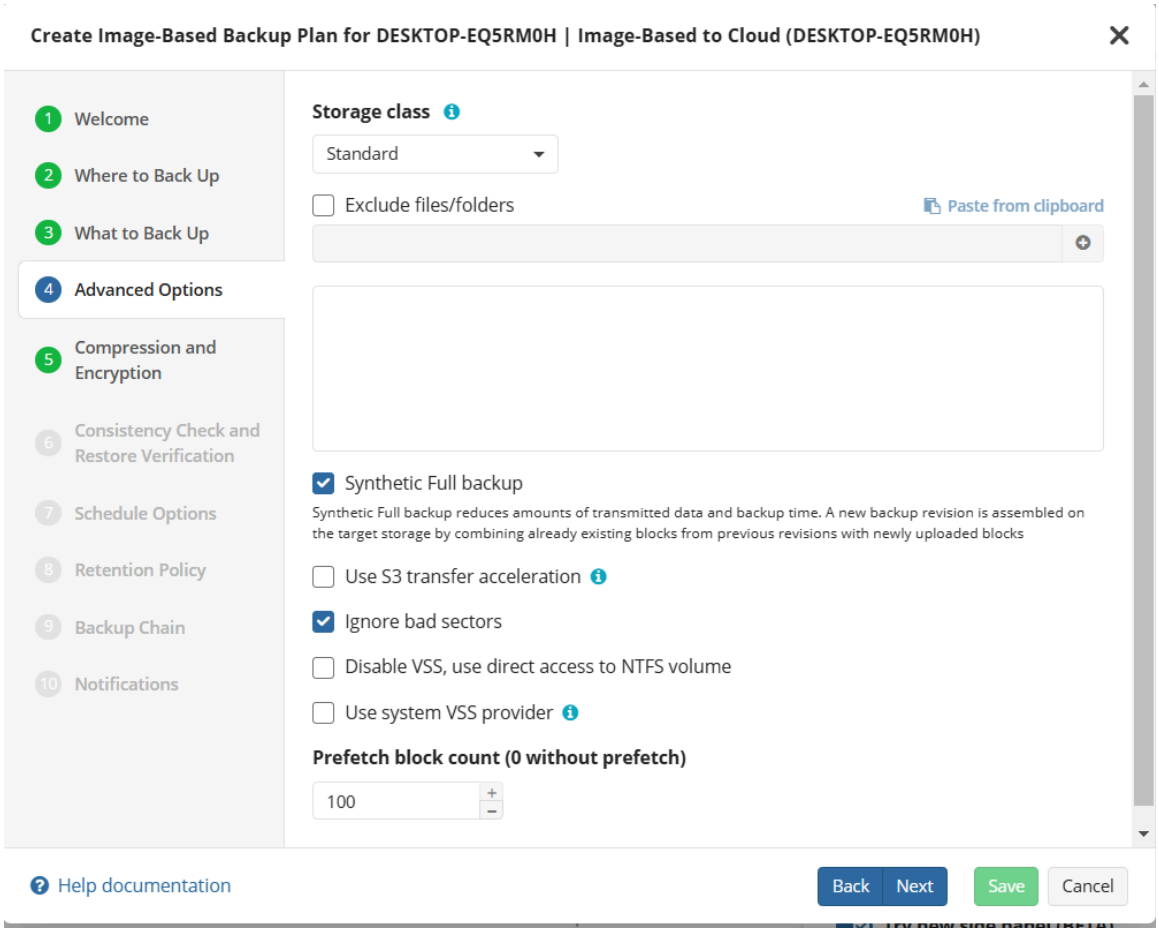
It is strongly recommended to leave the “Keep BitLocker” option disabled. The application will automatically disable BitLocker for the duration of the backup process and then re-enable it afterwards. This will ensure the integrity of the backup cannot be compromised from changes in the BitLocker encrypted data.

Enabling “Keep BitLocker” will prevent Incremental backups from functioning as intended, thus each backup will be considered a full backup.

- **UseVSS:** Enabled by default, this allows the system to be fully backed up including any files or partitions which are currently locked in use by another process.

“VSS” will automatically be disabled if keeping BitLocker

Step 7. The next step shows some Advanced Options which can be used to control what data within the selected partitions is excluded as well as some additional control over backup parameters.



- **Exclude files/folders:** Checking this will let you specify paths which should be excluded from the image backup. They may be typed, or pasted from the clipboard.

> On Windows system partitions it is recommended to exclude the \Users\ folder from the image, and set up a separate File backup for that folder.

- **Use synthetic full backup:** A synthetic full backup is a type of backup that creates a full backup using in-cloud data copying, significantly improving speed and efficiency by saving time and reducing network traffic. You can find more information about the supported cloud providers and storage classes in this article.

Synthetic full backup usage for long-term (cold) storage tiers can result in high storage costs

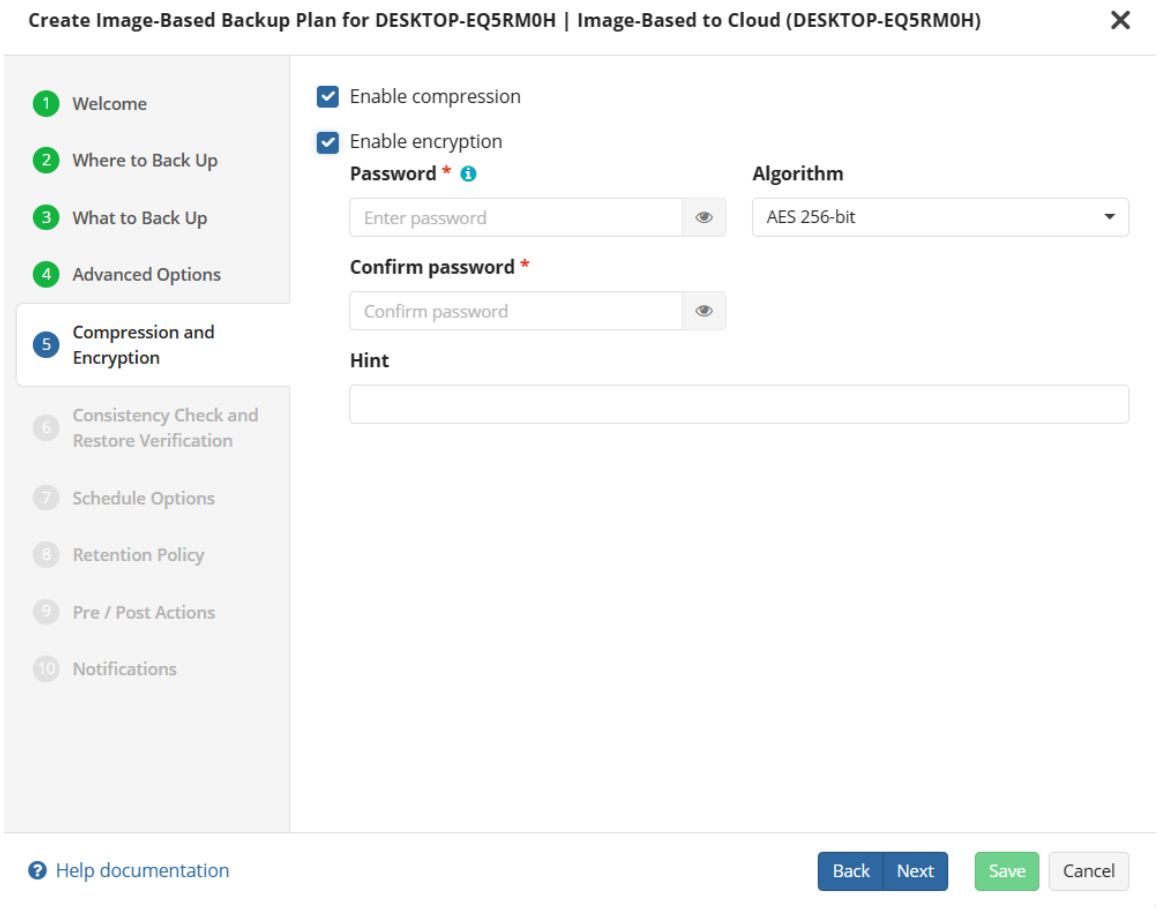
- **Ignore Bad Sectors:** Enabled by default, this allows the backup to skip any bad sectors found on the disk. It is recommended to leave this enabled unless there is a specific requirement to backup the bad sectors.
- **Disable VSS, Use Direct Access to NTFS Volume:** Disabled by default, this option should only be enabled in the event that VSS continues to fail after using the “Use system VSS provider” option.
- **Use System VSS Provider:** Disabled by default, this will force the application to use the native VSS provider for the operating system in the event that another provider has been installed by another application which is causing the backup to fail.

If VSS is failing continuously, consider enabling the “Disable VSS, use direct access to NTFS volume” option.

- **Prefetch block count:** Determines the number of individual blocks the application will simultaneously cache for uploading.

Changing the prefetch block count is not recommended except as a reaction to extreme system performance degradation during backup.

Step 8. Next, you will choose whether to enable compression and encryption of the backup.

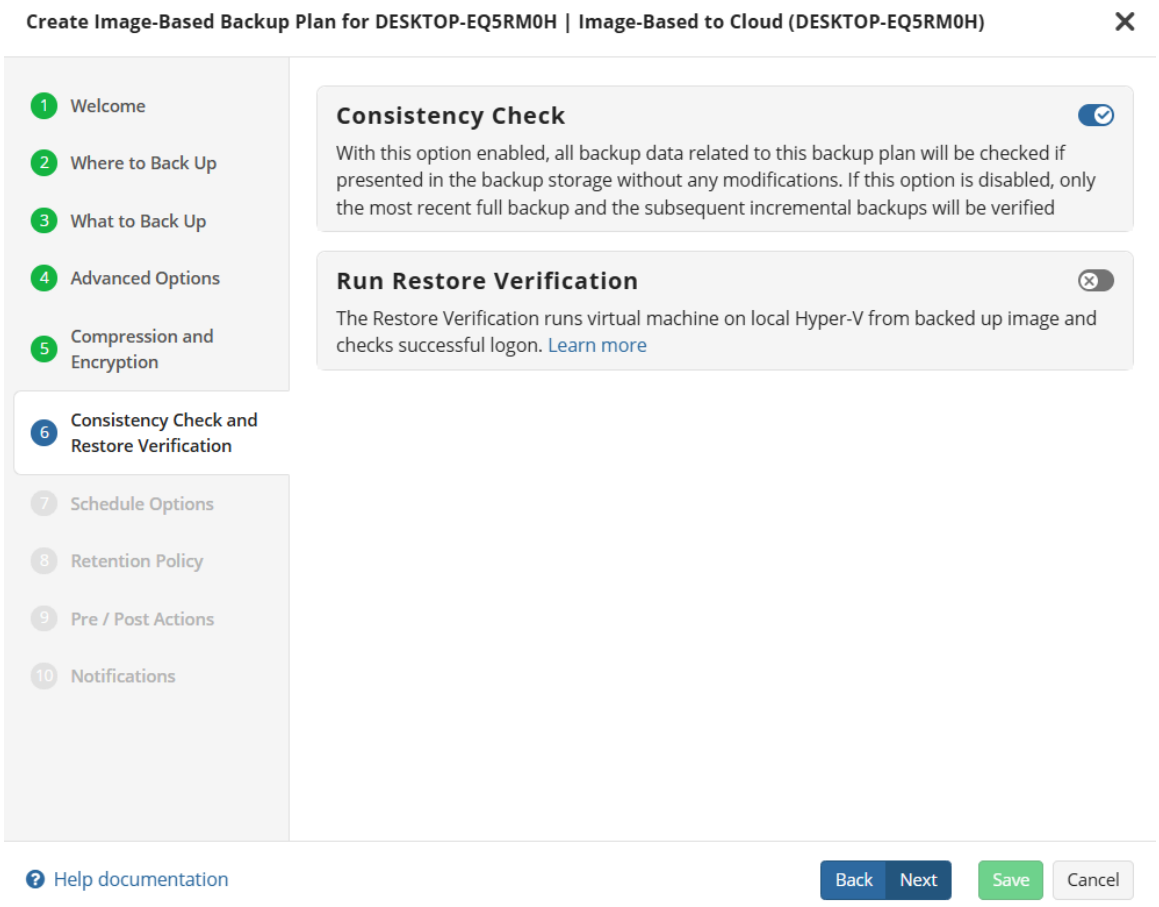


Enabling compression will reduce the size of the backup and reduce the time to upload it, both of which may decrease the cost of the backup.

Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

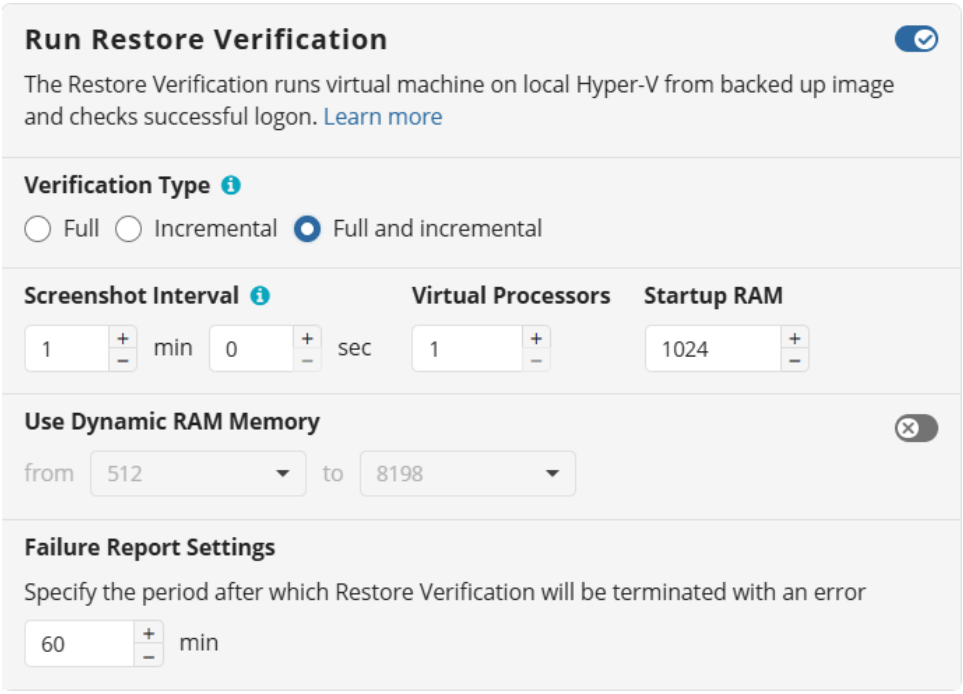
It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place and enable the Password Recovery Service

Step 9. Next you are presented with the Consistency Check and Restore Verification Options.



It is recommended that you leave "**Enable Full Consistency Check**" enabled.

Although a successful Consistency Check ensures the backup integrity, an additional Restore Verification process can be executed as well.



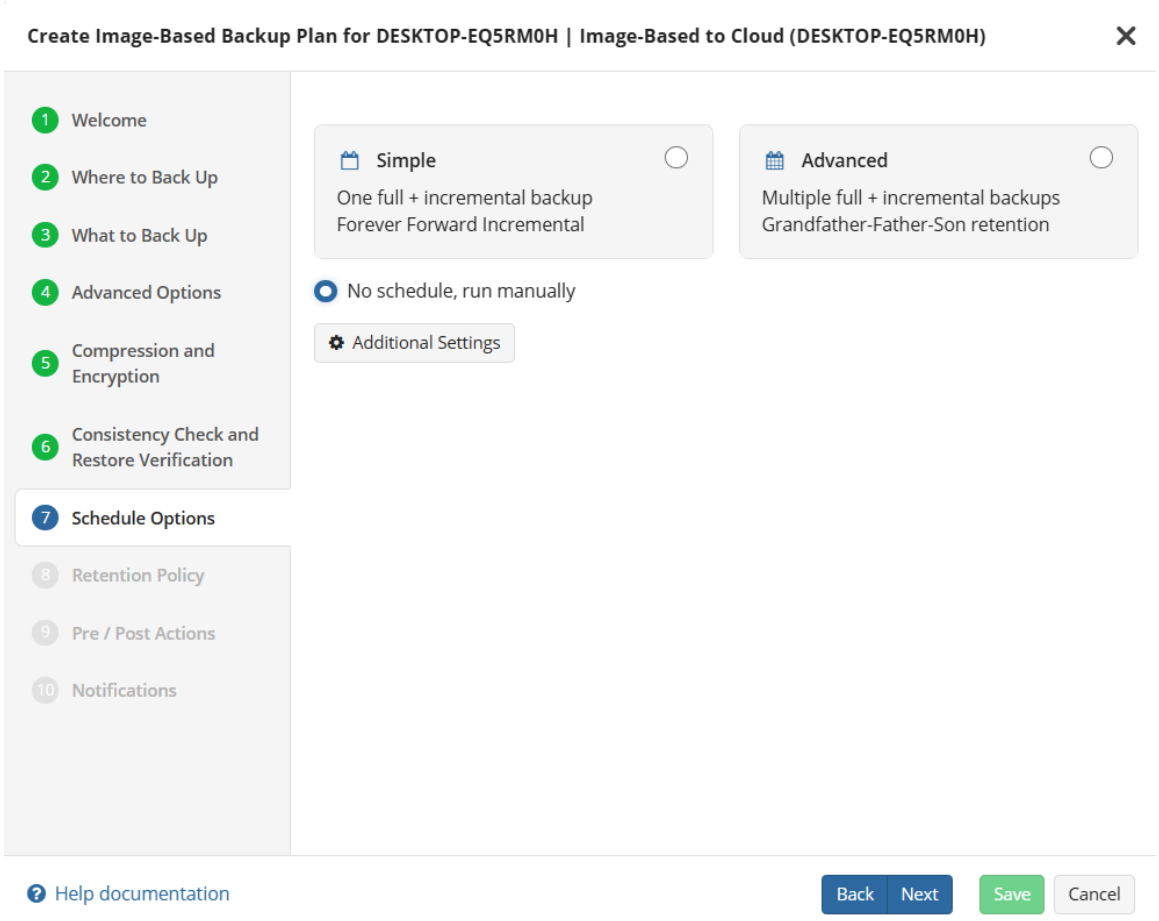
This process uses a temporary Hyper-V virtual machine on the source endpoint to test Windows startup. It only retrieves the necessary backup parts from storage without the need to download the entire backup.

> Since the **Restore Verification** feature is based on Hyper-V mechanisms, a Hyper-V environment is required on your operating system. You can find more information here.

You can run the Restore Verification for incremental backups only, full backups only, for every backup, or do not run it at all.

Along with the Restore Verification running mode, customize the Hyper-V auxiliary virtual machine configuration to run the Restore Verification (number of virtual processors, RAM).

Step 10. Next you are prompted to set the schedule for your backup plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.

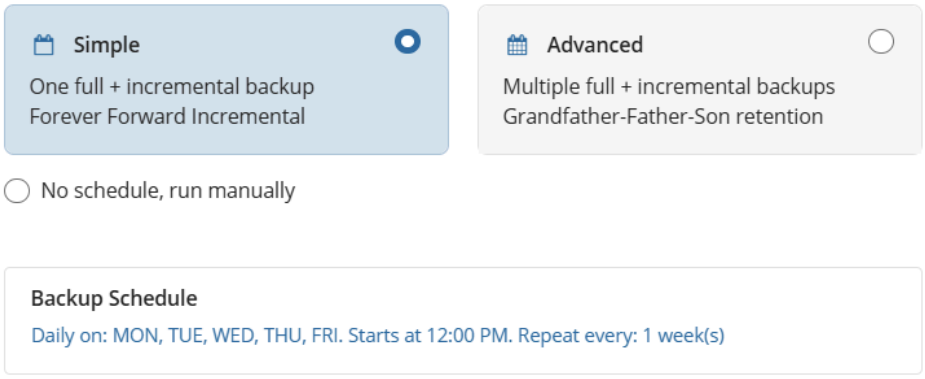


Synthetic Full Backups allow the system to merge a series of incremental backups together to form a new full backup, greatly reducing the time and bandwidth needed to perform full backups after the initial full. If the storage destination does not support Synthetic full, then a traditional full will be made instead.

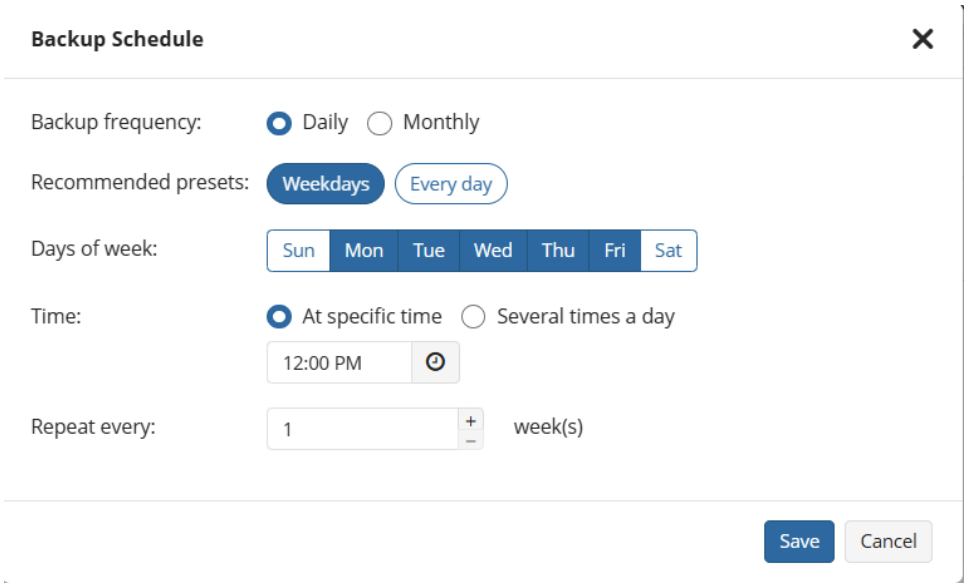
The retention policy will only perform properly with regular scheduled full backups.

- **Simple (Forever forward):** Select the Simple (Forever Forward) option to use the Forever Forward Incremental (FFI). This schedule offers one full backup followed by a

limited number of incrementals. Once the limit is exceeded, a new full backup is created using in-cloud copying (synthetic full backup).
The simple schedule is unavailable if the selected storage account does not support synthetic full backups. To find more information about the supported storage providers and storage classes, please refer to the Forever Forward Incremental article.



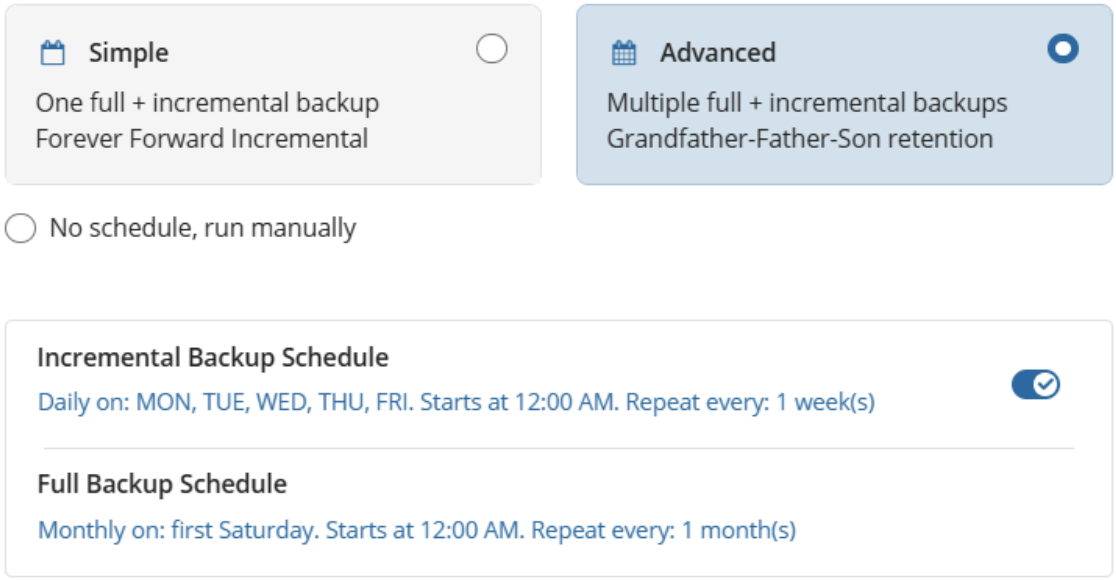
You can modify the “Backup Schedule” by clicking on the section as displayed below:



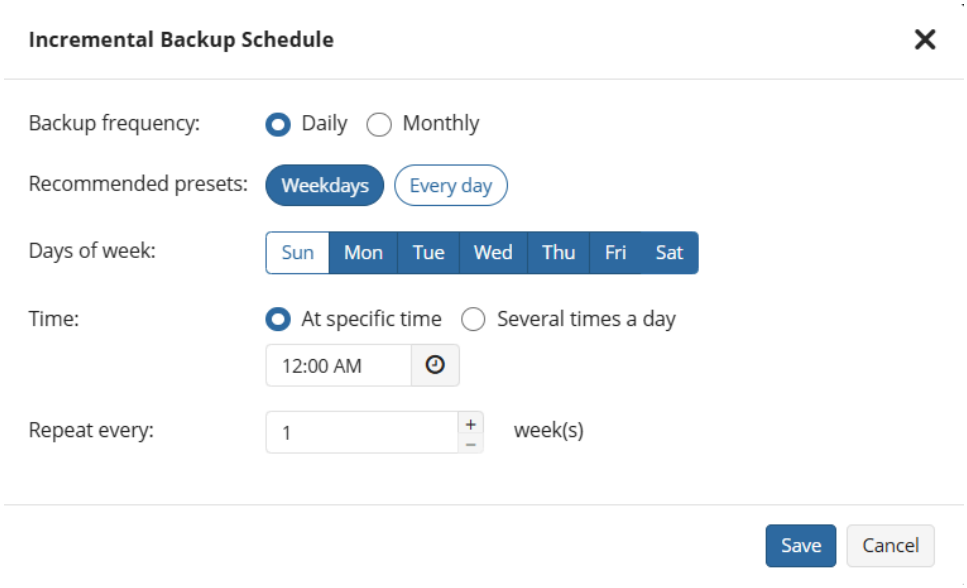
The Simple (Forever forward) schedule is a good option to use for the short-term retention policy such as 30 days (1 months) or 90 days (3 months).

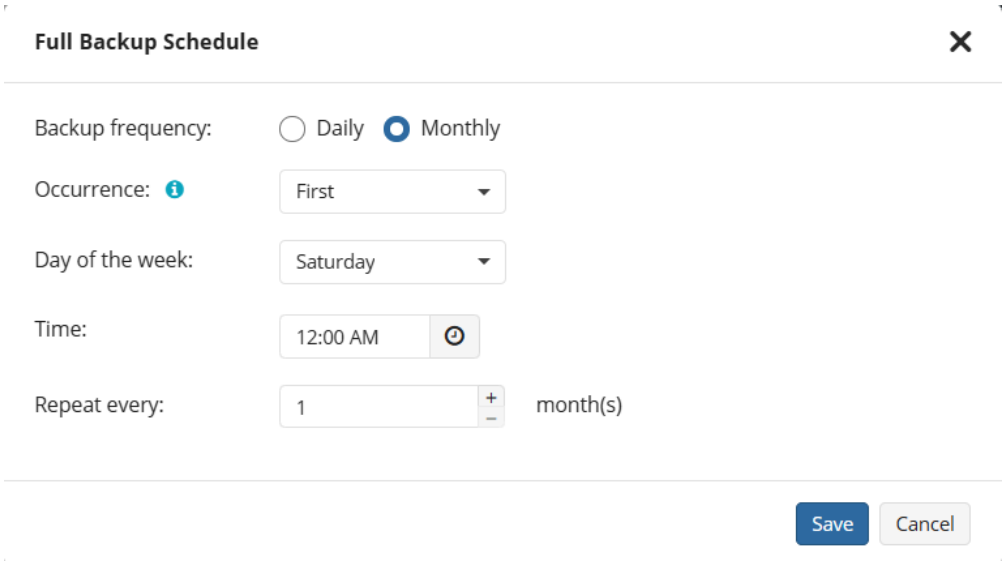
> It is not recommended to select the Simple (Forever forward) schedule for long-term storage and archival purposes. If you planning to retain more than 100 restore points (days), please consider using the Advanced schedule.

- **Advanced (GFS, Object Lock):** Select the Advanced option to set up a flexible, recurring schedule with generations. Every generation contains one full backup followed by incrementals.



The “Advanced” option allows you to configure different schedules for your Incremental and Full backups:

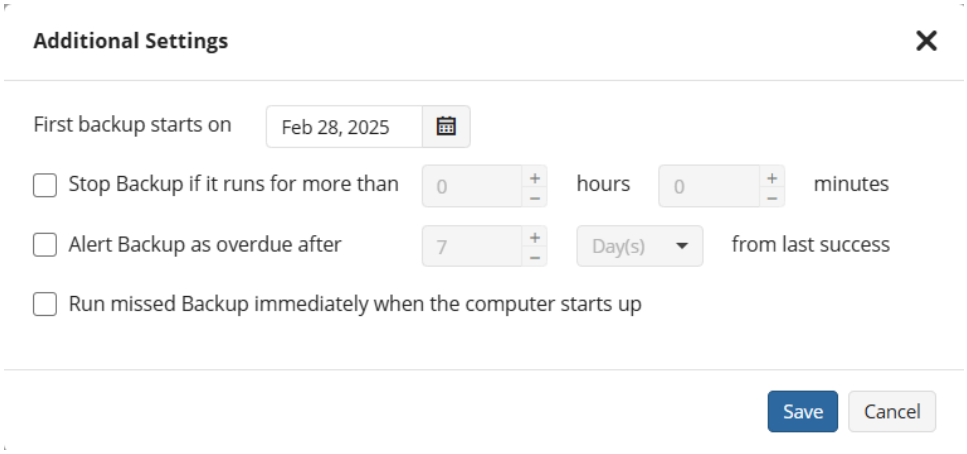




It is recommended to use the Advanced (GFS, Object Lock) option and regularly scheduled full backups for long-term storage (longer than 6 months), archival, and legal purposes.

The most common setup for the Advanced Schedule is daily Incremental backups with either weekly or monthly Full backups.

By clicking on the **Additional Settings** button, you can see the options below:

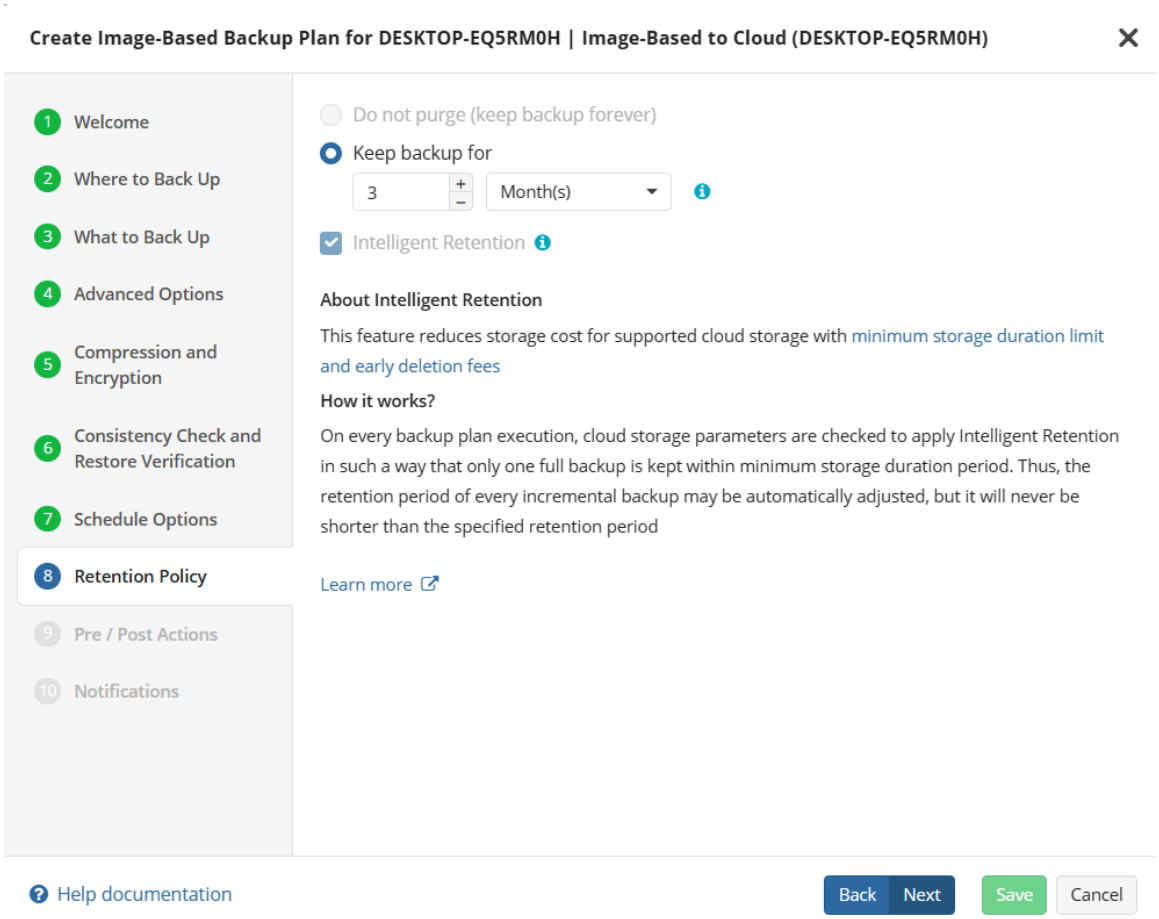


Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

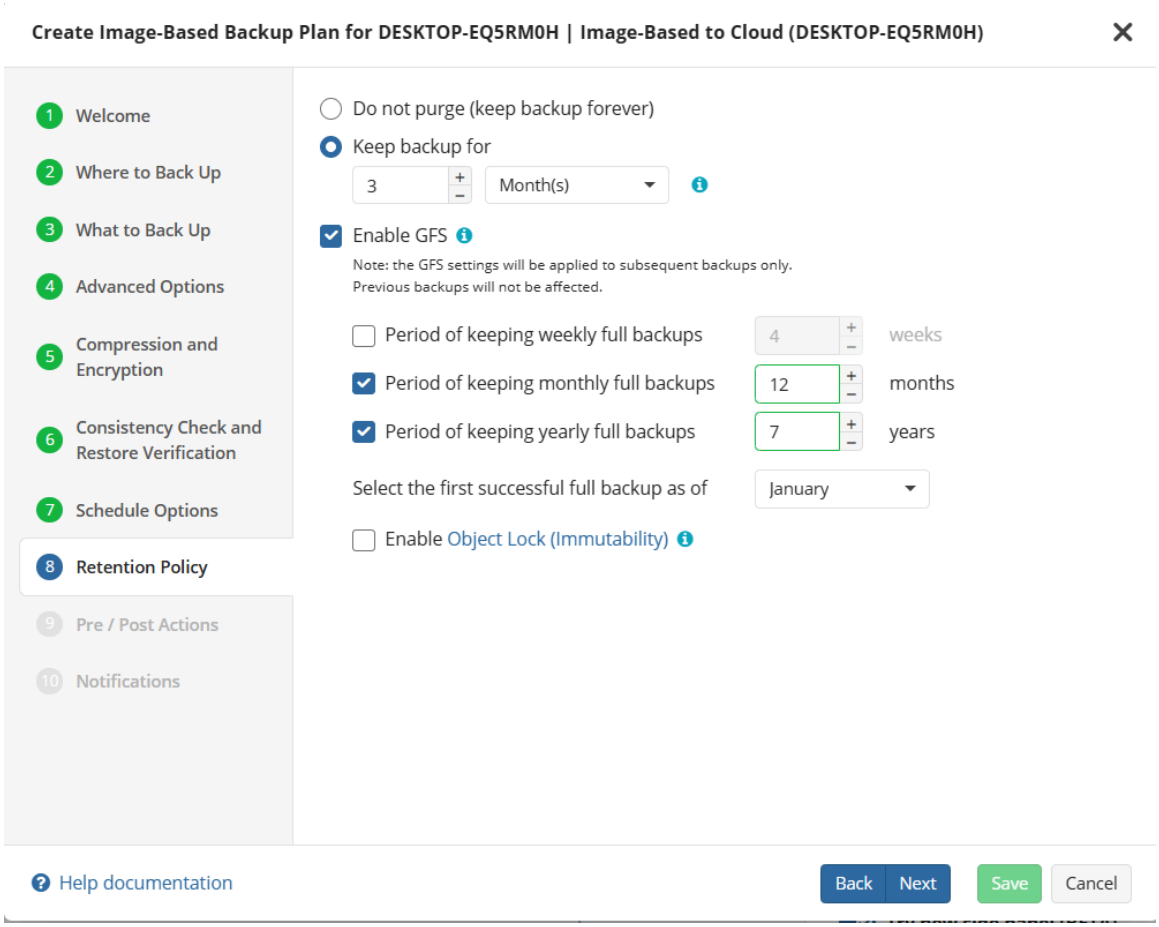
Step 11. On the “Retention Policy" step, you can set the policies the application will use to determine which data to purge at regular intervals.

If you have selected the Simple (Forever forward) schedule you will be presented with the following options:



- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.

If you have selected the Advanced (GFS, Object Lock) schedule, you will also have an option to define the multigenerational Grandfather-Father-Son (GFS) parameters if required.
This allows you to retain full backups for longer periods while purging the incremental backups after a shorter period.



- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.
- **Enable GFS**: Select this option if you want to keep Full Backups for archival purposes at the selected intervals.
- **Period of keeping weekly full backups**: Set the number of Weekly Full Backups to retain. This is determined separately from the “Keep backup for” value and relies on Full Backups to be scheduled on at least a weekly basis in the previous step.
- **Period of keeping monthly full backups:** Number of Monthly Full Backups to retain. A Full Backup can be flagged as both a Weekly and Monthly backup, but once the number of Weekly Full Backups has exceeded their retention setting, only those also flagged as a Monthly will be retained.
- **Period of keeping yearly full backups:** Set the number of Yearly Full Backups to retain. A Full Backup can be flagged as a Weekly, Monthly, and Yearly Backup. Once the number of Monthly Full Backups has exceeded their retention setting, only those also flagged as a Yearly will be retained.

- **Select the first successful full backup as of**: Select the first Monthly Full Backup you would like to flag and retain as the first Yearly Full Backup.

Restore Points will not be deleted until the youngest point in the chain has met the retention criteria.

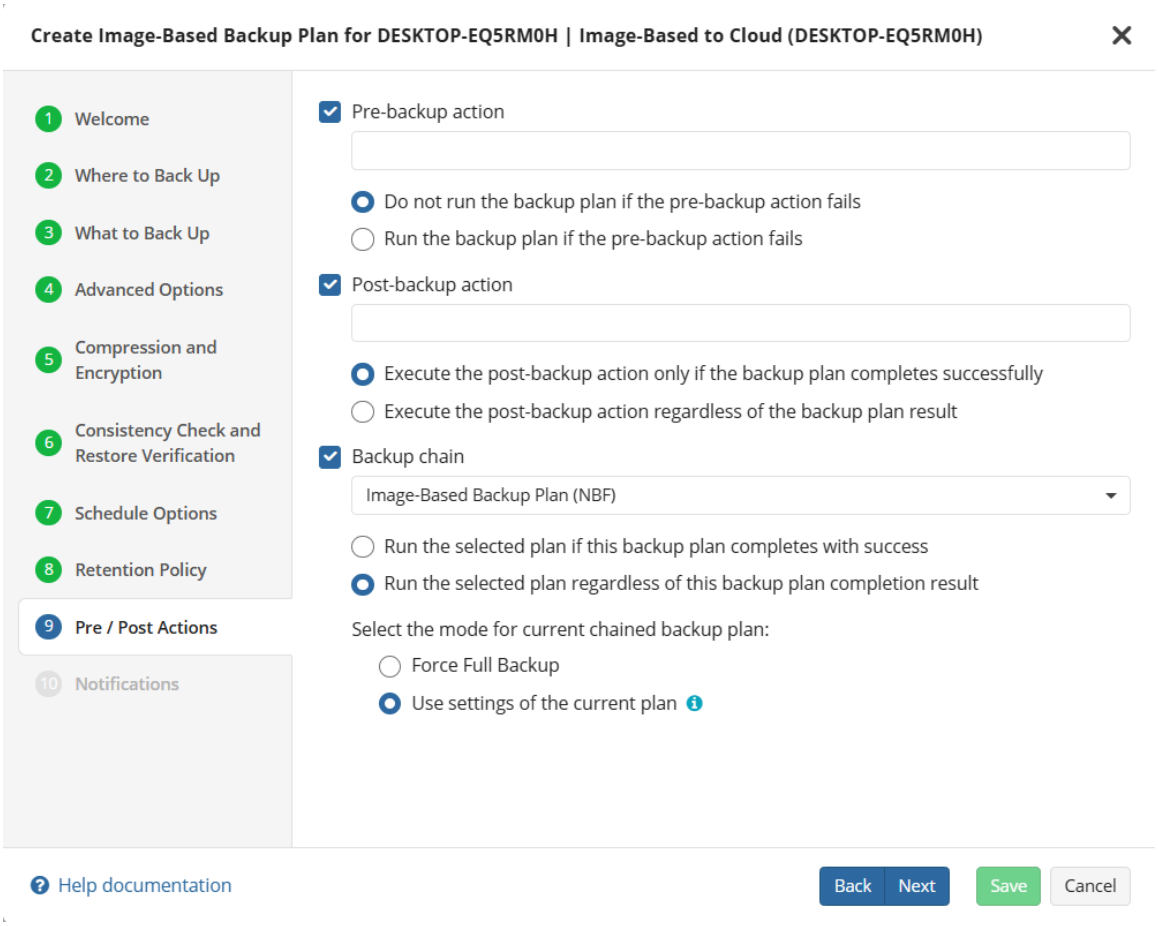
GFS Retention provides an excellent way to efficiently archive data for compliance. Additional information can be found in GFS Policy topics in the MBS Documentation

- **Enable Object Lock (Immutability):** is a feature that locks backup datasets for a period specified by GFS retention policy. Within this period, backup data is kept unmodified.

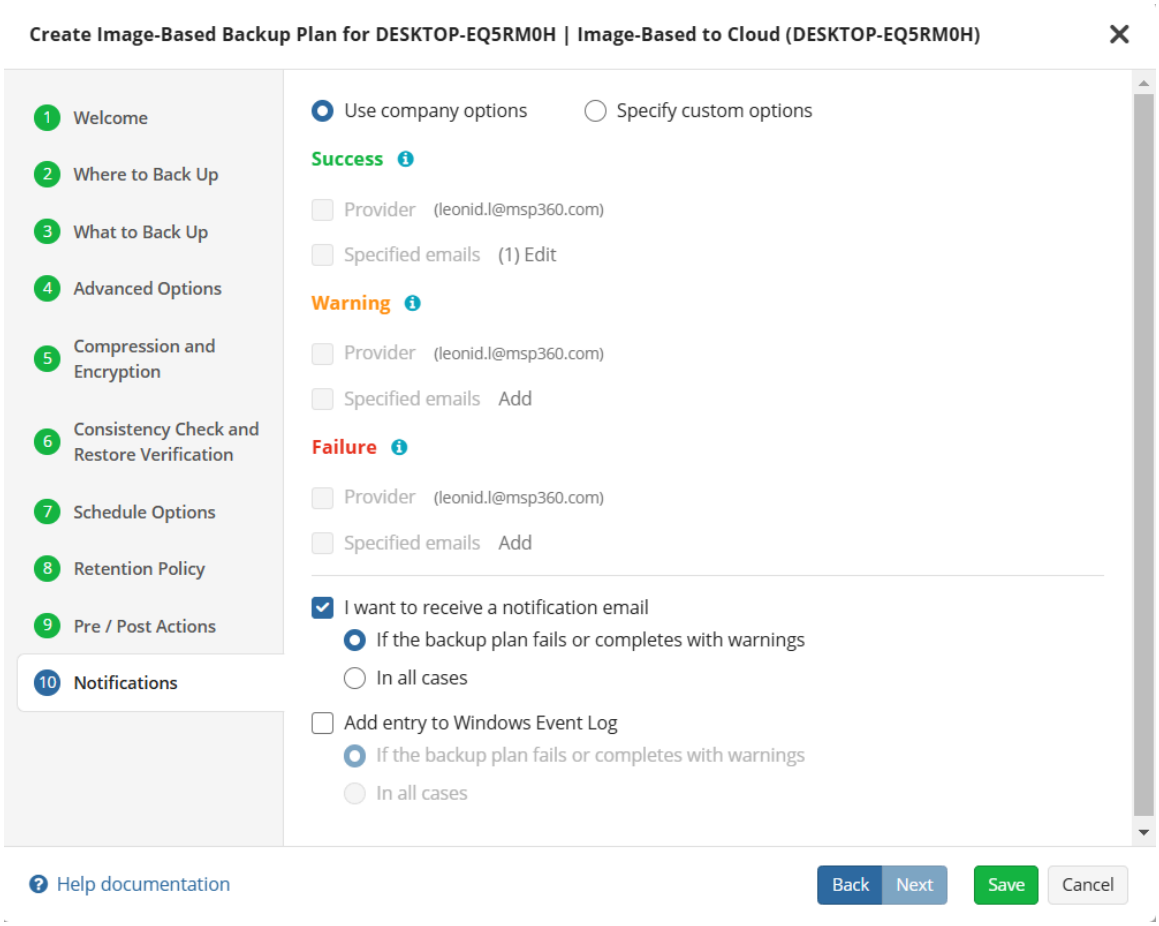
Use the Immutability feature with extreme caution. Once a backup data becomes immutable in Compliance mode, there is no way to delete them from the storage until the specified GFS keeping period expires except for the storage account termination. Incorrect settings can cause high storage bills.

To find more information about the Object Lock feature, supported storage providers, and required permissions, please refer to this article.

Step 12. The “Pre/Post Actions” page allows the execution of custom scripts before and/or after the running of a backup task, and can chain multiple backup tasks together for sequential execution.



Step 13. The final step when creating a Backup Plan is to review the Notifications and Logging. The default settings applied at the Company level are selected by default, however you are also able to specify custom options per plan.

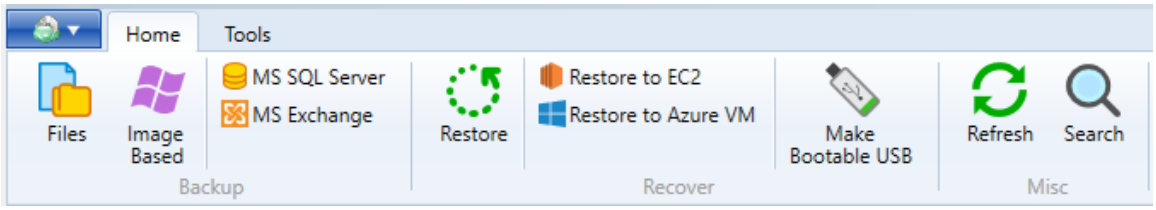


Once you are satisfied with the selected notifications and logging, clicking “Save” will create the new plan and close the wizard.

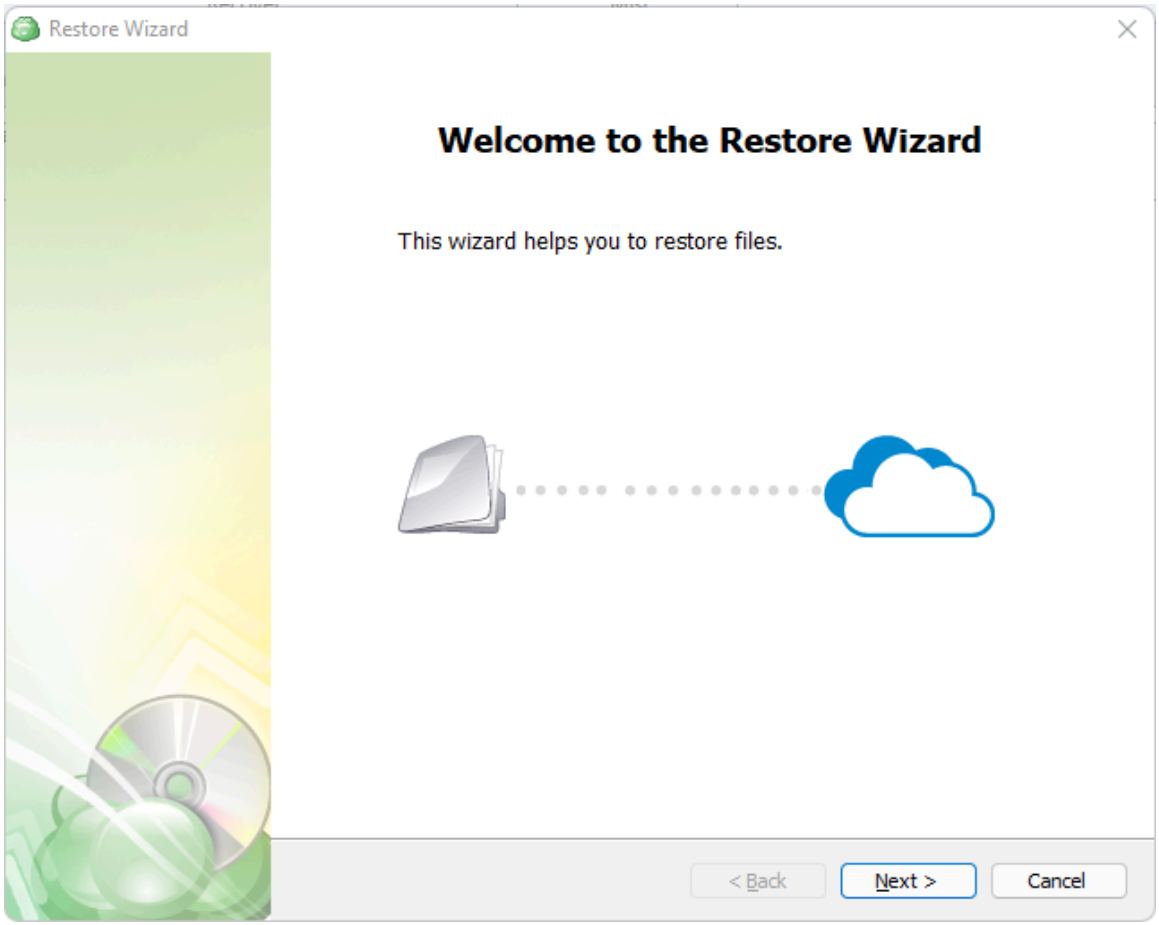
Image-Based Restore Plans

Restore to Physical Disk using the Agent

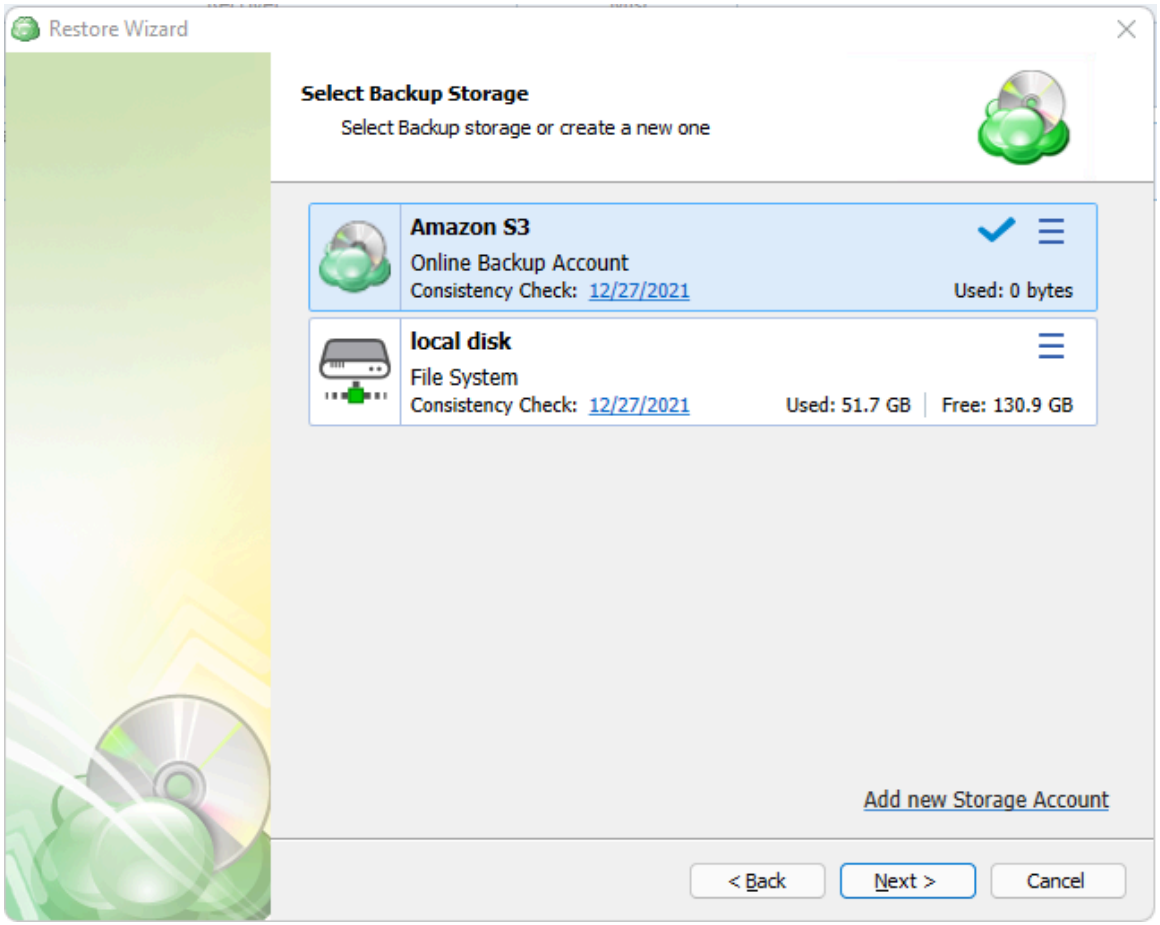
Step 1. After launching the Online Backup, you can run the Restore Wizard by “Restore” on the application's main toolbar.



Step 2. The first step of the wizard indicates that you have started the wizard.

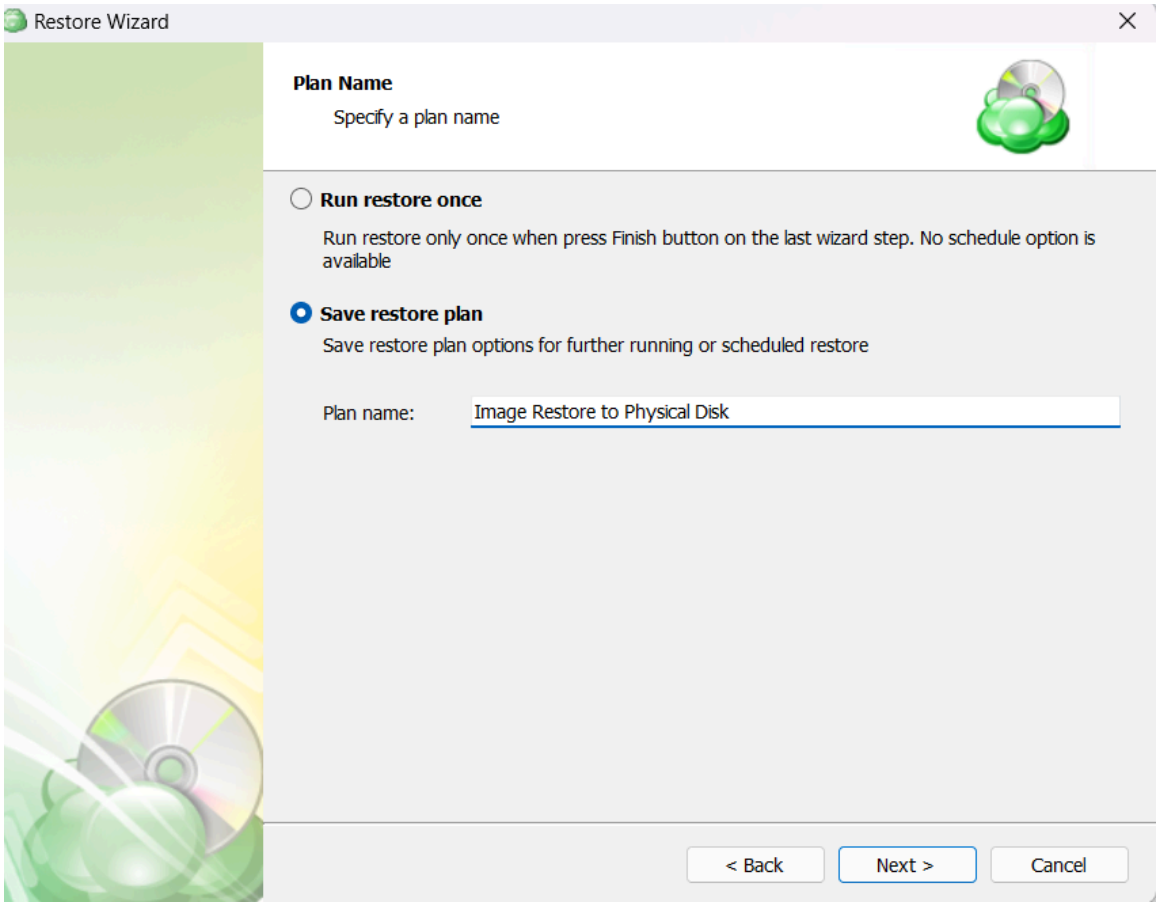


Step 3. The next step will prompt you to select the storage location for the source.

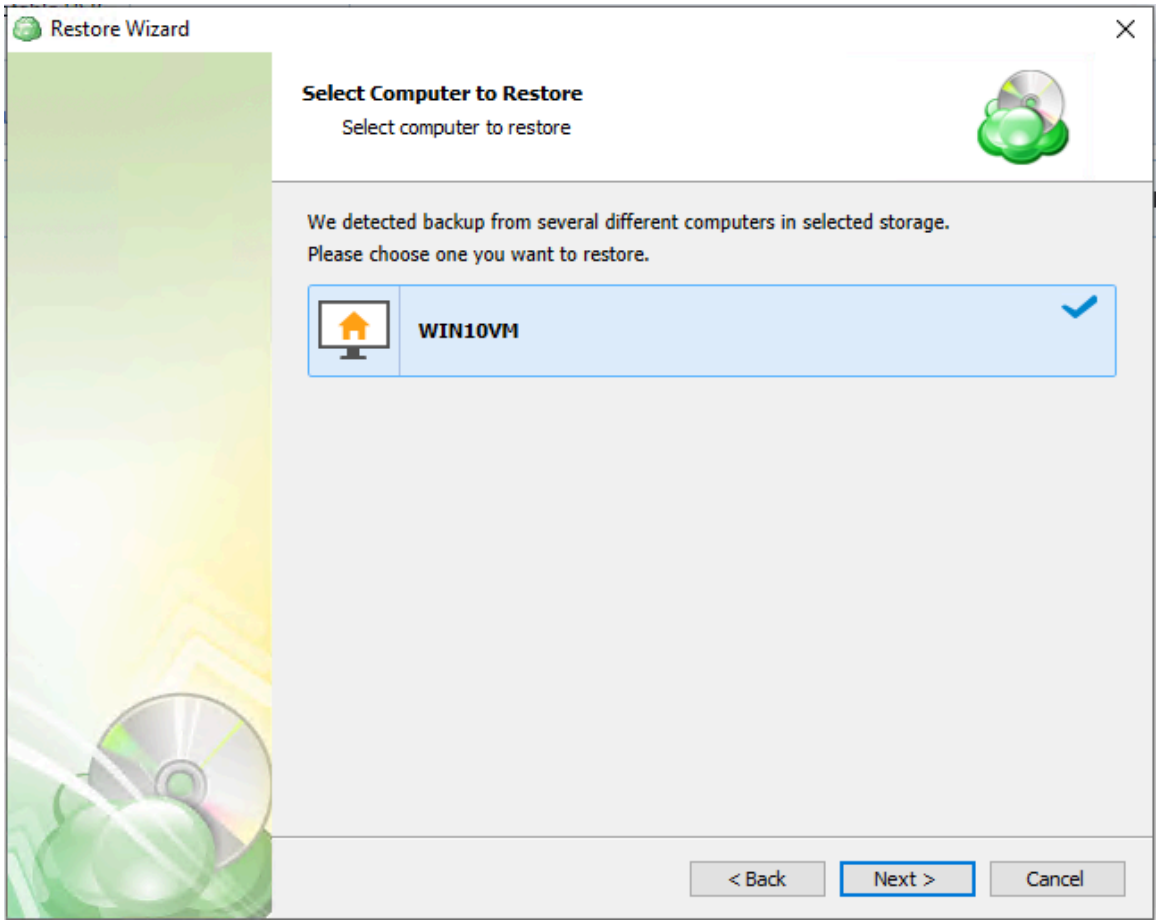


If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

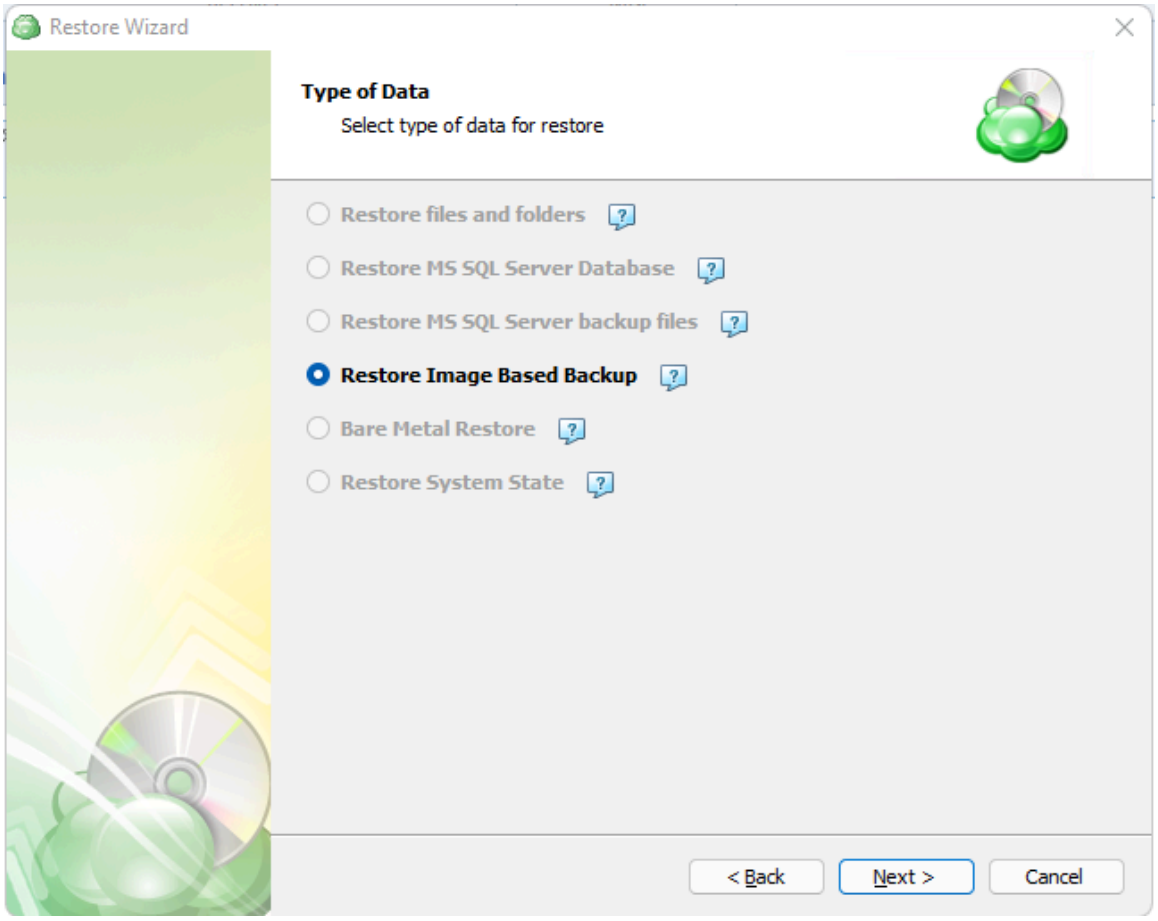
Step 4. Next you will choose whether to run the restore operation only once, or to save it for later use. The latter will allow you to name the plan.



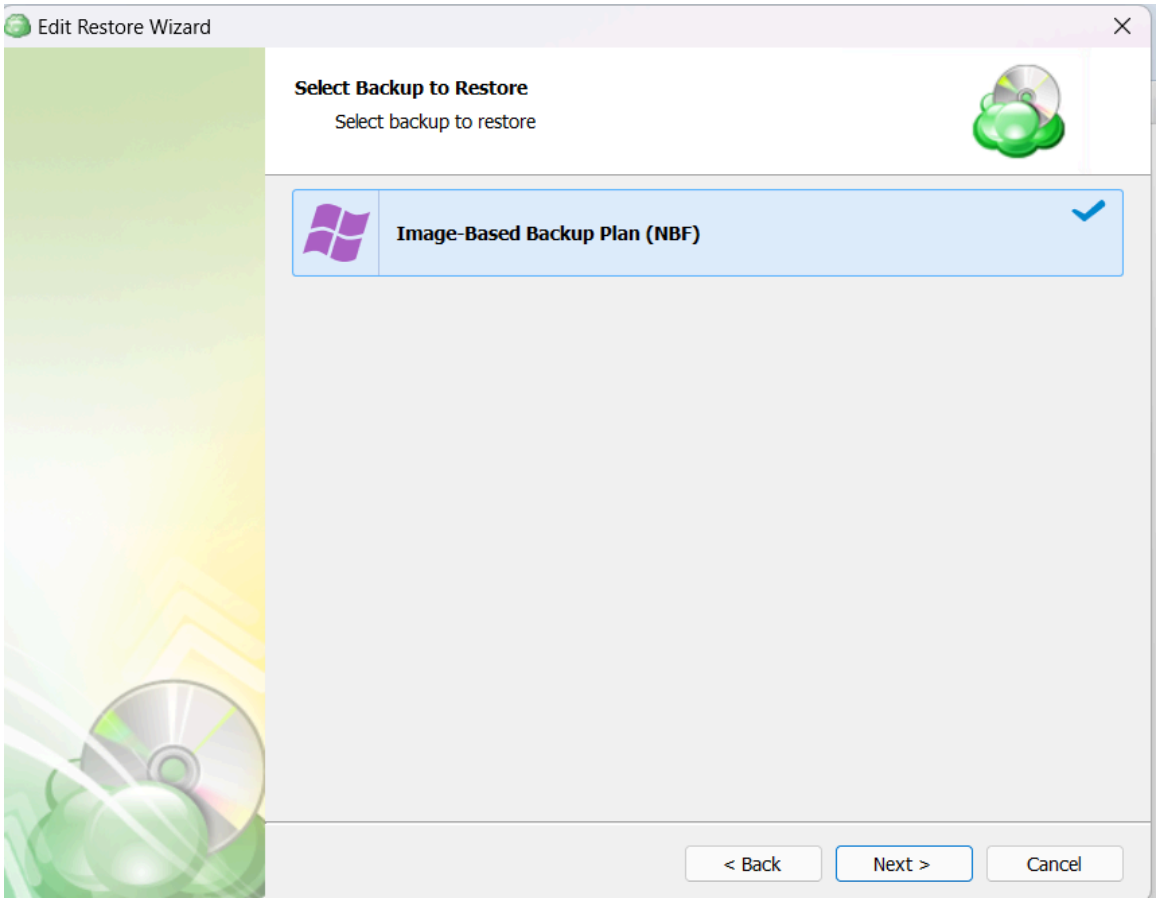
Step 5. Next you will be presented with a list of computers with the same prefix and associated "Backup User" as the computer on which the Agent is currently running. Click to select the desired computer then click on "Next".



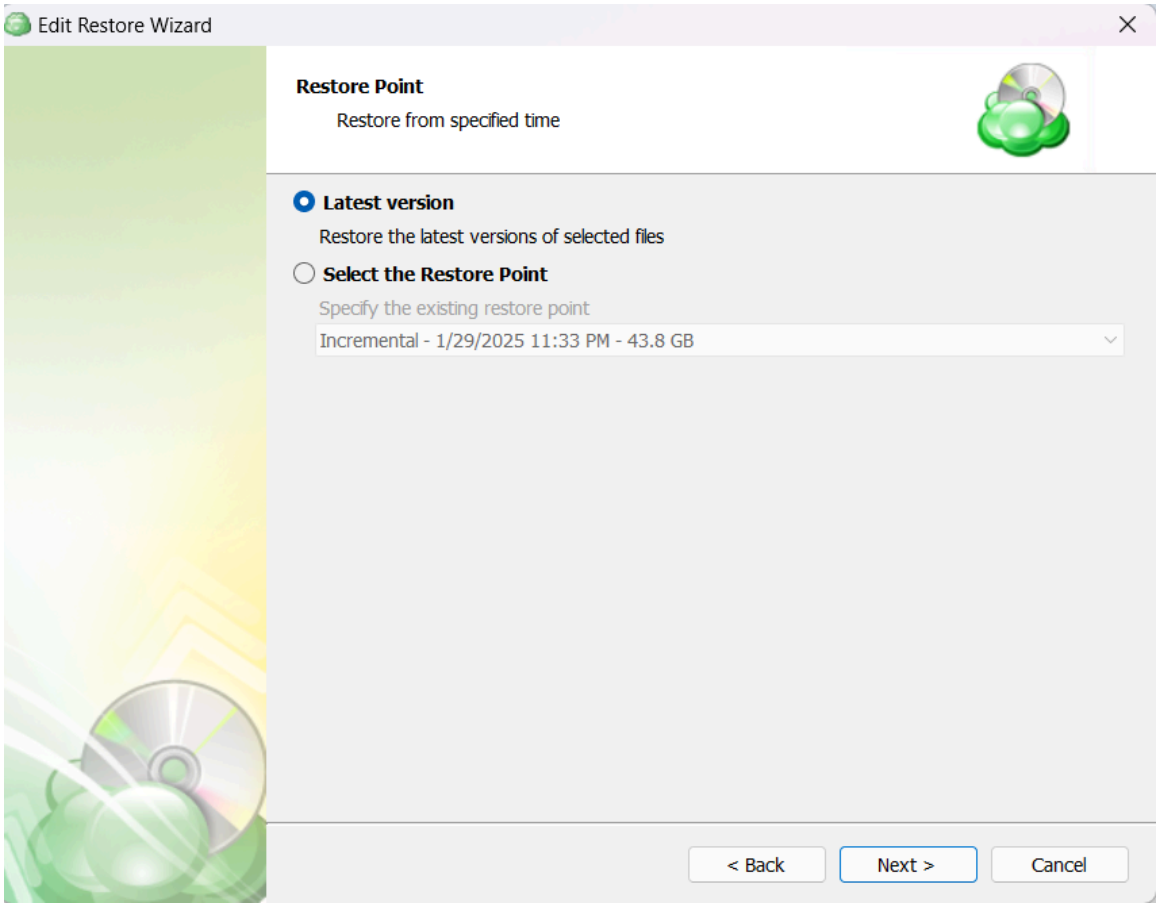
Step 6. Based on the contents of the selected source and computer, the next step is to choose the type of restore. Select “Restore Image Based Backup” then continue to the next step by clicking “Next”.



Step 7. With the correct type of restore selected, the application will generate a list of available backup plans.

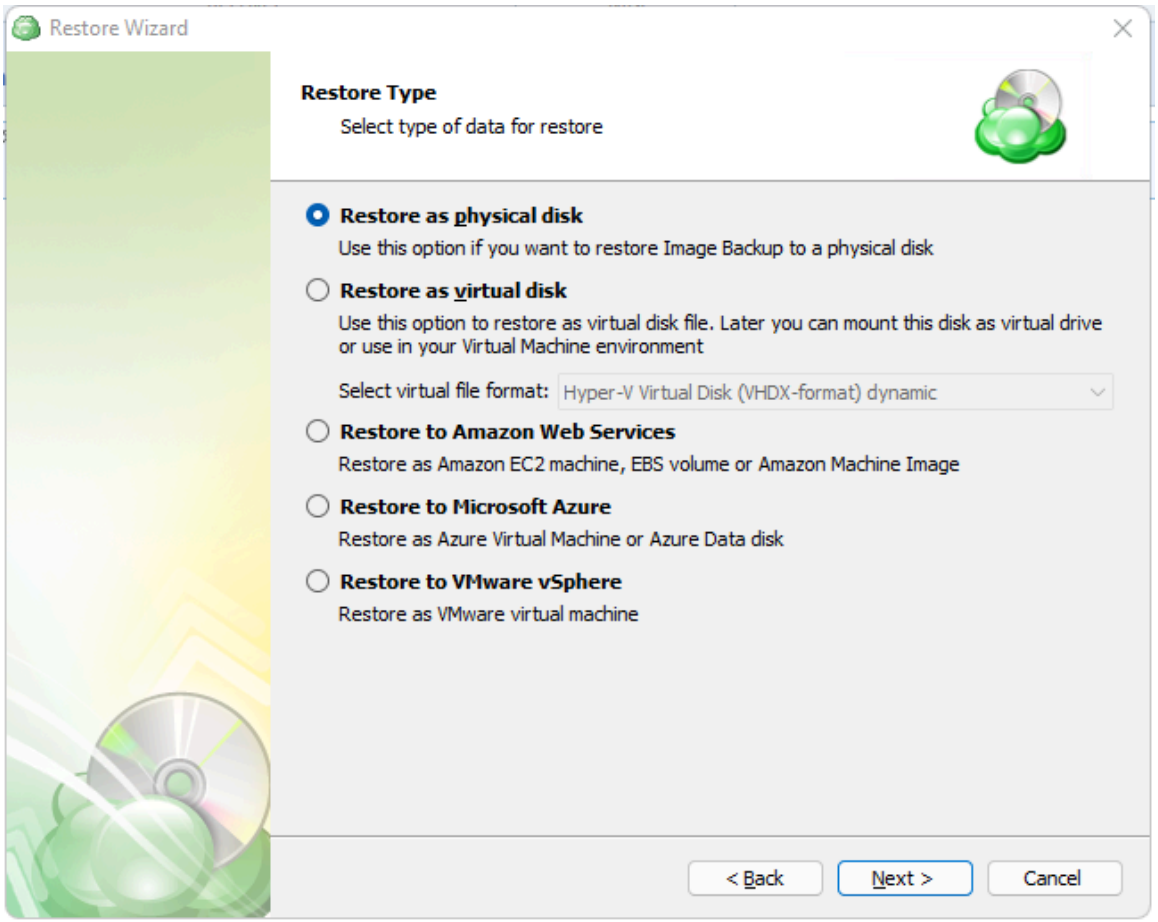


Step 8. The next step is to select the desired point in time to restore to.



- **Latest Version:** Automatically restores the newest version of each file in the source regardless of which restore point it belongs to.
- **Select the Restore Point:** Allows you to select which restore point to restore from the dropdown list.

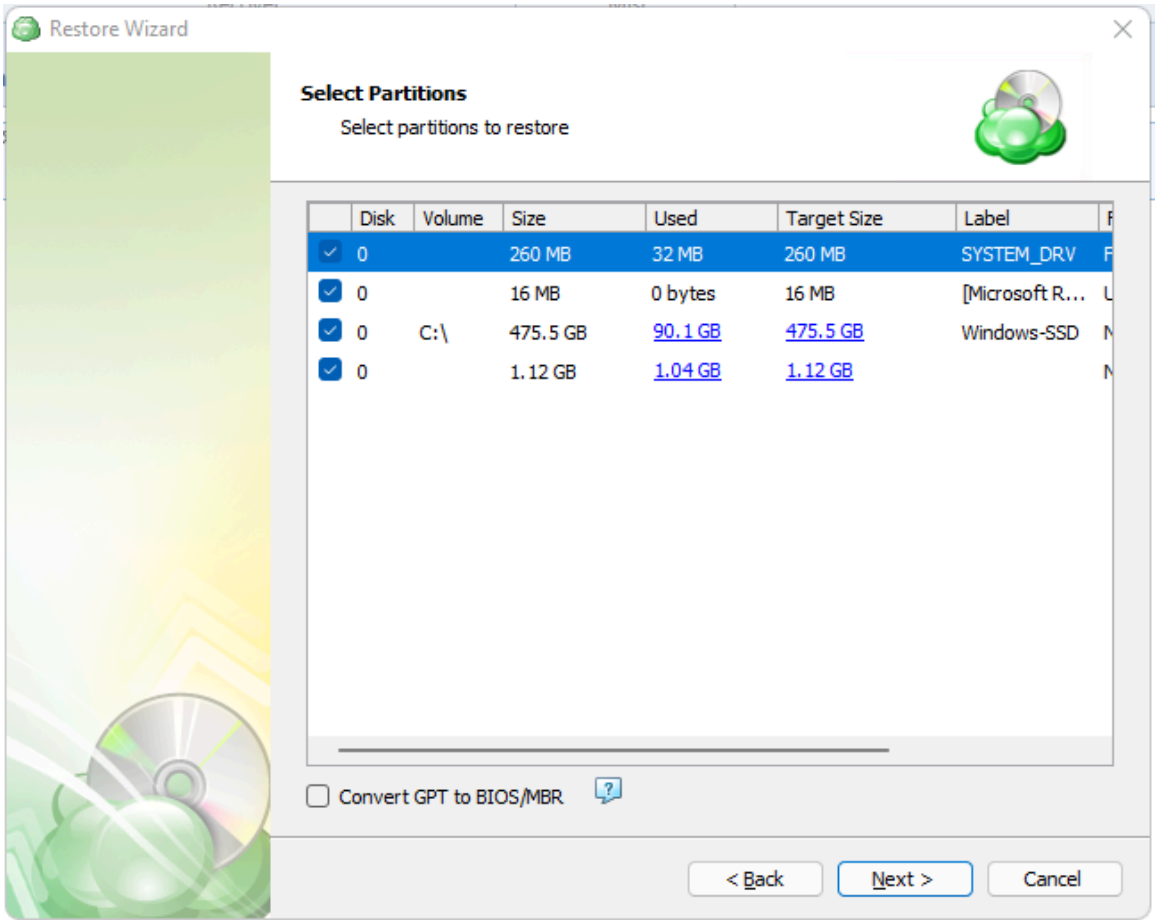
Step 9. Next, select the desired target format for the restored data



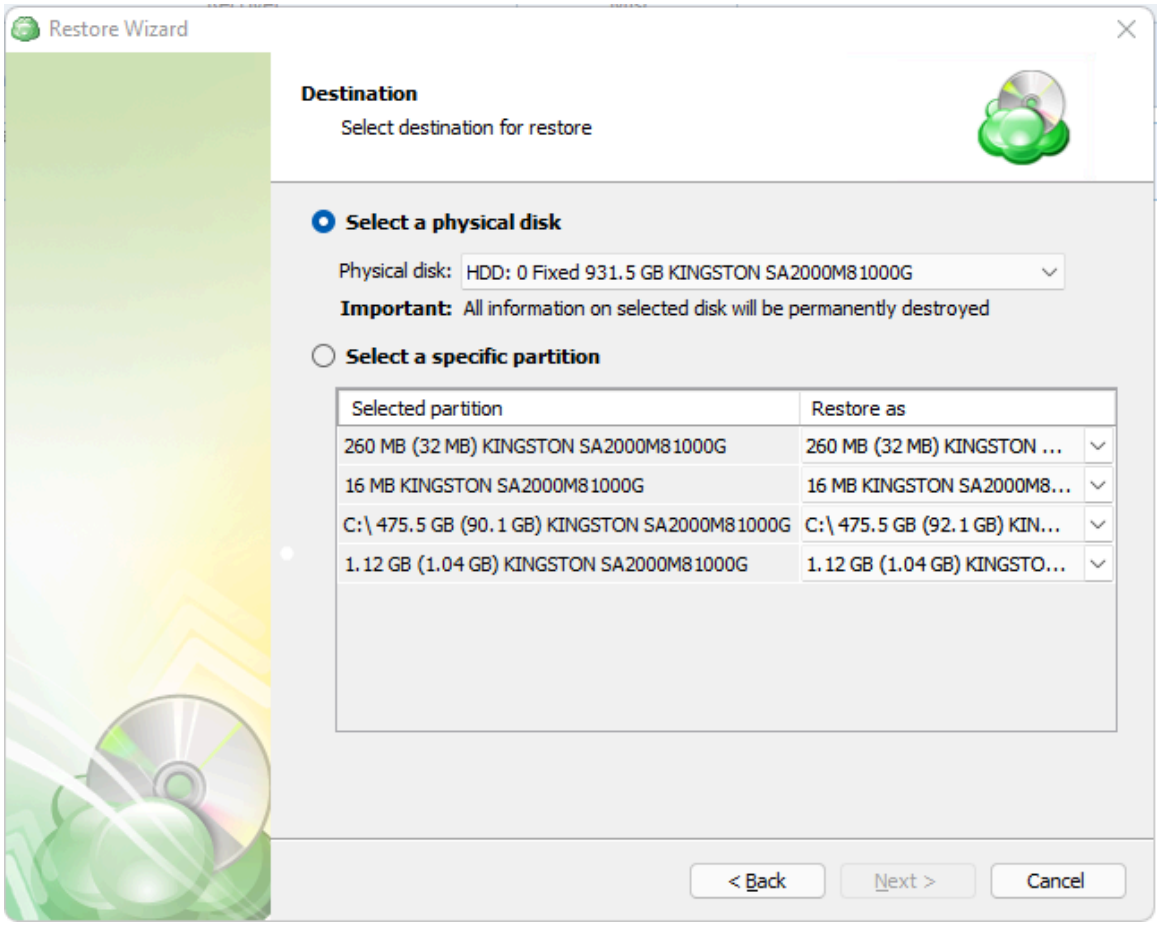
- **Restore as physical disk:** Restores the partitions selected later to a physical disk.
- **Restore as virtual disk:** Restores the data as a virtual disk in multiple supported formats.
- **Restore to Amazon Web Services:** Restores the data as either an EC2 machine, EBS volume, or Amazon Machine Image.
- **Restore to Microsoft Azure:** Restores the image to either an Azure Virtual Machine or Azure Data Disk.
- **Restore to VMware vSphere:** Restores the image as a new virtual machine in vSphere.

For AWS and Azure destinations, a storage account must already be specified through the MBS portal

Step 10. After selecting the type of restore target in the previous step, you now need to select which partitions to restore.



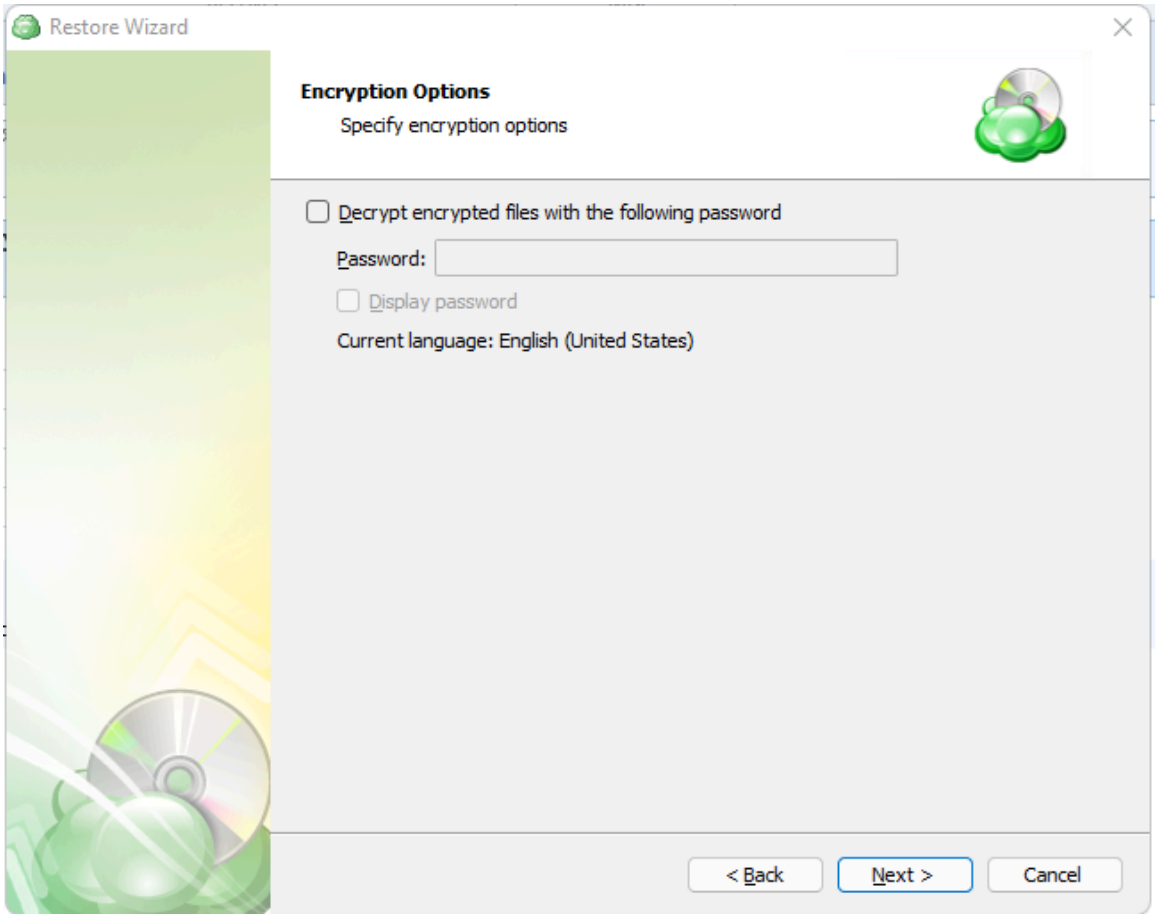
Step 11. Once the partitions are selected, the next step allows you to choose the physical disk to restore to.



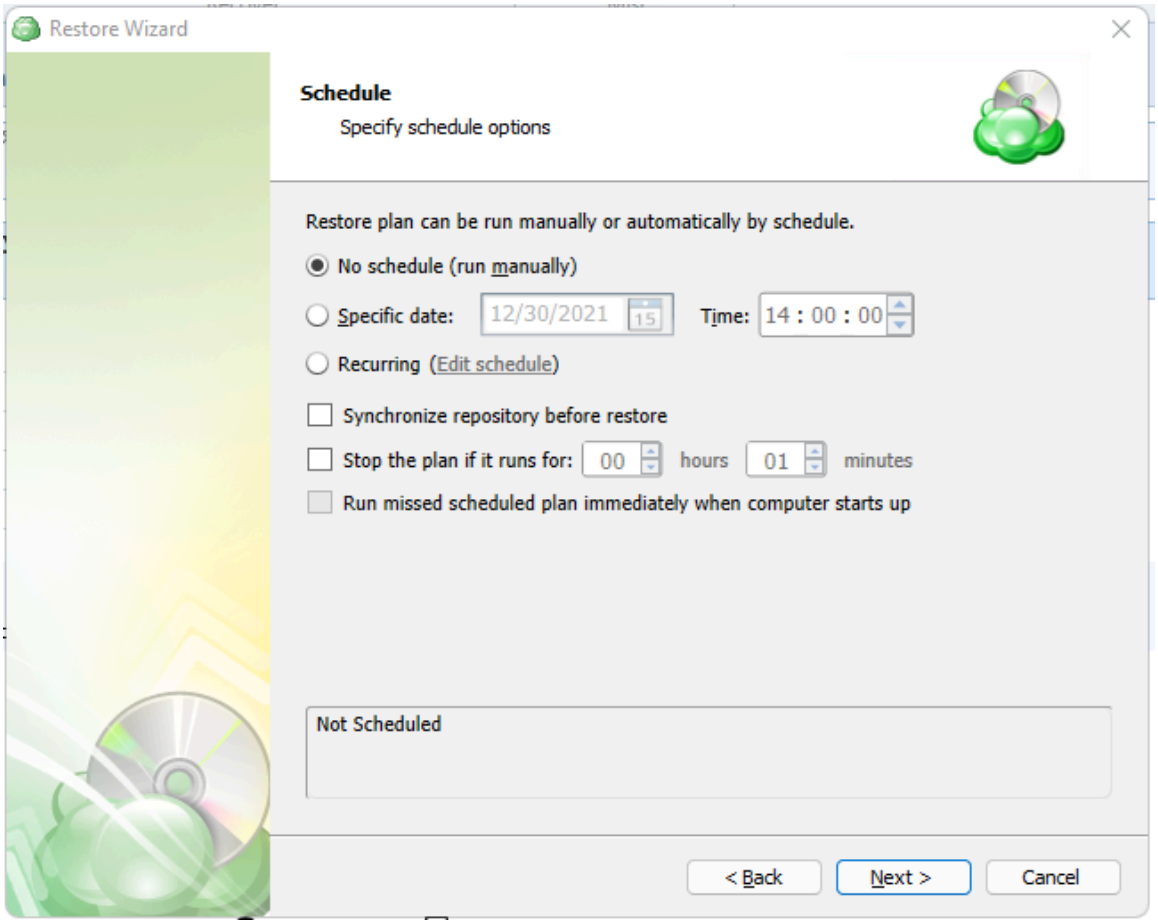
- **Select a physical disk:** select the physical disk from the list which you would like to restore over.
- **Select a specific partition:** Allows specific currently existing partitions to be used as a target for each restored partition.

> Be careful to select the correct target disk(s) and partition(s). All data in the selected targets will be permanently destroyed.

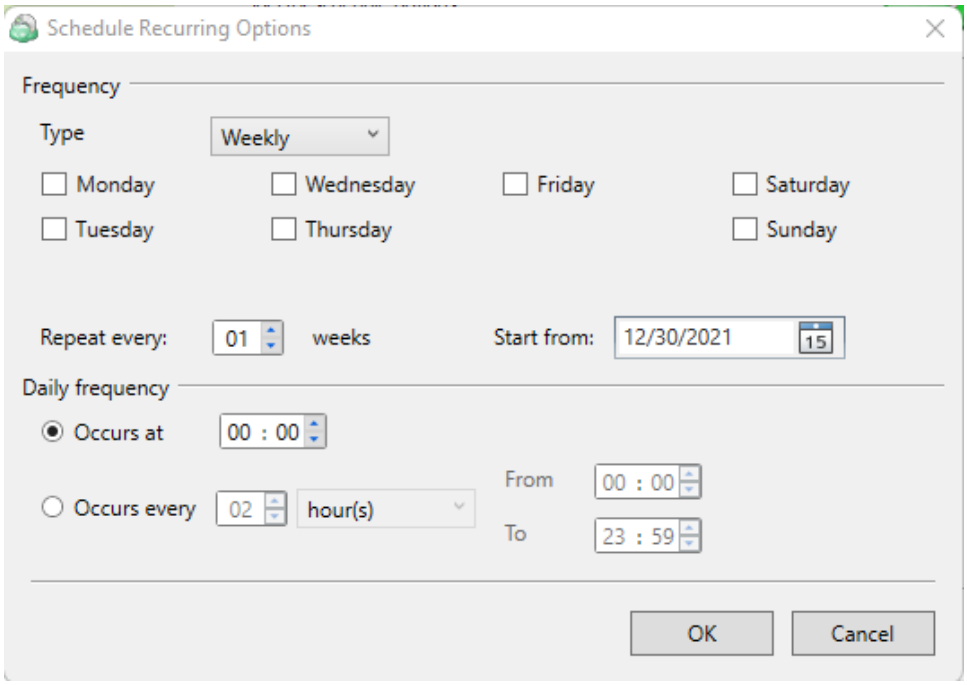
Step 12. If the backed up data was encrypted, the next step will be to enter the password for decryption. If the password is incorrect or missing, the restore plan will fail and you will need to edit the plan to input the correct password.



Step 13. If the restore plan is saved for later, next you will set the schedule for the plan, otherwise proceed to the next step.



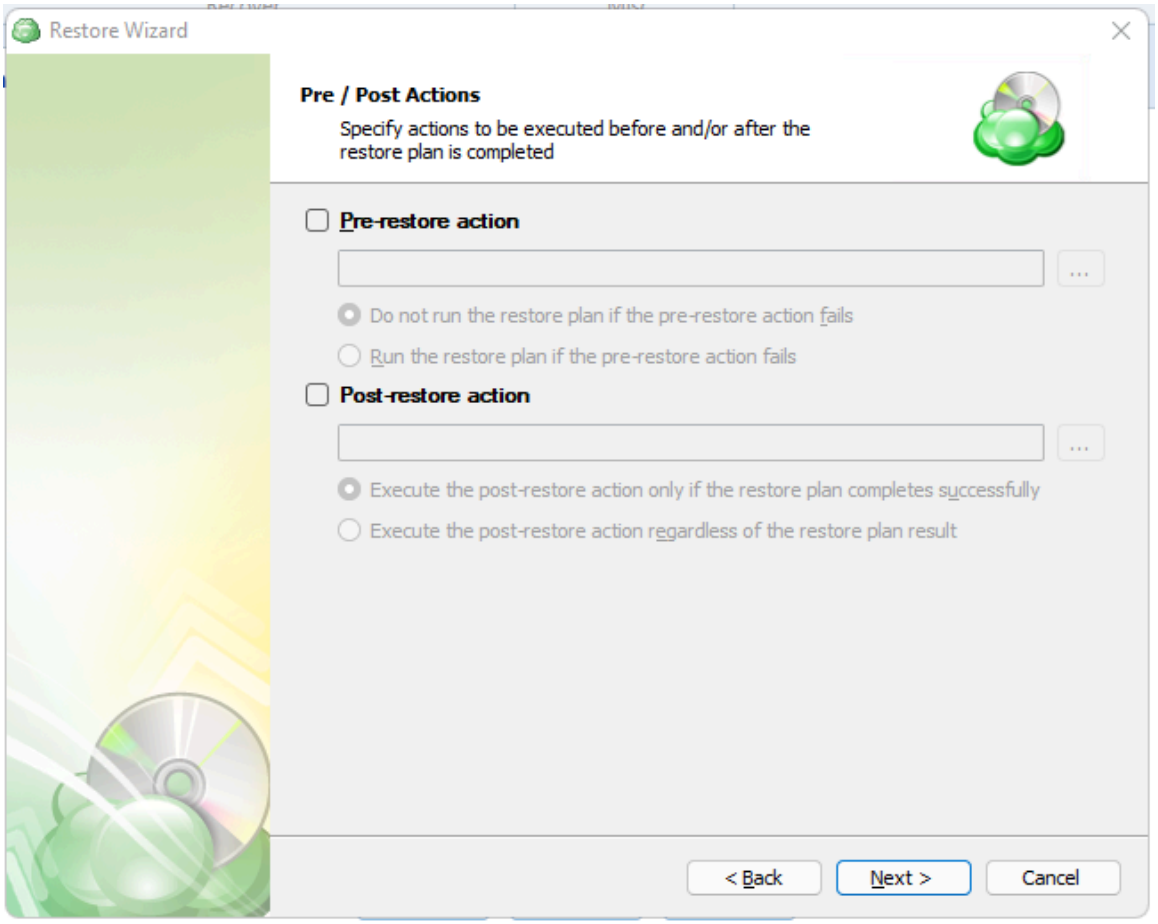
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria by clicking on the “Edit schedule” hyperlink to open this dialogue:



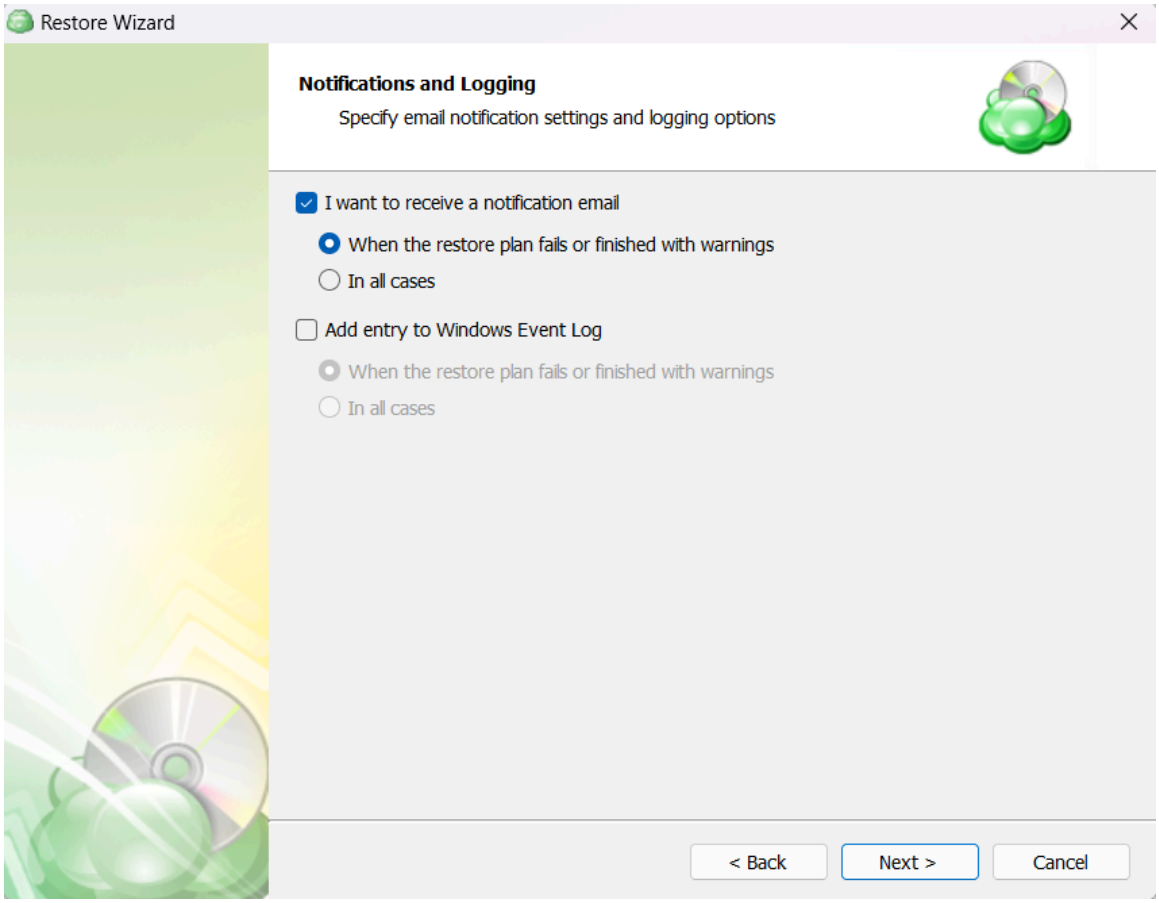
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

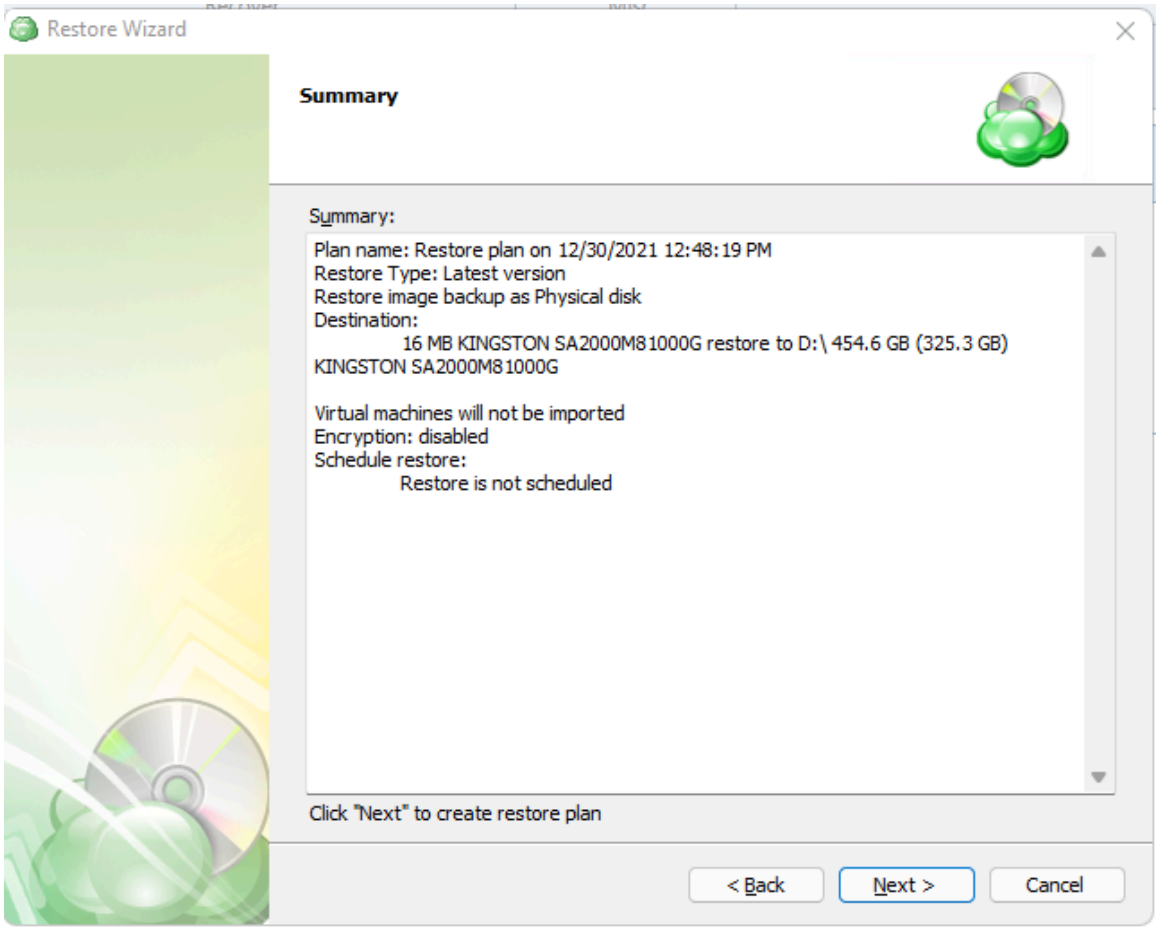
Step 14. The next step page allows the execution of custom scripts before and/or after the running of a Restore Plan.



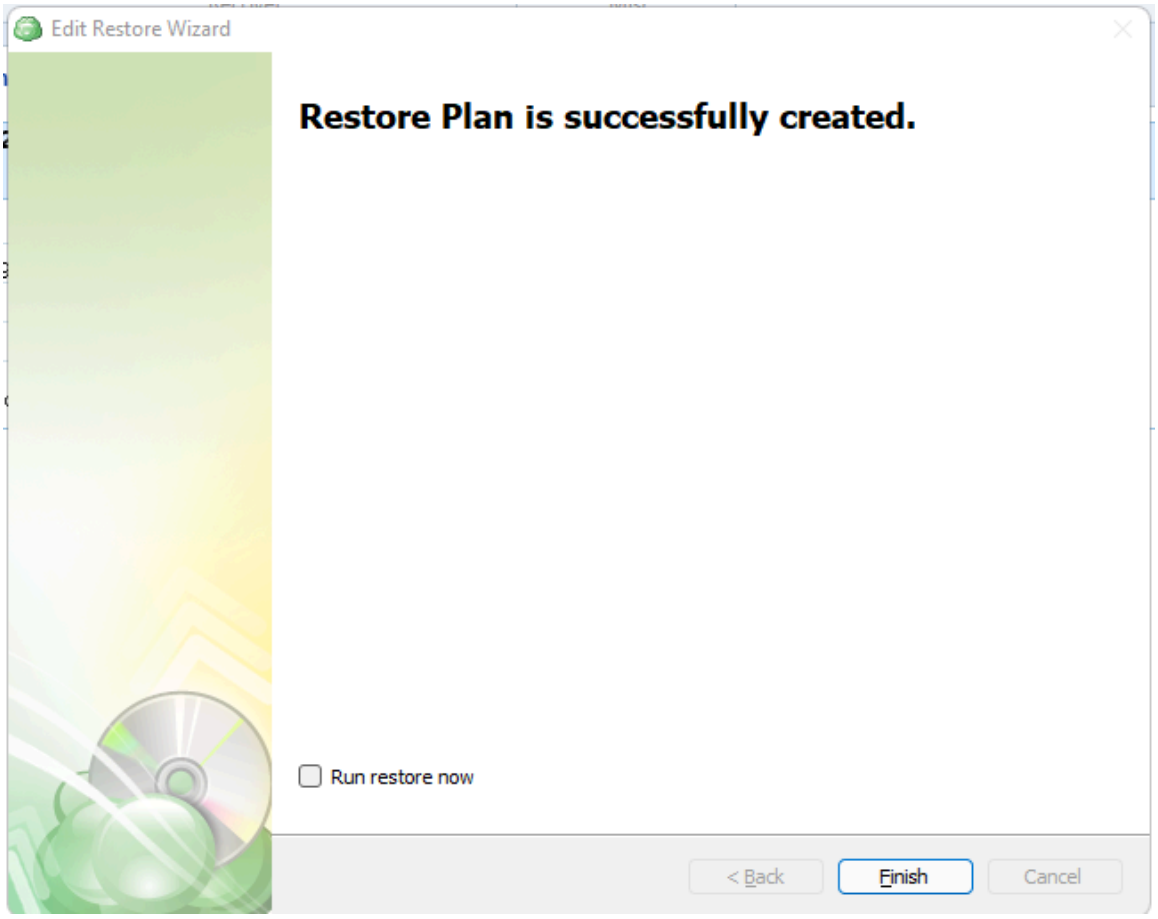
Step 15. The “Notifications and Logging” page allows you to enable notification email and add an entry to Windows Event Log upon restore plan completion or failure.



Step 16. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.

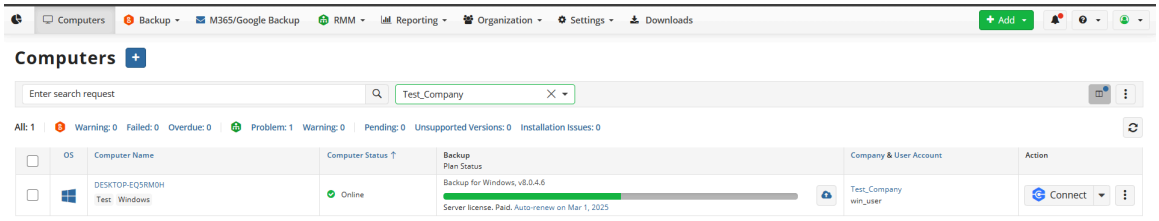


Step 17. The final step of the process is to select when the Restore Plan will start running. To have it start immediately, select the “Run Backup Now” option and click “Finish”. Otherwise, click “Finish” and the plan will begin at the next scheduled time.

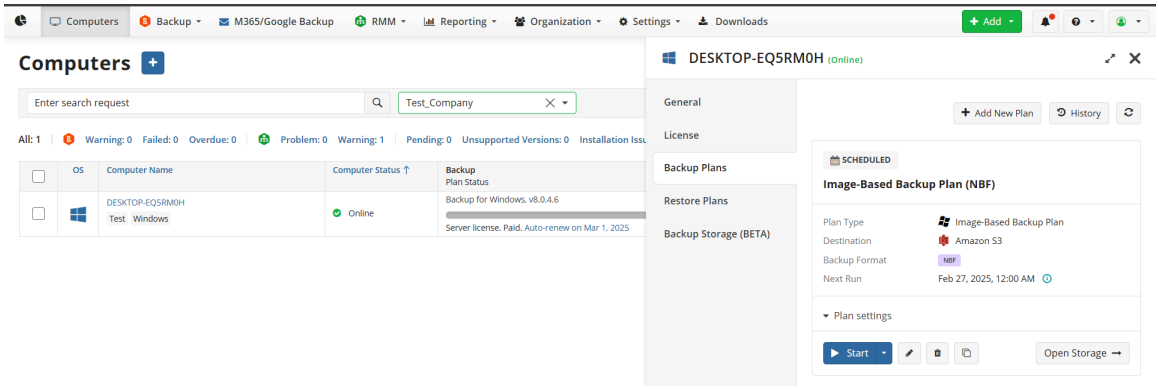


Restore to Physical Disk using MBS

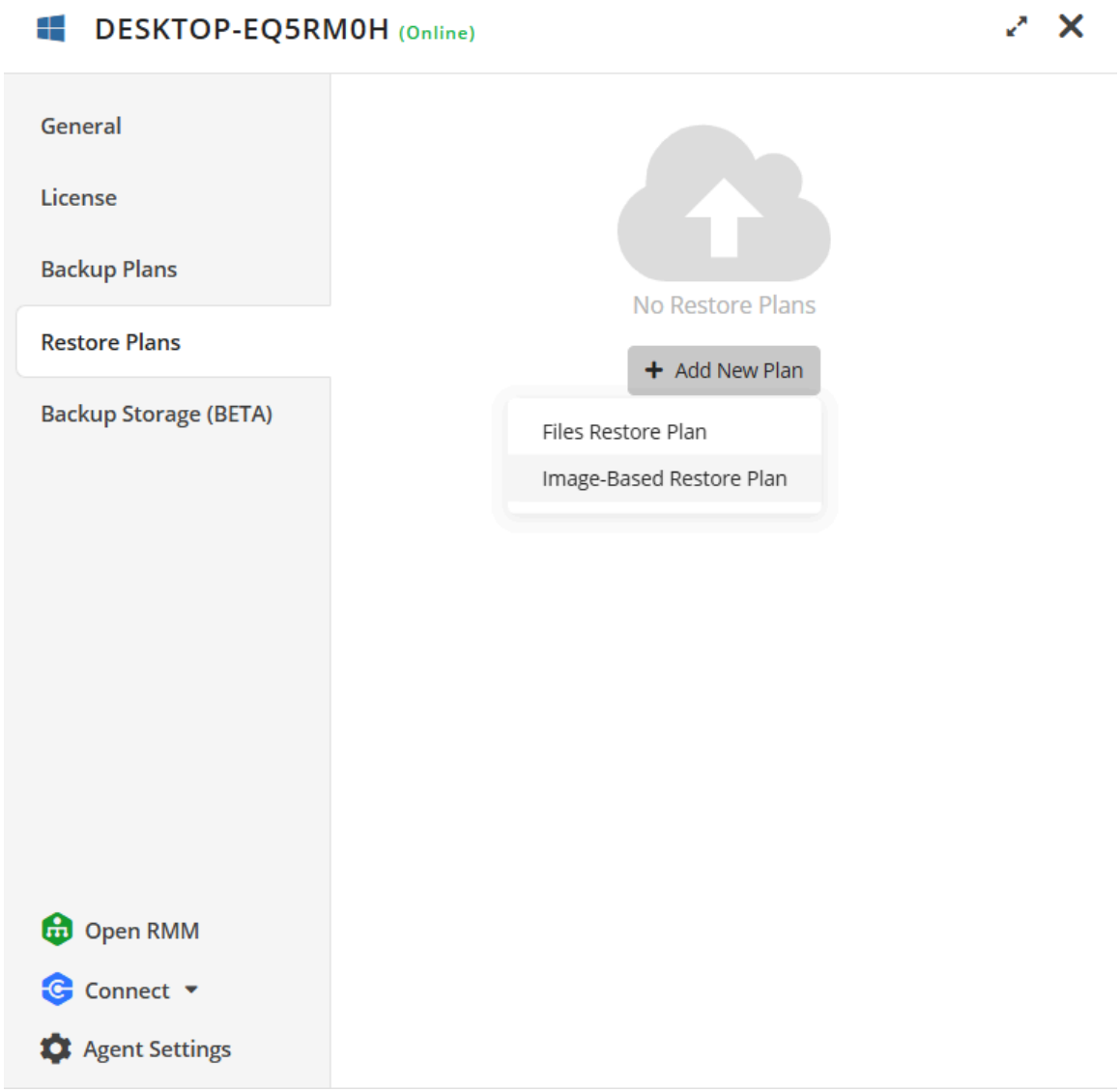
Step 1. Navigate to the MBS Portal and select the “Computers” page on the main menu.



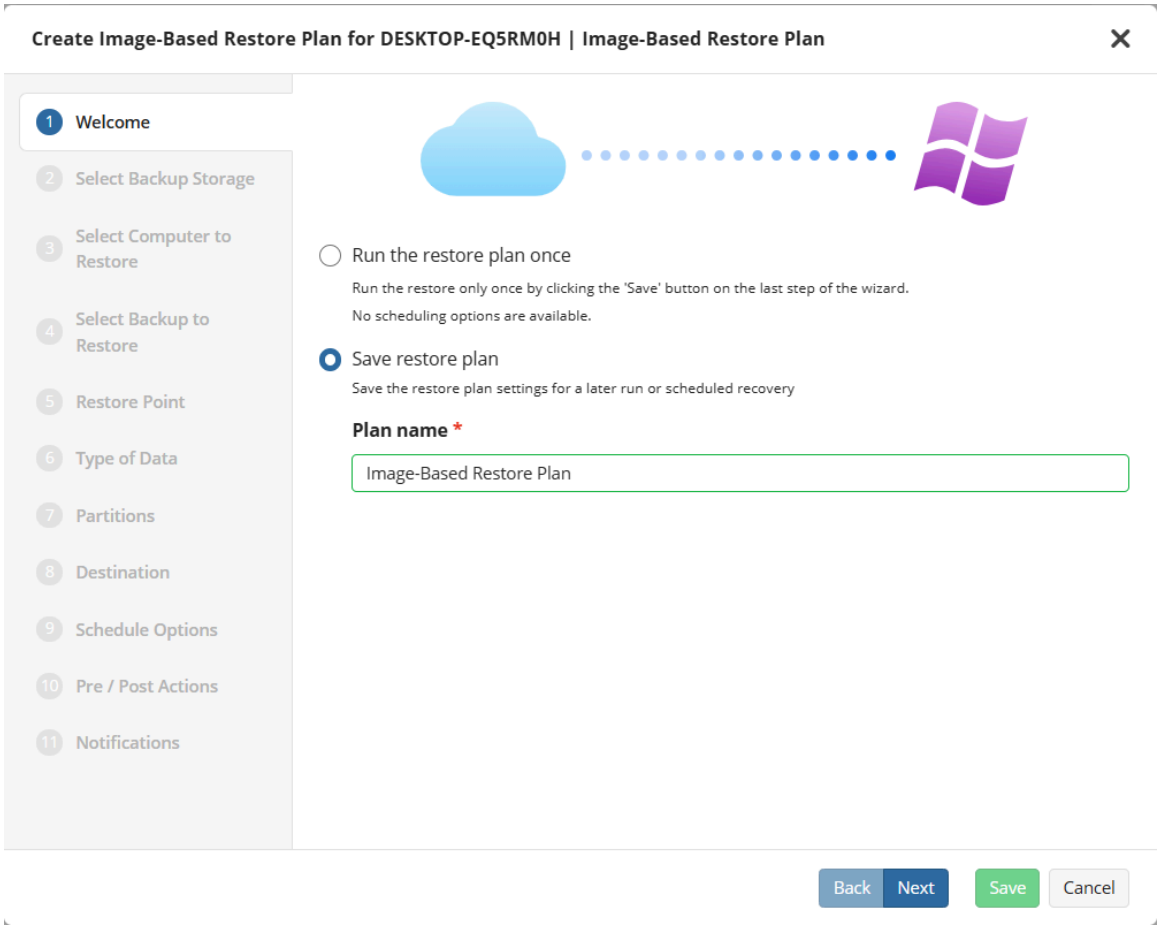
Step 2. Locate the computer which backup dataset you wish to restore from and click on the name of the computer or the backup status bar.



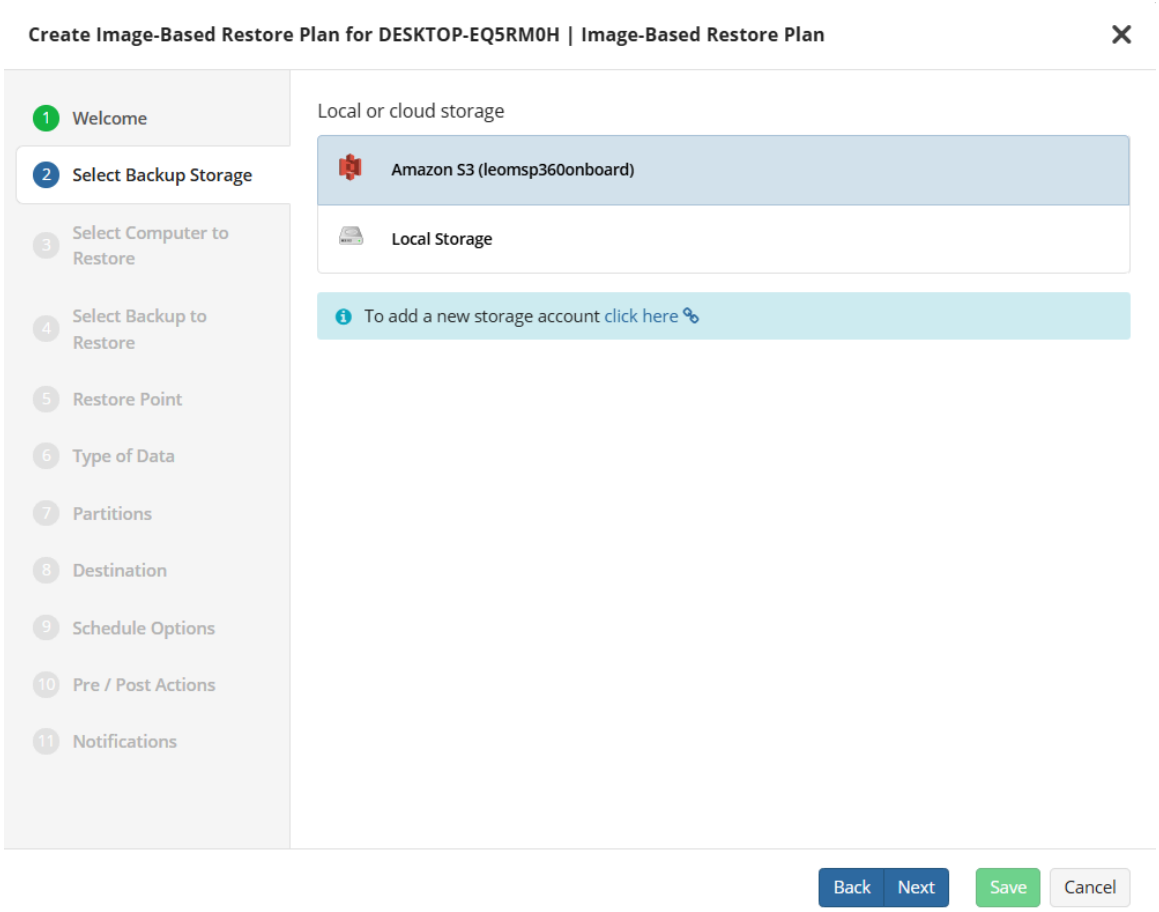
Step 3 Switch to the “Restore Plans” tab. Click on the “+ Add New Plan” button and select “Image-Based Restore Plan”



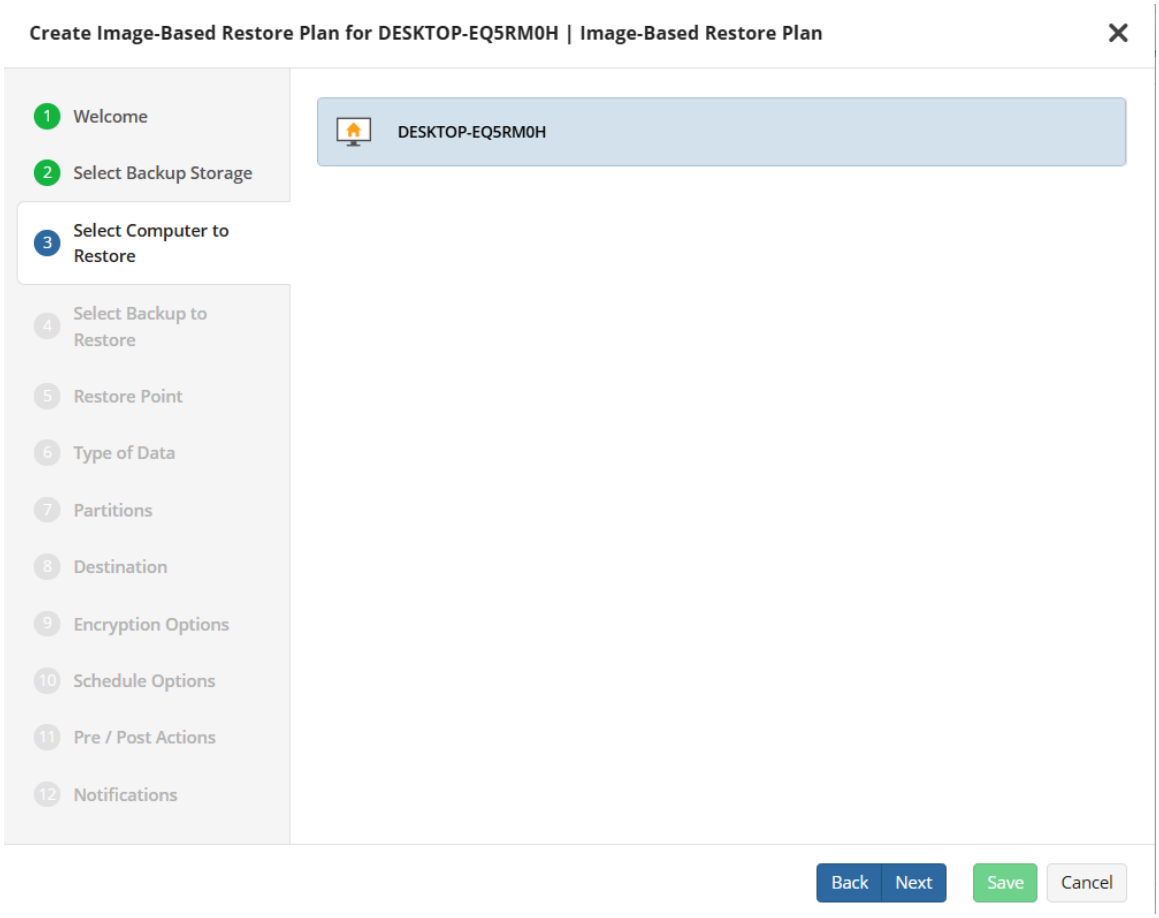
Step 4. The first step when making a Restore Plan is to select if it should run only once, or if it should be saved for future or scheduled use. The latter will allow you to name the plan.



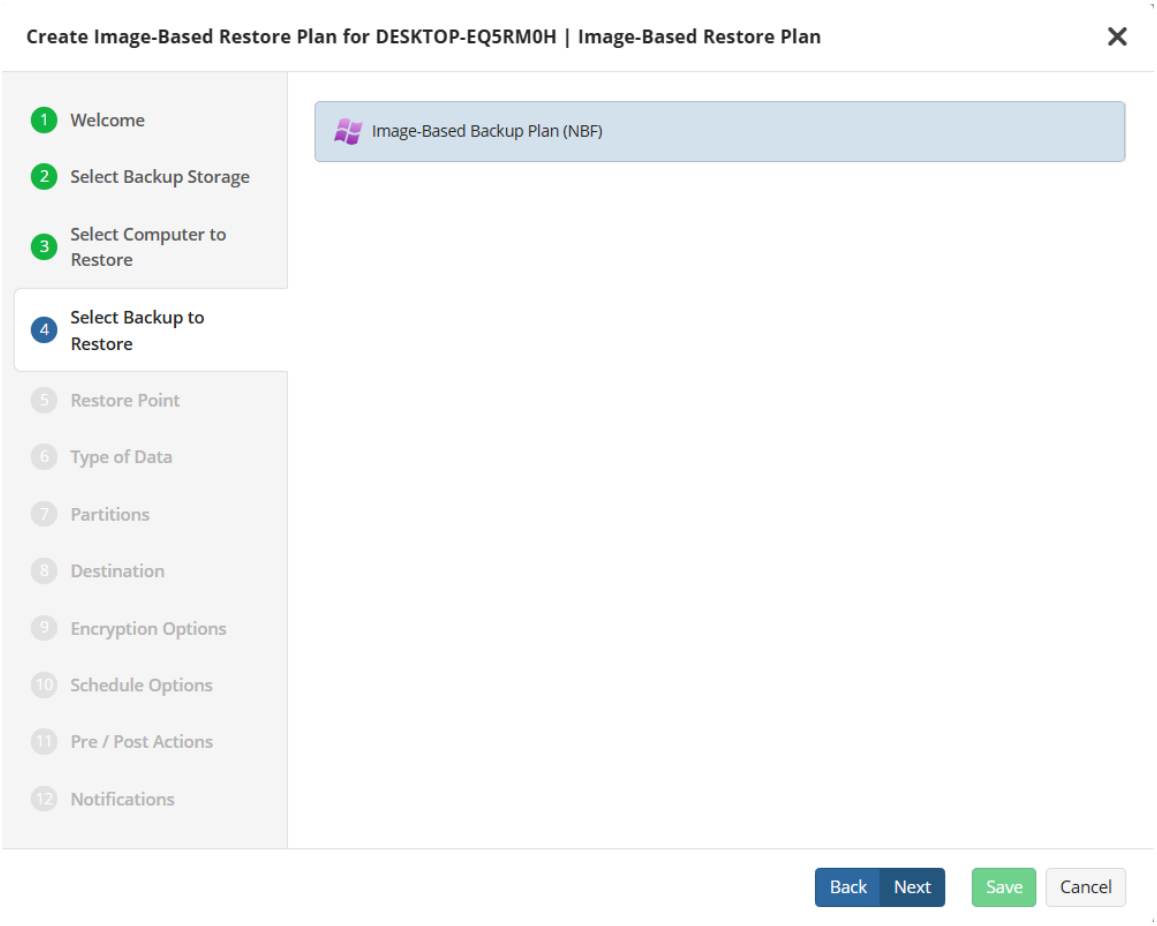
Step 5. Next you will need to select the restore source



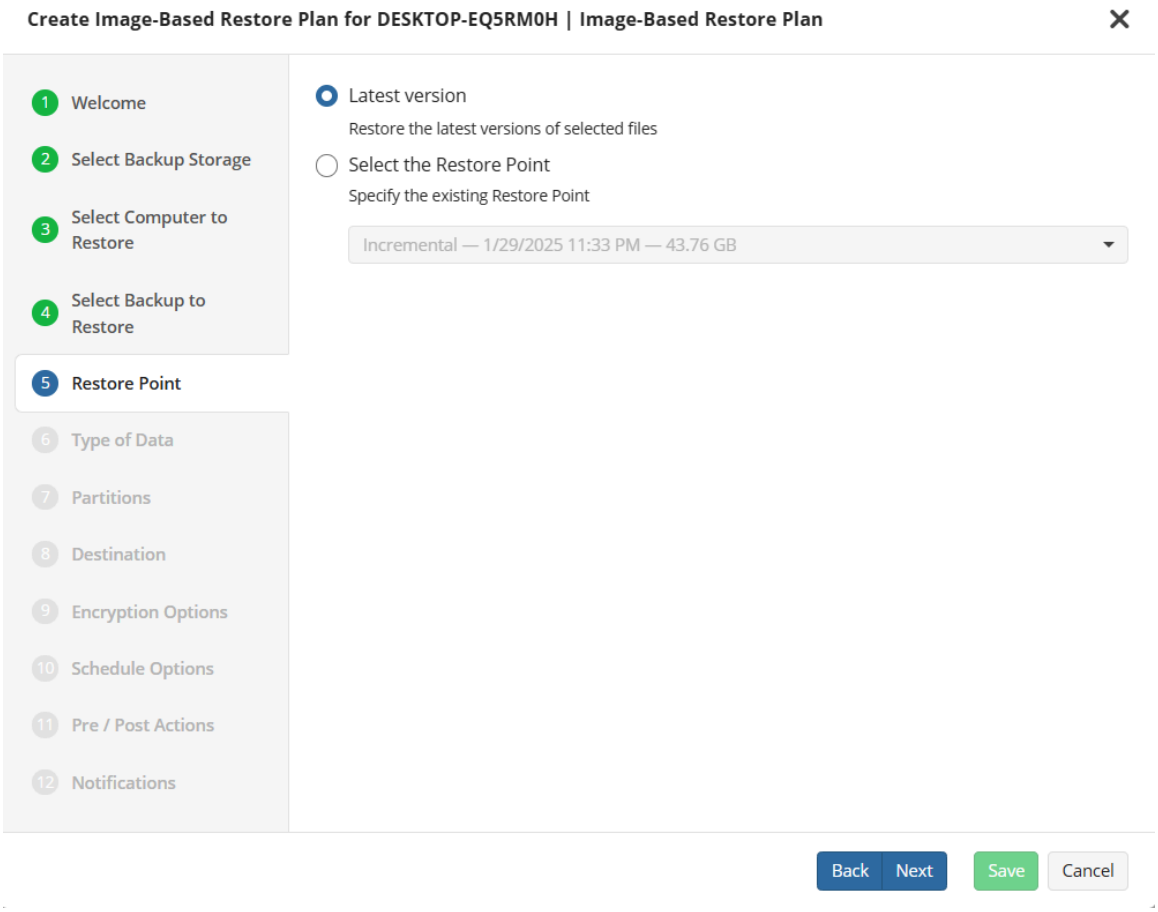
Step 6. Next you will need to select the computer to be restored.



Step 7. Next you will need to select the backup plan which contains the desired restore point.

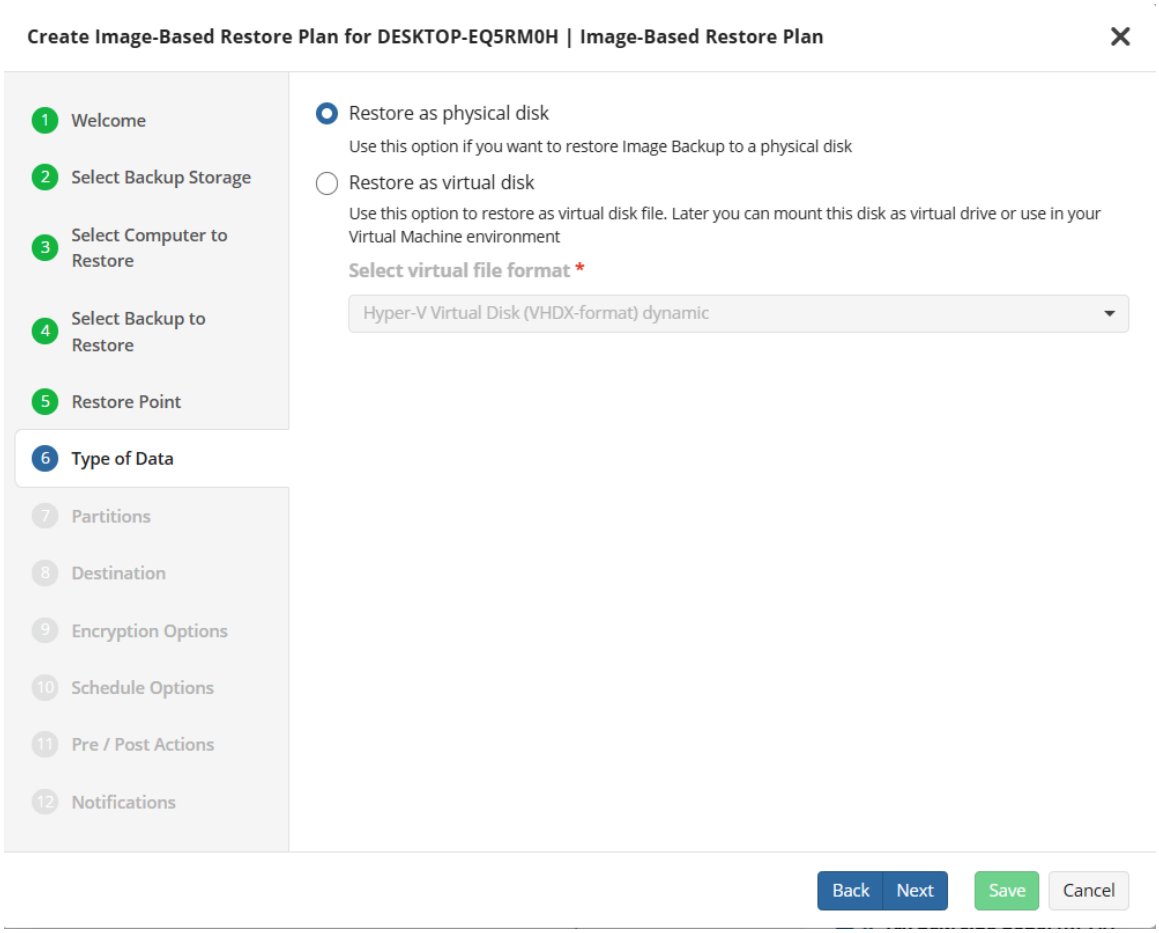


Step 8. The next step is to select the desired point in time to restore to.



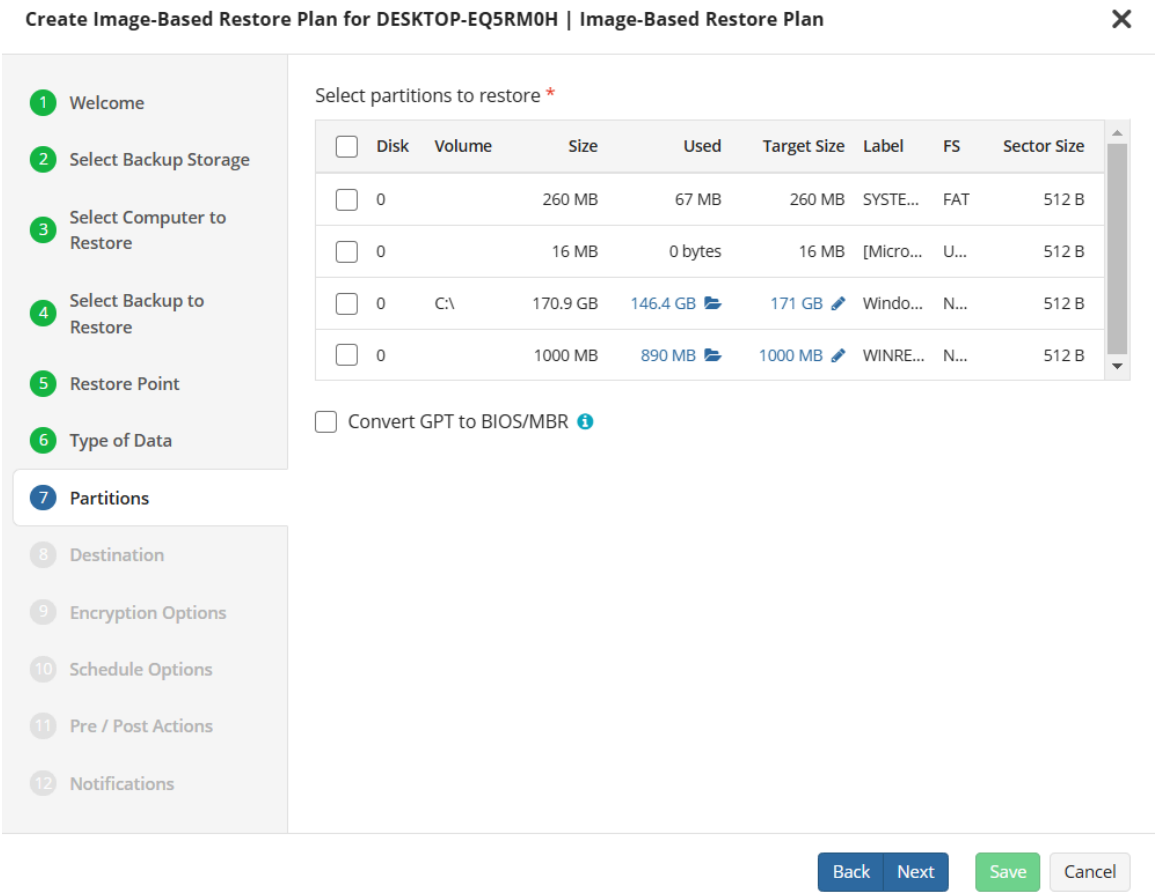
- **Latest Version:** Automatically restores the newest version of each file in the source regardless of which restore point it belongs to.
- **Select the Restore Point:** Restores the image as it existed at the specified restore point

Step 9. Next, select the desired target format for the restored data



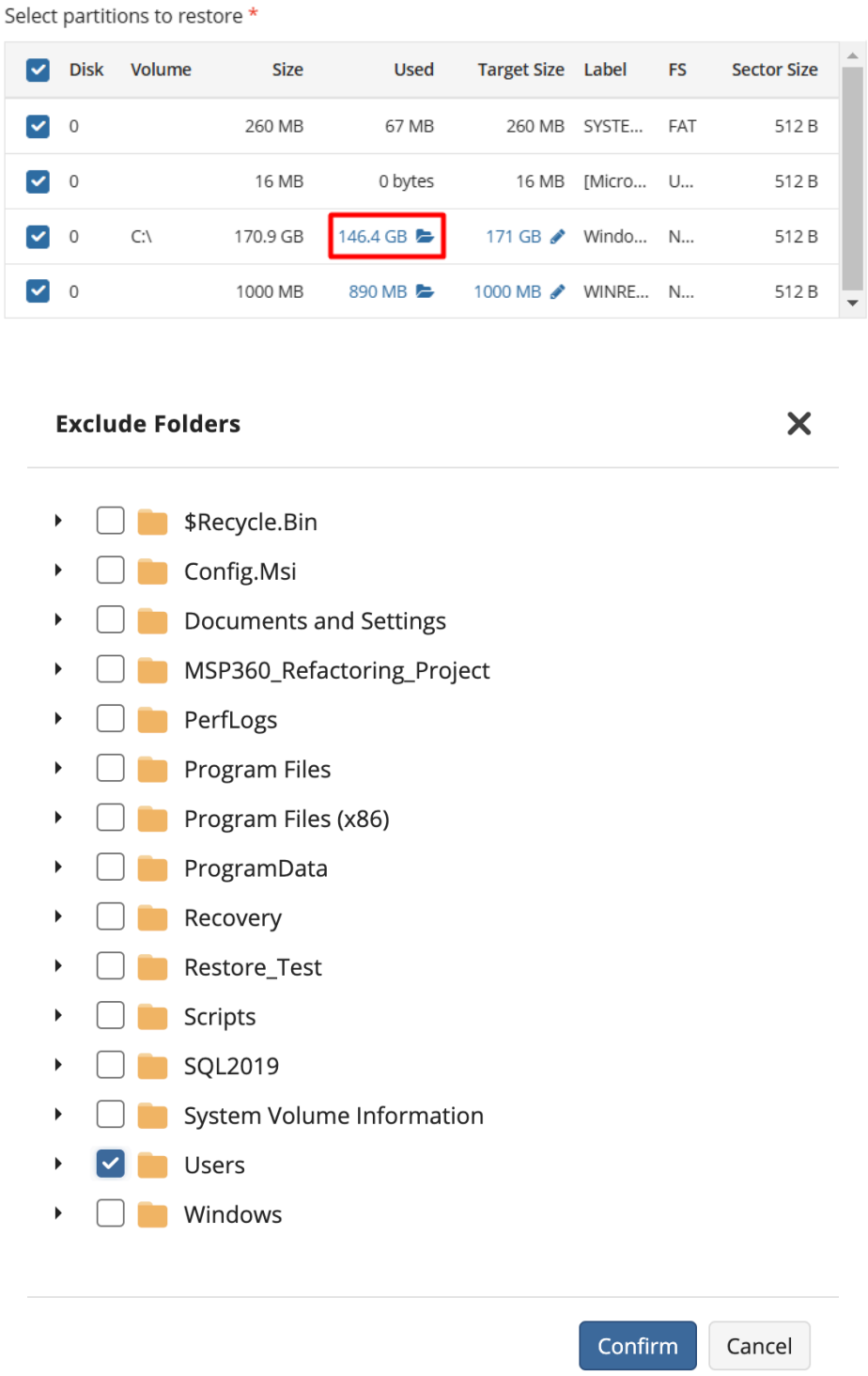
- **Restore as physical disk:** Restores the partitions selected later to a physical disk.
- **Restore as virtual disk:** Restores the data as a virtual disk in multiple supported formats.

Step 10. After selecting the type of restore target in the previous step, you now need to select which partitions to restore. You can also select to convert GPT to MBR if needed.

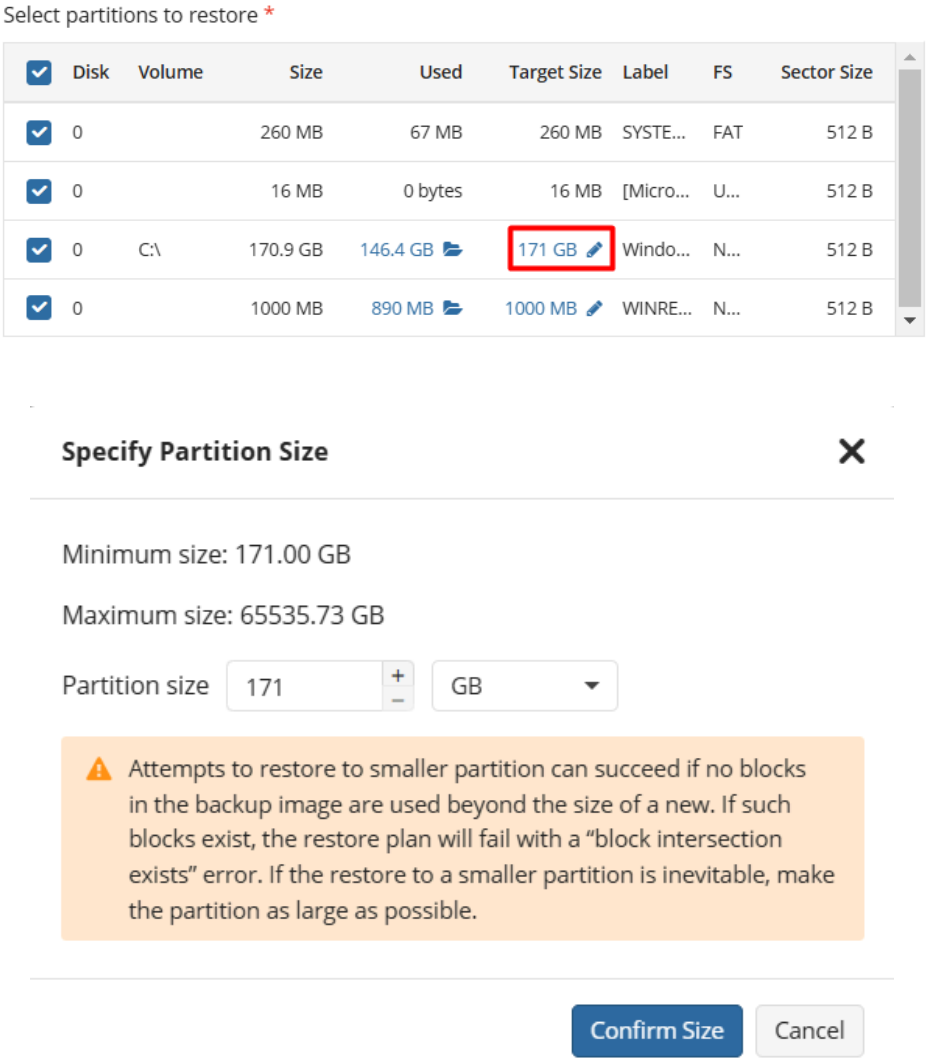


- **Covert GPT to BIOS/MBR:** Select this checkbox if the target instance or the target OS does not support UEFI boot and requires BIOS boot.

If you click on the blue hyperlinked data size and folder icon in the Used column, it will open a separate menu where you can choose to exclude certain data from the restore:

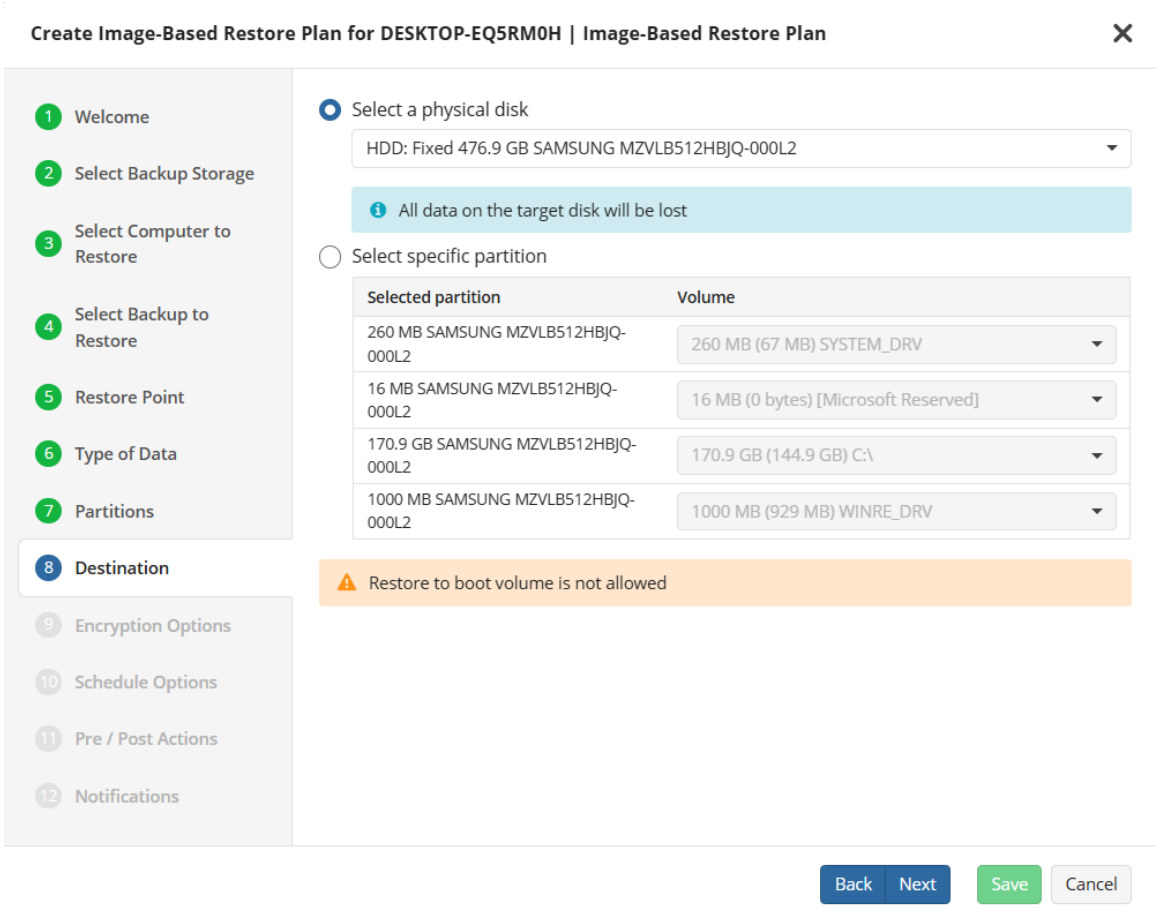


If you click on the blue hyperlink value under the Target Size column, it will open a separate menu where you can specify the target size of the partition:



Attempts to restore to a smaller partition can succeed if no blocks in the backup image are used beyond the size of a new. If such blocks exist, the restore plan will fail with a “block intersection exists” error. If the restore to a smaller partition is inevitable, make the partition as large as possible.

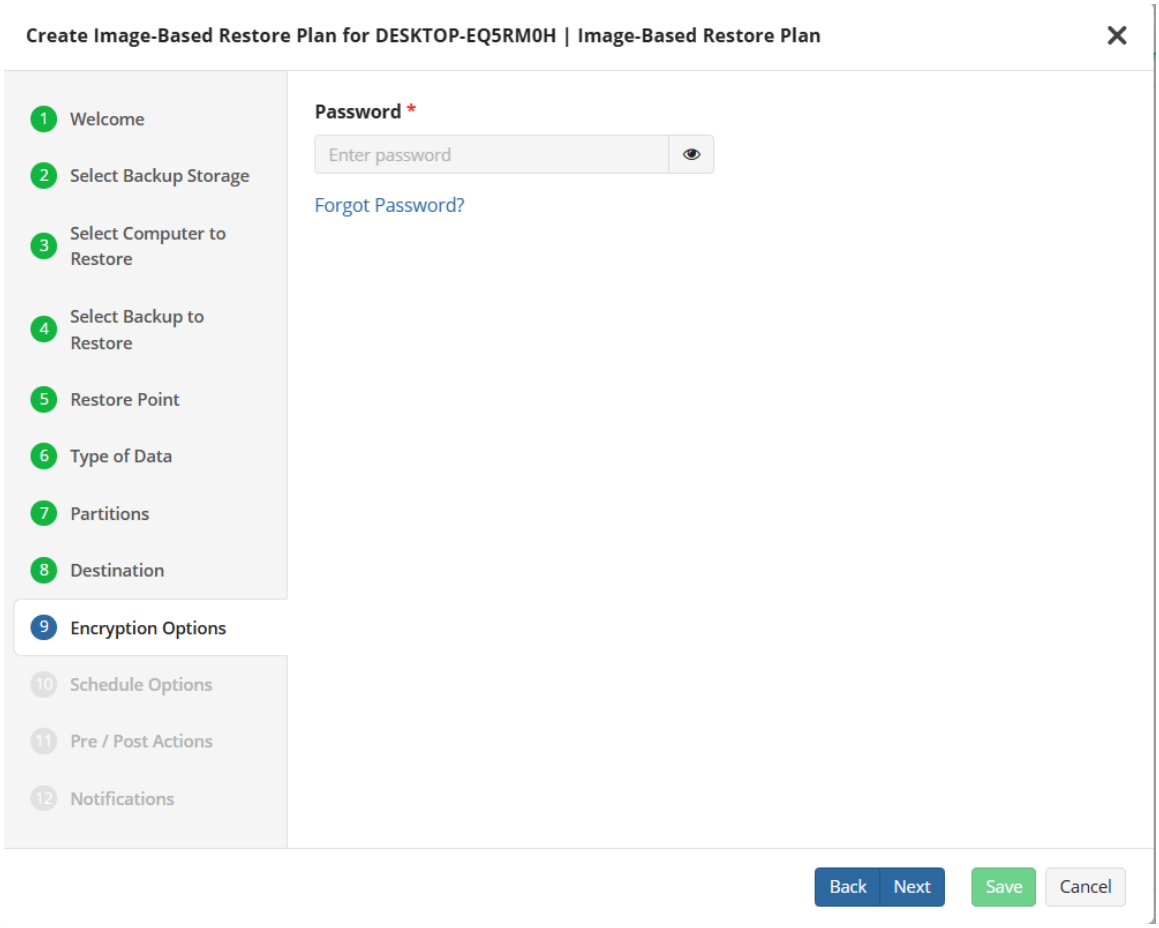
Step 11. After selecting the partitions to be restored, next you will be prompted to select the destination disk or partitions.



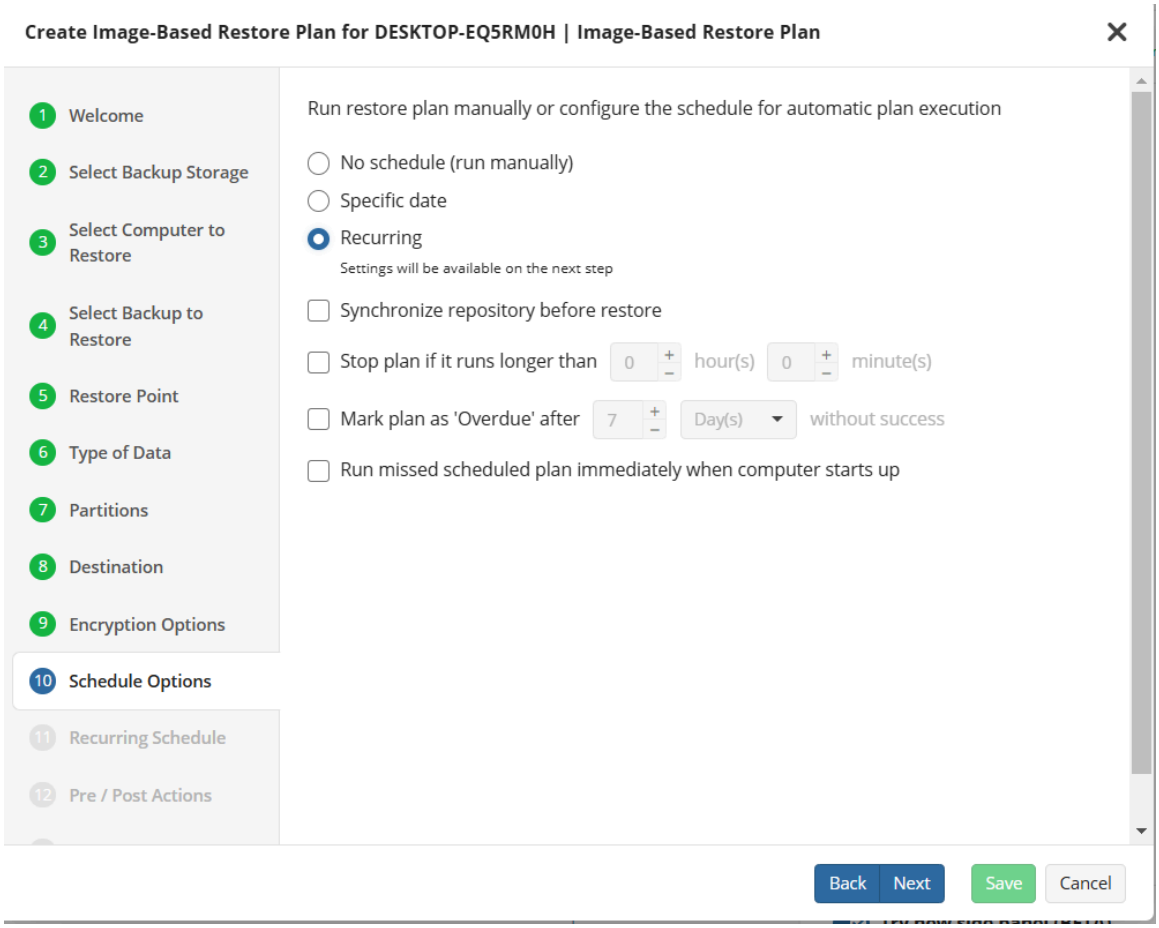
Be careful to select the correct target disk(s) and partition(s). All data in the selected targets will be permanently destroyed.

The application will not allow you to restore to the boot volume of the target computer from Windows or MBS. To restore the boot volume, use the Bare Metal Restore bootable USB.

Step 12. If the image backup dataset was encrypted, the restore plan will prompt you to enter the password.



Step 13. If the restore plan is saved for later, next you will set the schedule for the plan, otherwise proceed to the next step.



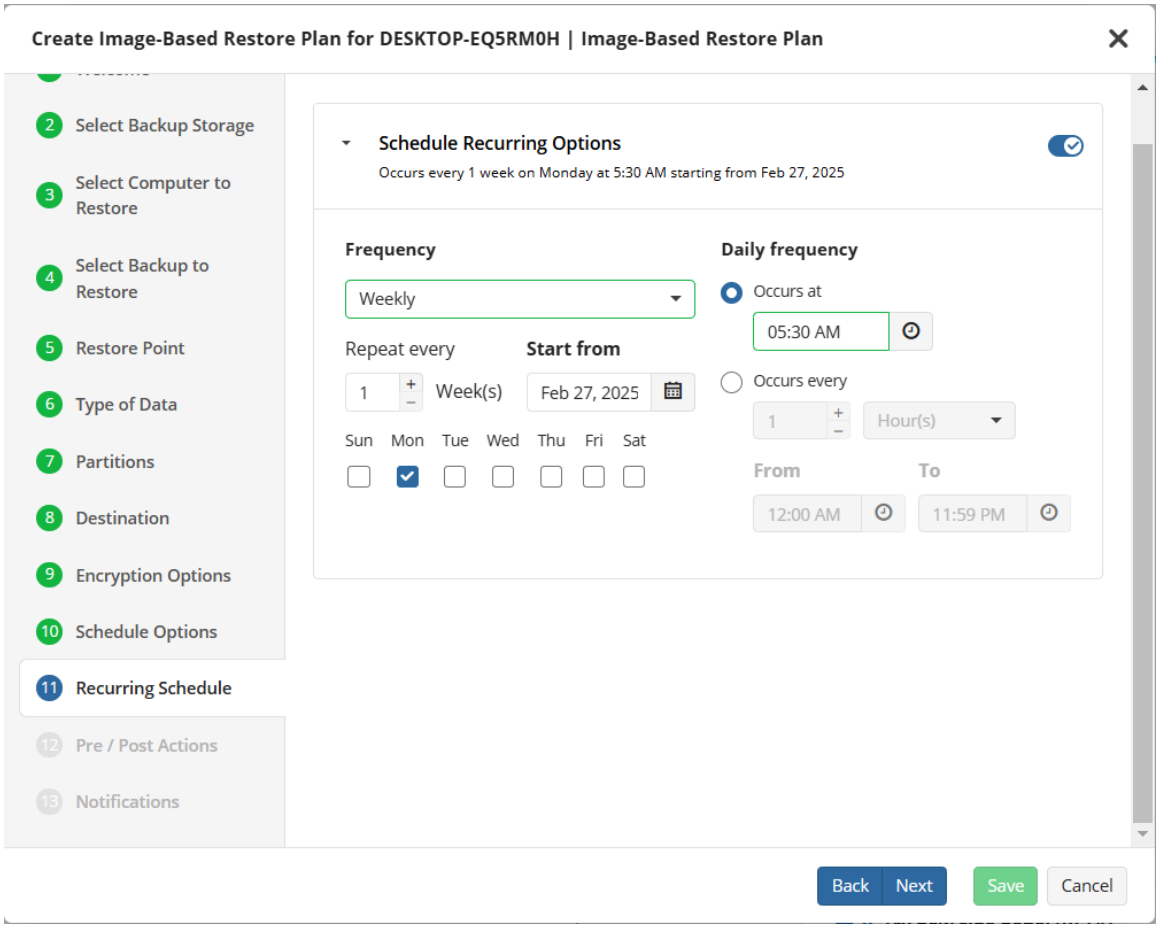
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option will add an additional step to the wizard which enables you to schedule recurring Restorations at custom intervals:

It is recommended to **Synchronize repository before restore** if you are restoring a backup dataset for a computer different from the original or if you are signed in with a different backup user.

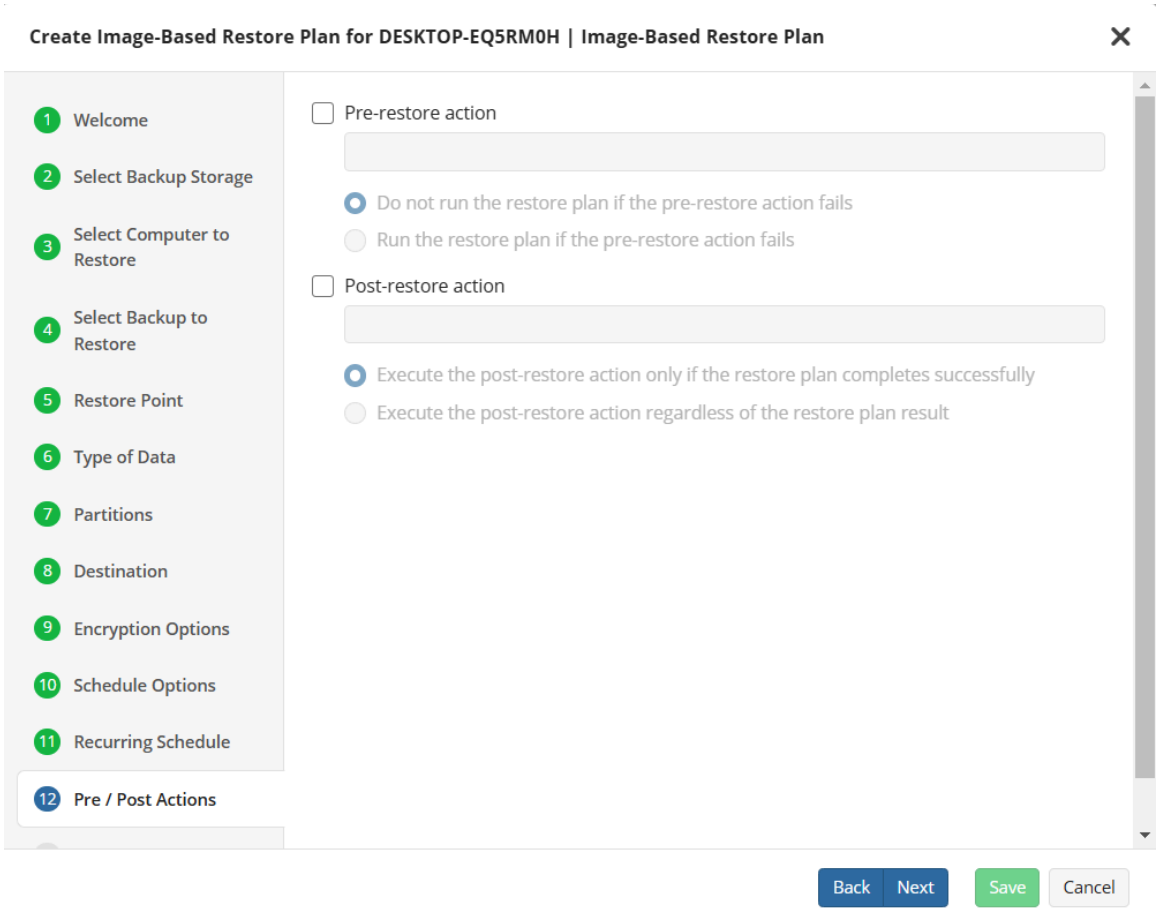
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

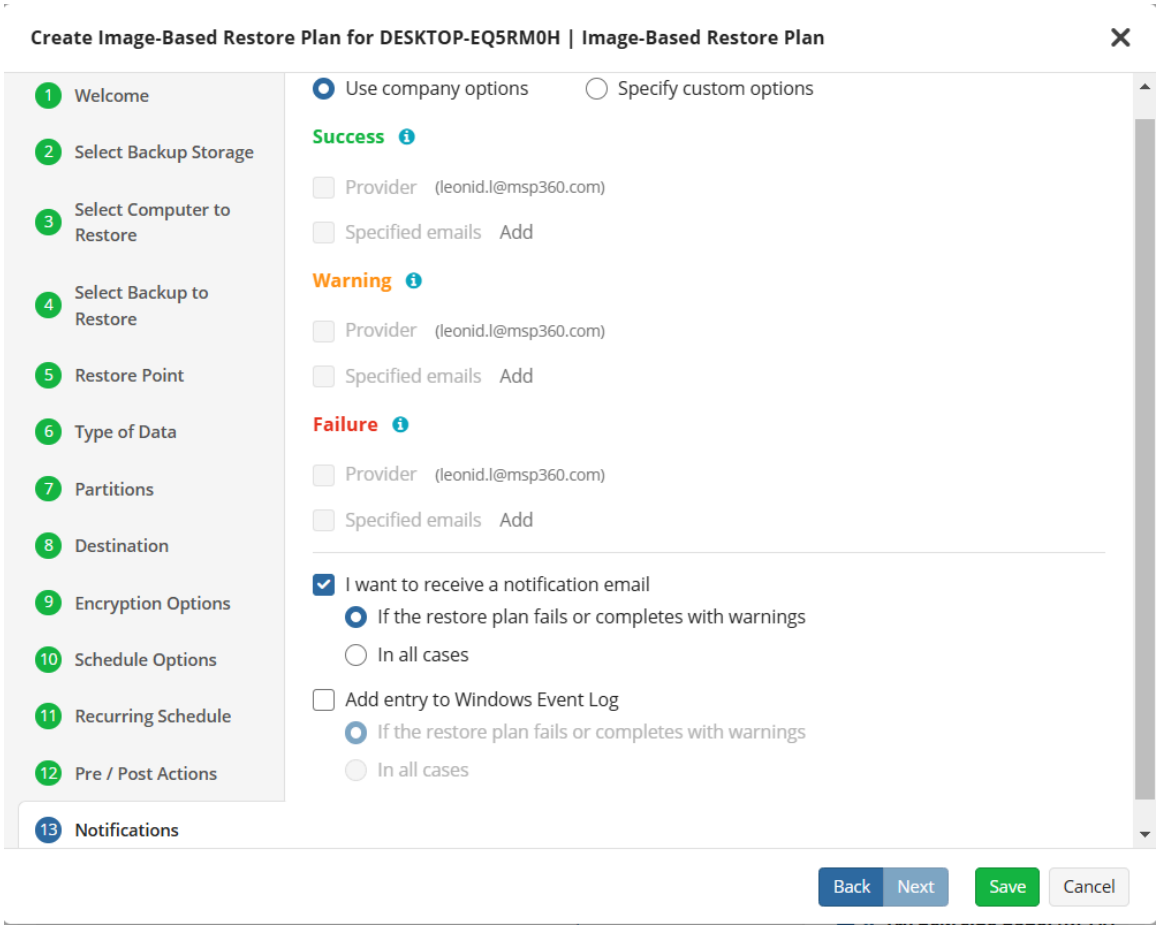
- **Recurring Schedule:** if you have selected the "Recurring" option, the next step will enable you to configure schedule based on the criteria in the fields below:



Step 14. The next step is to specify any Pre or Post Actions which should be triggered by the Restore Plan.



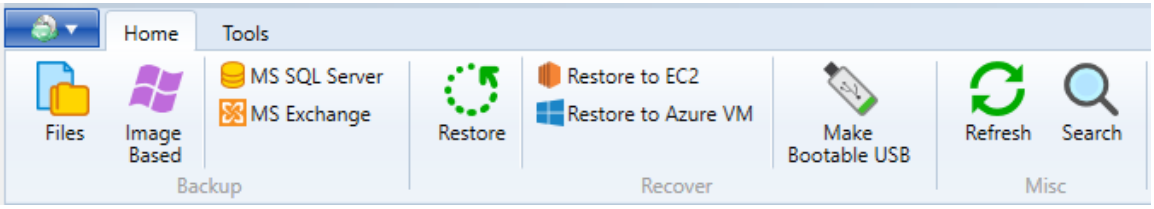
Step 15. Finally, specify any notifications you would like to receive when the plan runs.



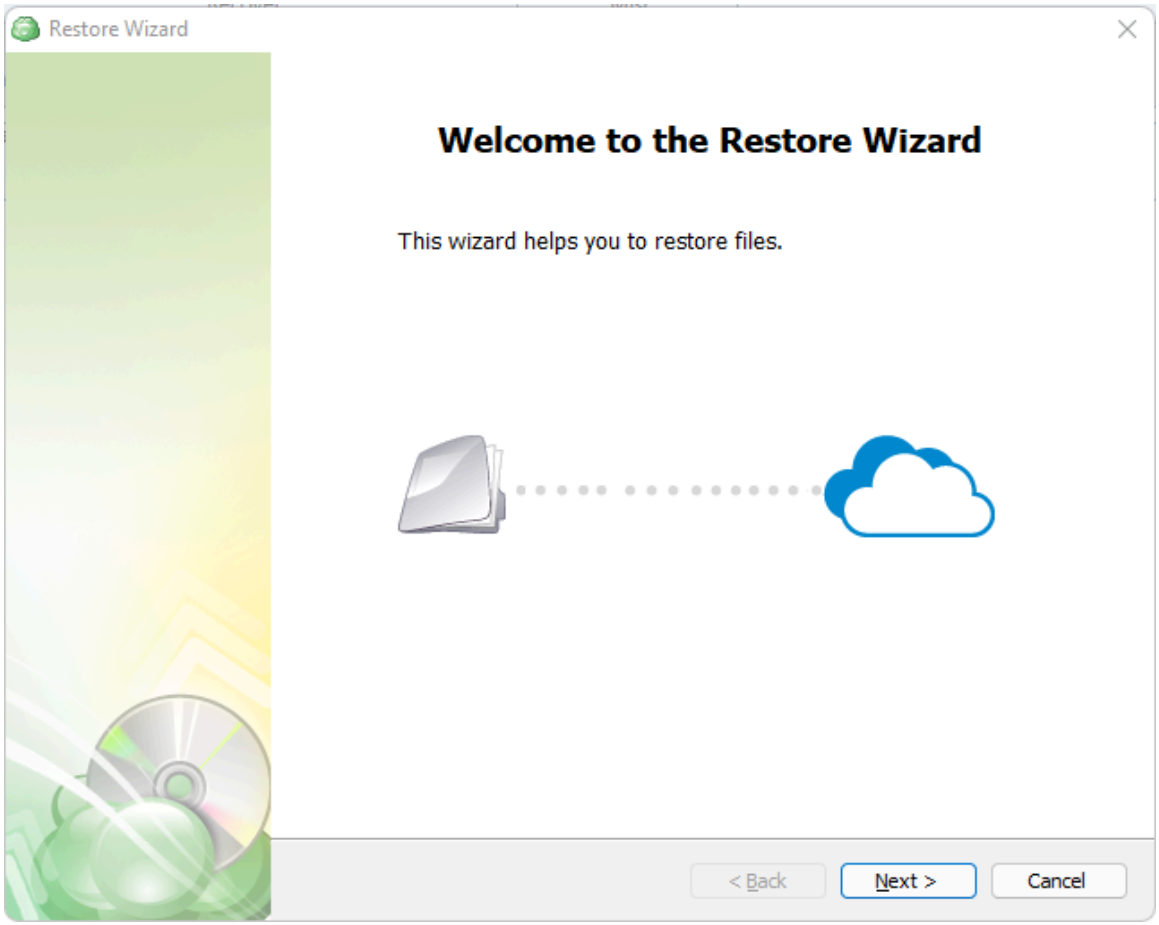
Step 16. Click on Save when you are happy with your selections. If the plan is set to run only a single time and has no set schedule, it will automatically start. Otherwise, if it is set to run only once and is scheduled, it will display in the list of plans until the scheduled time. If it is only set to run once, then when it completes successfully it will remove itself from the list of plans. Only Restore Plans which are saved will remain in the list for future use.

Restore to Virtual Disk using the Agent

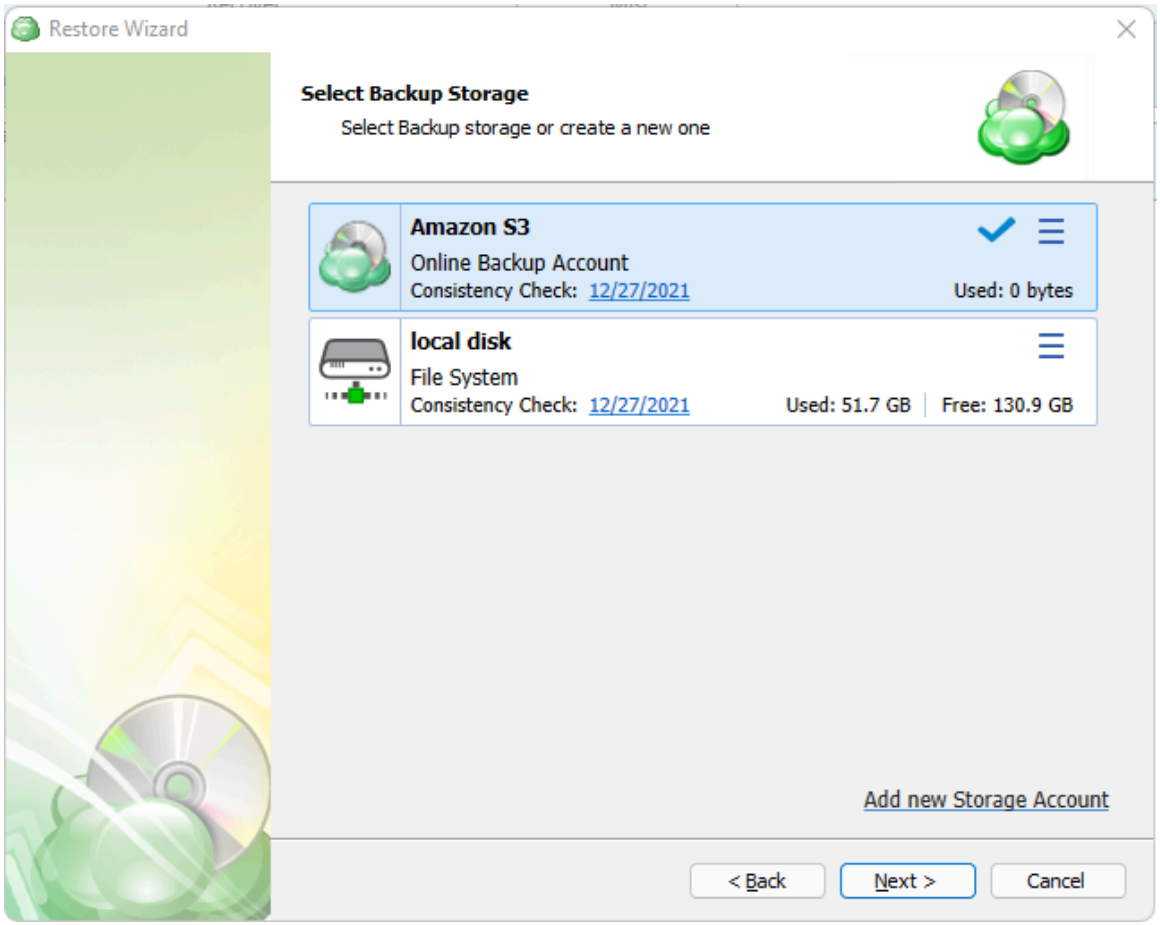
Step 1. After launching the Online Backup, you can run the Restore Wizard by “Restore” on the application's main toolbar.



Step 2. The first step of the wizard indicates that you have started the wizard.

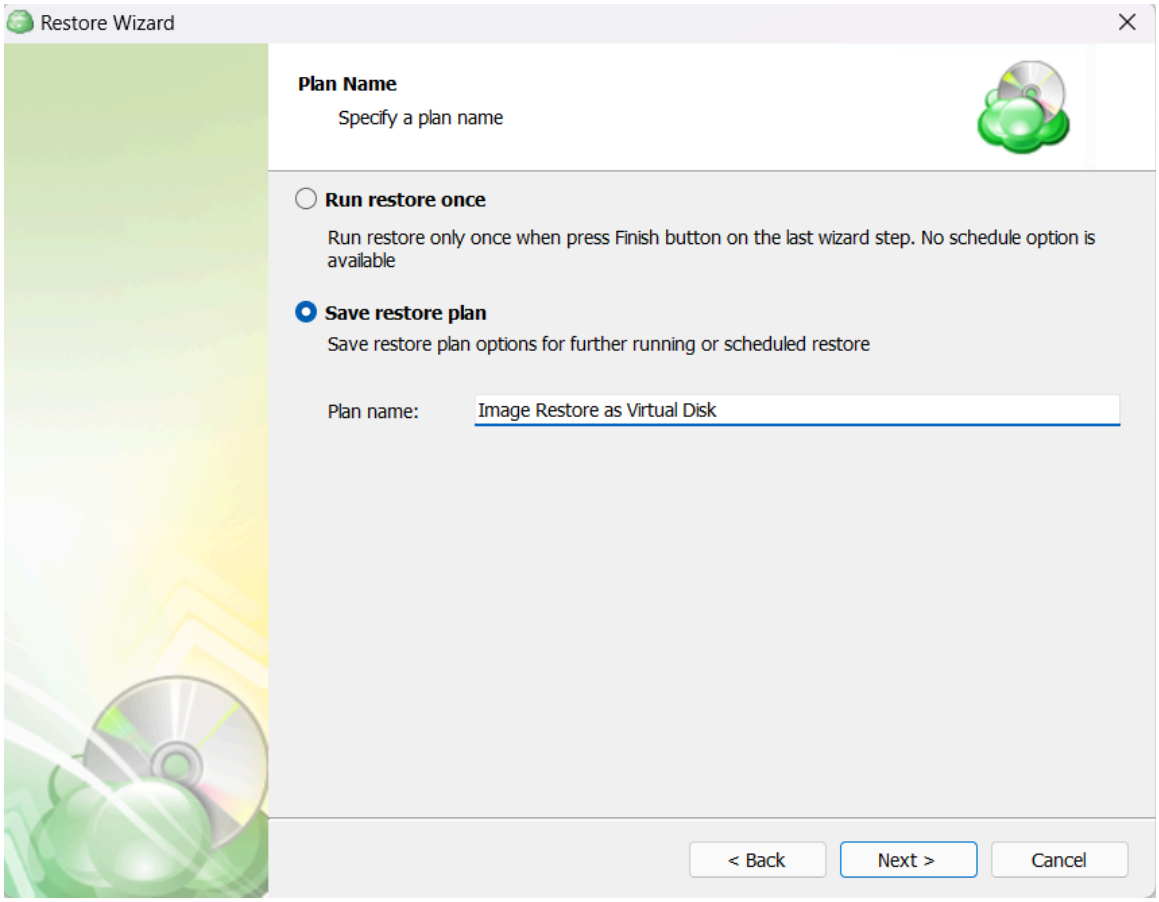


Step 3. The next step will prompt you to select the storage location for the source.

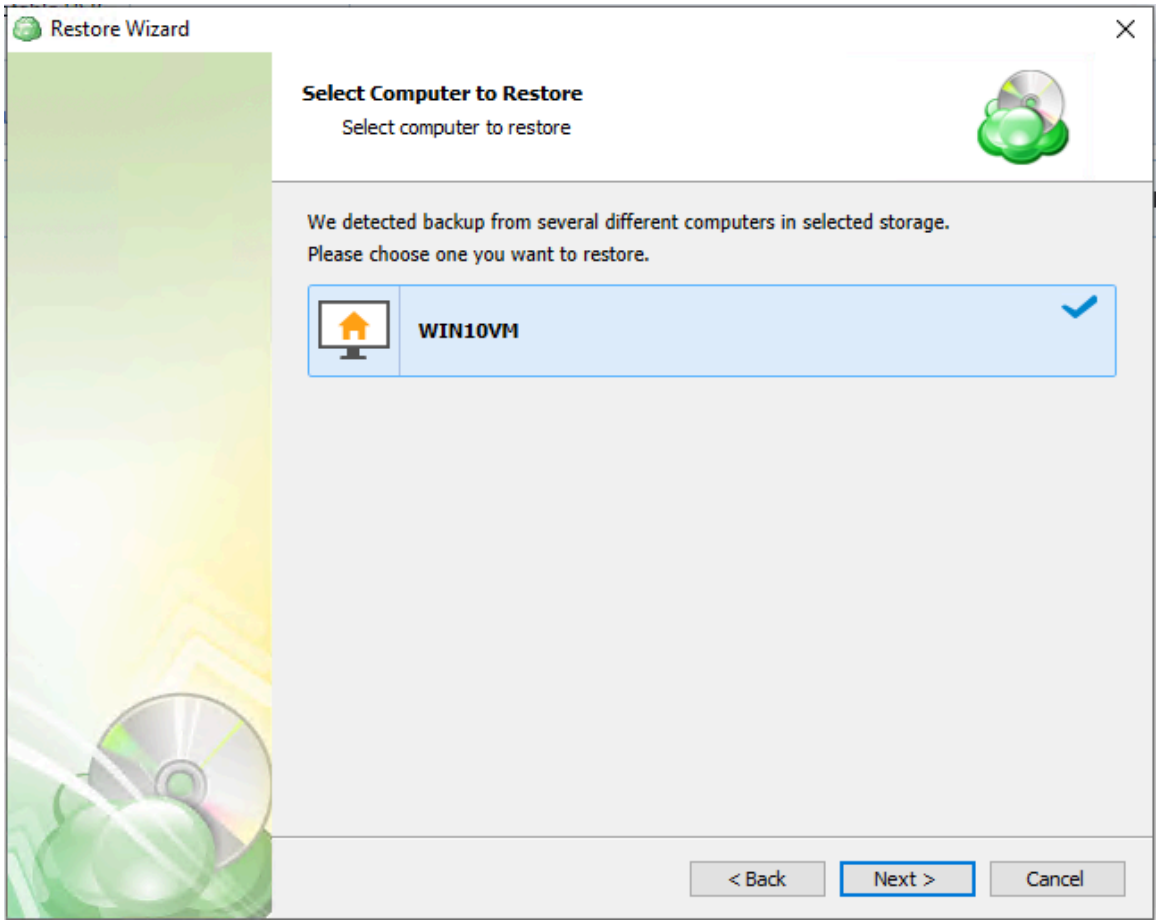


If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

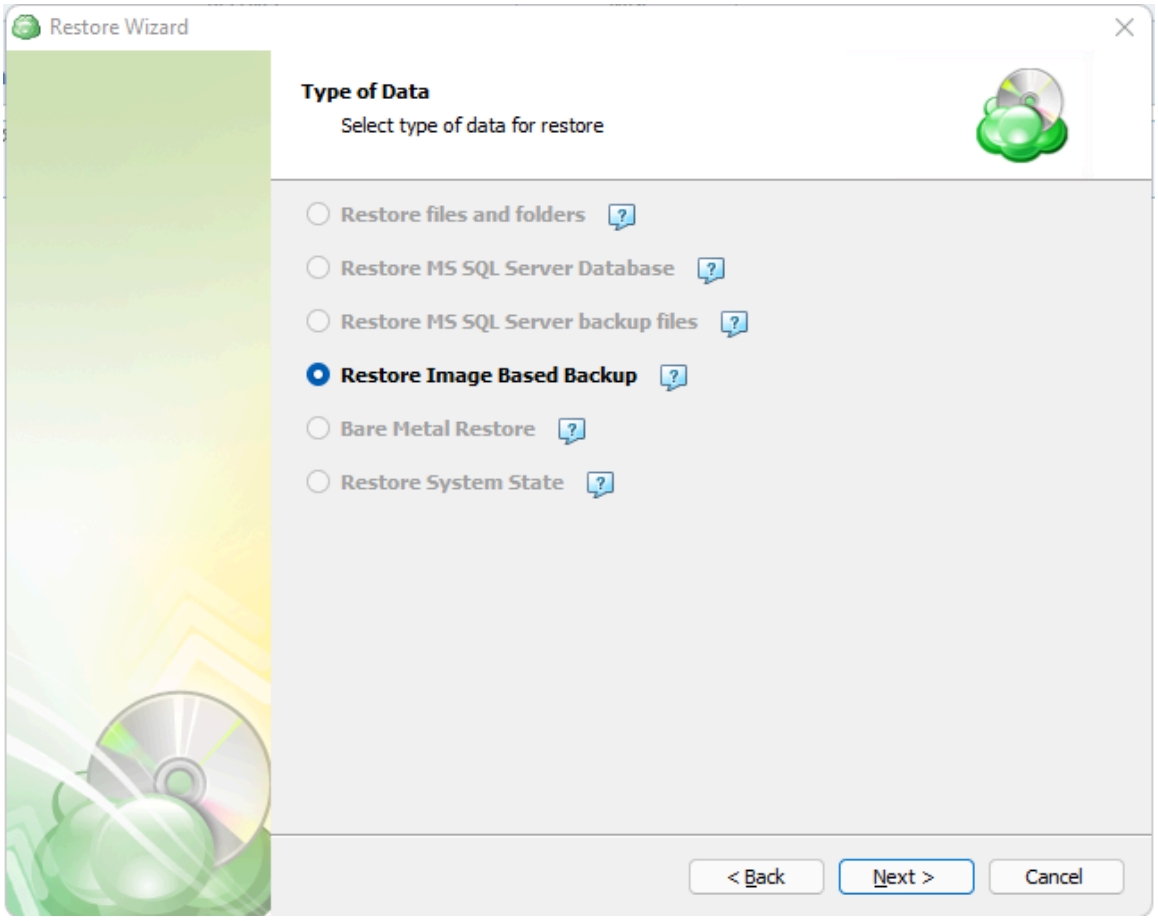
Step 4. Next you will choose whether to run the restore operation only once, or to save it for later use. The latter will allow you to name the plan.



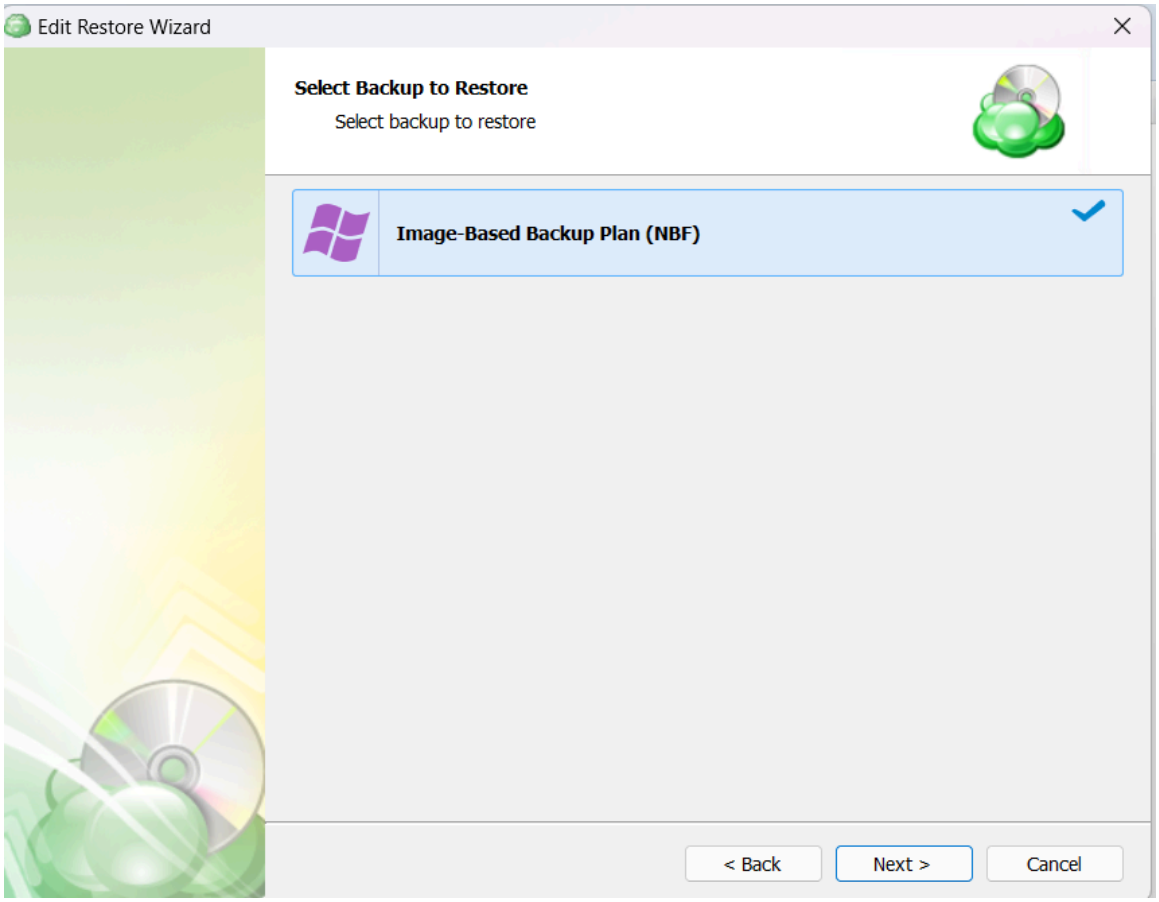
Step 5. Next you will be presented with a list of computers with the same prefix and associated "Backup User" as the computer on which the Agent is currently running. Click to select the desired computer then click on "Next".



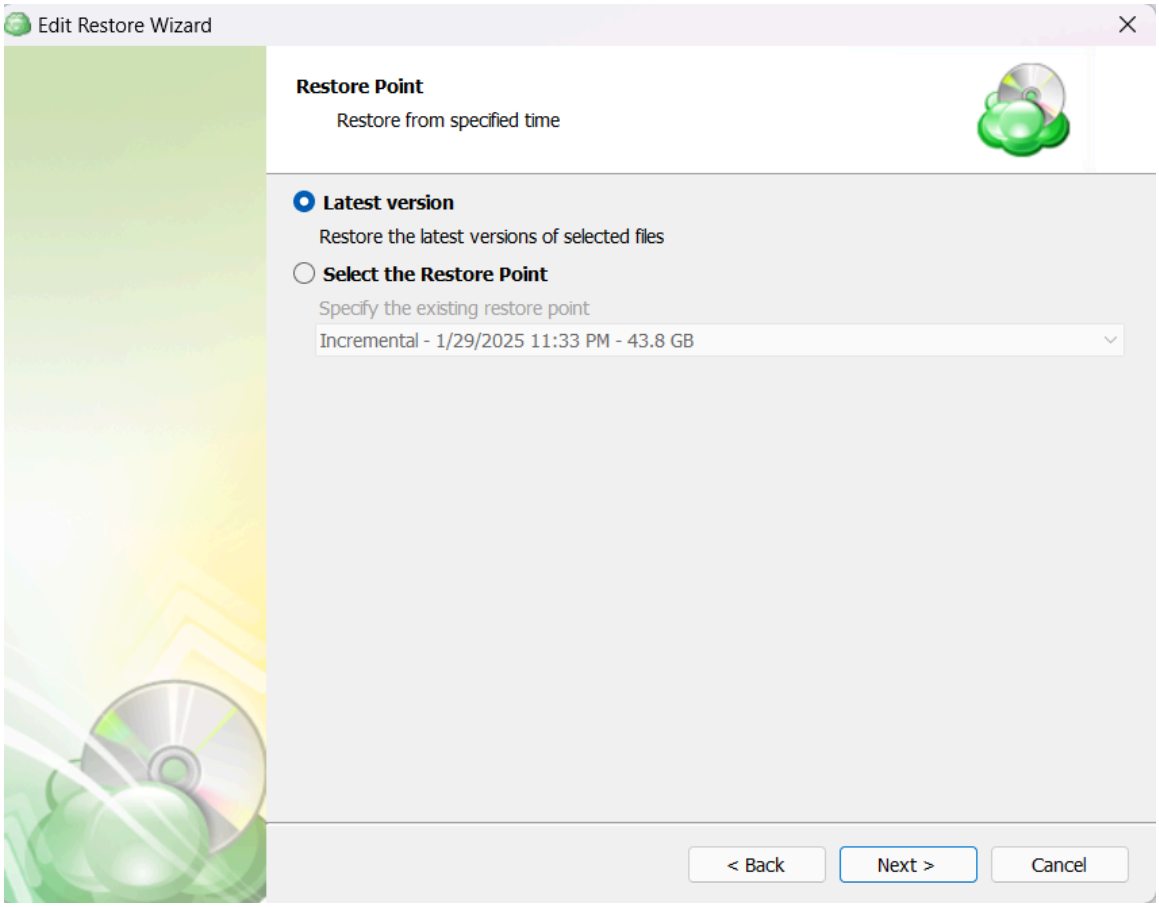
Step 6. Based on the contents of the selected source and computer, the next step is to choose the type of restore. Select “Restore Image Based Backup” then continue to the next step by clicking “Next”.



Step 7. With the correct type of restore selected, the application will generate a list of available backup plans.

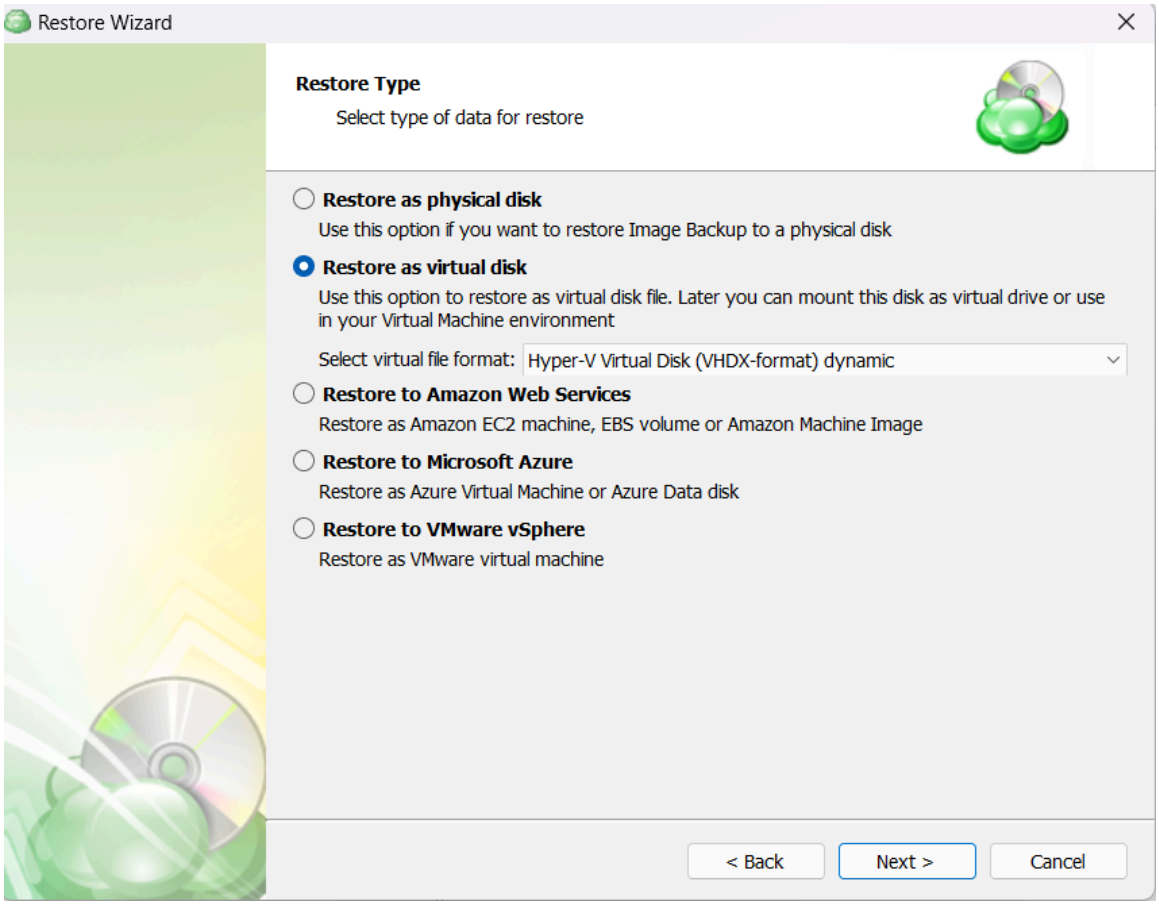


Step 8. The next step is to select the desired point in time to restore to.



- **Latest Version:** Automatically restores the newest version of each file in the source regardless of which restore point it belongs to.
- **Select the Restore Point:** Allows you to select which restore point to restore from the dropdown list.

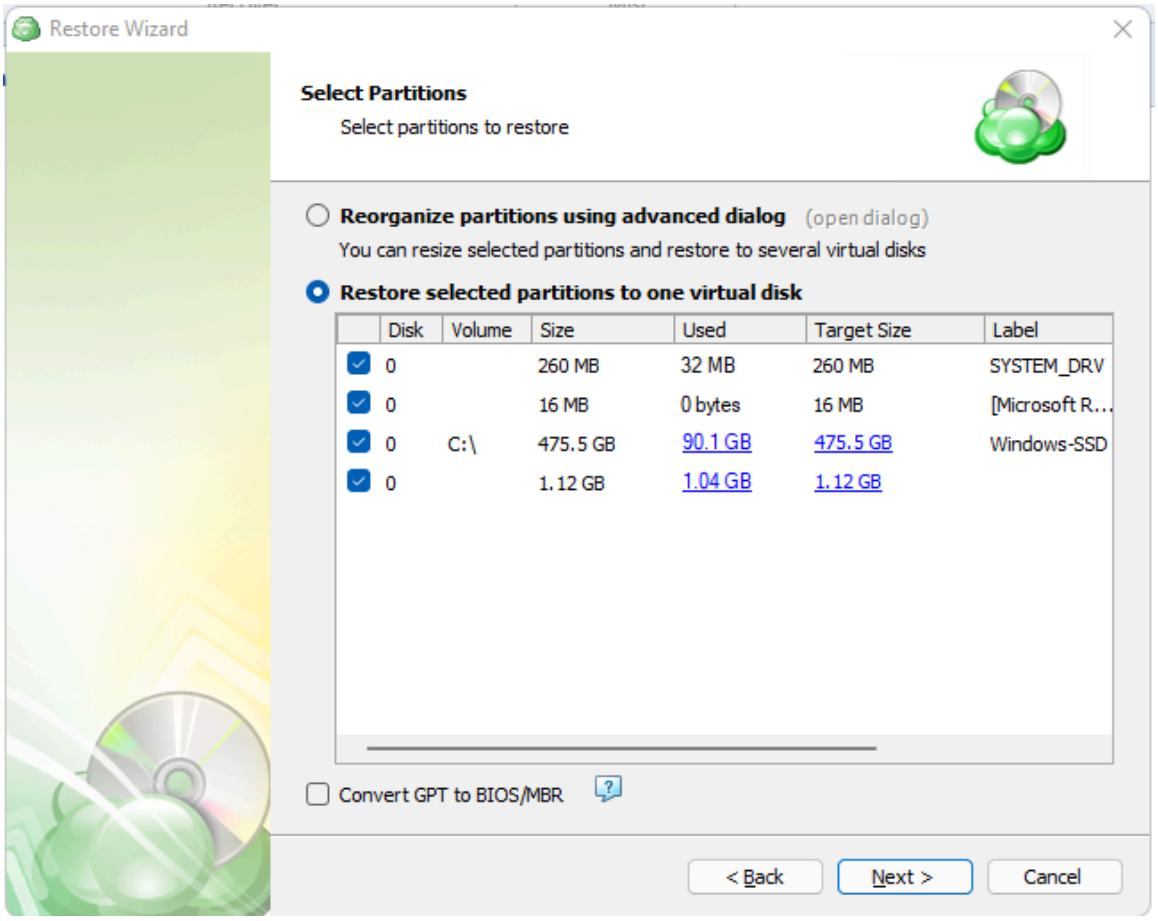
Step 9. Next, select the desired target format for the restored data



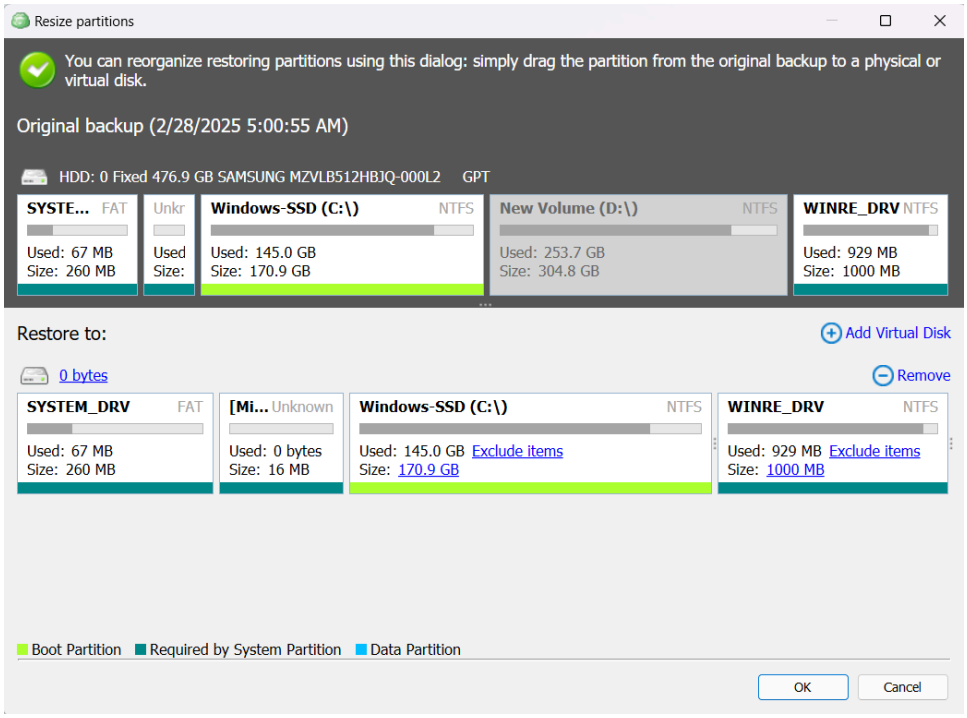
- **Restore as physical disk:** Restores the partitions selected later to a physical disk.
- **Restore as virtual disk:** Restores the data as a virtual disk in multiple supported formats.
- **Restore to Amazon Web Services:** Restores the data as either an EC2 machine, EBS volume, or Amazon Machine Image.
- **Restore to Microsoft Azure:** Restores the image to either an Azure Virtual Machine or Azure Data Disk.
- **Restore to VMware vSphere:** Restores the image as a new virtual machine in vSphere.

For AWS and Azure destinations, a storage account must already be specified through the MBS portal

Step 10. After selecting the type of restore target in the previous step, you can now choose to restore the partitions with their existing parameters or to reorganize and resize them.

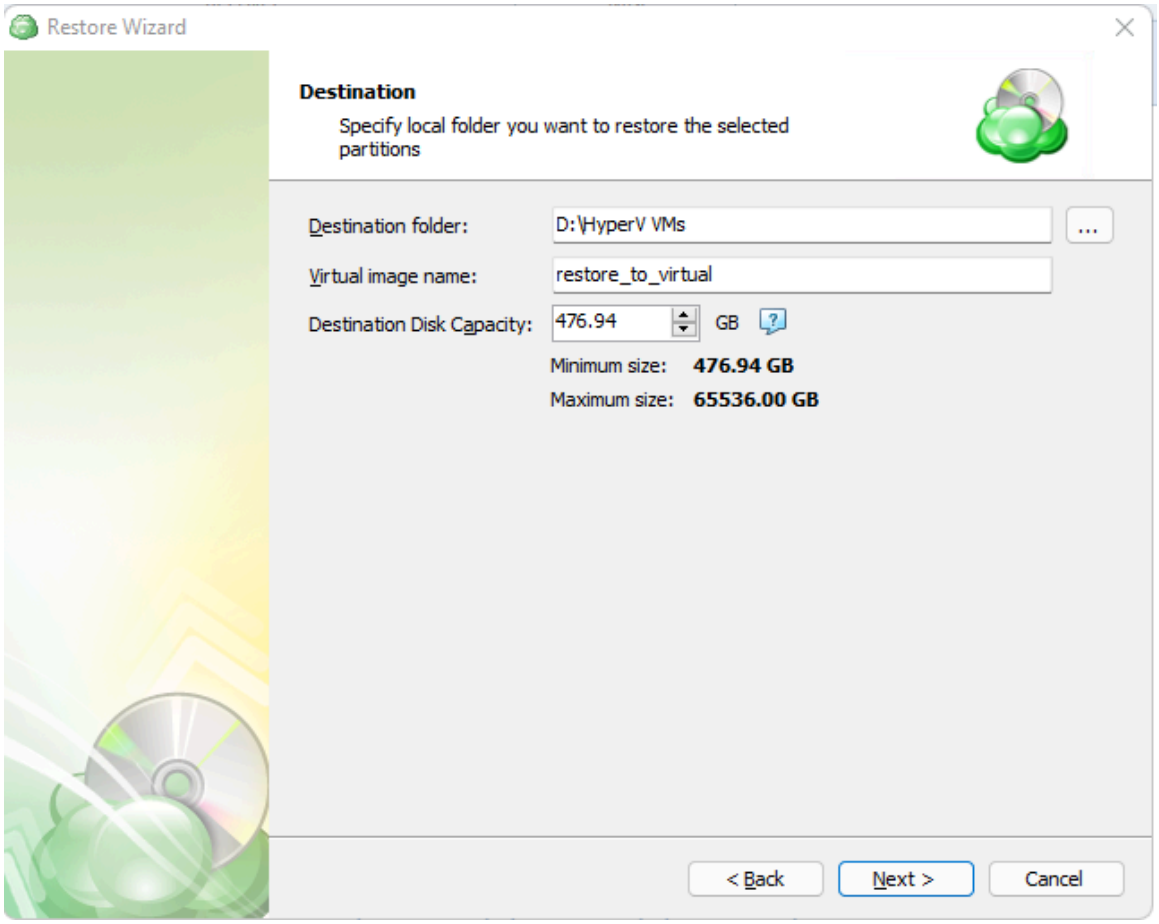


If you select “Reorganize partitions using advanced dialog” a new window will appear and allow you to resize the partitions and rearrange them on one or more virtual disks.

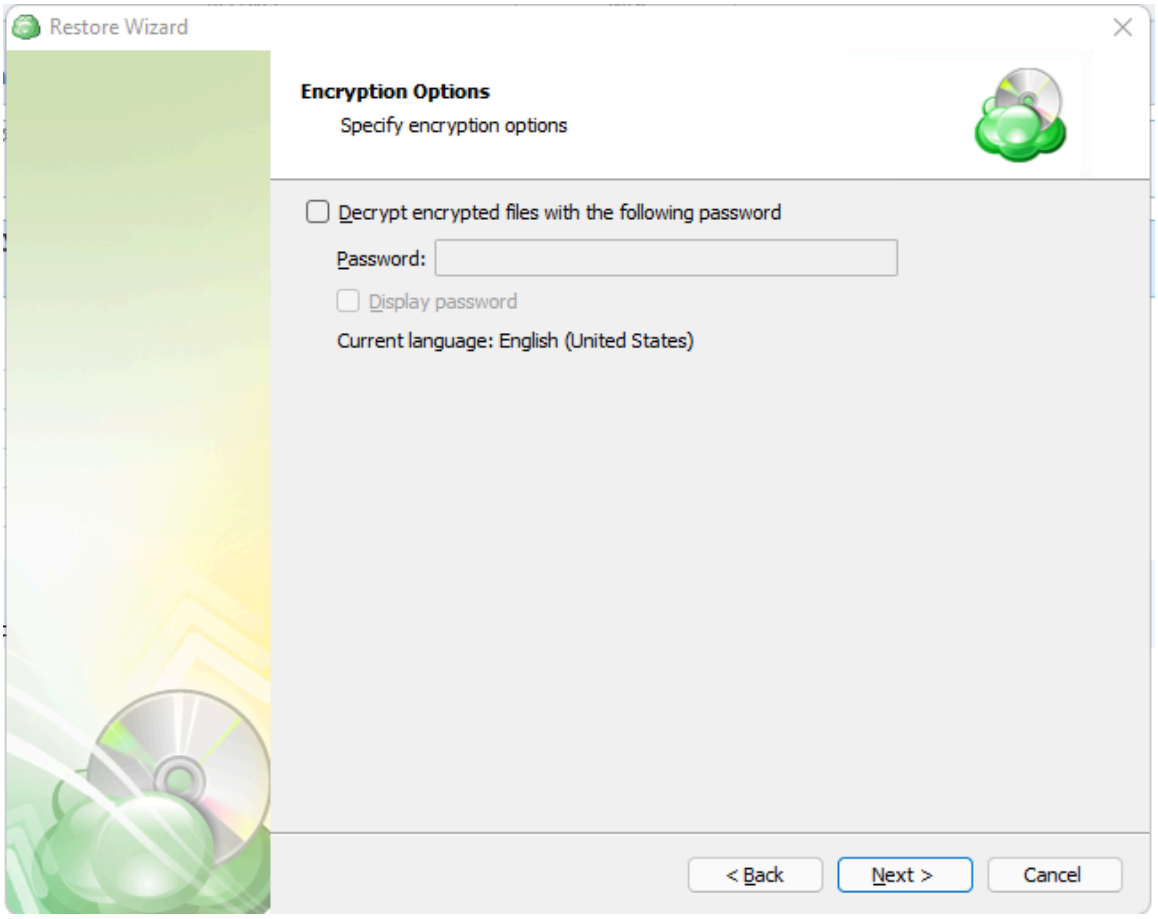


Click on any of the blue hyperlinks to open additional dialogue boxes allowing you greater control over the name and size of the virtual disk, as well as the ability to add additional virtual disks, and also exclude specific files or folders if desired.

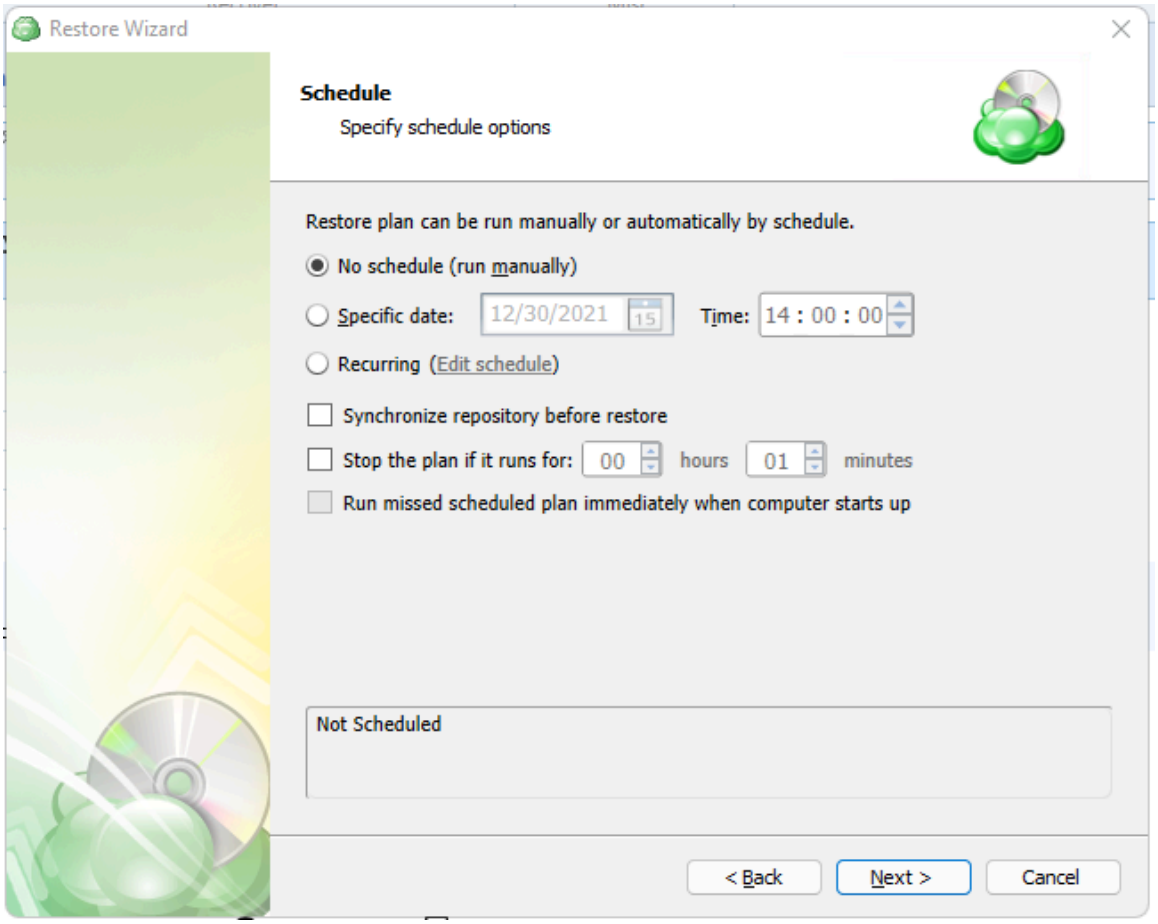
Step 11. Once the partitions are selected, the next step allows you to choose the name for the virtual disk as well as the path it should be created in.



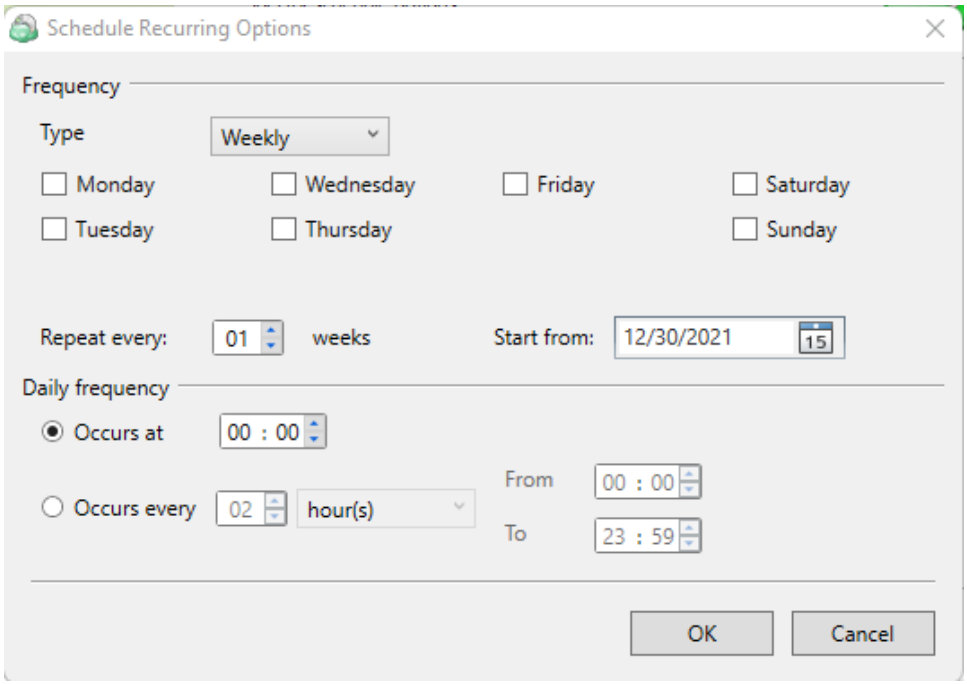
Step 12. If the backed up data was encrypted, the next step will be to enter the password for decryption. If the password is incorrect or missing, the restore plan will fail and you will need to edit the plan to input the correct password.



Step 13. If the restore plan is saved for later, next you will set the schedule for the plan, otherwise proceed to the next step.



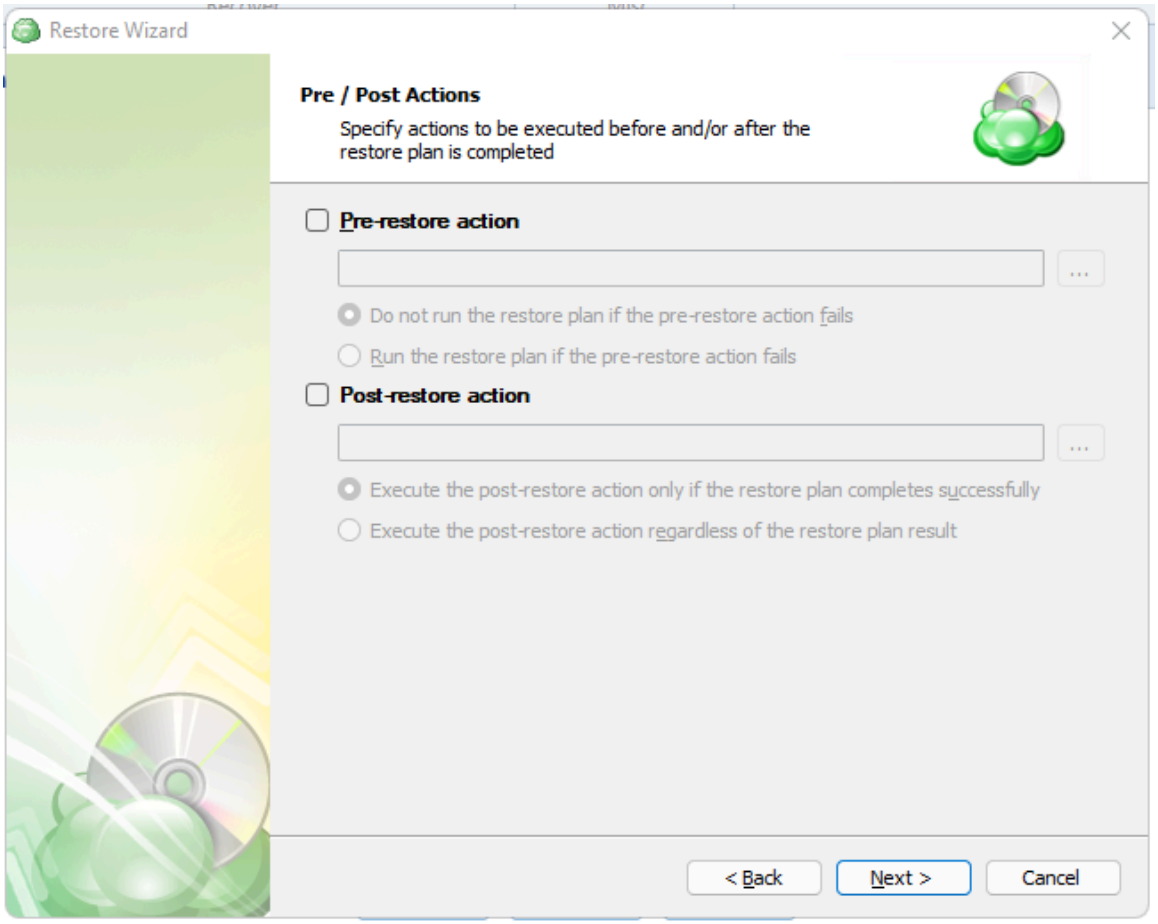
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria by clicking on the “Edit schedule” hyperlink to open this dialogue:



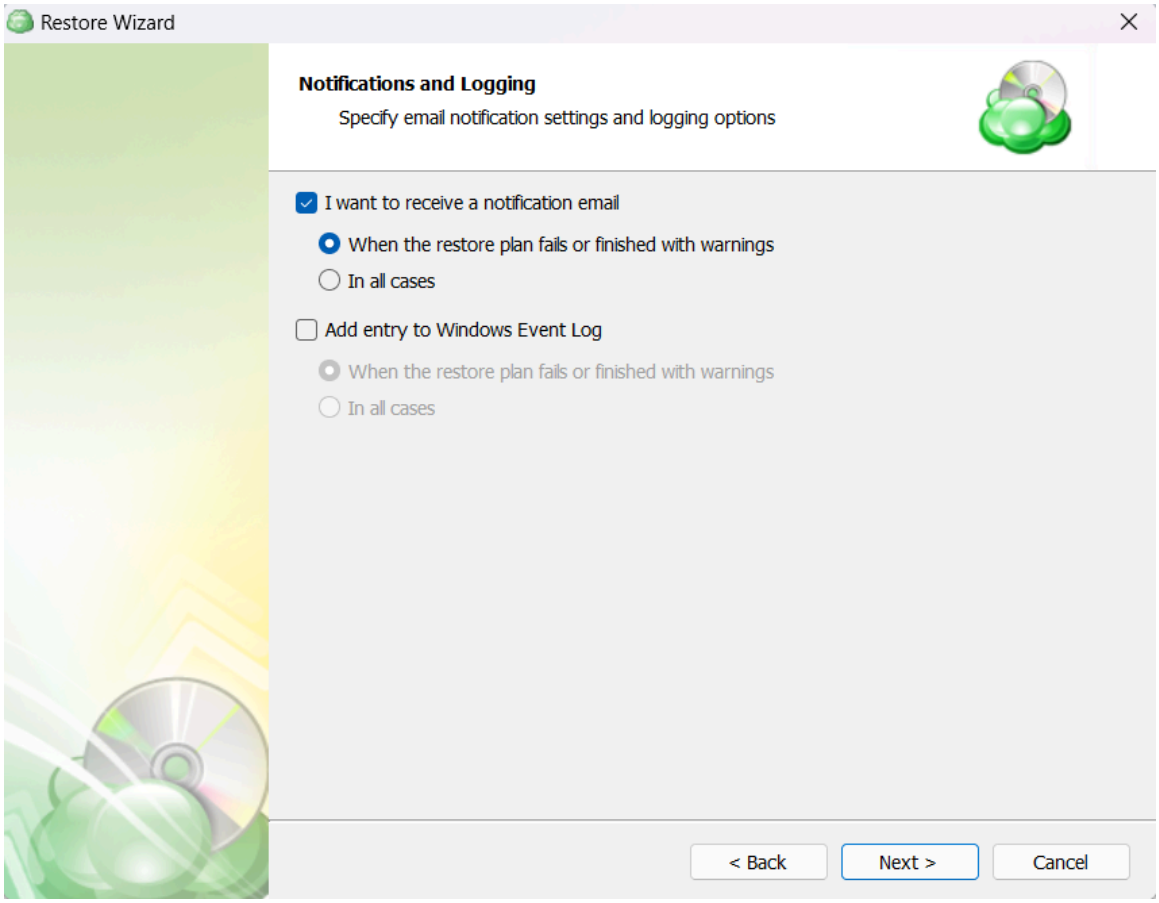
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

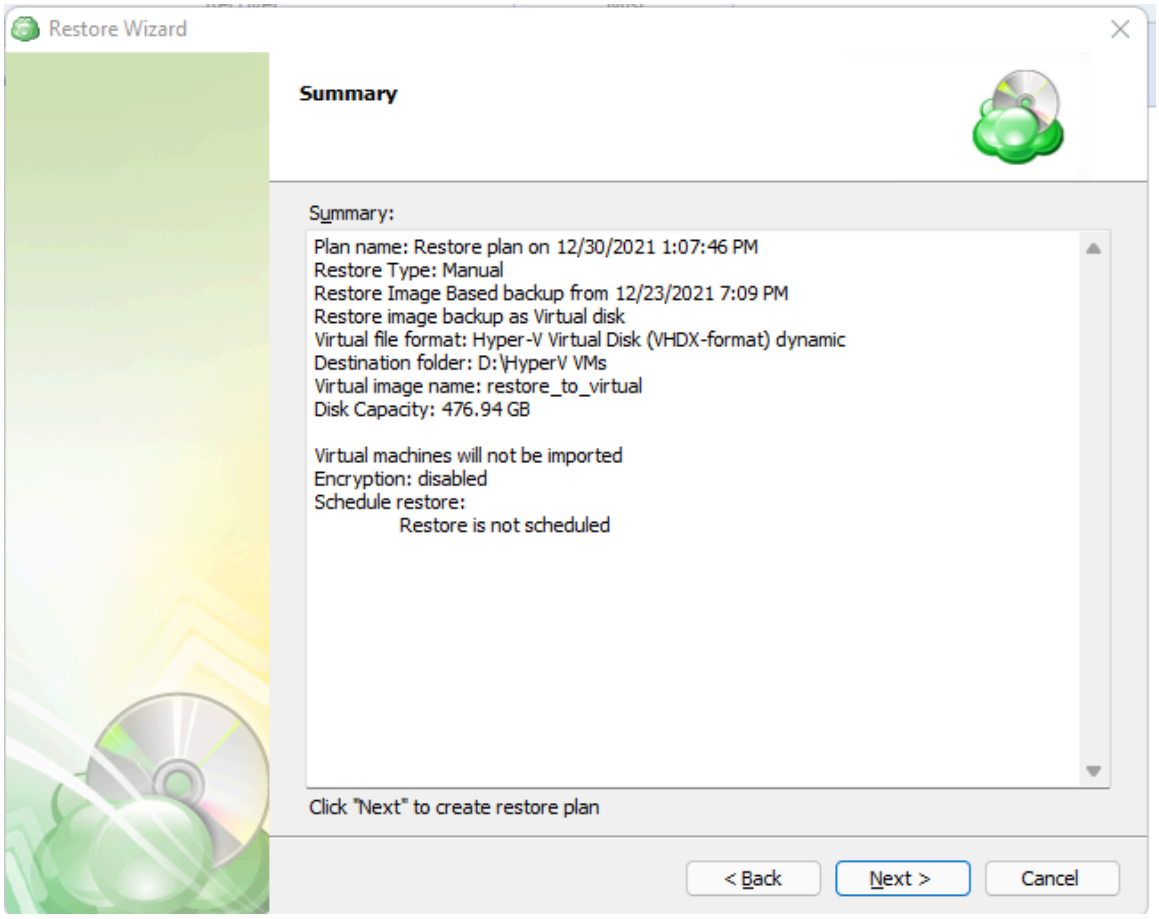
Step 14. The next step page allows the execution of custom scripts before and/or after the running of a Restore Plan.



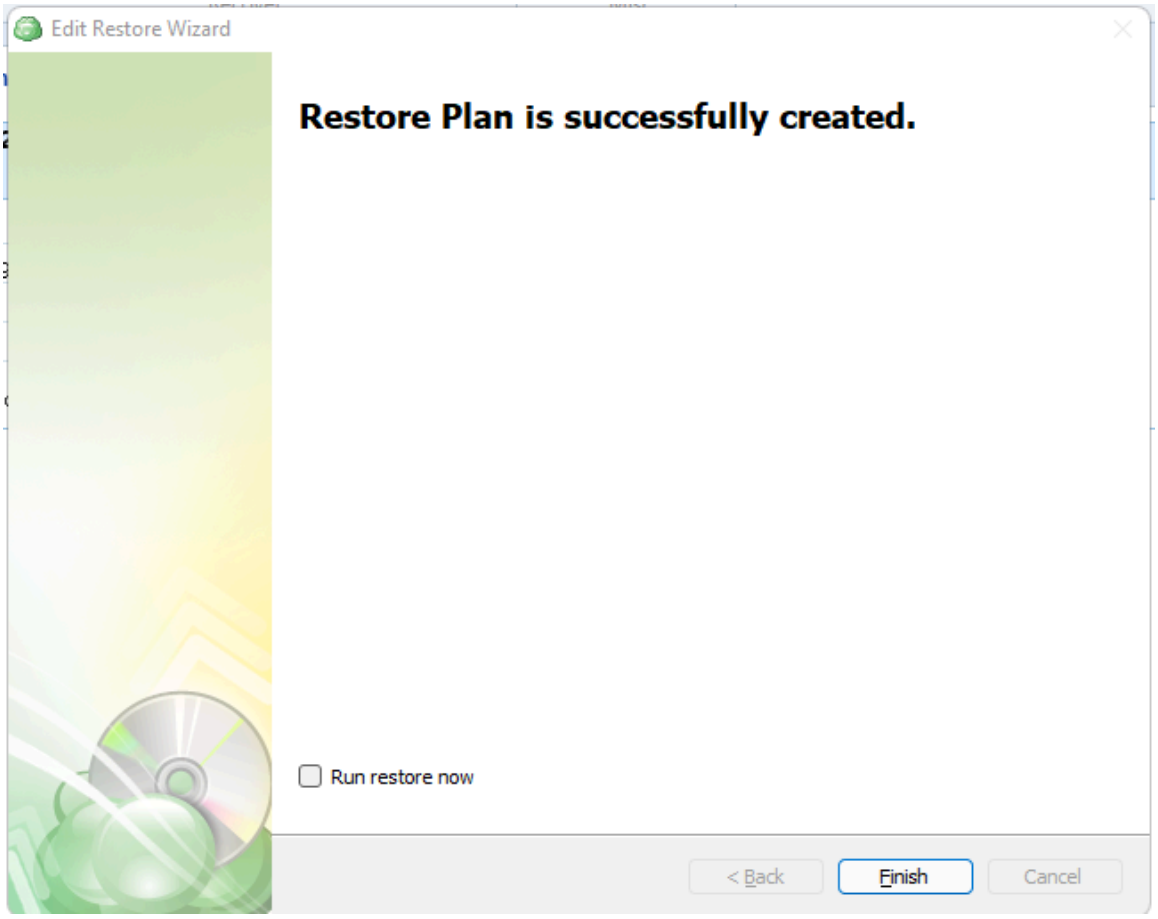
Step 15. The “Notifications and Logging” page allows you to enable notification email and add an entry to Windows Event Log upon restore plan completion or failure.



Step 16. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.

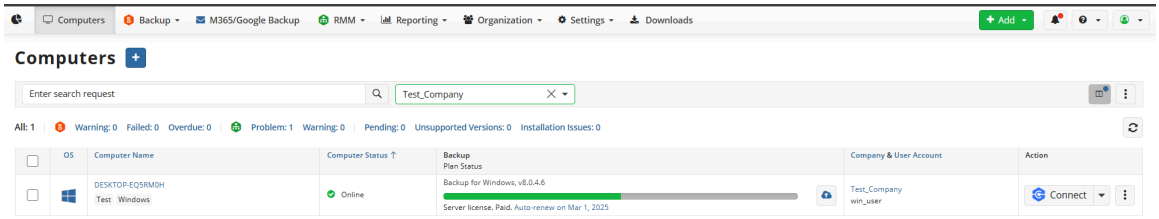


Step 17. The final step of the process is to select when the Restore Plan will start running. To have it start immediately, select the “Run Backup Now” option and click “Finish”. Otherwise, click “Finish” and the plan will begin at the next scheduled time.

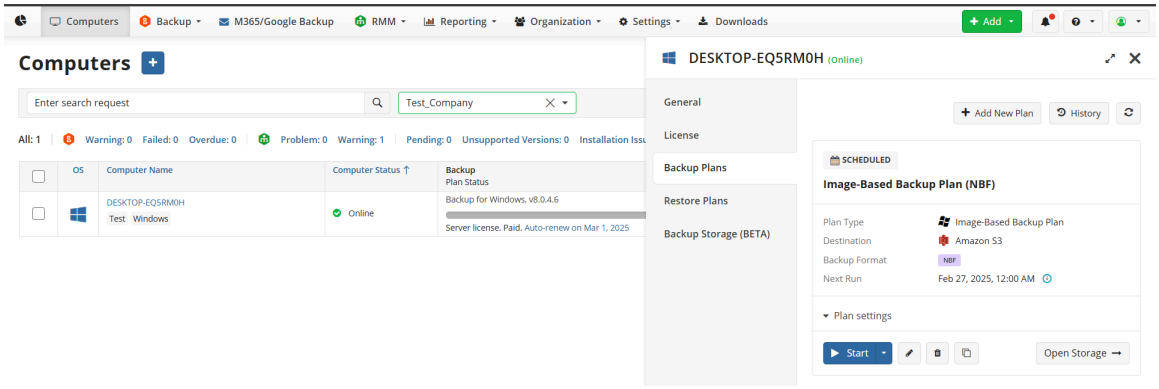


Restore to Virtual Disk using MBS

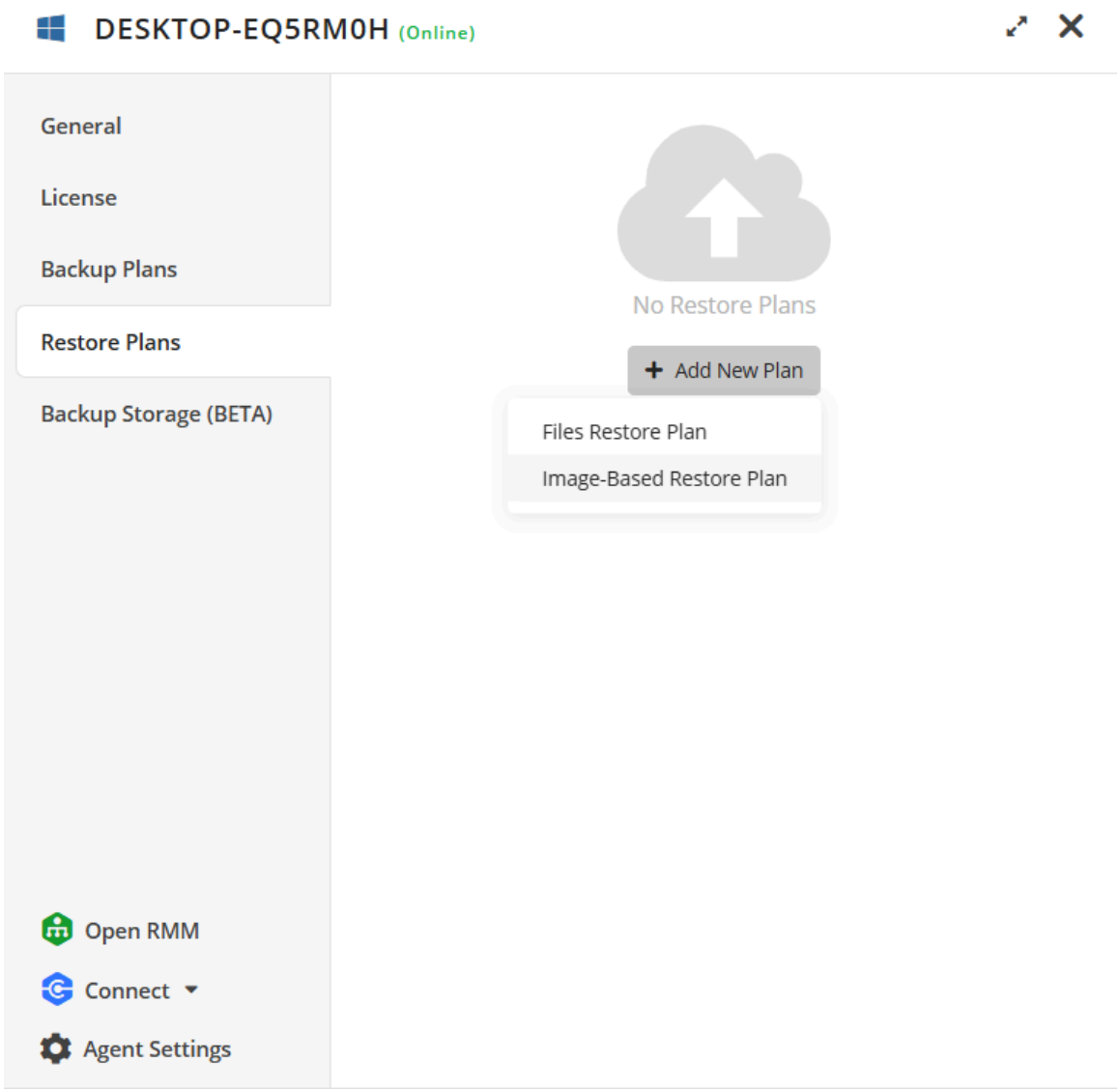
Step 1. Navigate to the MBS Portal and select the “Computers” page on the main menu.



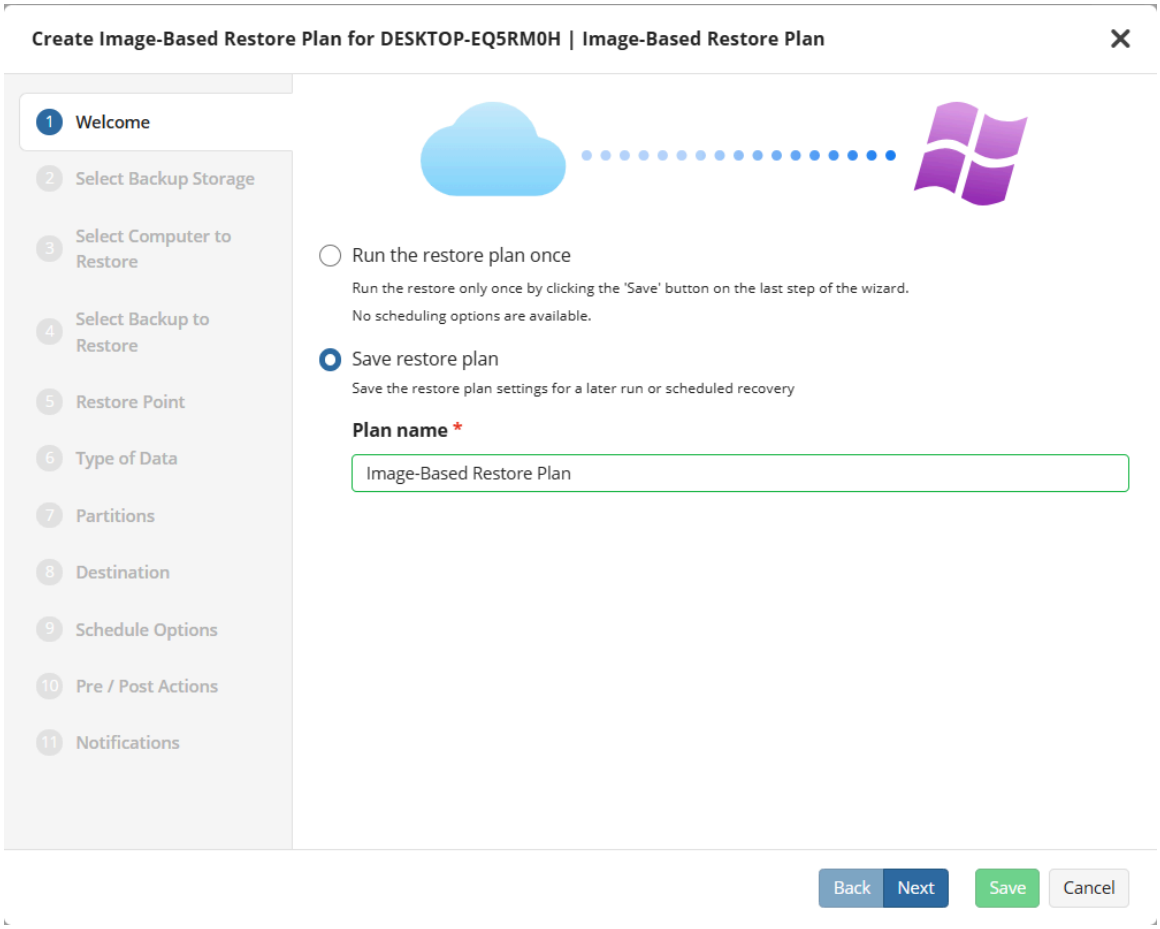
Step 2. Locate the computer which backup dataset you wish to restore from and click on the name of the computer or the backup status bar.



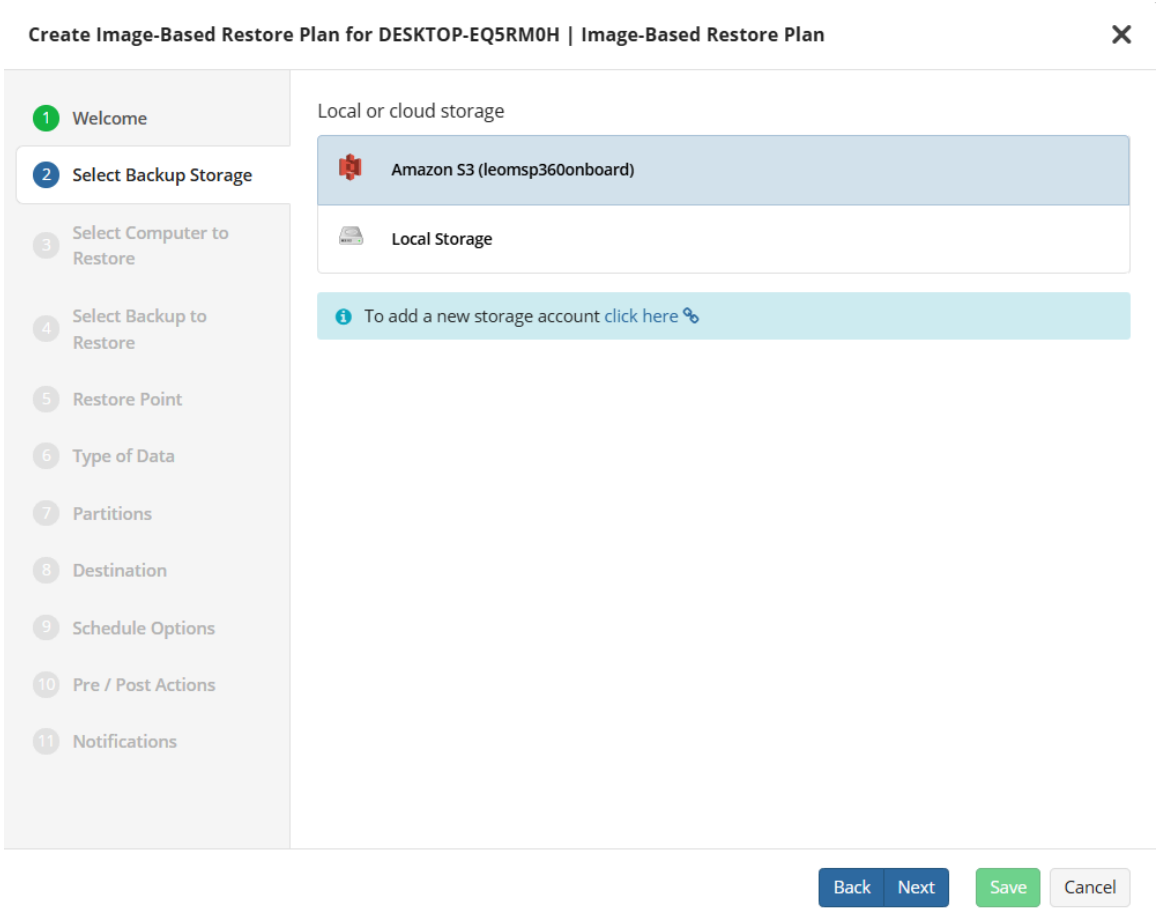
Step 3. Switch to the “Restore Plans” tab. Click on the “+ Add New Plan” button and select “Image-Based Restore Plan”



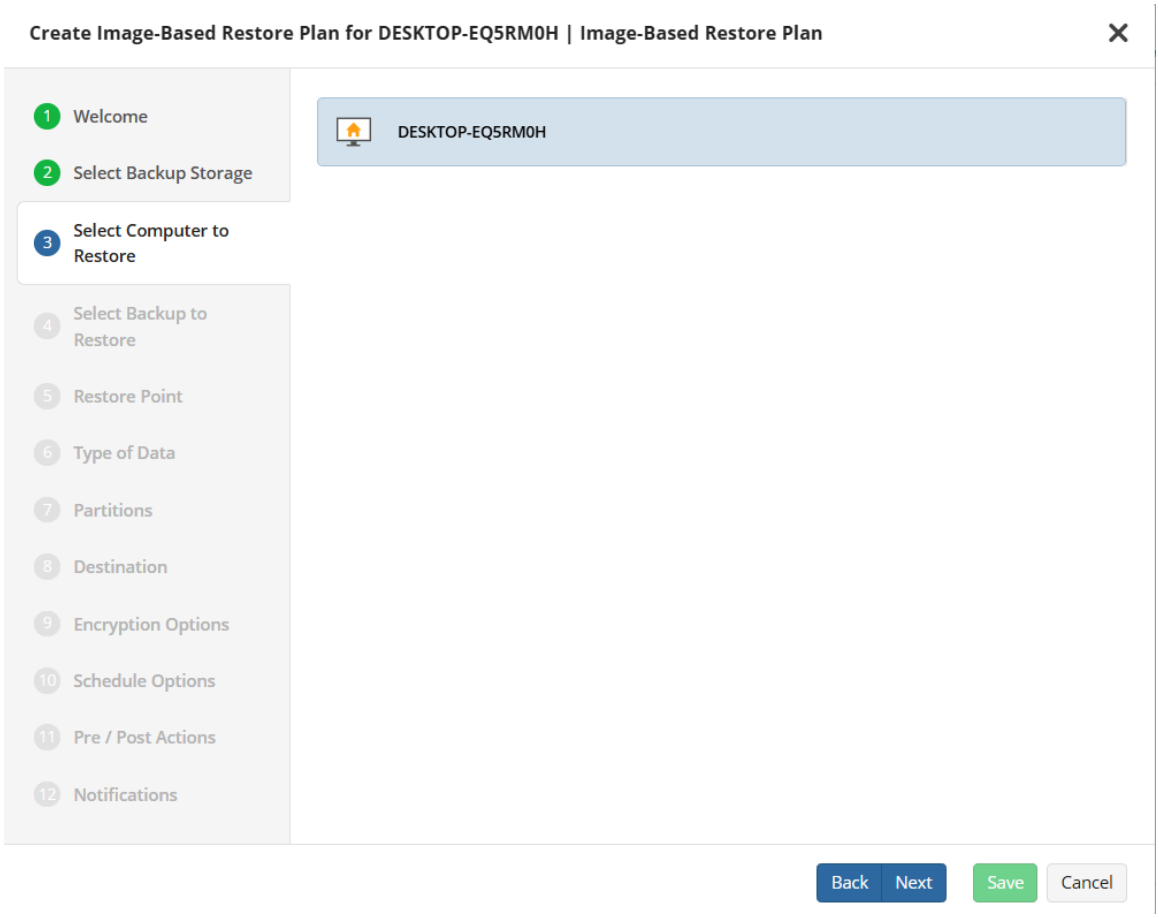
Step 4. The first step when making a Restore Plan is to select if it should run only once, or if it should be saved for future or scheduled use. The latter will allow you to name the plan.



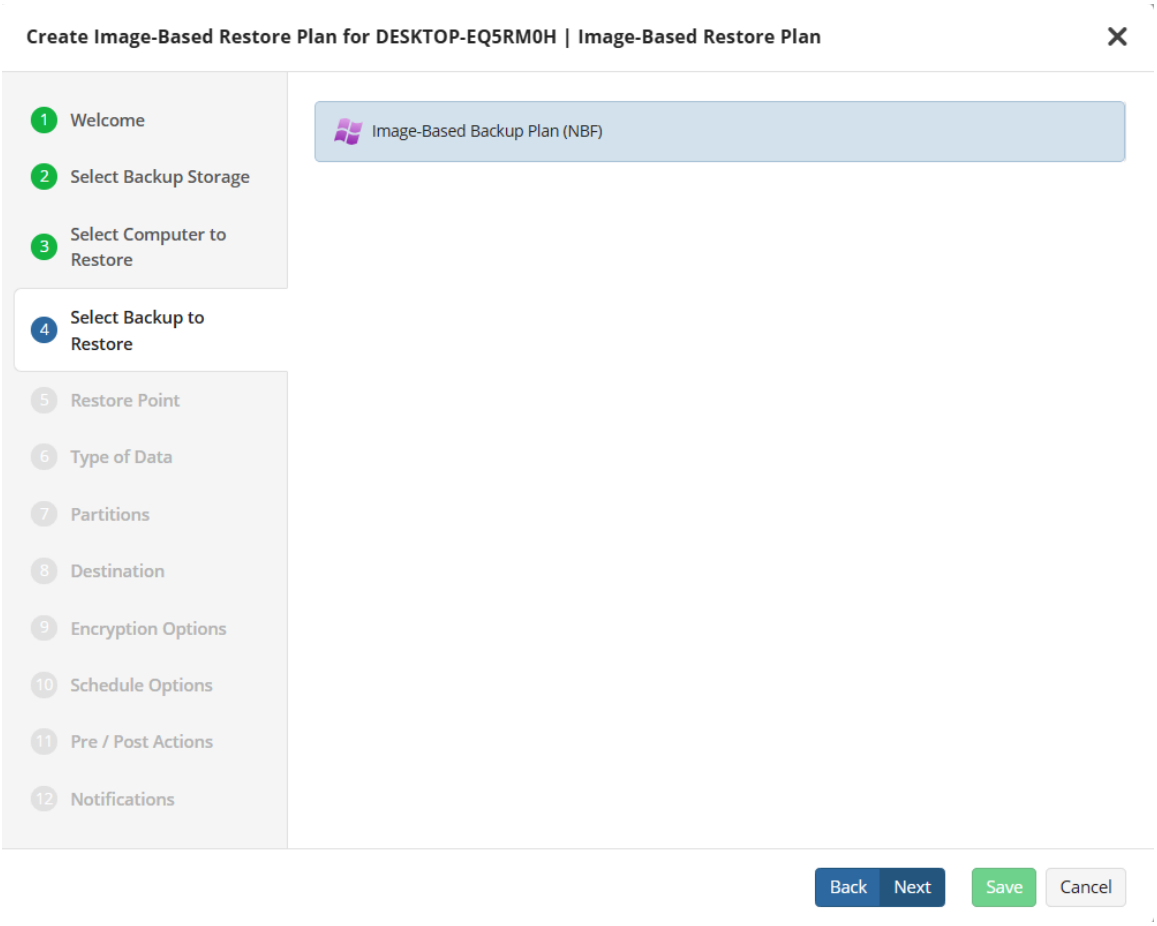
Step 5. Next you will need to select the restore source.



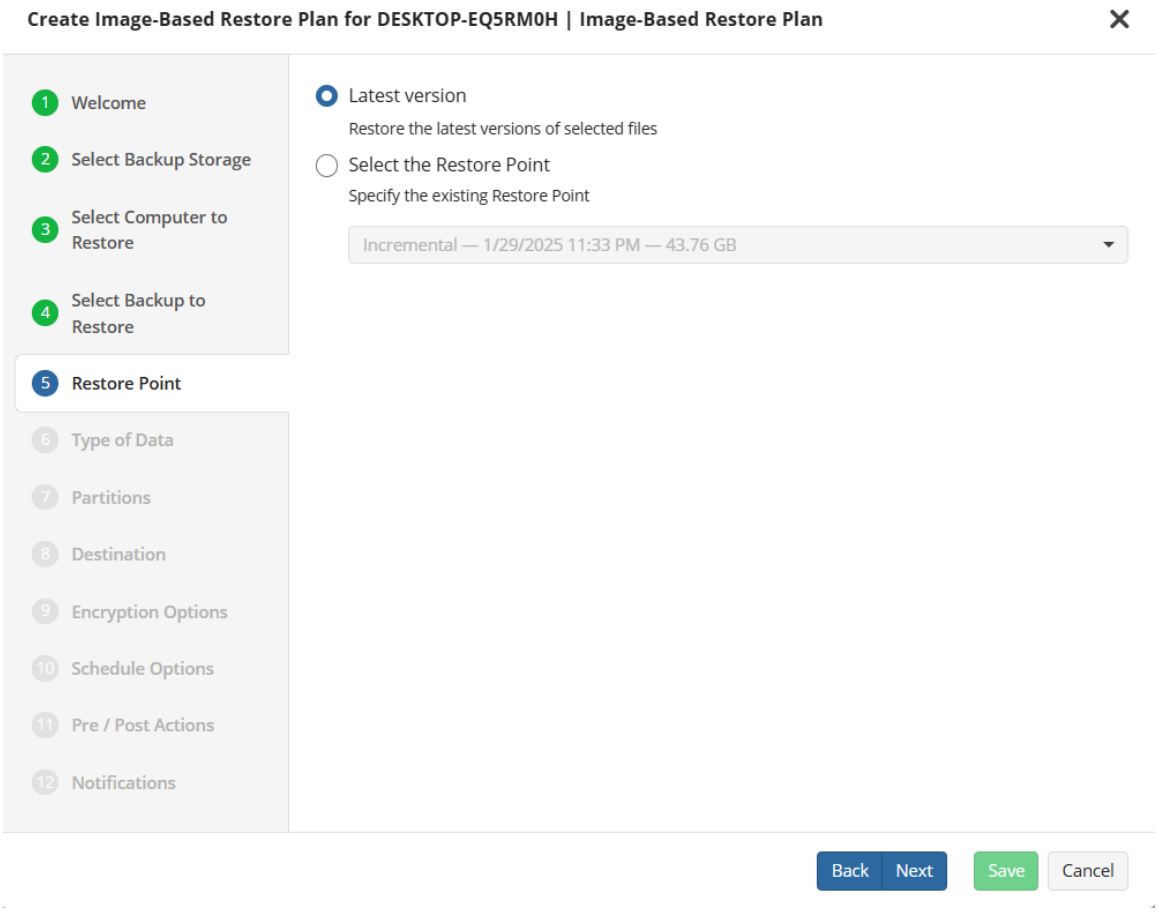
Step 6. Next you will need to select the computer to be restored.



Step 7. Next you will need to select the backup plan which contains the desired restore point.

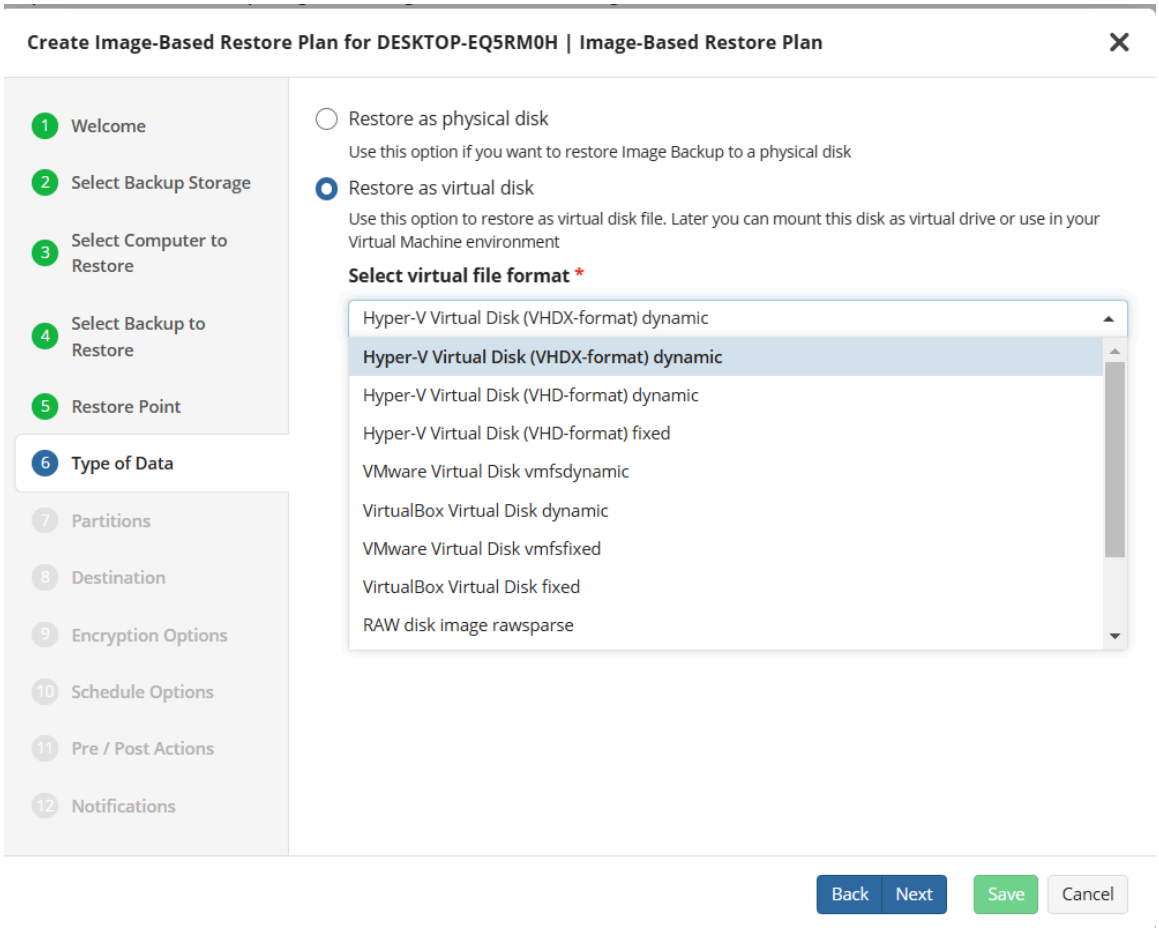


Step 8. The next step is to select the desired point in time to restore to.



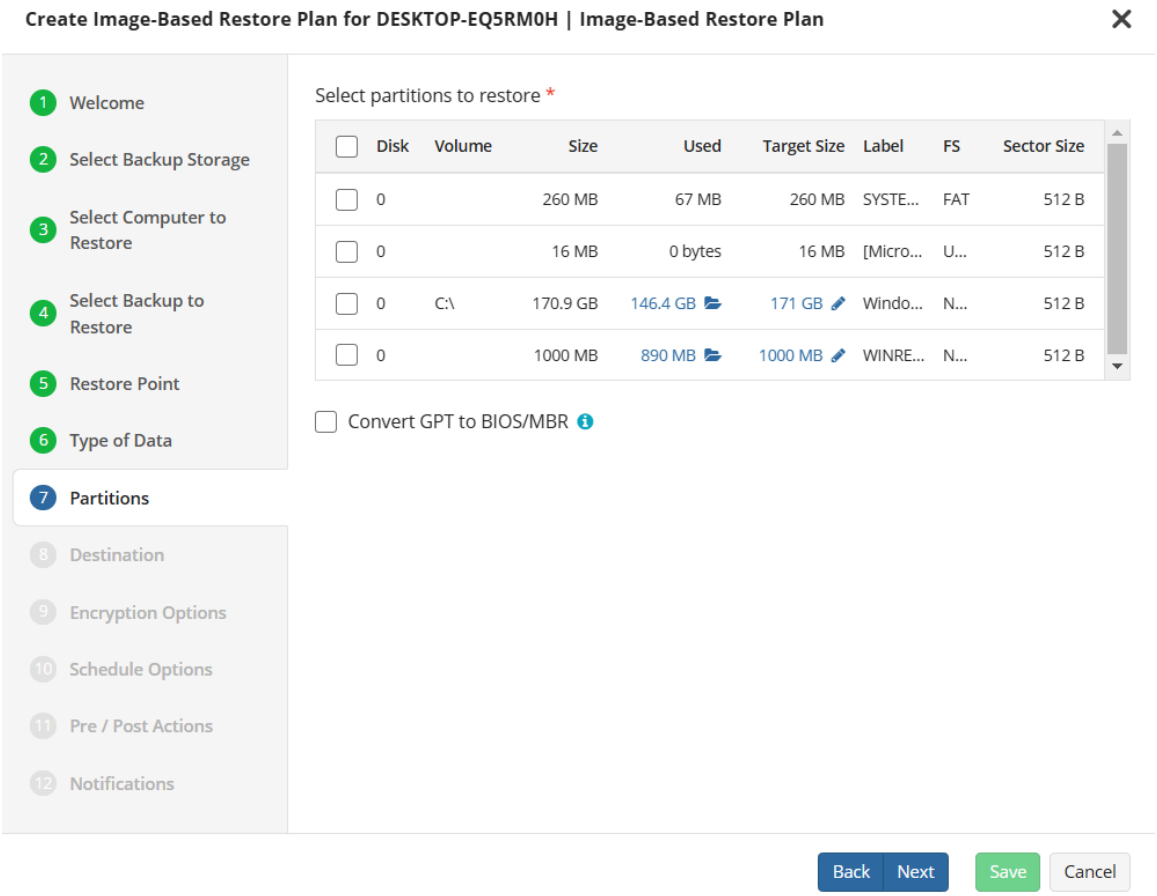
- **Latest Version:** Automatically restores the newest version of each file in the source regardless of which restore point it belongs to.
- **Select the Restore Point:** Restores the image as it existed at the specified restore point

Step 9. Next, select the desired target format for the restored data.



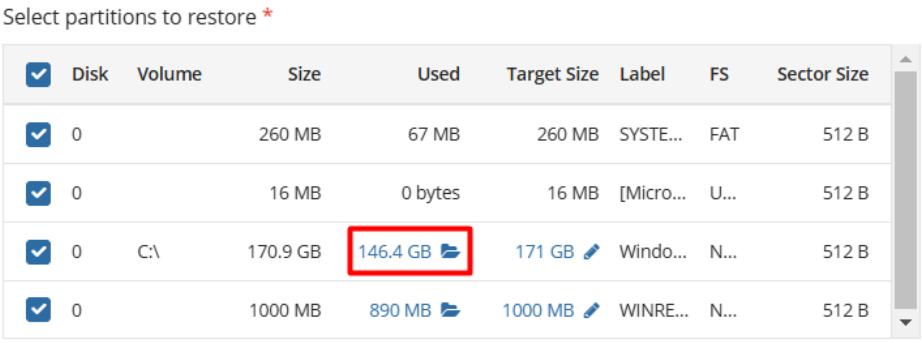
- **Restore as physical disk:** Restores the partitions selected later to a physical disk.
- **Restore as virtual disk:** Restores the data as a virtual disk in multiple popular formats.

Step 10. After selecting the type of restore target in the previous step, you now need to select which partitions to restore. You can also select to convert GPT to MBR if needed.

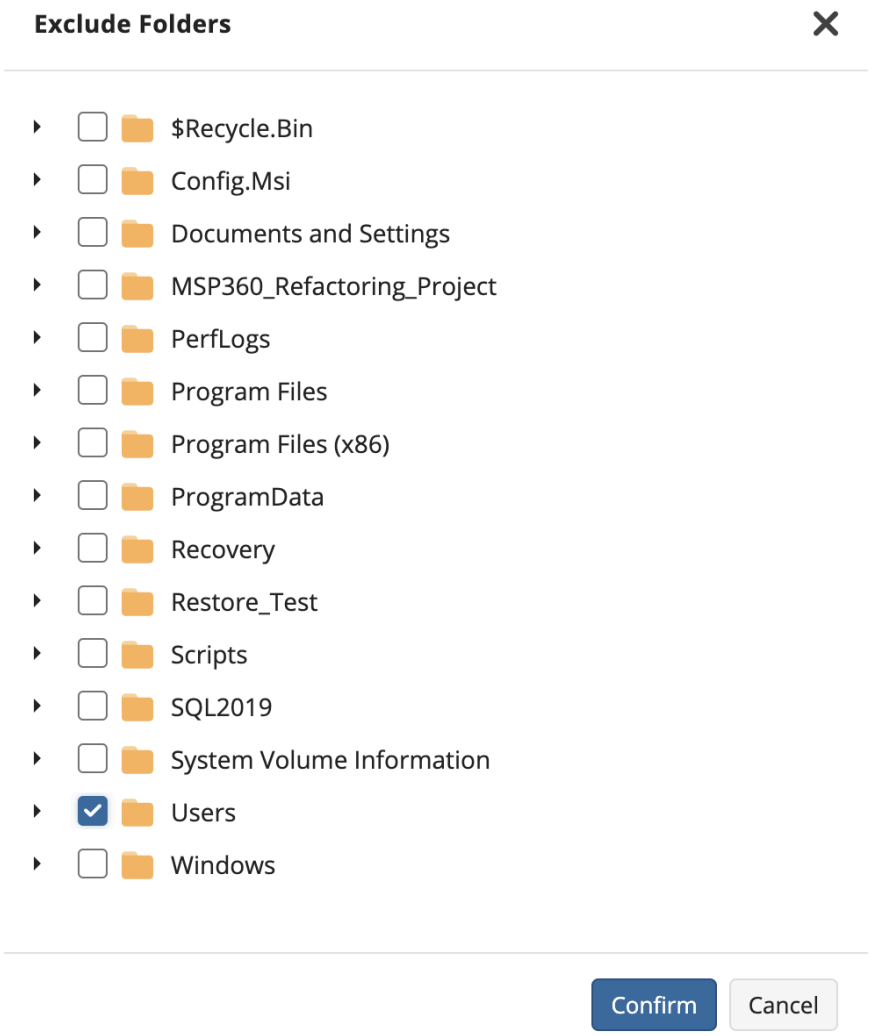


- **Covert GPT to BIOS/MBR:** Select this checkbox if the target instance or the target OS does not support UEFI boot and requires BIOS boot.

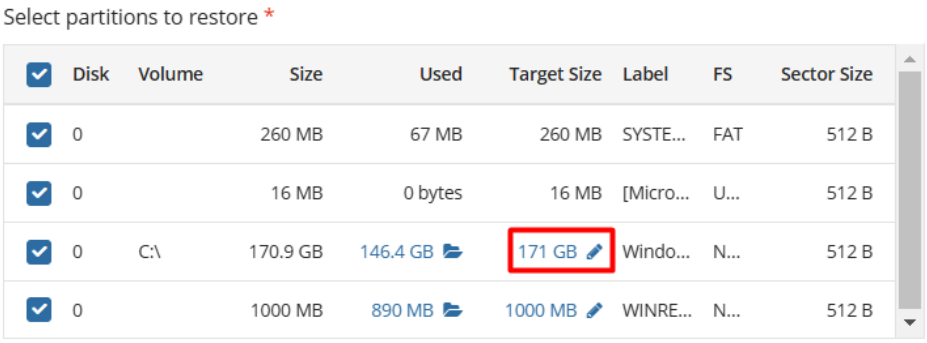
If you click on the highlighted in blue **used space** or folder icon, it will open an exclusion menu:



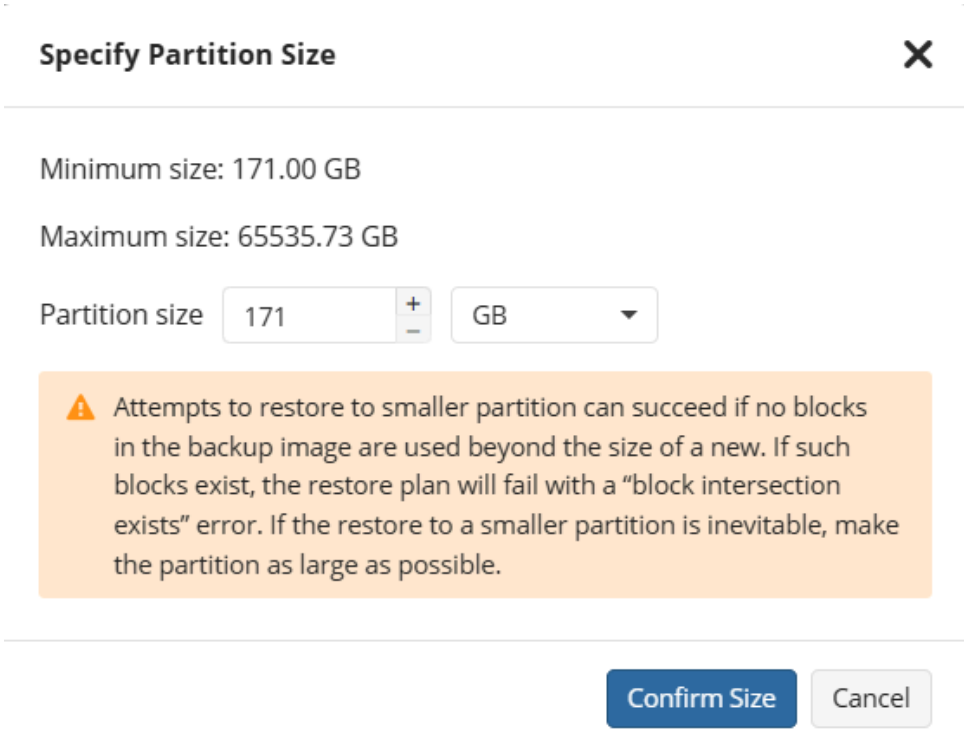
Using this menu, you can select folders you want to exclude from the restore job:



If you click on highlighted in blue **target size** or pen icon, it will open the partition size menu:

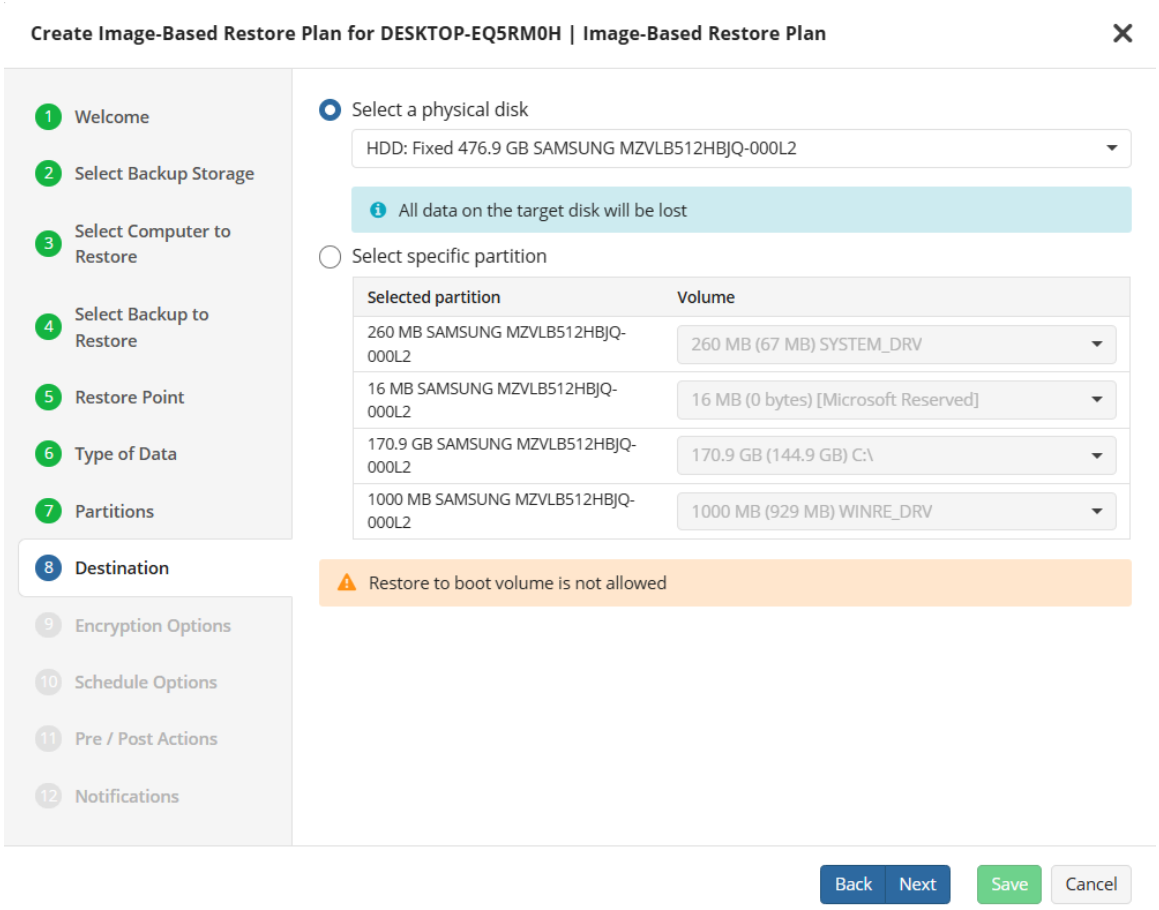


Using the partition size menu, you can extend your target partition:



> Attempts to restore to a smaller partition can succeed if no blocks in the backup image are used beyond the size of a new. If such blocks exist, the restore plan will fail with a "block intersection exists" error.

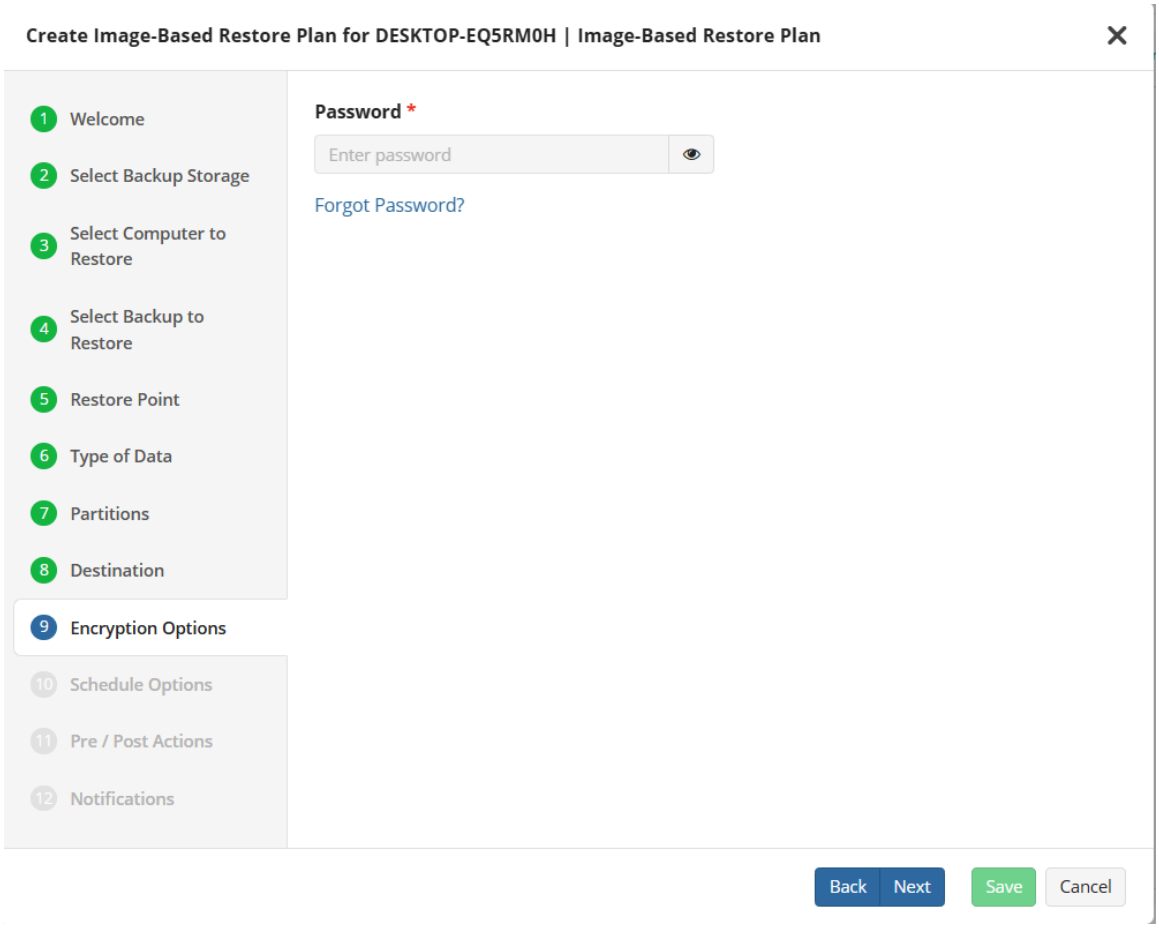
Step 11. After selecting the partitions to be restored, next you will be prompted to select the destination disk or partitions.



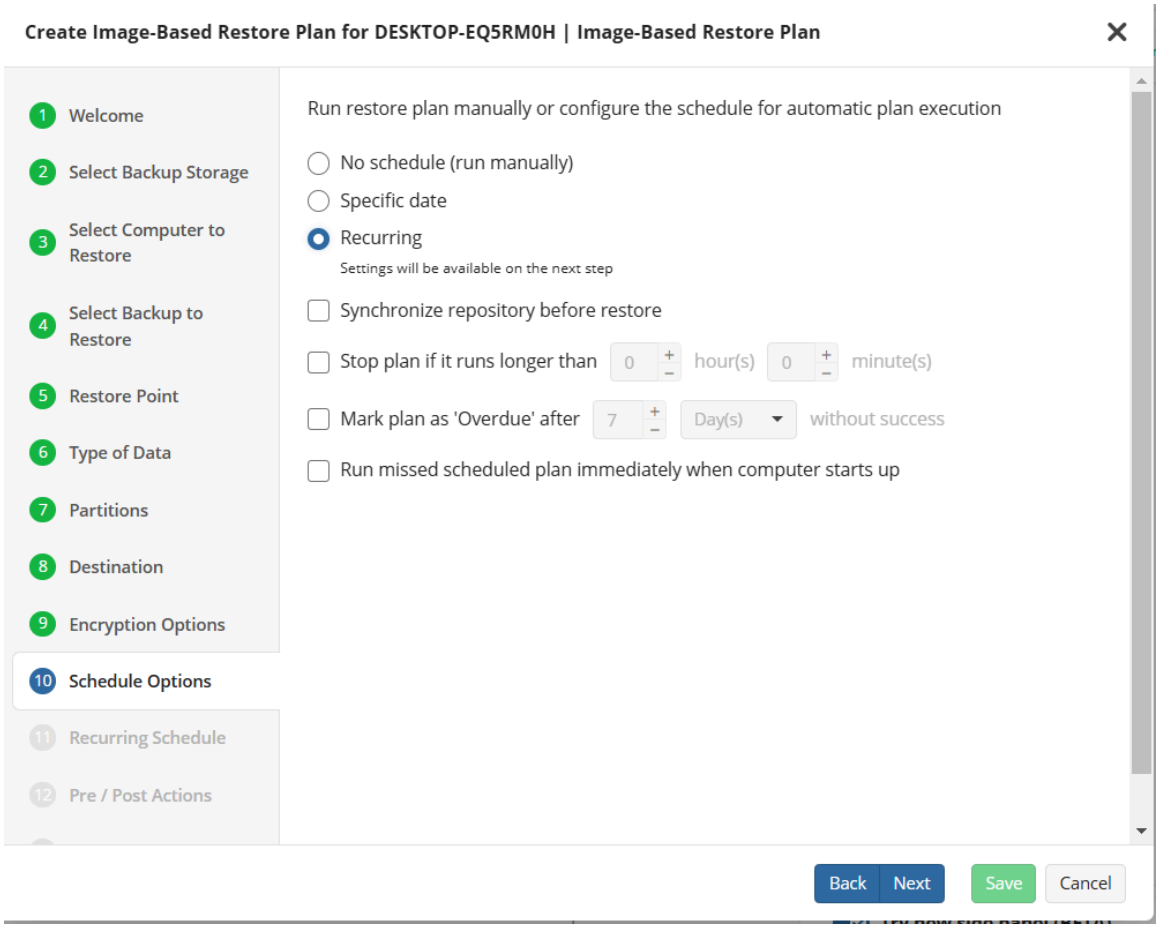
Be careful to select the correct target disk(s) and partition(s). All data in the selected targets will be permanently destroyed.

The application will now allow you to restore to the boot volume of the target computer from Windows or MBS. To restore the boot volume, use the Bare Metal Restore bootable USB.

Step 12. If the image backup dataset was encrypted, the restore plan will prompt you to enter the password.



Step 13. If the restore plan is saved for later, next you will set the schedule for the plan, otherwise proceed to the next step.



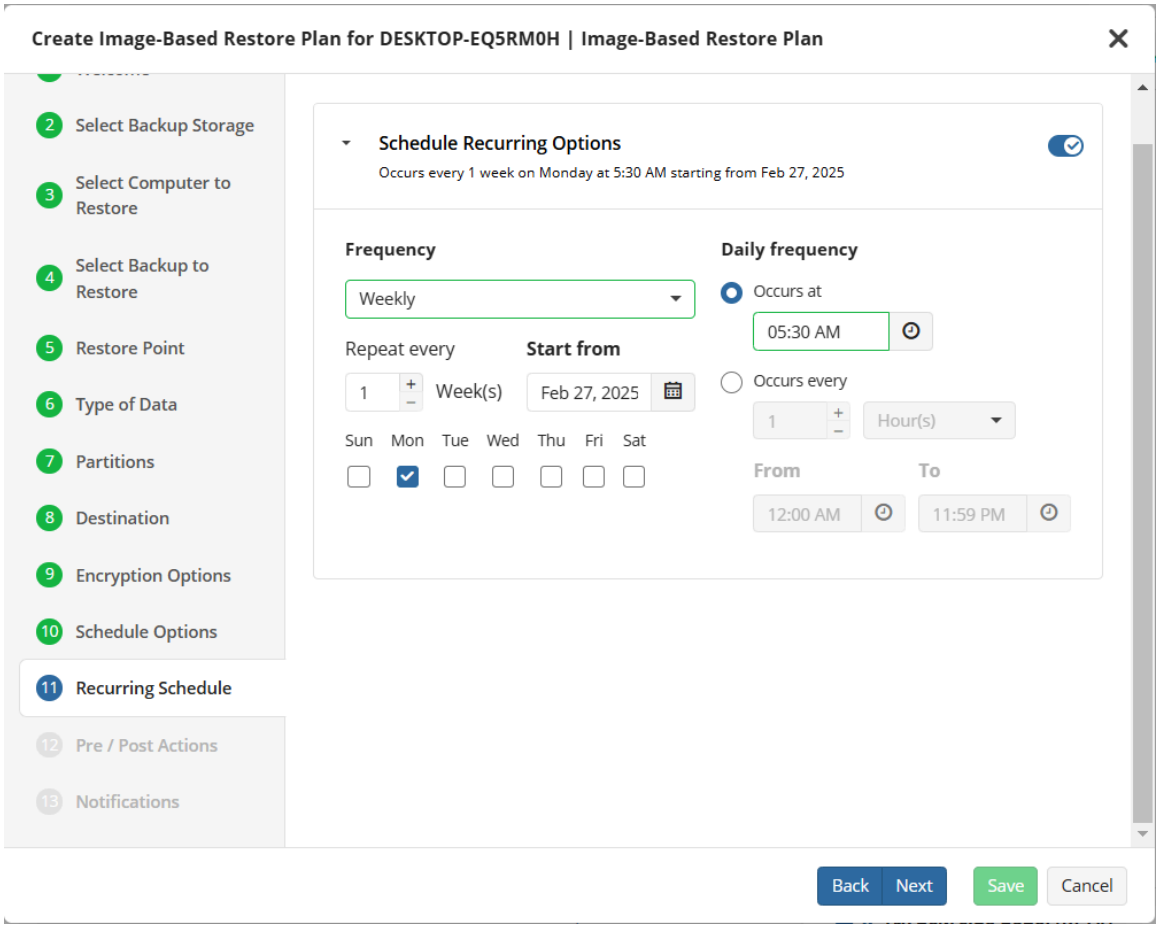
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option will add an additional step to the wizard which enables you to schedule recurring Restorations at custom intervals:

> It is recommended to **Synchronize repository before restore** if you are restoring a backup dataset for a computer different from the original or if you are signed in with a different backup user.

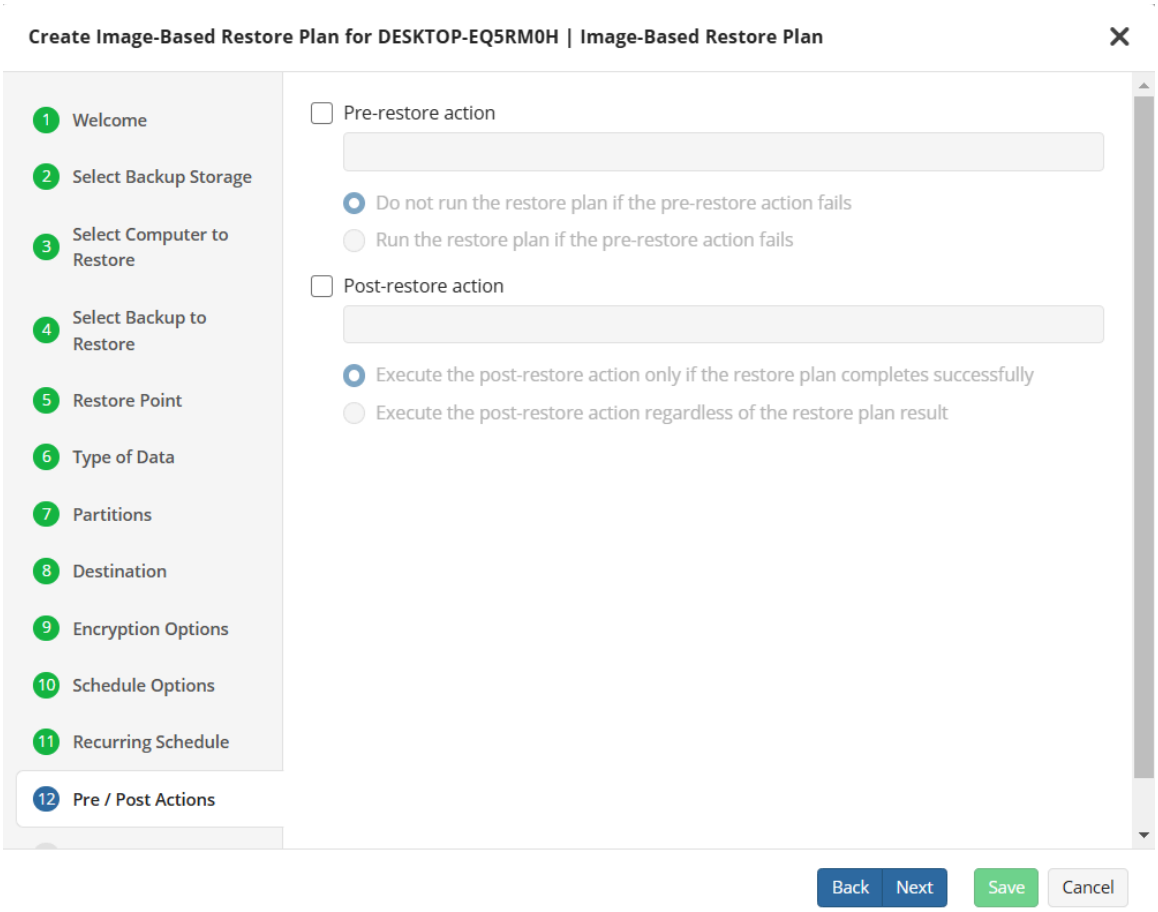
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

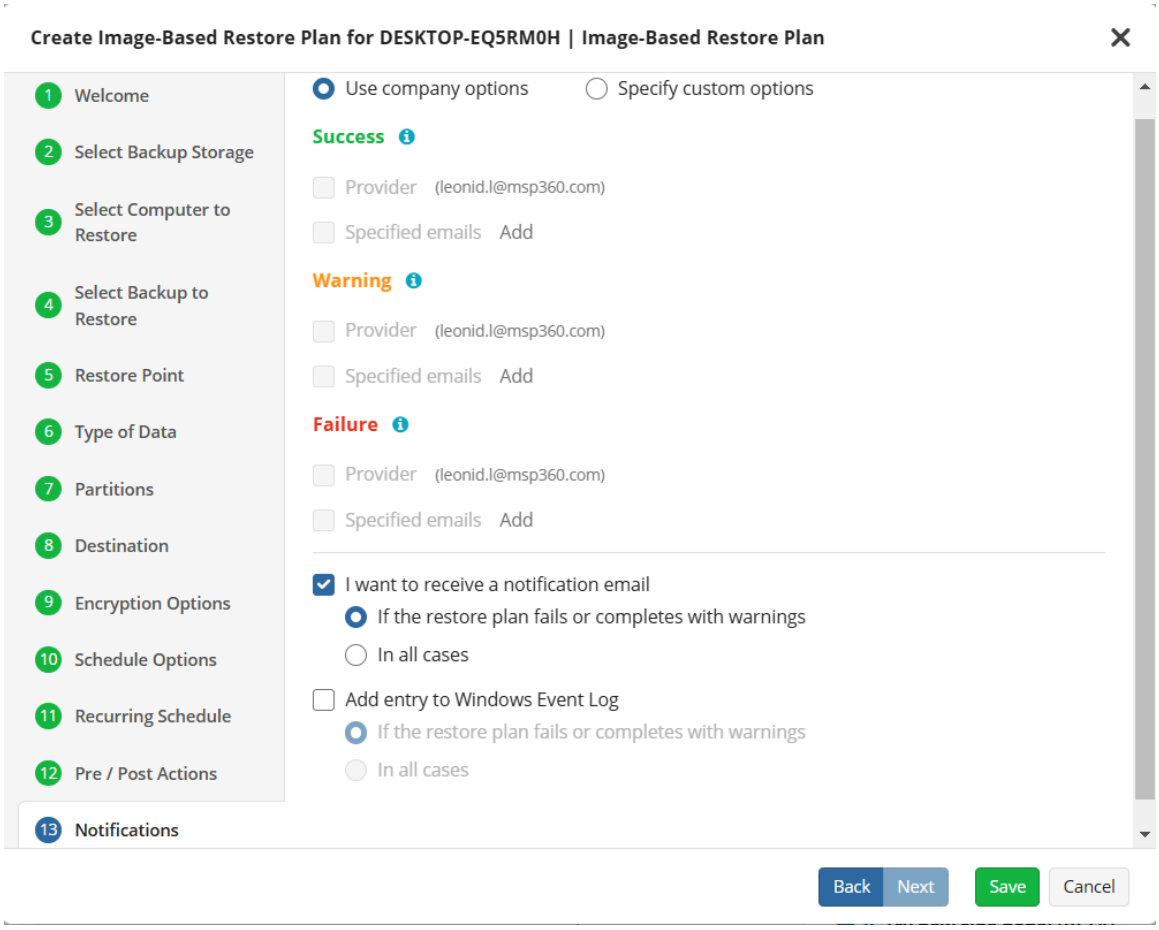
- **Recurring Schedule:** if you have selected the "Recurring" option, the next step will enable you to configure schedule based on the criteria in the fields below:



Step 14. The next step is to specify any Pre or Post Actions which should be triggered by the Restore Plan.



Step 15. Finally, specify any notifications you would like to receive when the plan runs.

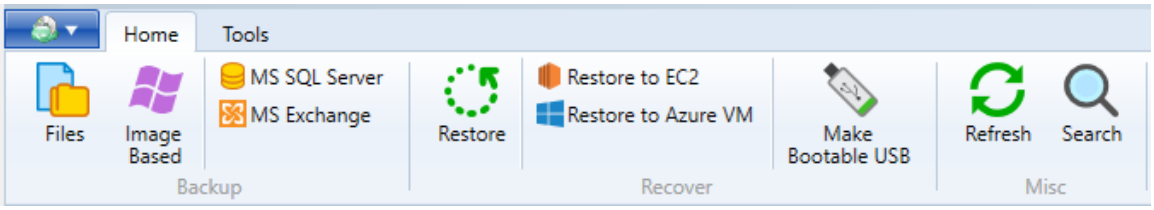


Step 16. Click on Save when you are happy with your selections. If the plan is set to run only a single time and has no set schedule, it will automatically start. Otherwise, if it is set to run only once and is scheduled, it will display in the list of plans until the scheduled time. If it is only set to run once, then when it completes successfully it will remove itself from the list of plans. Only Restore Plans which are saved will remain in the list for future use.

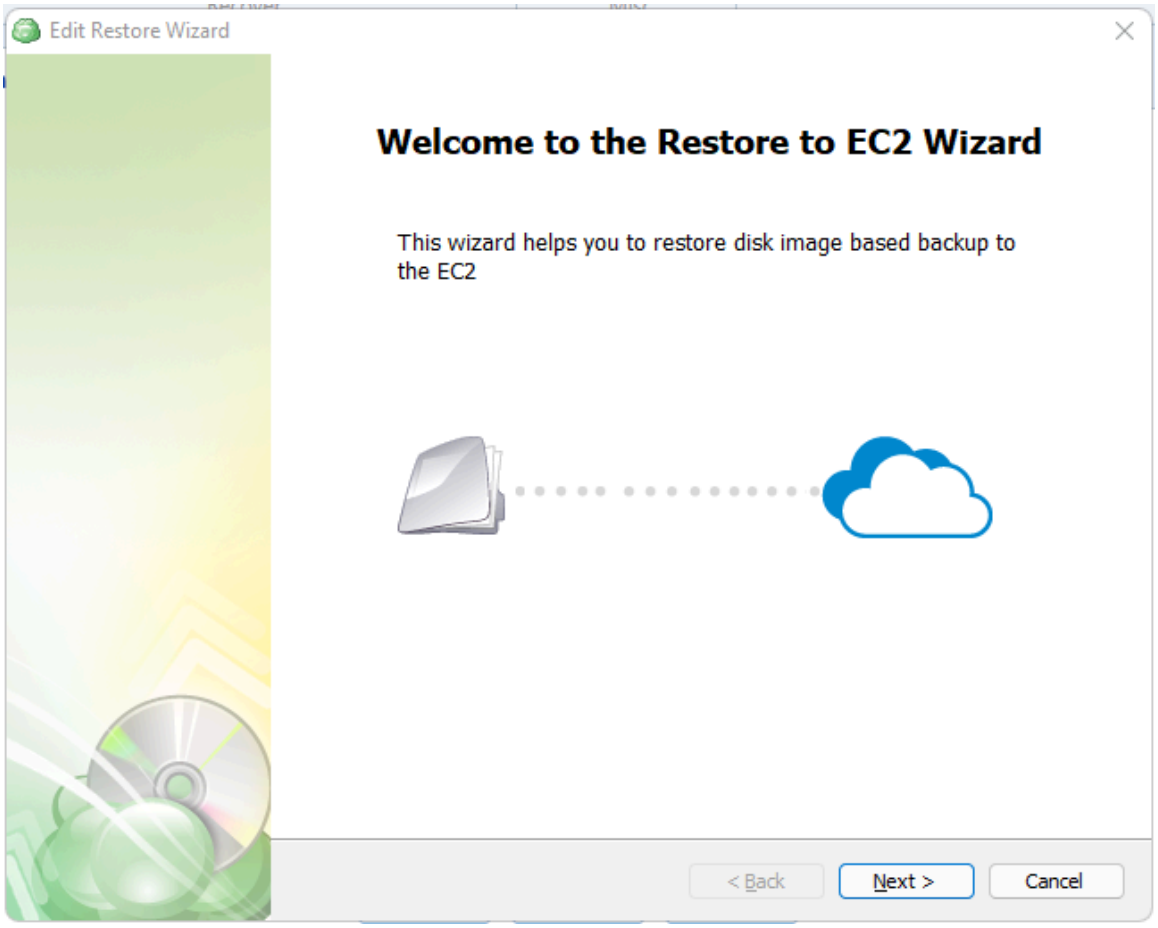
Restore to an EC2 Instance using the Agent

> Please note that in order to enable restore to EC2 and EBS capabilities, the **vmimport** role must be created in advance. You can find more info in the help article below:
> https://help.mspbackups.com/billing-storage/storage-providers/amazon/required-permissions

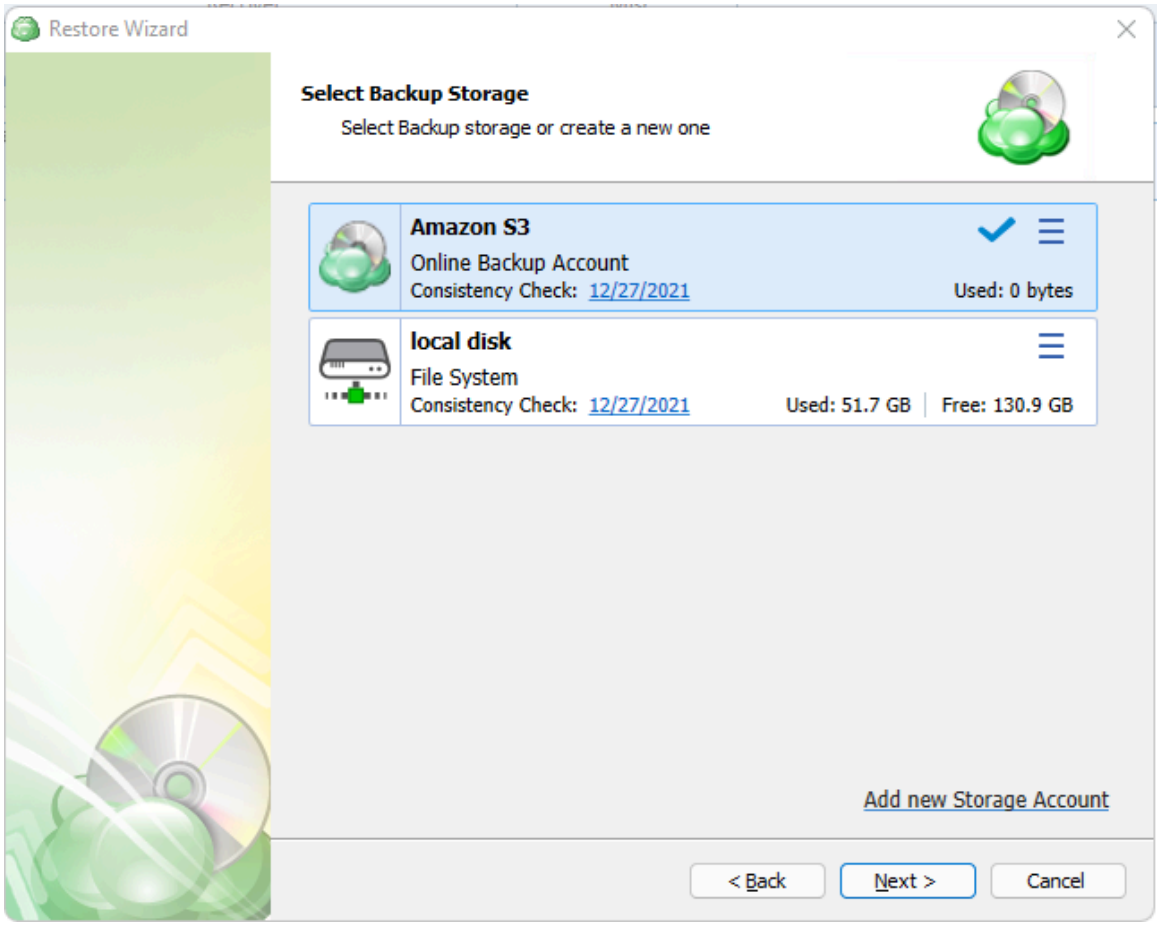
Step 1. After launching the Online Backup, click on “Restore to EC” in the top menu



Step 2. The first step of the wizard indicates that you have started the wizard.

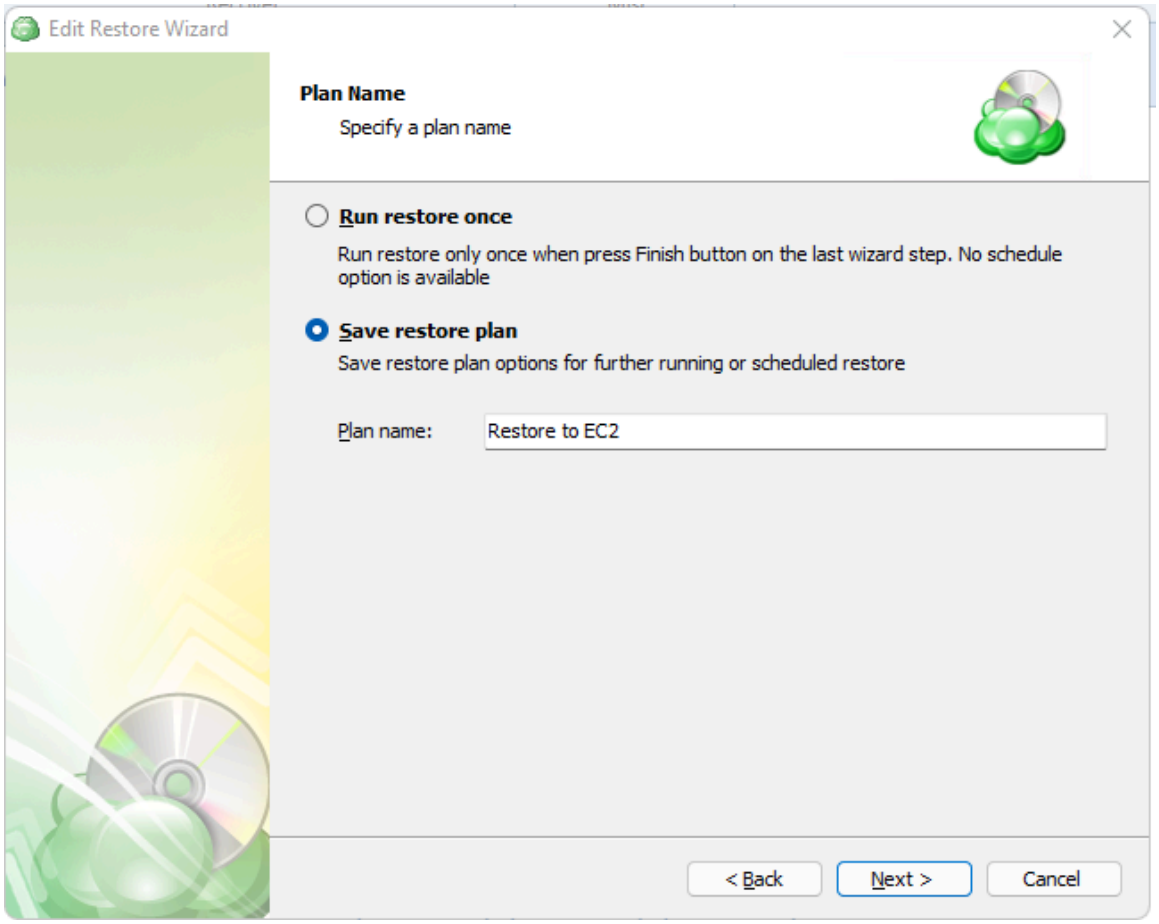


Step 3. The next step will prompt you to select the storage location for the source.

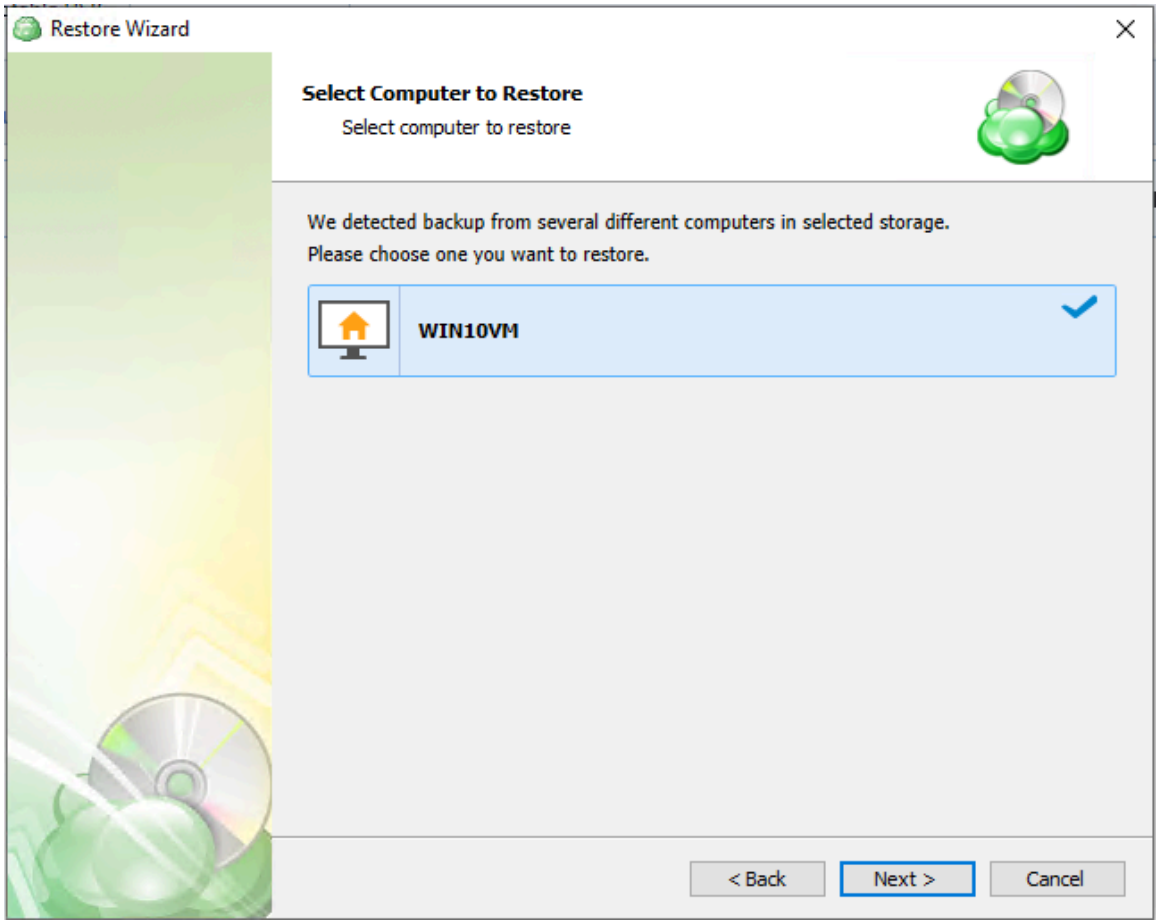


If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

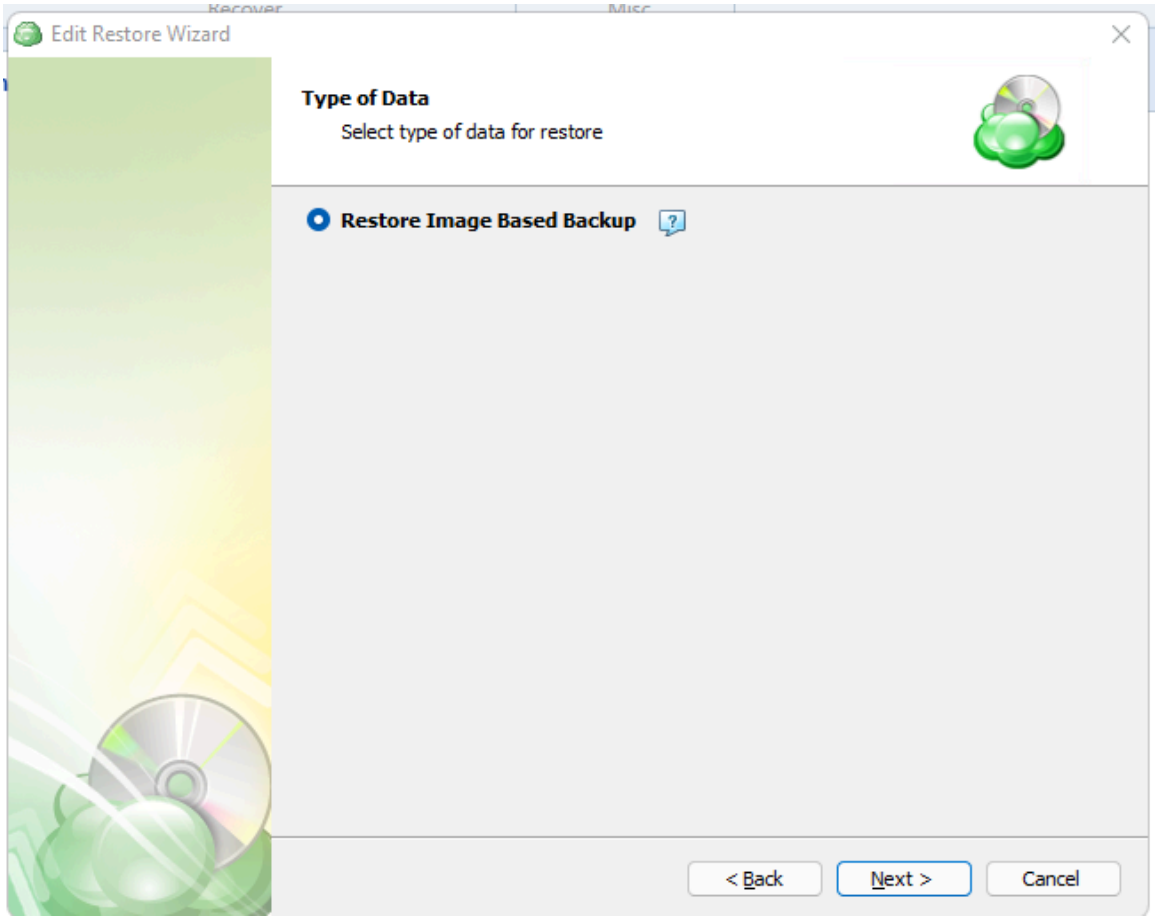
Step 4. Next you will choose whether to run the restore operation only once, or to save it for later use. The latter will allow you to name the plan.



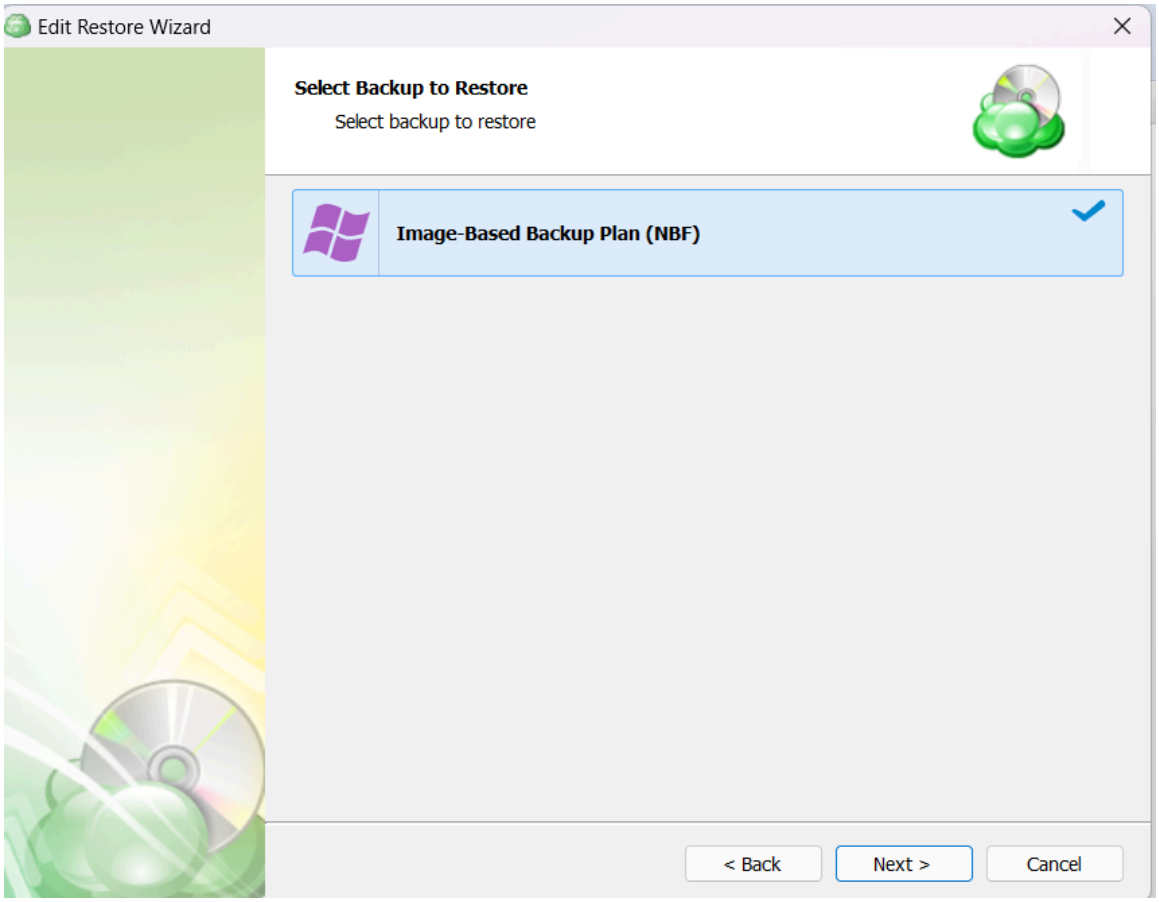
Step 5. Next you will be presented with a list of computers with the same prefix and associated "Backup User" as the computer on which the Agent is currently running. Click to select the desired computer then click on "Next".



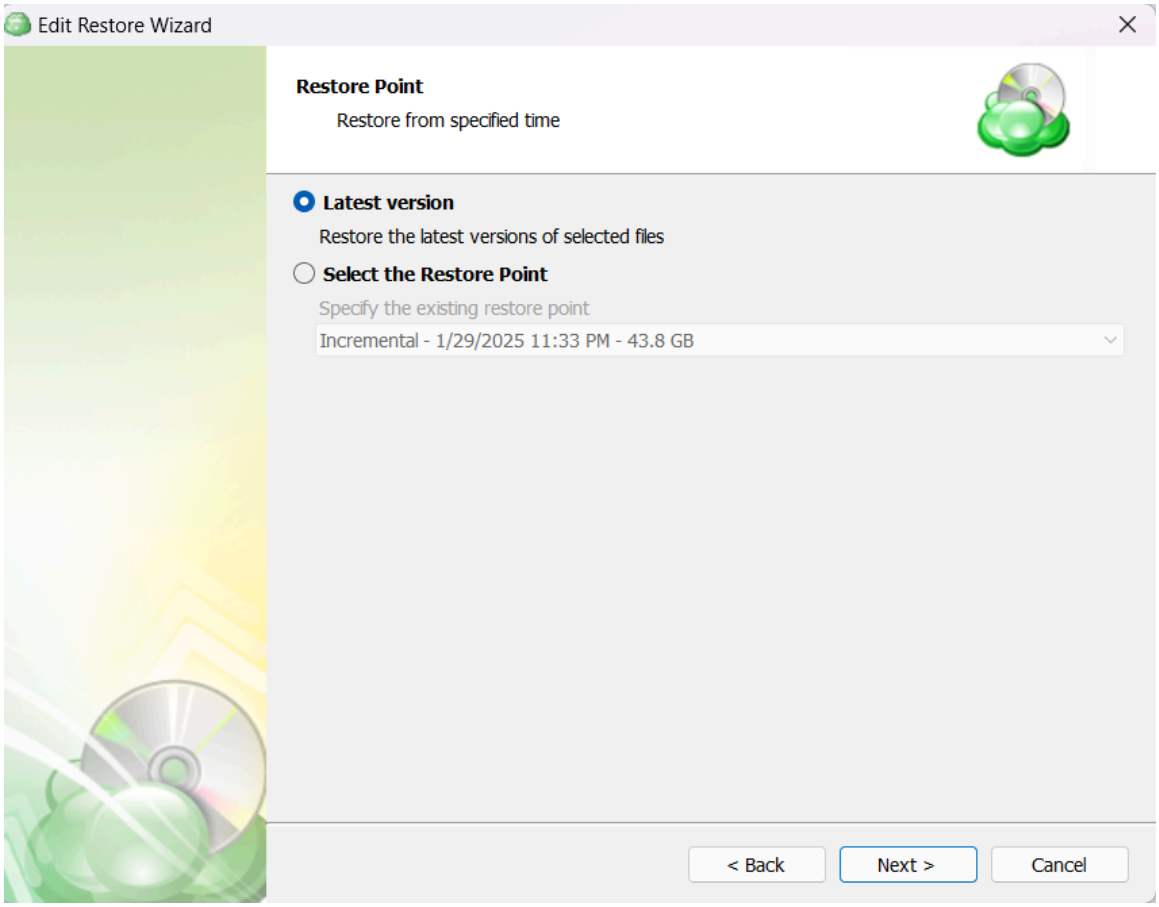
Step 6. Based on the contents of the selected source and computer, the next step is to choose the type of restore. Select “Restore Image Based Backup” then continue to the next step by clicking “Next”.



Step 7. With the correct type of restore selected, the application will generate a list of available backup plans.

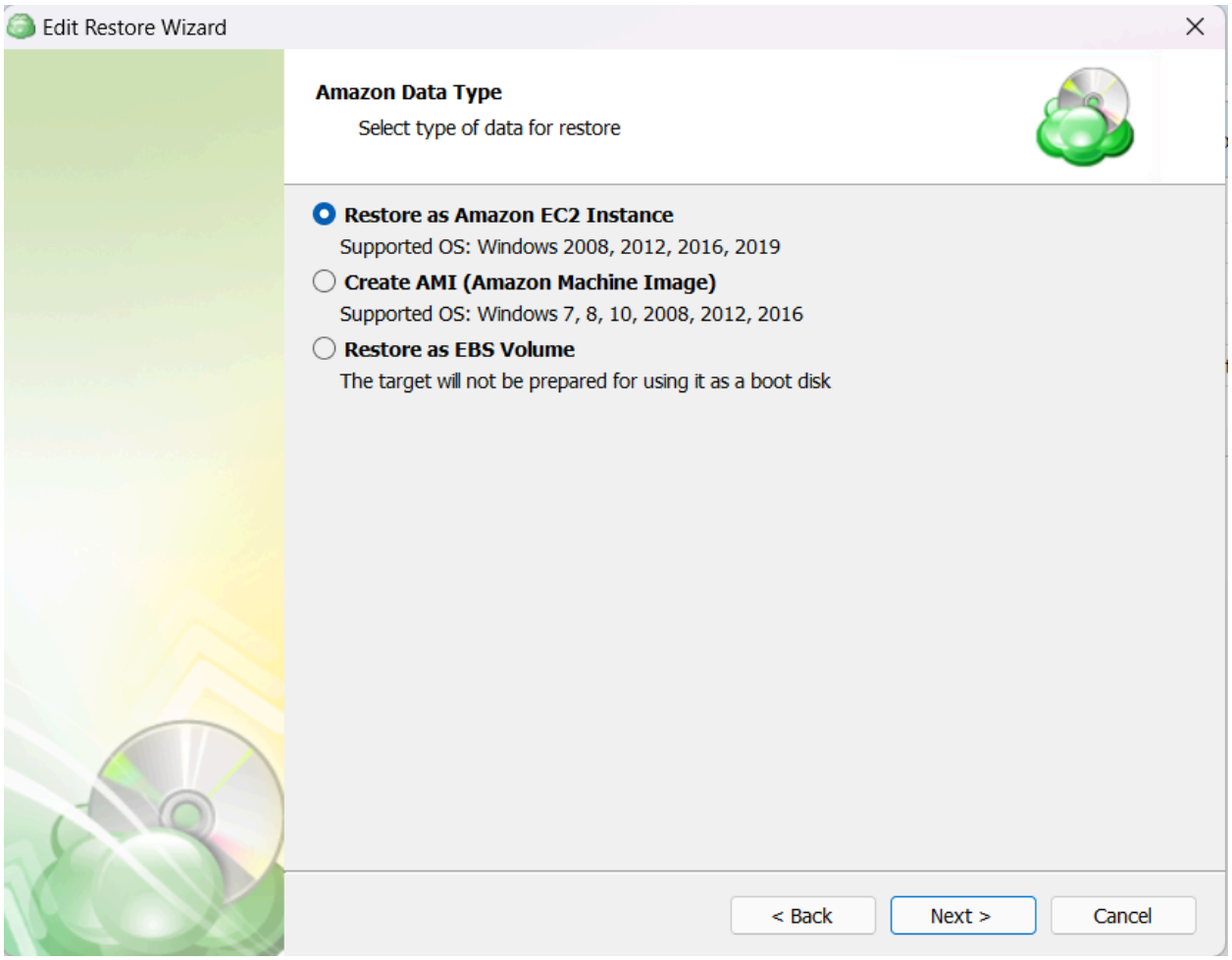


Step 8. The next step is to select the desired point in time to restore to.



- **Latest Version:** Automatically restores the most recent backup restore point.
- **Select the Restore Point:** Allows you to select a specific restore point (date) to restore.

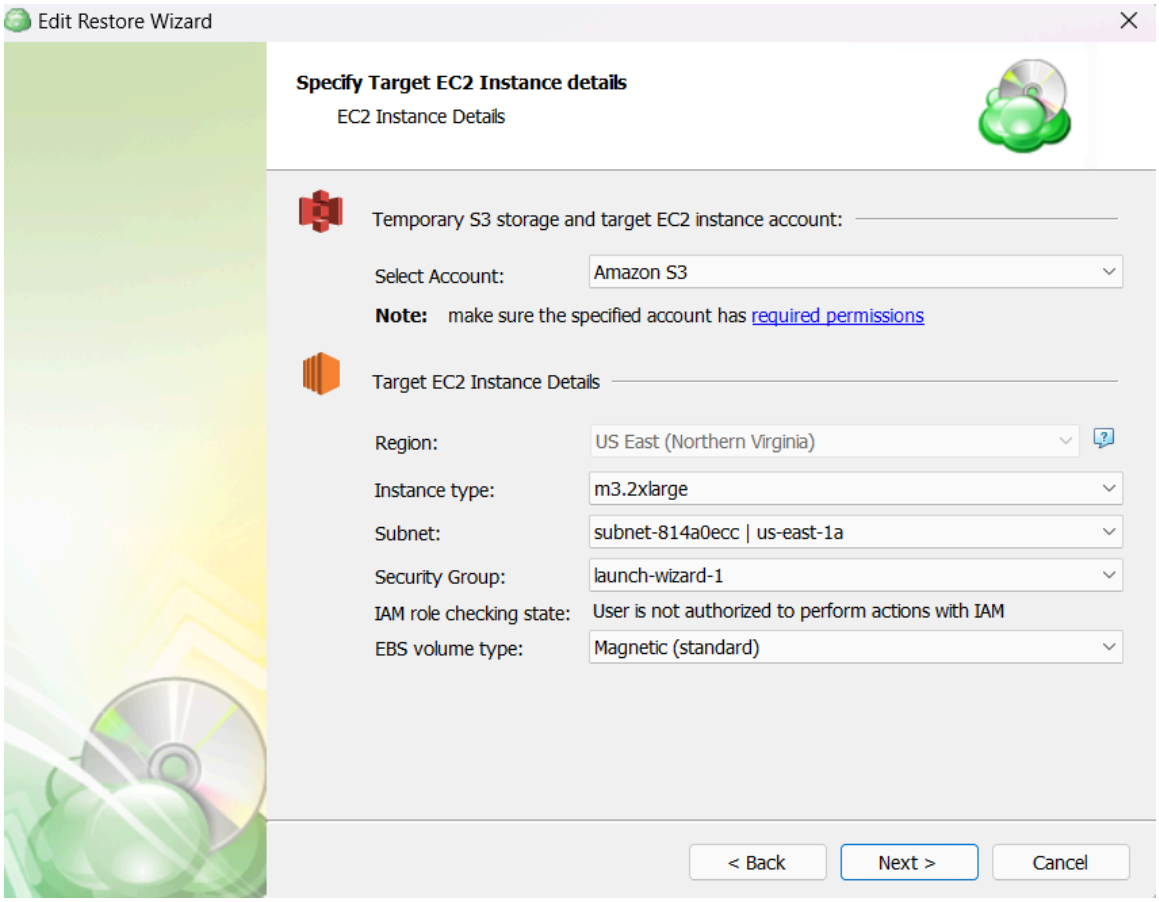
Step 9. Next, select the desired target format for the restored data



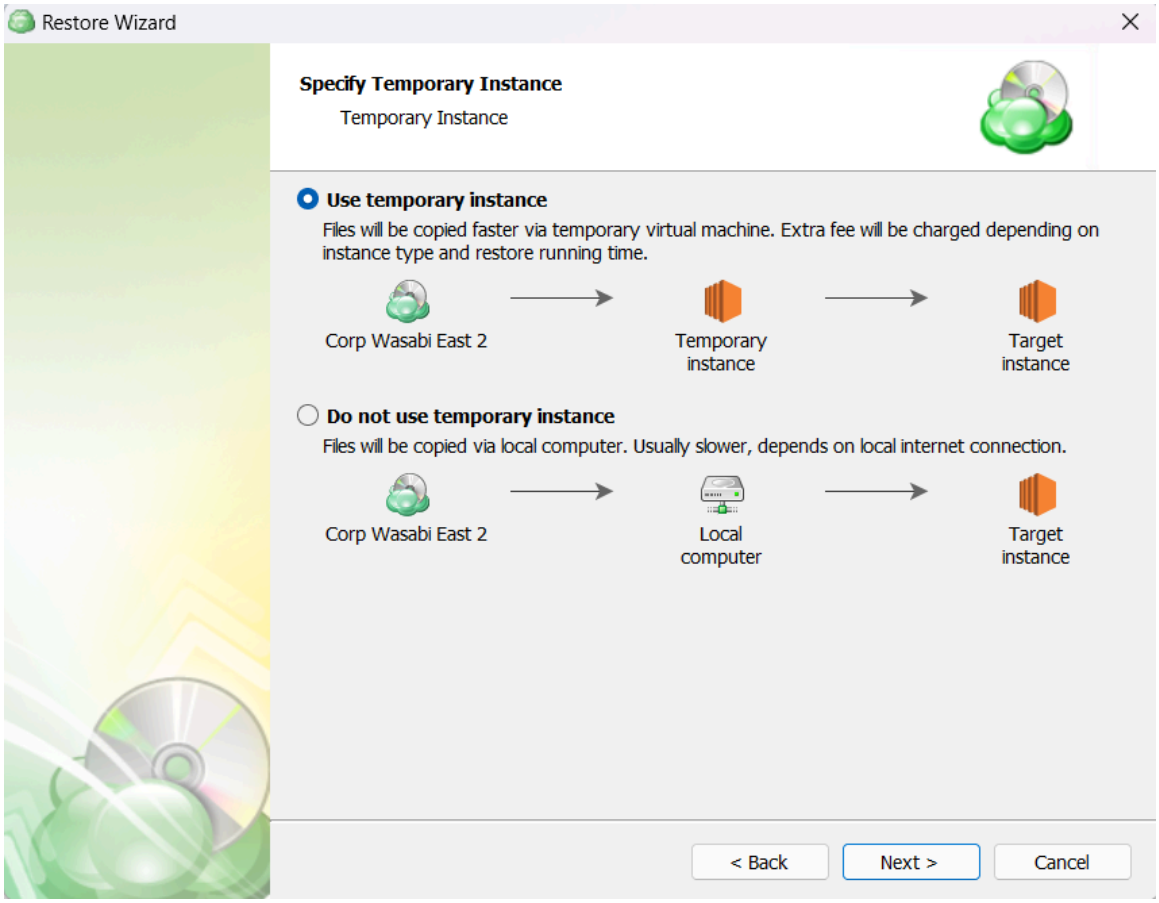
- **Restore as Amazon EC2 Instance:** Restores the partitions selected later to a physical disk.
- **Create AMI (Amazon Machine Image):** Restores the data as a virtual disk in multiple supported formats.
- **Restore as an EBS Volume:** Restores the data as either an EC2 machine, EBS volume, or Amazon Machine Image.

For AWS and Azure destinations, a storage account must already be specified through the MBS portal

Step 10. After selecting the type of restore target in the previous step, you are prompted to specify the parameters of the new EC2 instance.



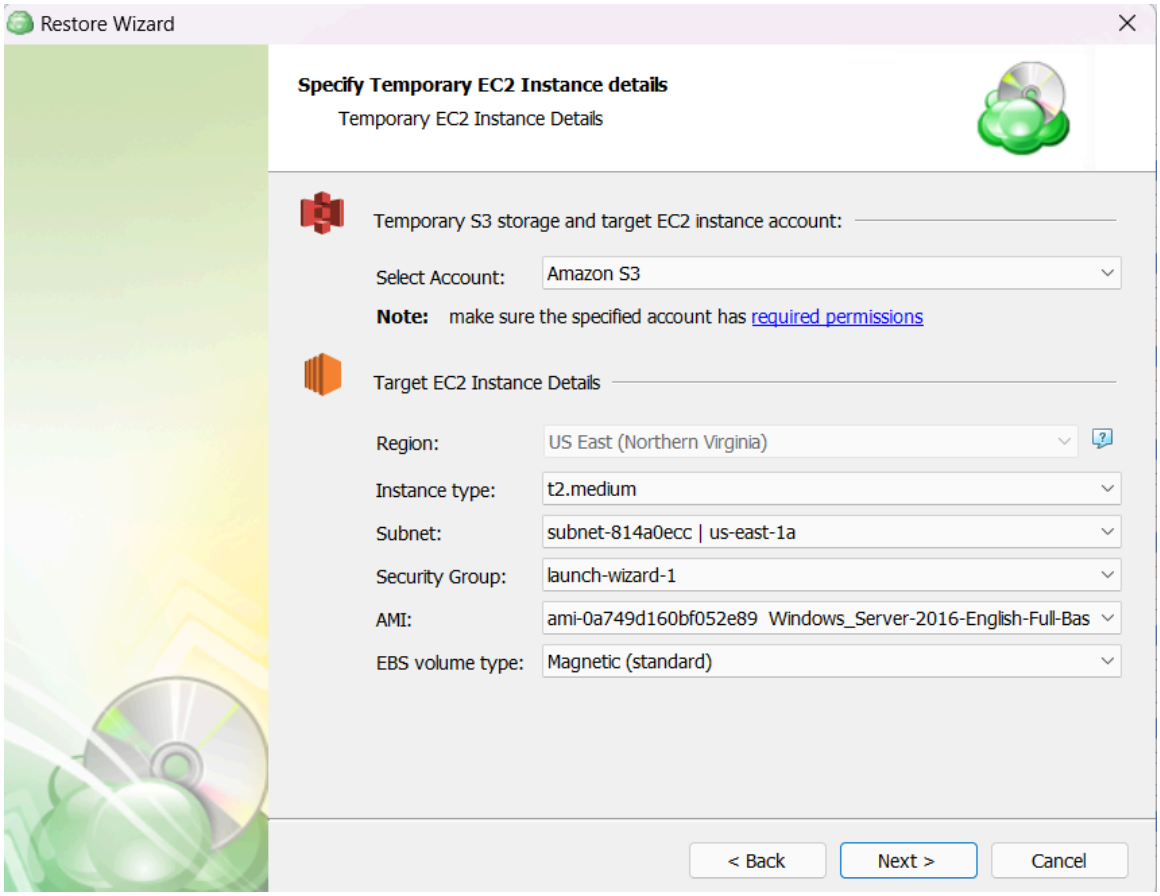
Step 11. After specifying the target EC2 instance details, you will need to choose between using a temporary EC2 instance or local computer for the restore operation.



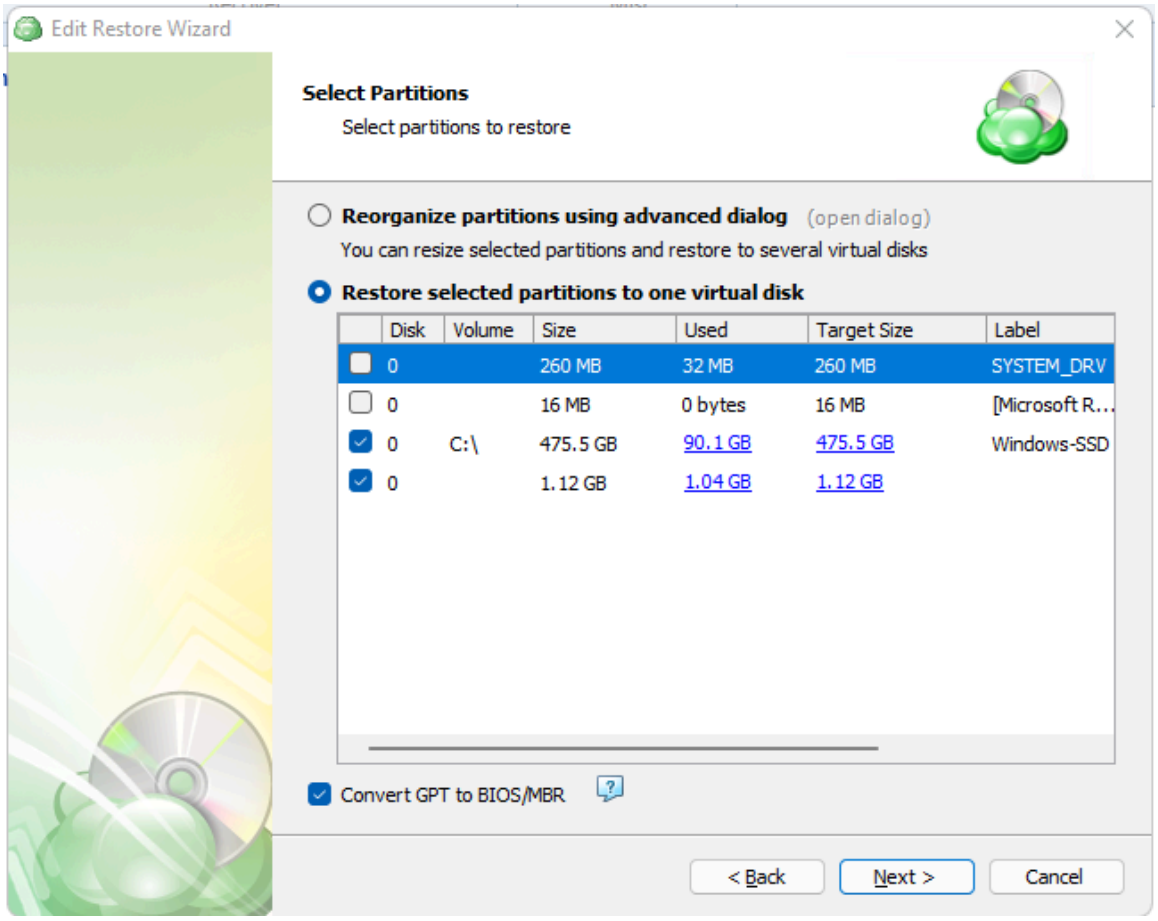
- **Use temporary instance:** This option creates a temporary EC2 instance in Amazon Web Services that will download backup data from the storage destination and restore it as a target instance. Usually, this method is faster as the temporary and target instance are located in the same AWS network.
- **Do not use temporary instance:** When selecting this option, the restore operation will be performed using the resources of the local computer. Usually, this approach is slower, depending on the local internet connection.

> Enabling the "**Use temporary instance"** option will lead to additional charges in Amazon Web Services for running the temporary EC2 instance. Please check the AWS documentation on instance types and pricing for more information.

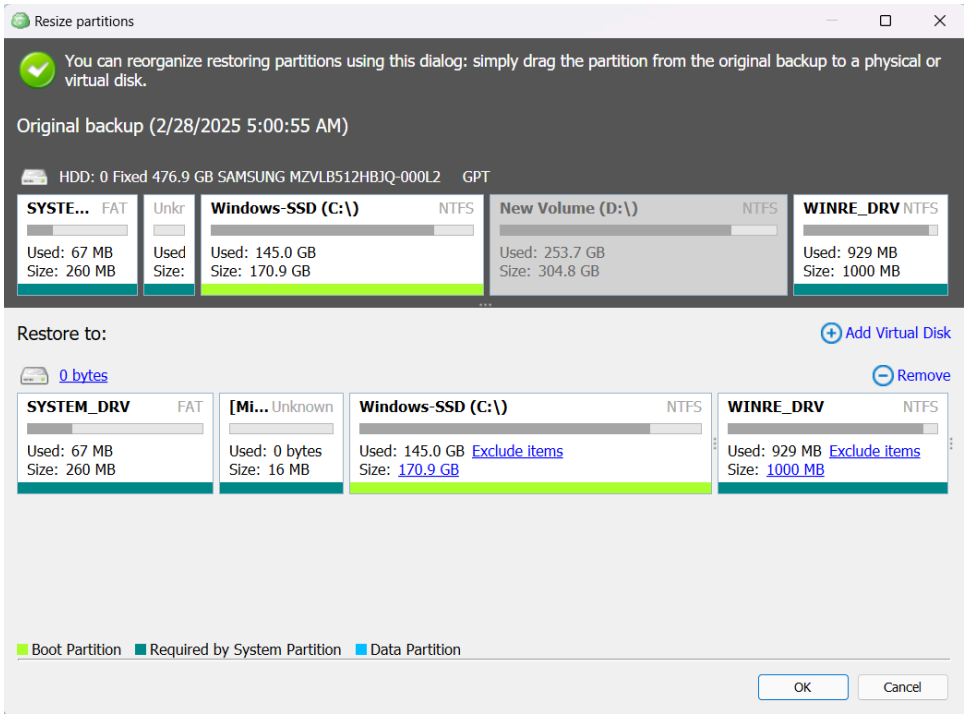
Step 12. If you have selected to use a temporary instance, the next page will allow you to select the Amazon account from the upper dropdown box, and specify the Temporary EC2 Instance details below.



Step 13. After selecting the type of restore target in the previous step, you can now choose to restore the partitions with their existing parameters or to reorganize and resize them.

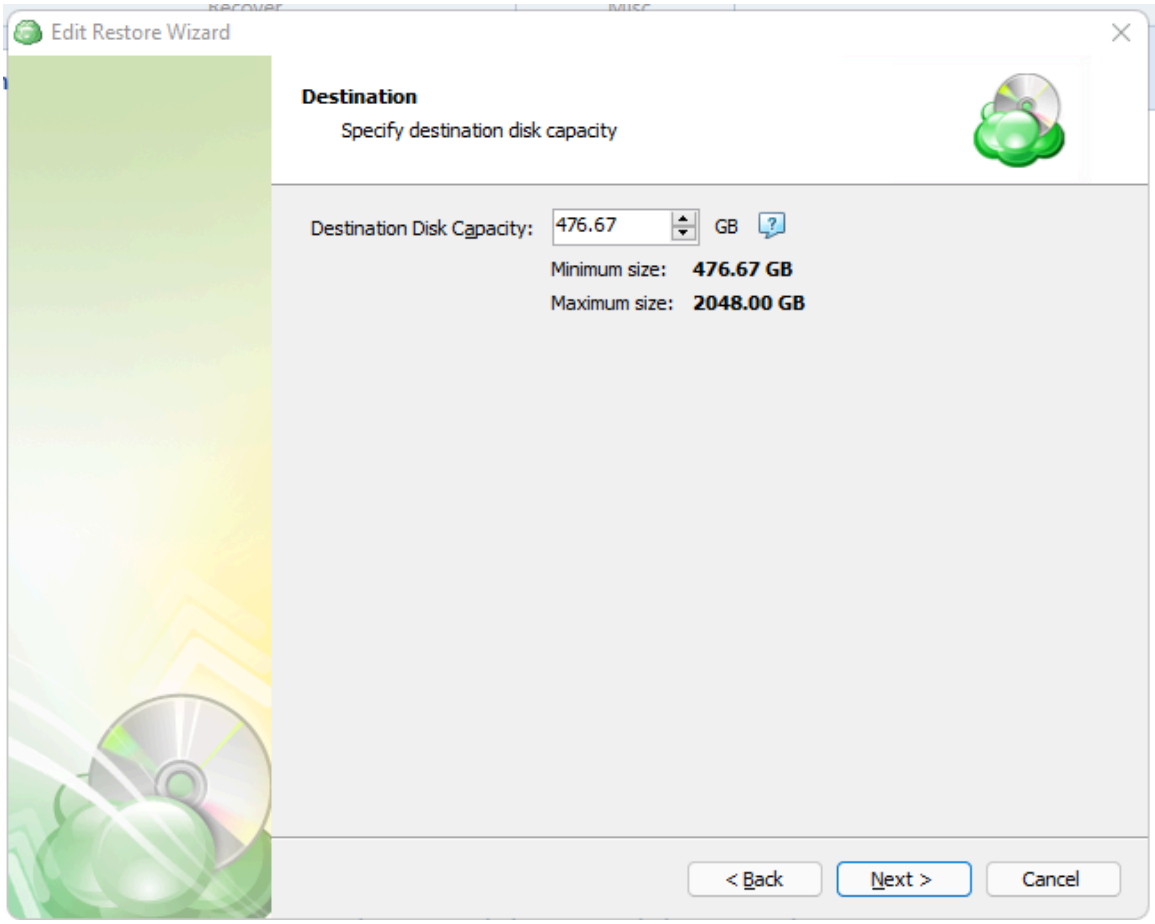


If you select “Reorganize partitions using advanced dialog” a new window will appear and allow you to resize the partitions and rearrange them on one or more virtual disks.

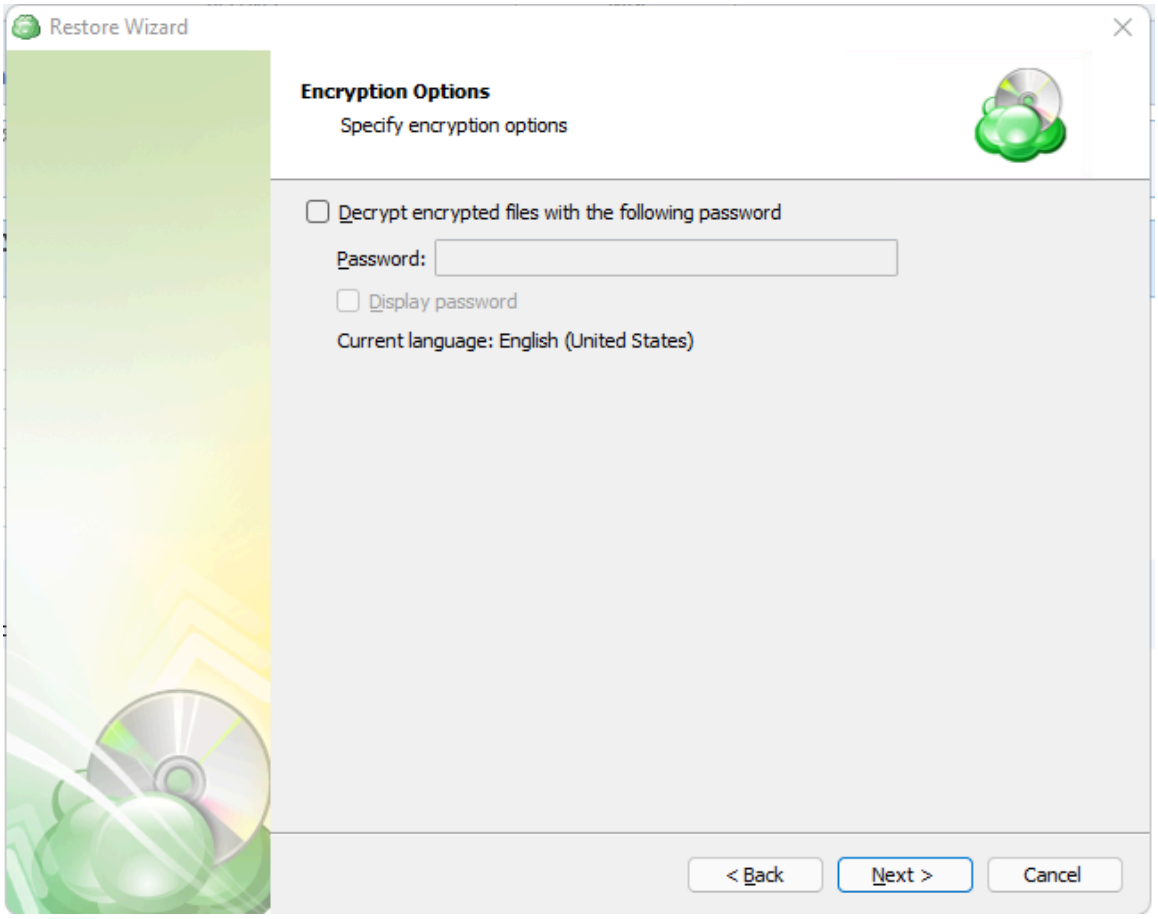


Click on any of the blue hyperlinks to open additional dialogue boxes allowing you greater control over the name and size of the virtual disk, as well as the ability to add additional virtual disks, and also exclude specific files or folders if desired.

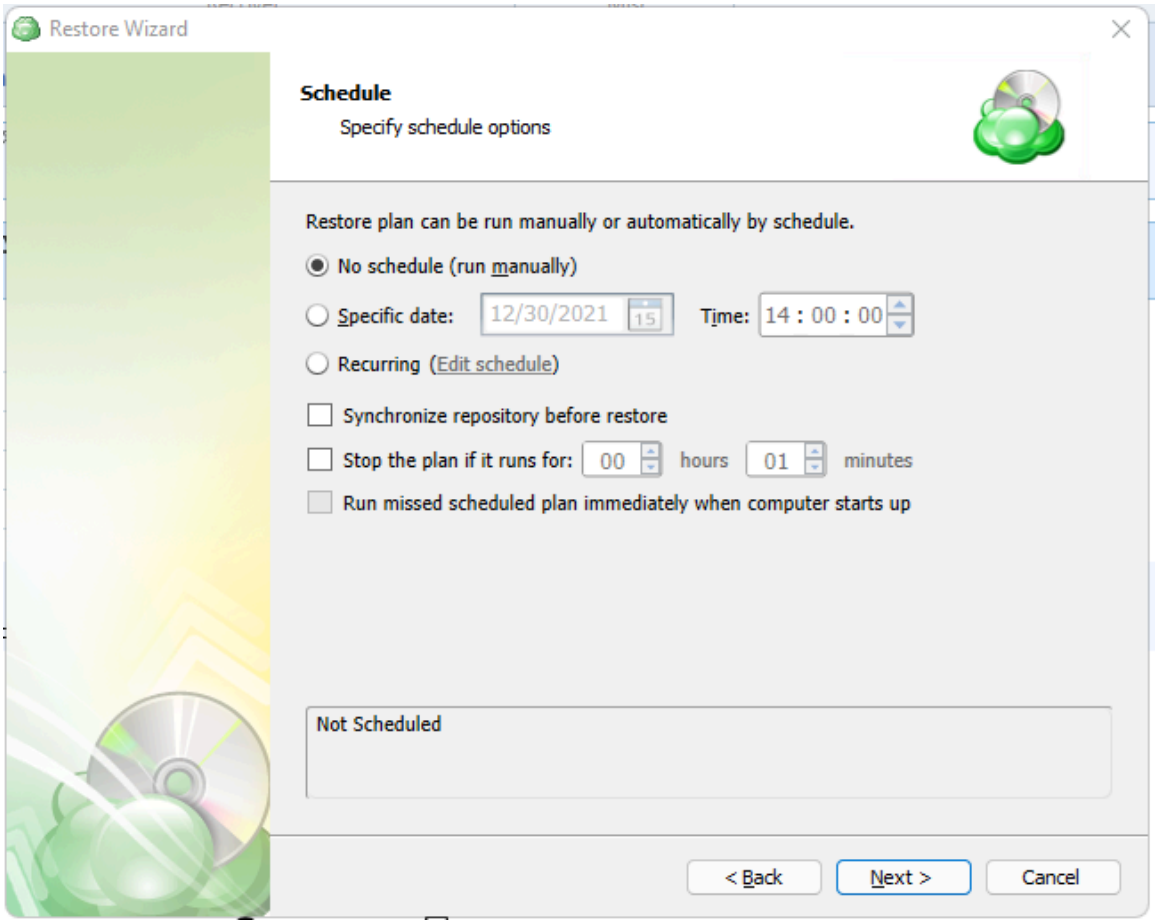
Step 14. Once the partitions are selected, the next step allows you to choose the size of the virtual disk used by the instance.



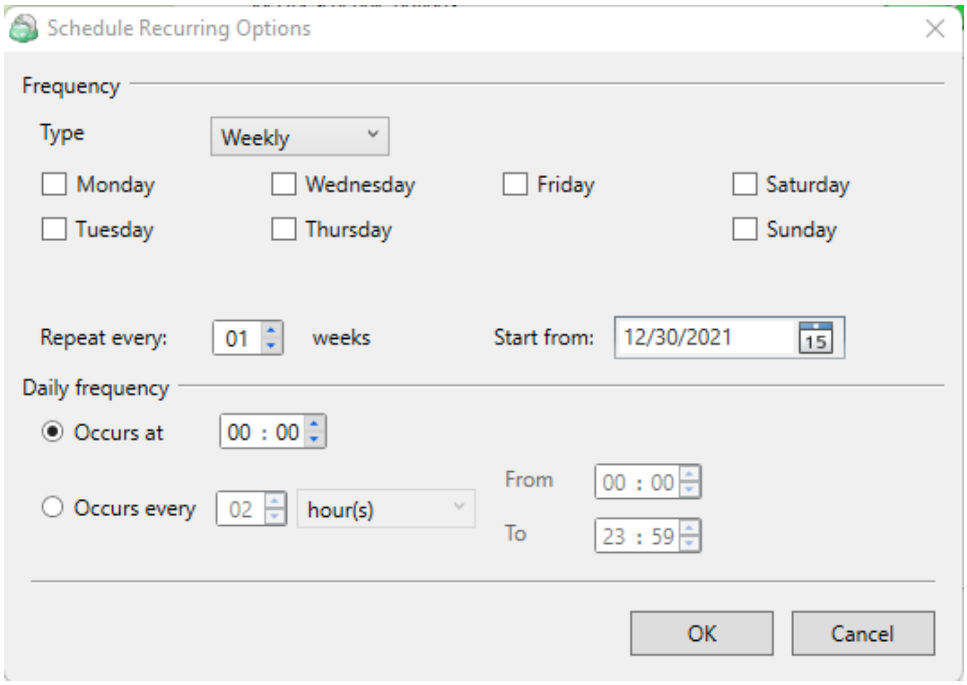
Step 15. If the backed up data was encrypted, the next step will be to enter the password for decryption. If the password is incorrect or missing, the restore plan will fail and you will need to edit the plan to input the correct password.



Step 16. If the restore plan is saved for later, next you will set the schedule for the plan, otherwise proceed to the next step.



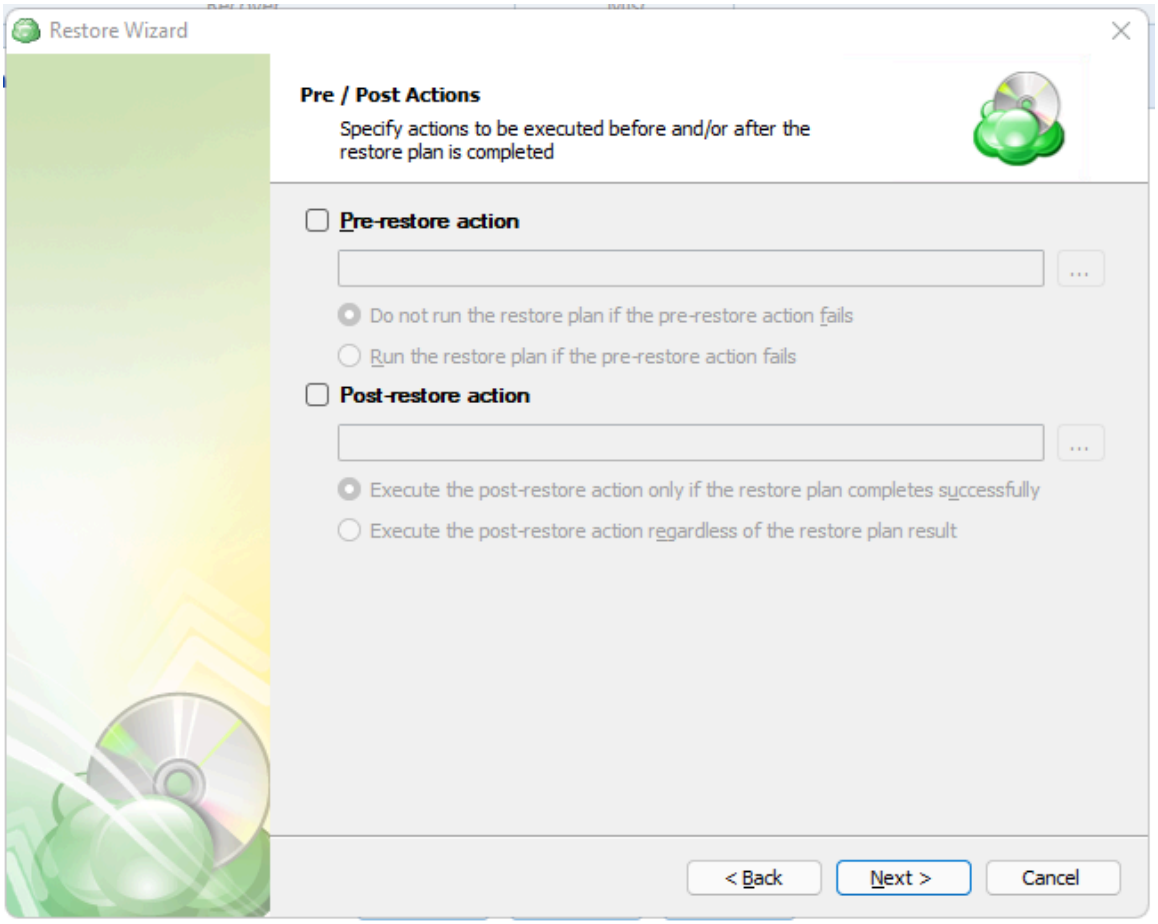
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria by clicking on the “Edit schedule” hyperlink to open this dialogue:



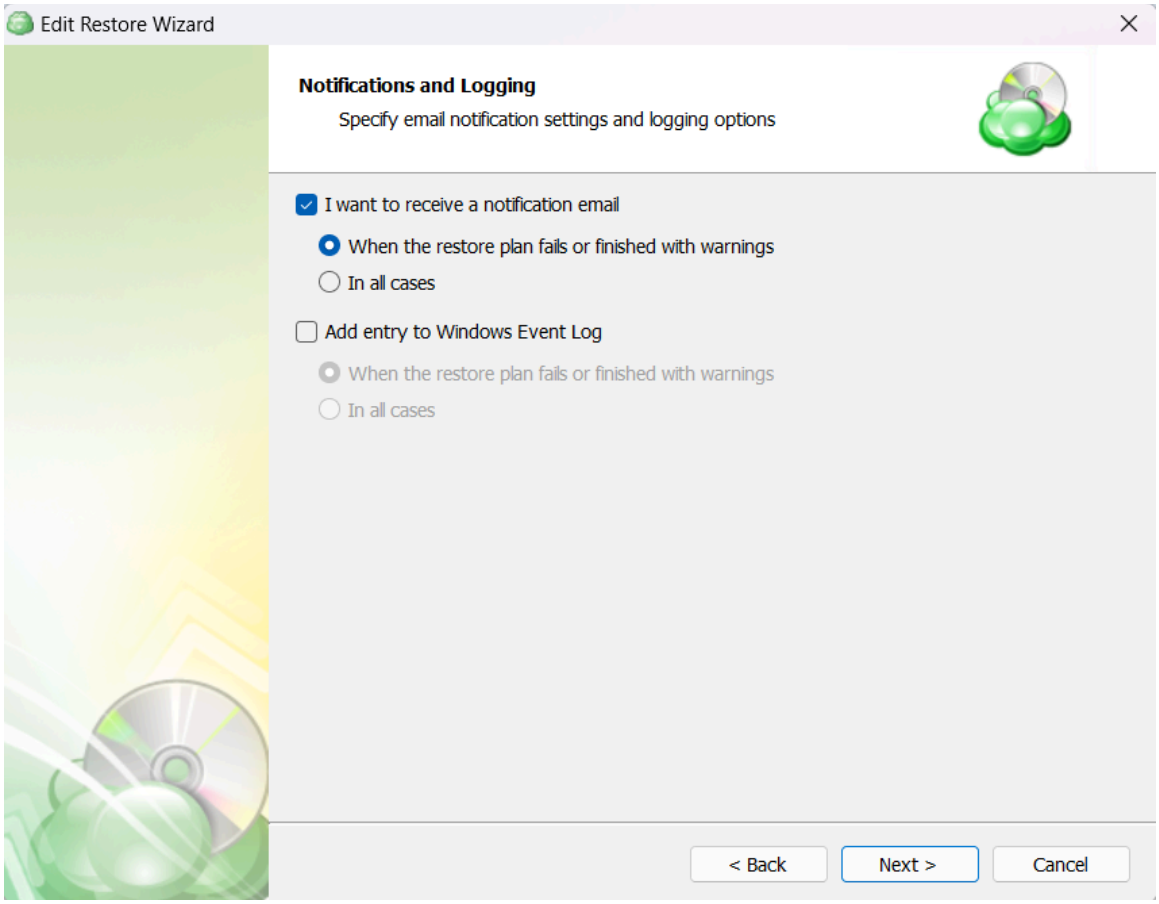
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

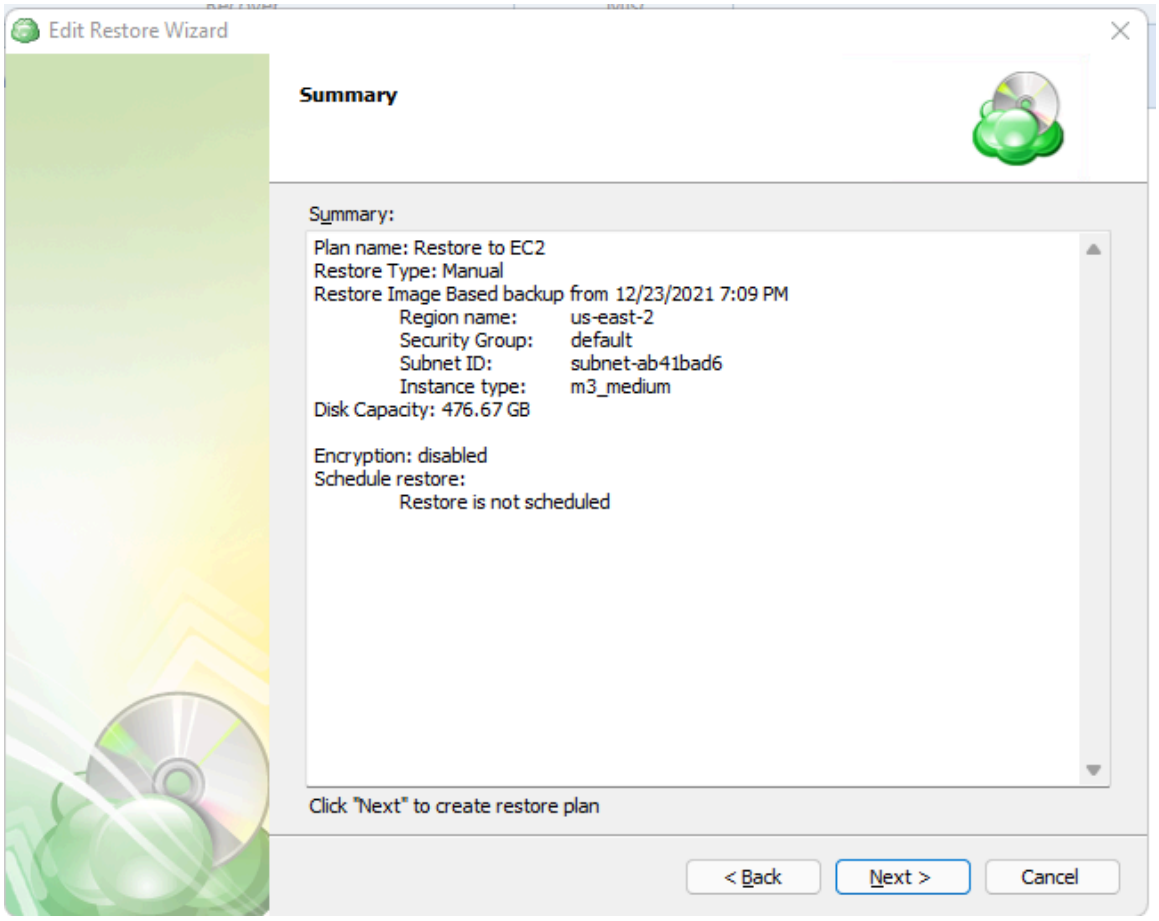
Step 17. The next step page allows the execution of custom scripts before and/or after the running of a Restore Plan.



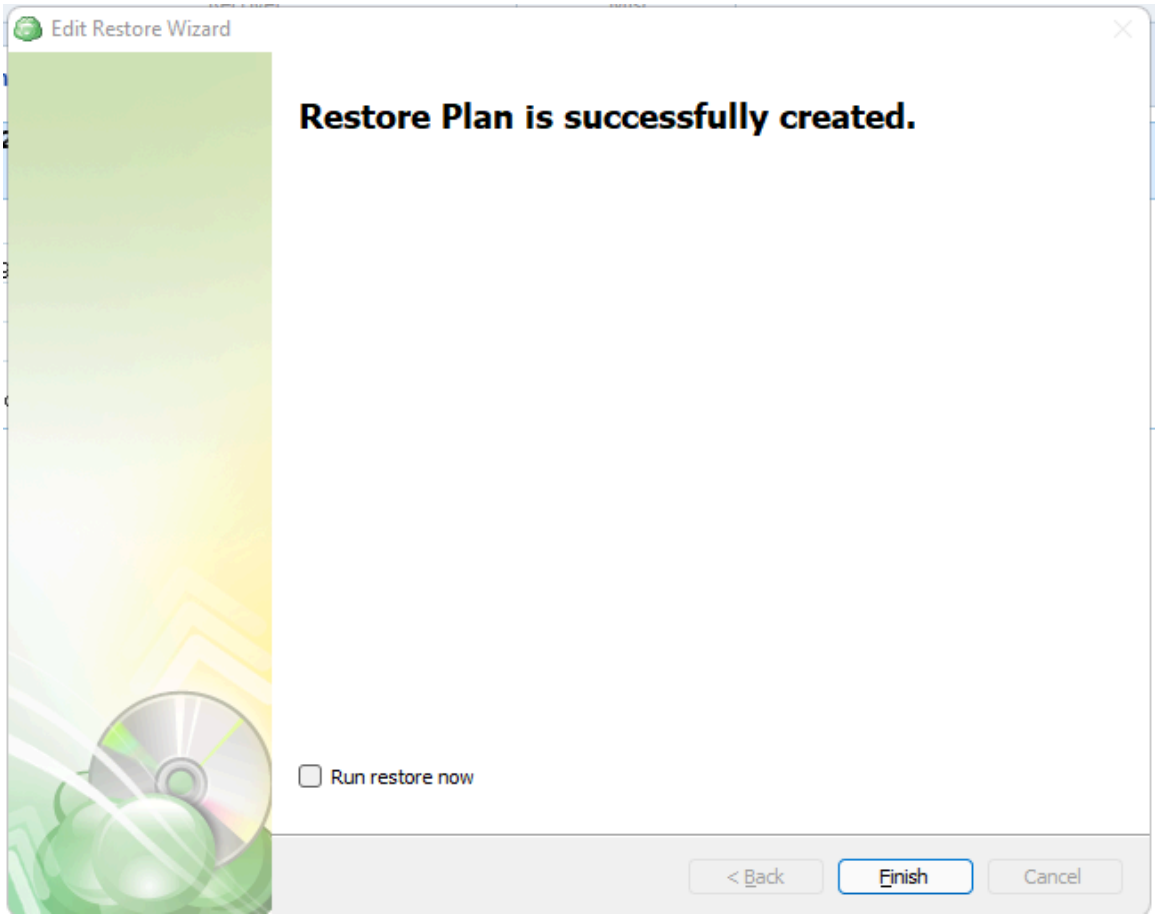
Step 18. The “Notifications and Logging” page allows you to enable notification email and add an entry to Windows Event Log upon restore plan completion or failure.



Step 19. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.



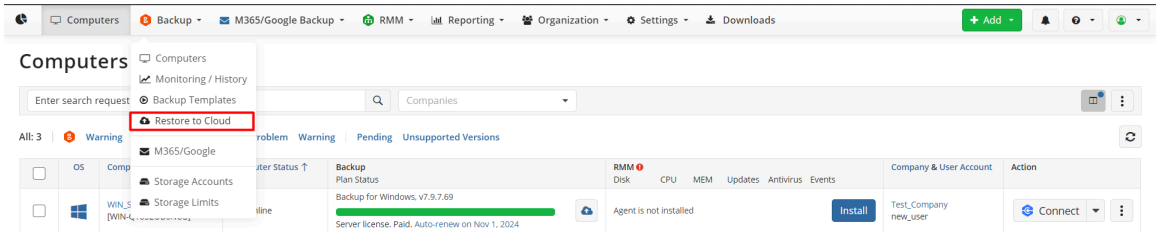
Step 20. The final step of the process is to select when the Restore Plan will start running. To have it start immediately, select the “Run Backup Now” option and click “Finish”. Otherwise, click “Finish” and the plan will begin at the next scheduled time.



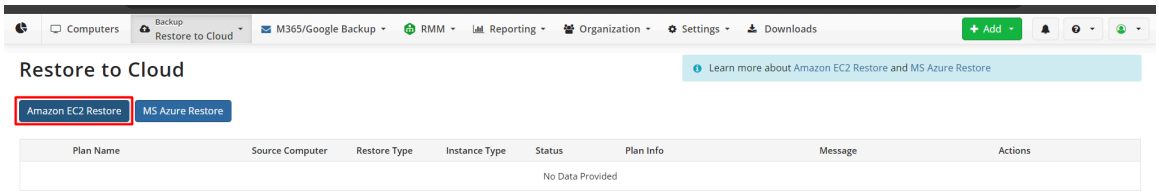
Restore to an EC2 Instance using MBS

> Please note that in order to enable restore to EC2 and EBS capabilities, the **vmimport** role must be created in advance. You can find more info in the help article below:
> https://help.mspbackups.com/billing-storage/storage-providers/amazon/required-permissions

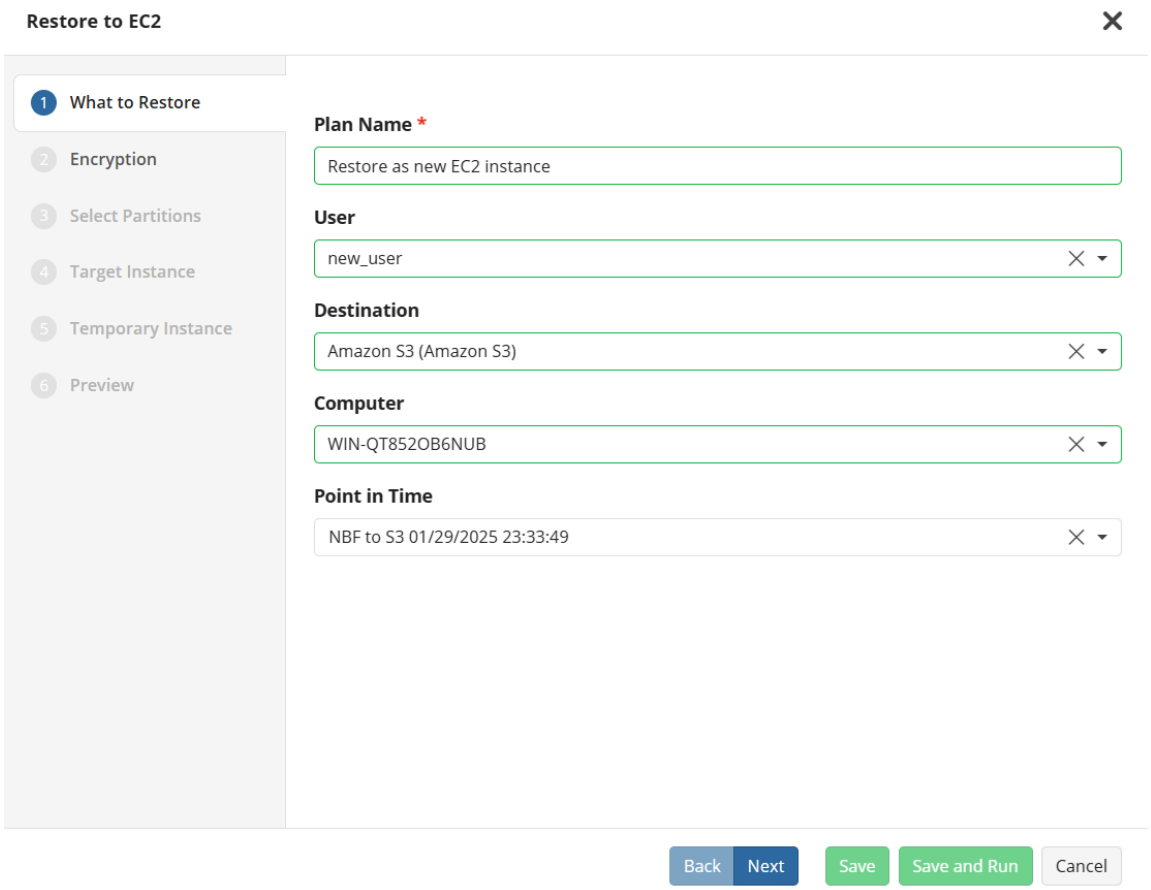
Step 1. Navigate to the MBS Portal and select “Backup” on the main menu, then click on “Restore to Cloud”:



Step 2. Next, please select the “Amazon EC2 Restore” option.



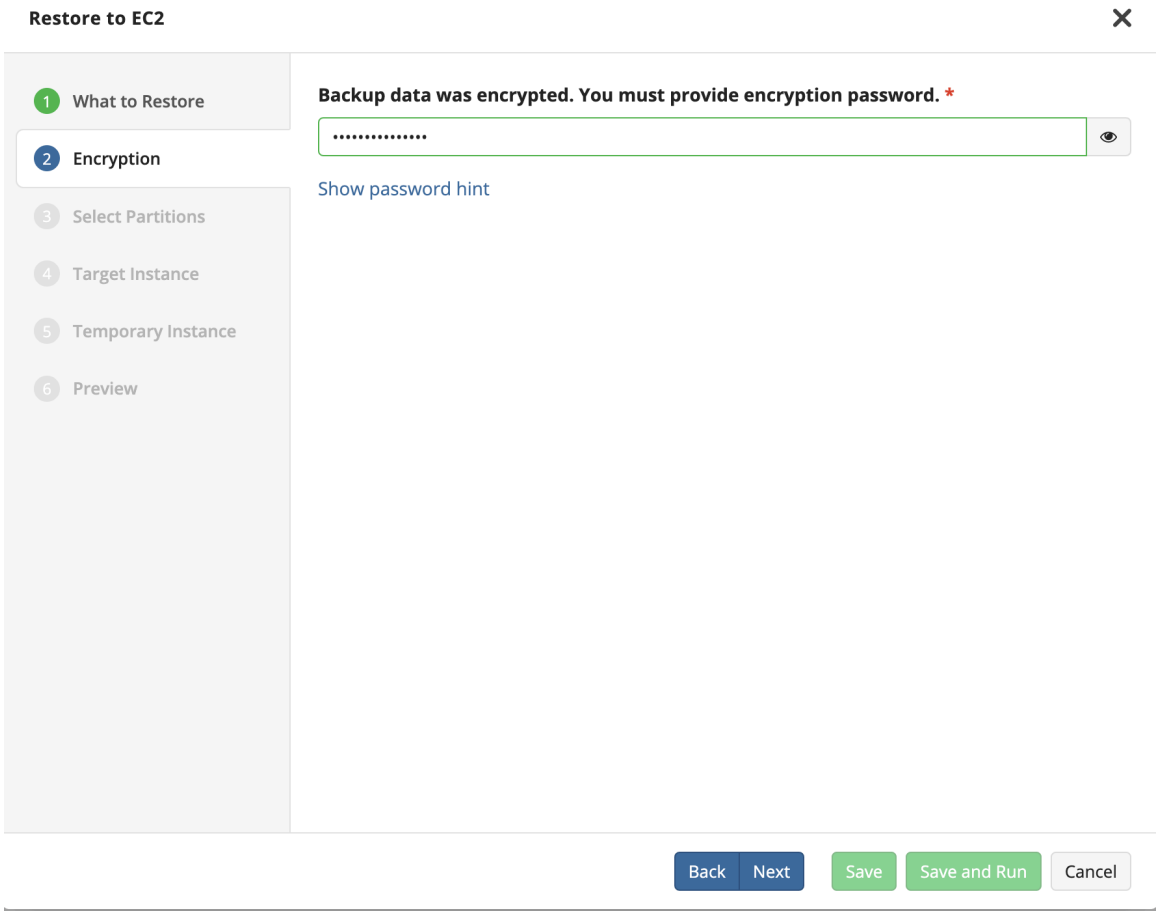
Step 3. The first page will prompt you to provide the restore plan name and select a backup dataset to restore.



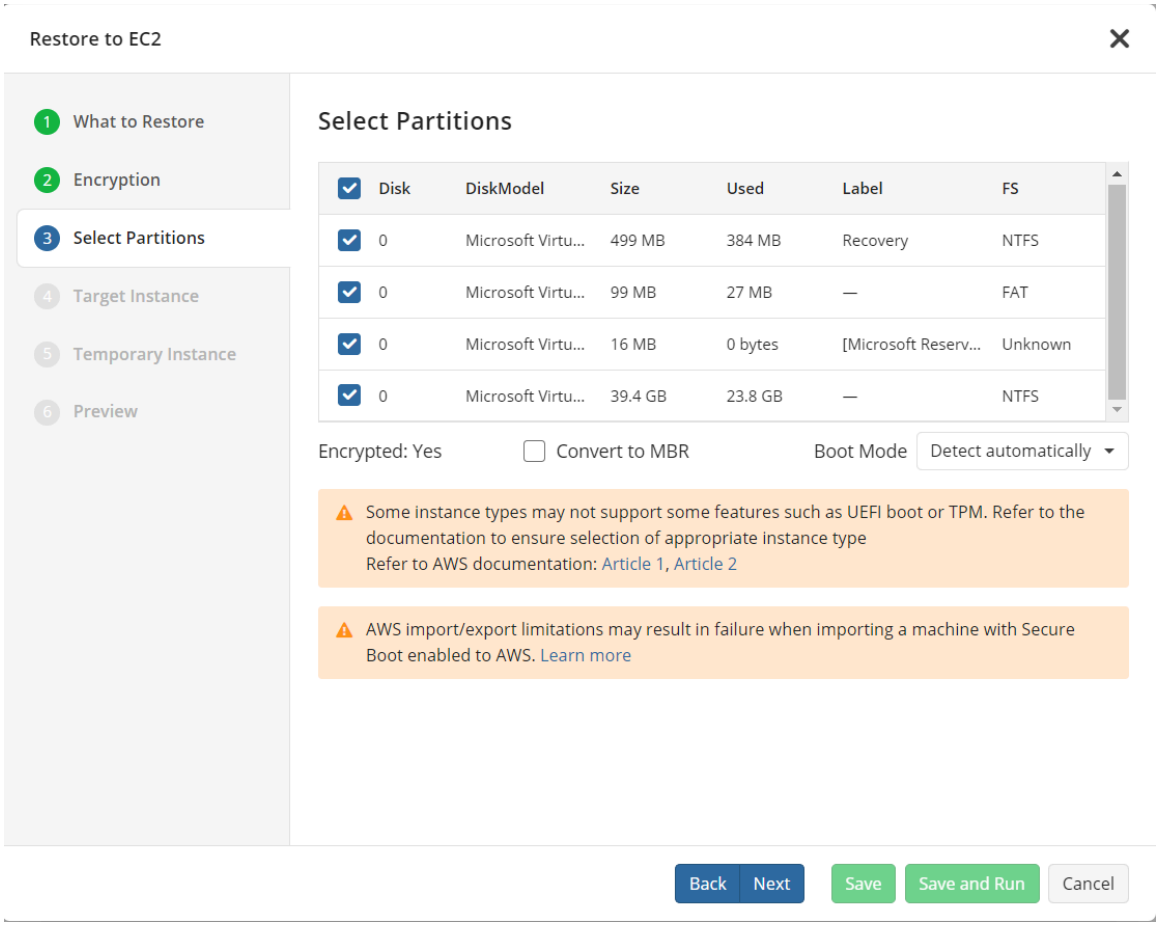
- **Plan Name:** The plan name is displayed on the **Restore to Cloud** dashboard
- **User:** Please select the user authorized during the creation of the backup dataset.
- **Destination:** Select the backup destination that contains the required backup data.
- **Computer:** Select the computer (prefix) containing the data to be restored.
- **Point in Time:** Pick the date/ backup version that is to be restored.

> Note that only cloud storage buckets can be used when restoring to EC2 from the MBS Console. Local storage can only be used when restoring from the Agent.

Step 4. If the backup dataset was encrypted, the next page will prompt for the encryption password.



Step 5. Next you will need to select the partitions to restore.

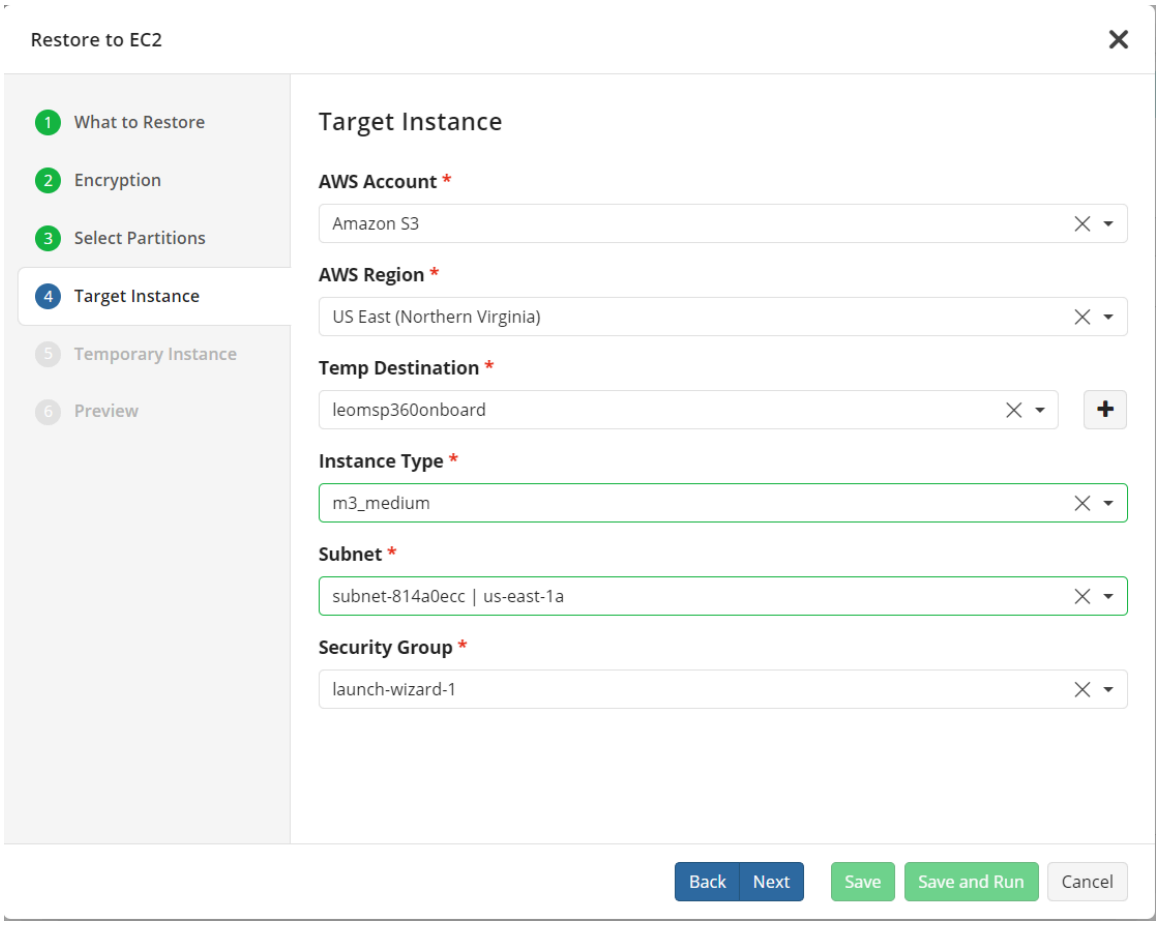


- **Convert to MBR:** Please select this option if the system does not support GPT (GUID Partition Table) and requires conversion to the Master Boot Record.
- **Boot Mode**: allows you to select “Detect automatically”, “Force UEFI boot mode”, or “Force BIOS boot mode”

> Some instance types may not support some features such as UEFI boot or TPM. Refer to the documentation to ensure selection of appropriate instance type. Refer to AWS documentation: Article 1, Article 2.

> AWS import/export limitations may result in failure when importing a machine with Secure Boot enabled to AWS. Learn more.

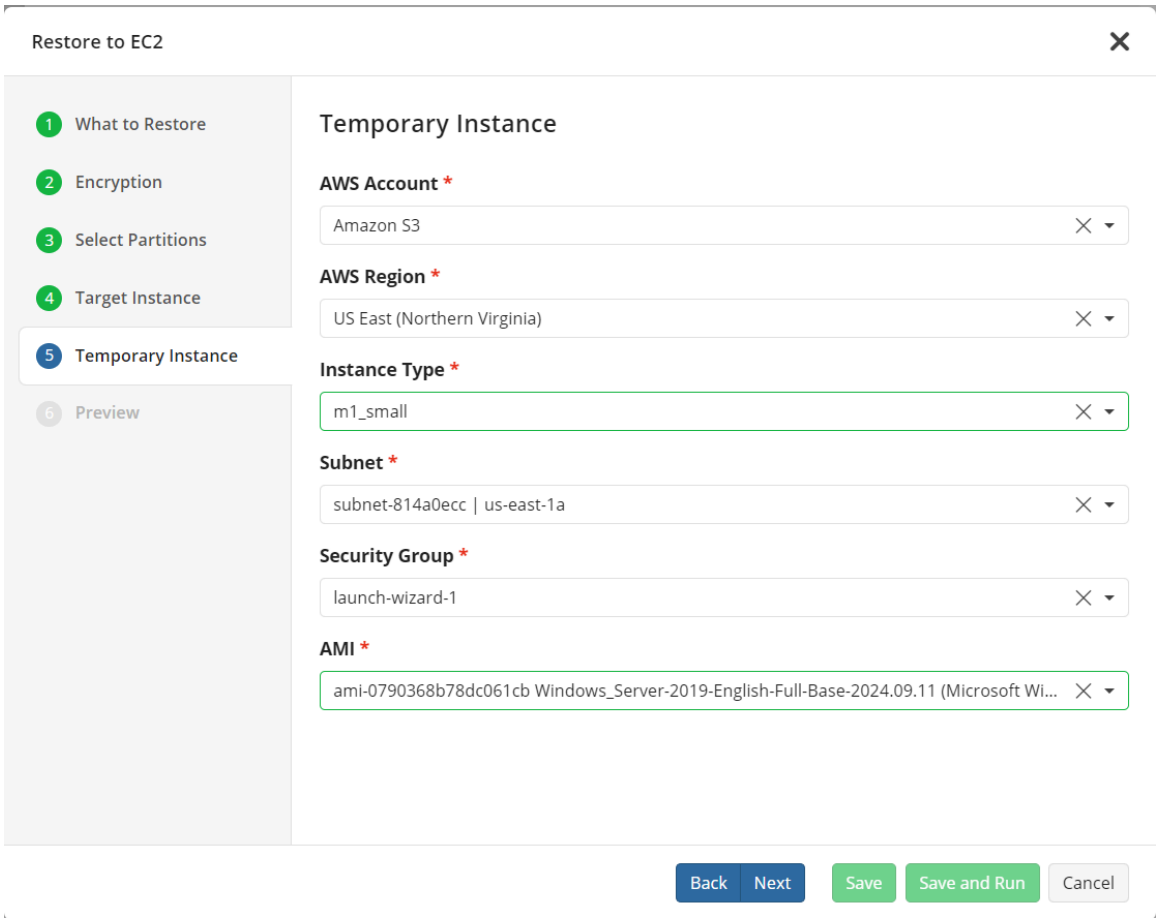
Step 6. The next step is to specify the parameters for your **target EC2 instance**:



- **AWS Account:** The account under which a new EC2 instance will be stored
- **AWS Region:** The region that is to store the newly created EC2 instance. Please note that the EC2 price is different depending on the AWS region selected. More information can be found here.
- **Temp Destination:** Storage destination to store temporary disk for VM import. Use the **+** button to create a new bucket, if necessary.
- **Instance Type:** The type of instance required. Learn more about EC2 instance types.
- **Subnet:** Select one of the subnets available. Learn more about EC2 subnets.
- **Security Group:** Select the default security group or the custom one you created yourself.

> When selecting the **Target Instance Type**, please make sure that the selected type has sufficient resources (RAM, storage, and vCPUs) to accommodate the restored computer.

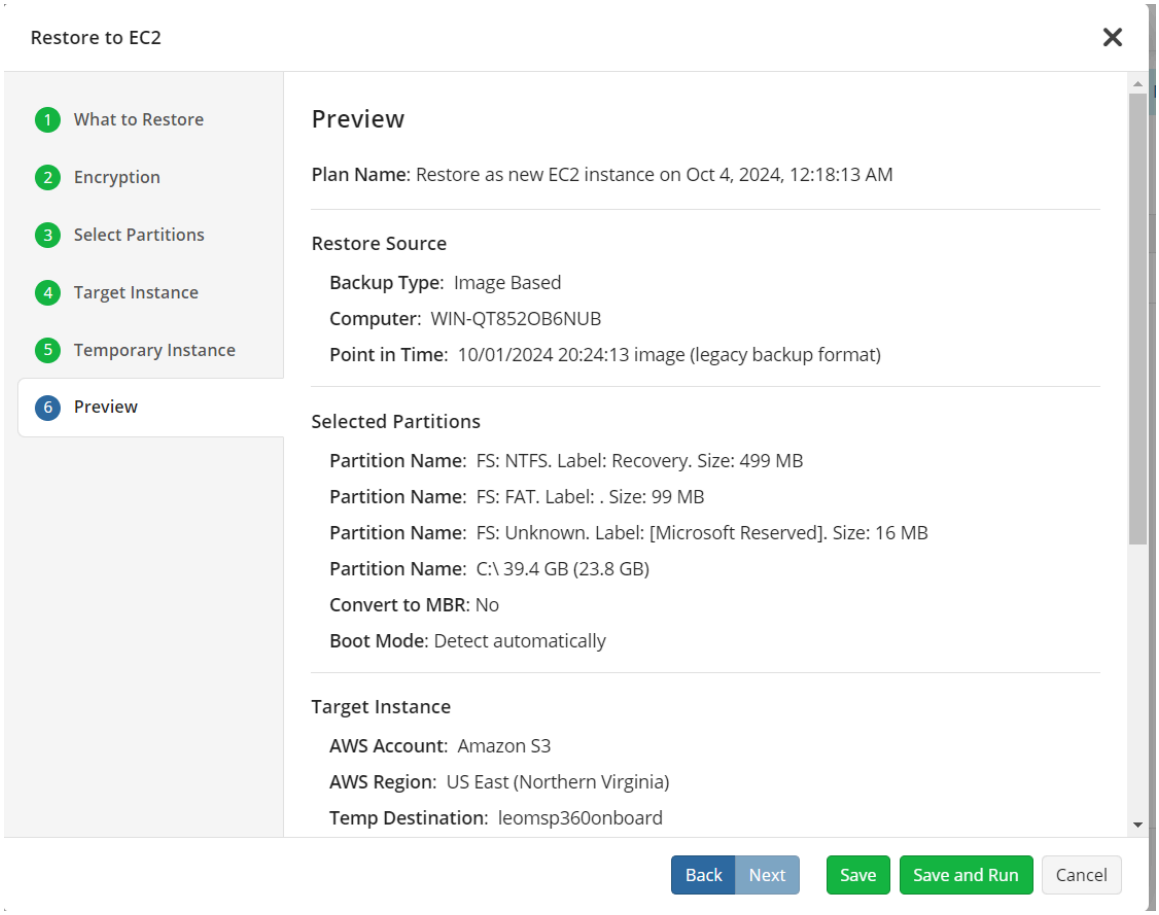
Step 7. Next, please specify the **Temporary Instance** parameters:



- **AWS Account:** The account under which a new EC2 instance will be stored
- **AWS Region:** The region that is to store the newly created EC2 instance. Please note that the EC2 price is different depending on the AWS region selected. More information can be found here.
- **Temp Destination:** Storage destination to store temporary disk for VM import. Use the **+** button to create a new bucket, if necessary.
- **Instance Type:** The type of instance required. Learn more about EC2 instance types.
- **Subnet:** Select one of the subnets available. Learn more about EC2 subnets.

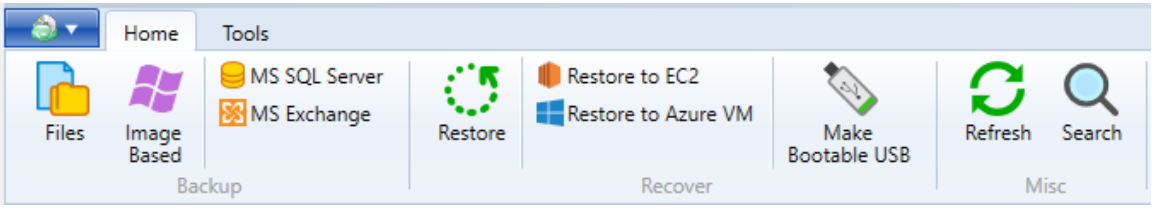
- **Security Group:** Select the default security group or the custom one you created yourself.
- **AMI:** AMI (Amazon Machine Image) allows you to create an Amazon machine image (based on your image backup configuration) in addition to a restored EC2 instance. The restored EC2 instance will be run automatically and it will have a public IP address. The created Amazon machine image can be used for setting up other EC2 instances in the future. You can find Amazon machine images on the *IMAGES* section of the AWS EC2 Management Console. More information here.

Step 8. Review all settings specified across the restore wizard and ensure that they are accurate. Click **Save and Run** to execute the restore to an EC2 instance.

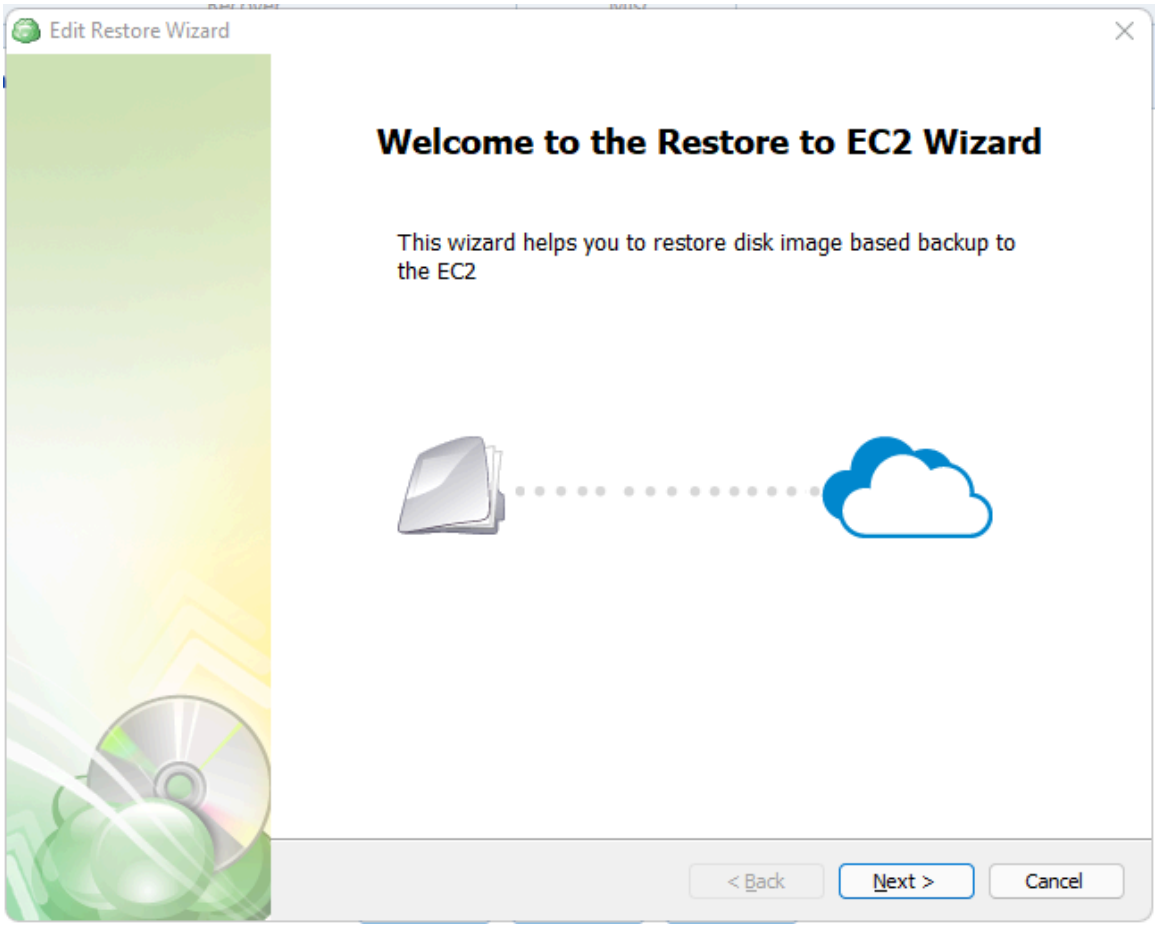


Restore to an Amazon Machine Image using the Agent

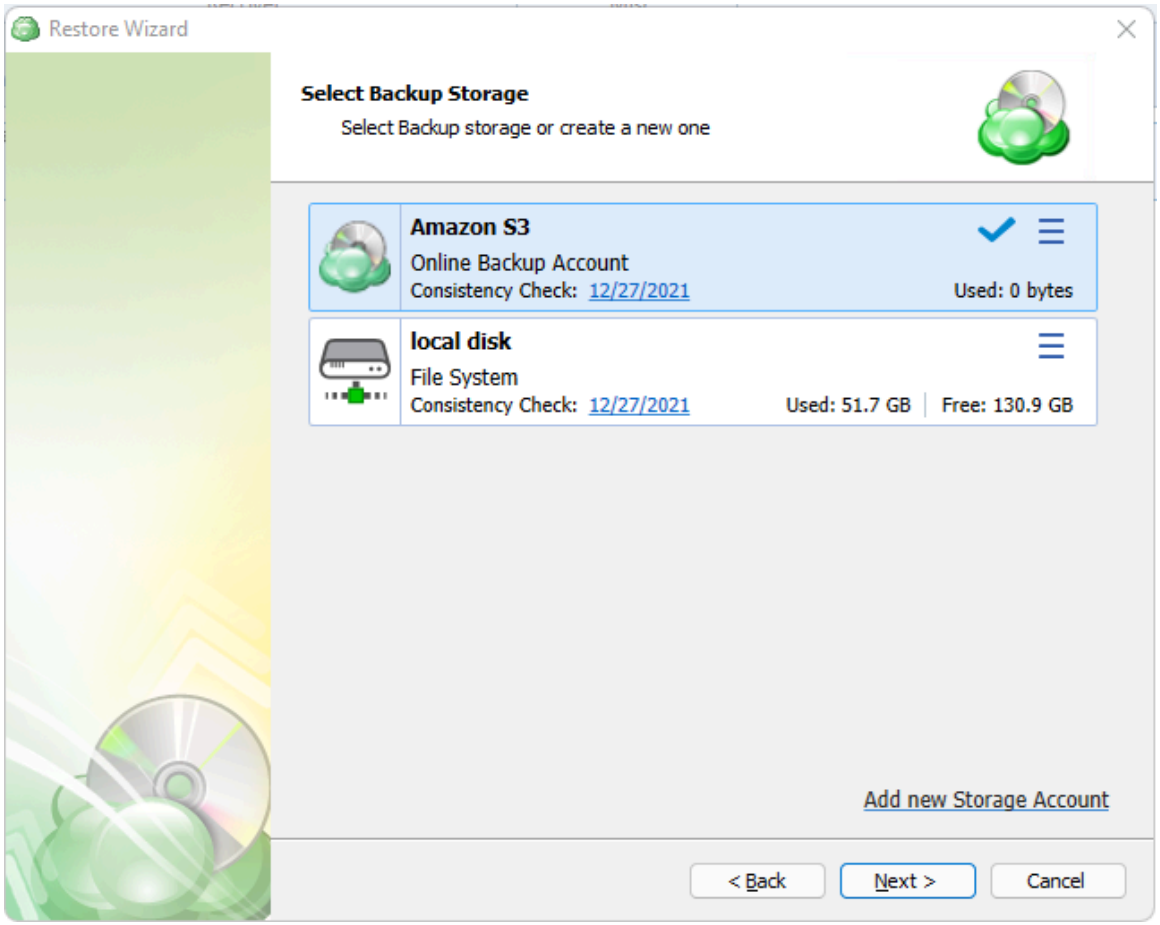
Step 1. After launching the Online Backup, click on “Restore to EC2” in the top menu



Step 2. The first step of the wizard indicates that you have started the wizard.

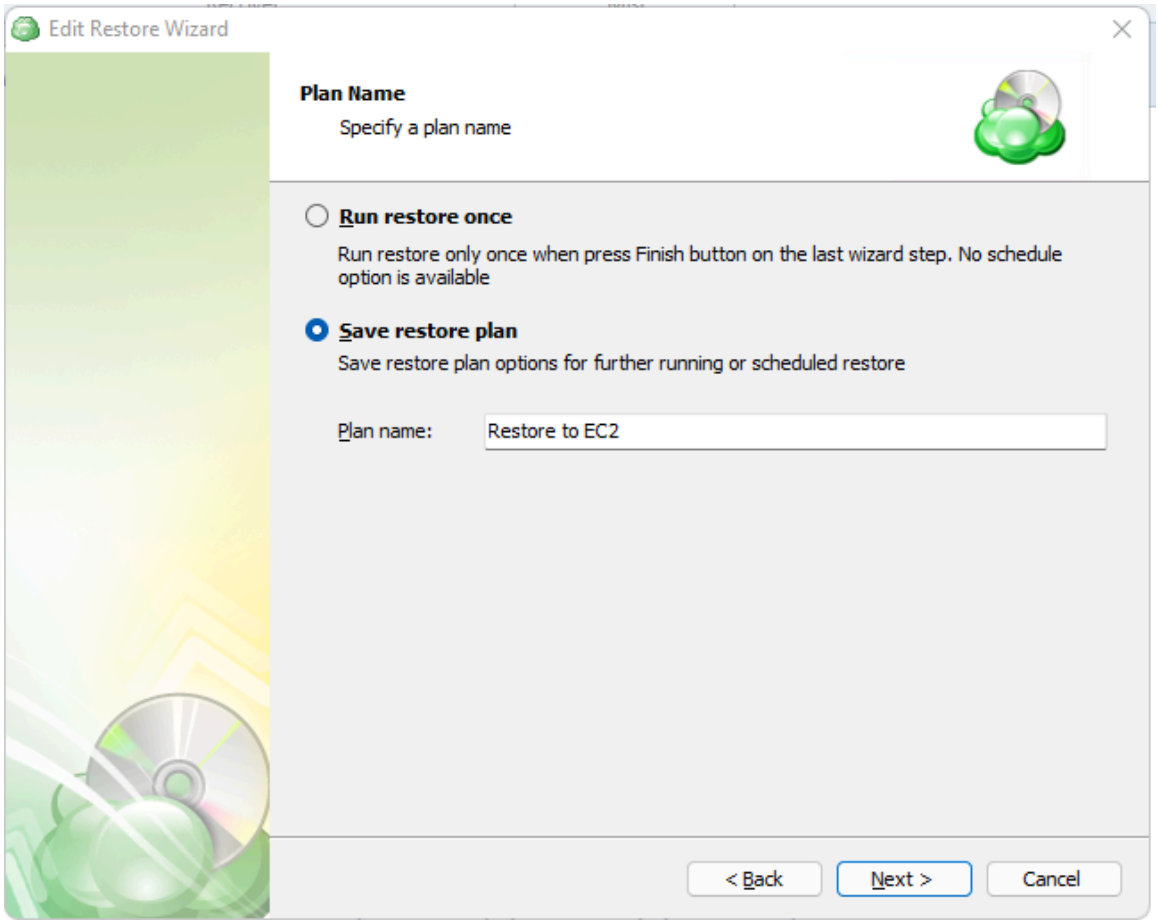


Step 3. The next step will prompt you to select the storage location for the source.

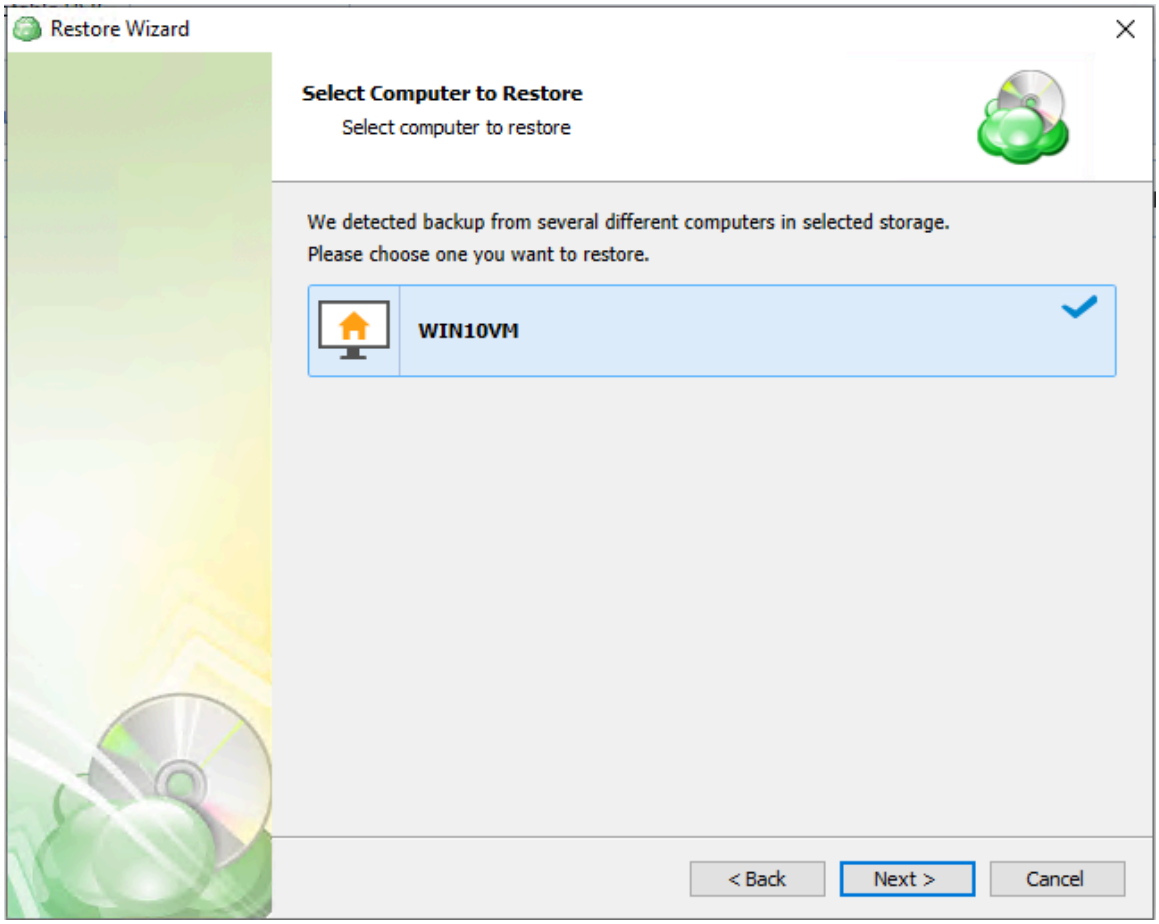


If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

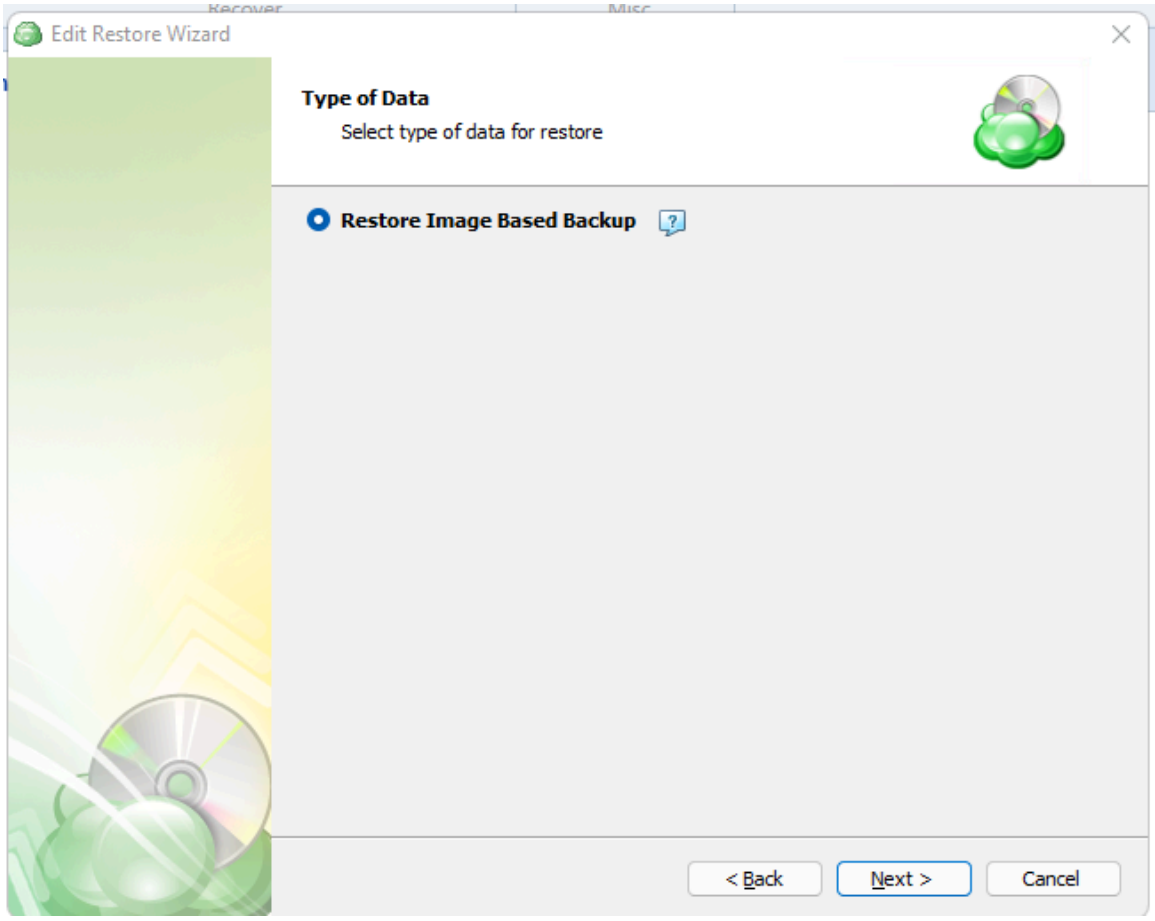
Step 4. Next you will choose whether to run the restore operation only once, or to save it for later use. The latter will allow you to name the plan.



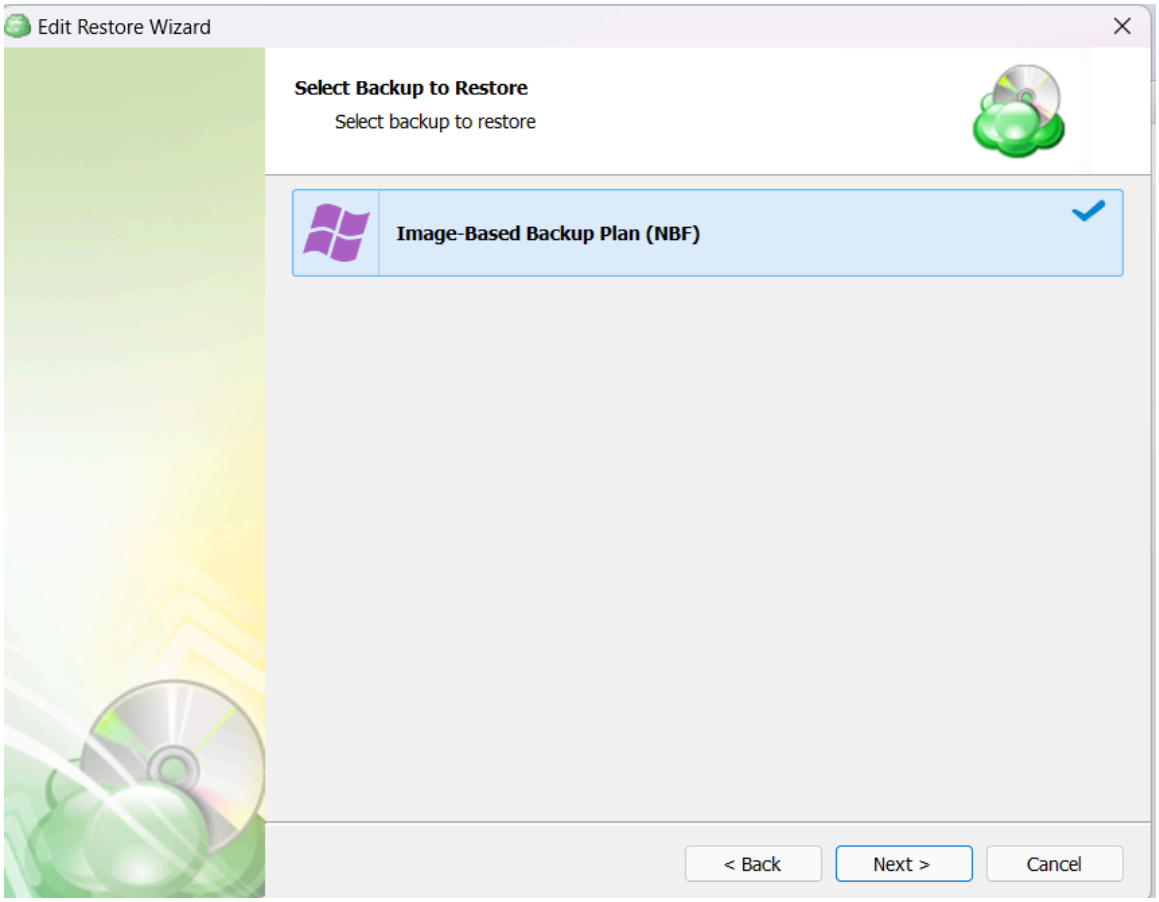
Step 5. Next you will be presented with a list of computers with the same prefix and associated "Backup User" as the computer on which the Agent is currently running. Click to select the desired computer then click on "Next".



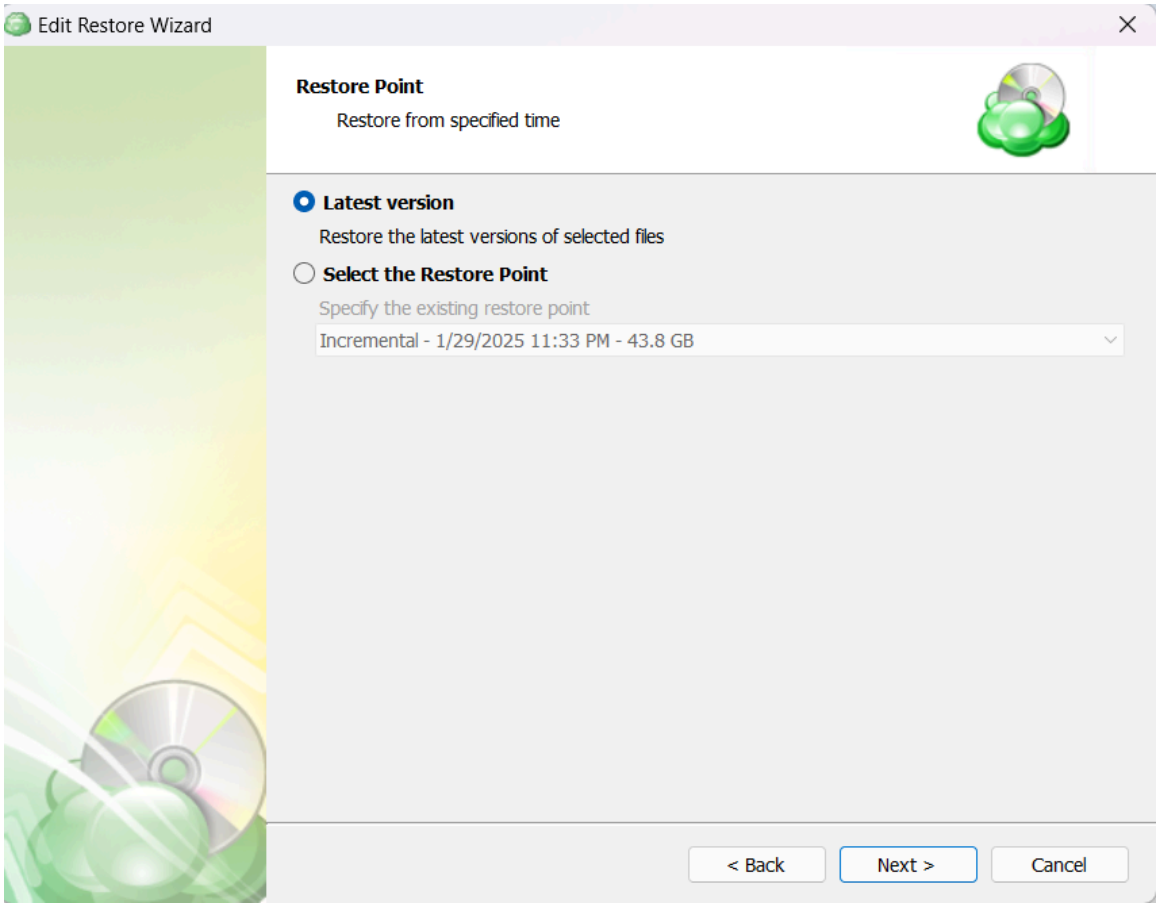
Step 6. Based on the contents of the selected source and computer, the next step is to choose the type of restore. Select “Restore Image Based Backup” then continue to the next step by clicking “Next”.



Step 7. With the correct type of restore selected, the application will generate a list of available backup plans.

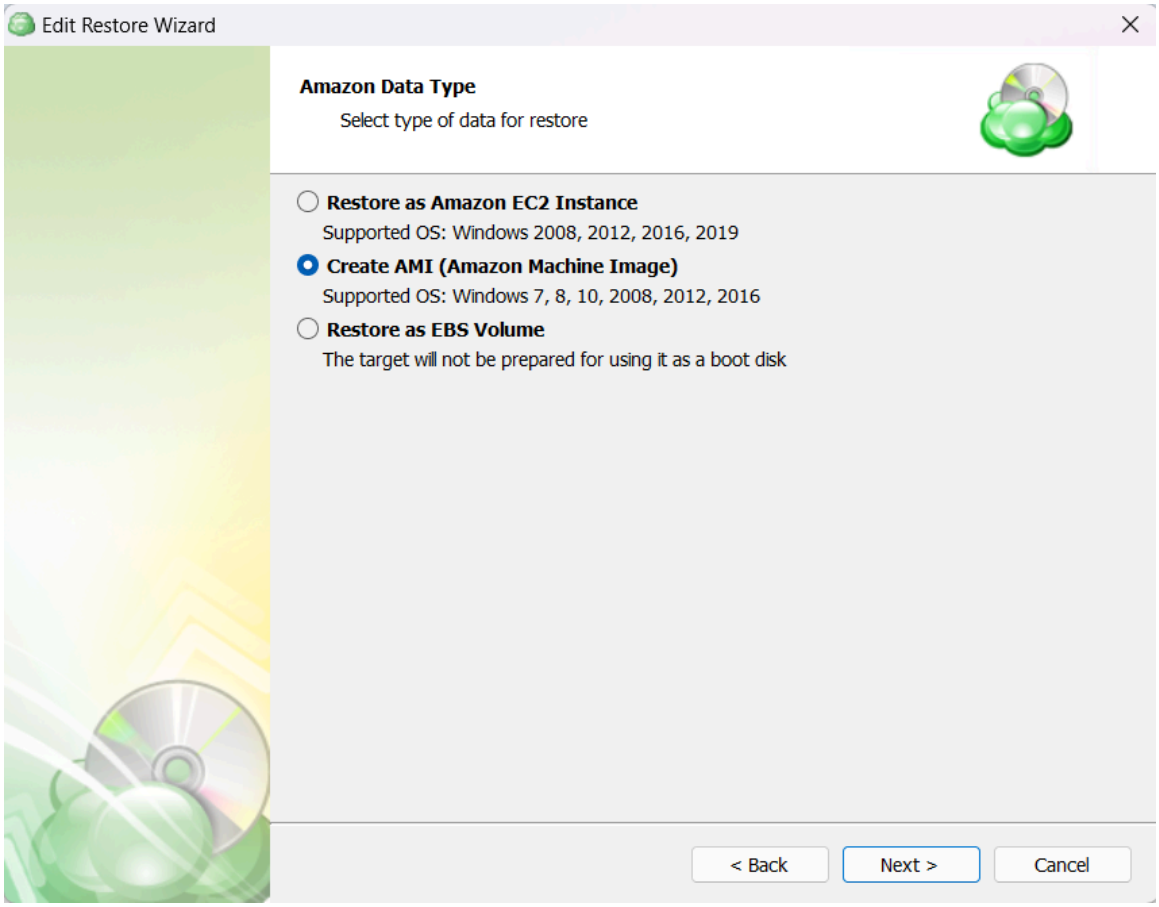


Step 8. The next step is to select the desired point in time to restore to.



- **Latest Version:** Automatically restores the most recent backup restore point.
- **Select the Restore Point:** Allows you to select a specific restore point (date) to restore.

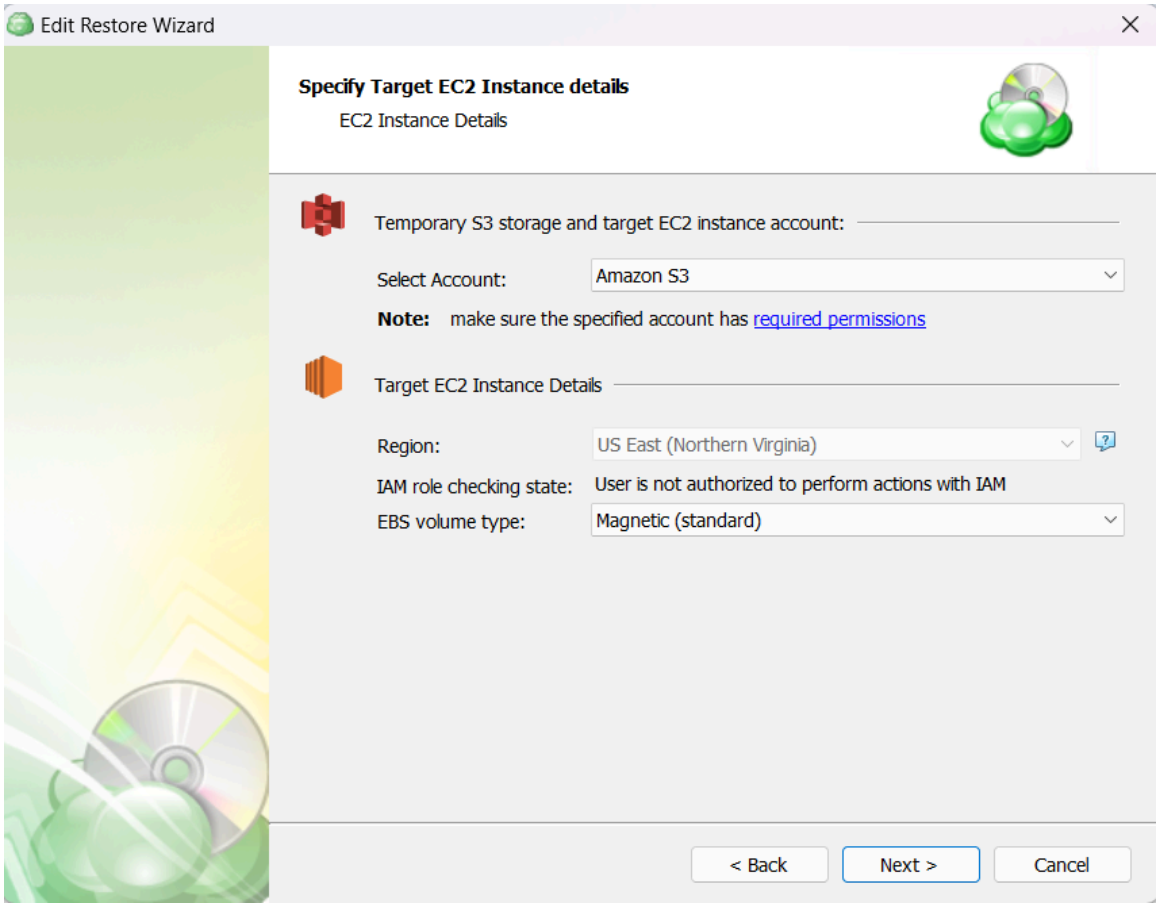
Step 9. Next, select the desired target format for the restored data



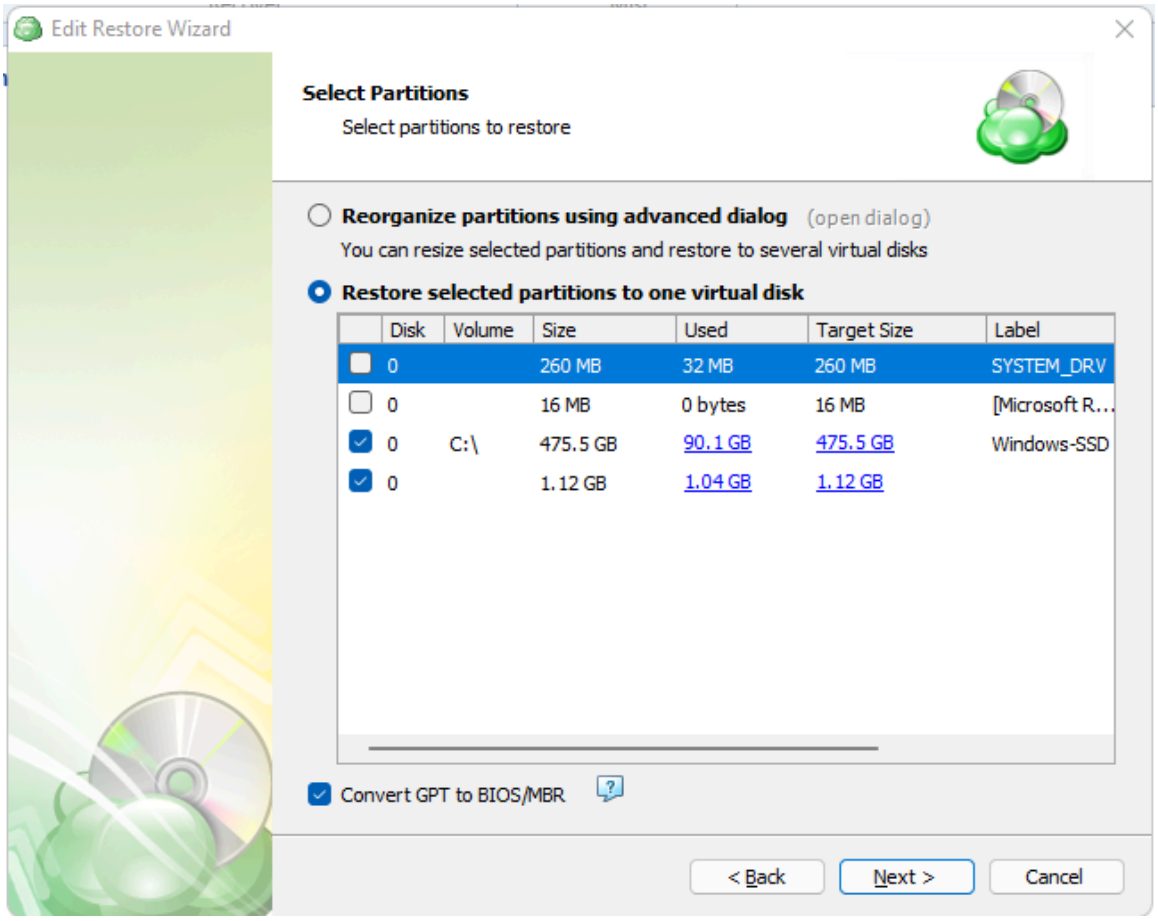
- **Restore as Amazon EC2 Instance:** Restores the partitions selected later to a physical disk.
- **Create AMI (Amazon Machine Image):** Restores the data as a virtual disk in multiple supported formats.
- **Restore as an EBS Volume:** Restores the data as either an EC2 machine, EBS volume, or Amazon Machine Image.

For AWS and Azure destinations, a storage account must already be specified through the MBS portal

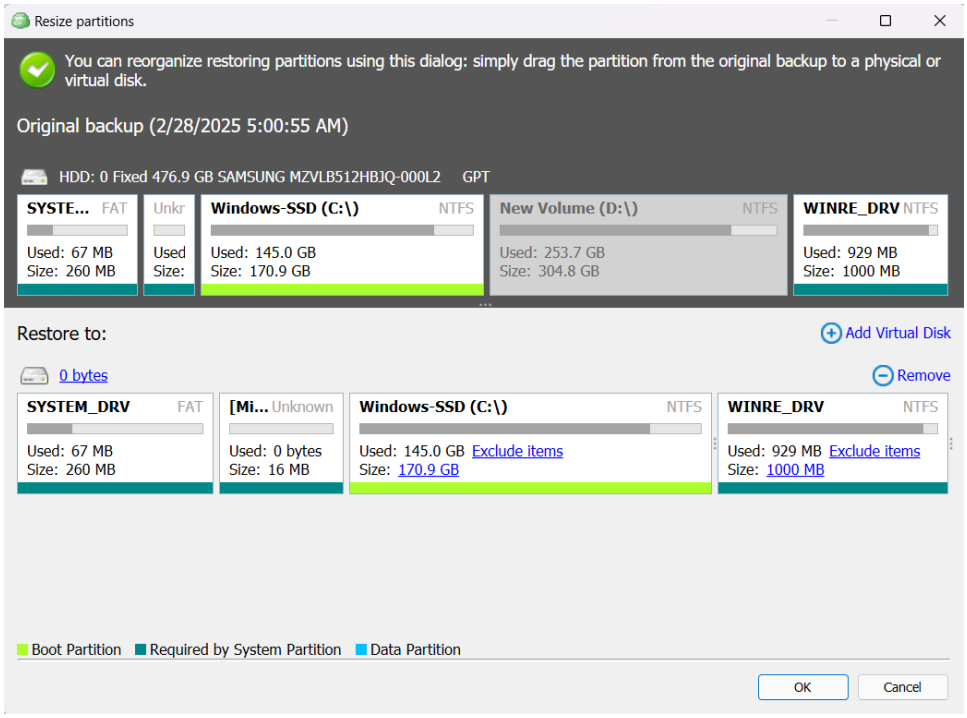
Step 10. After selecting the type of restore target in the previous step, you are prompted to specify the parameters of the new AMI.



Step 11. After selecting the type of restore target in the previous step, you can now choose to restore the partitions with their existing parameters or to reorganize and resize them.

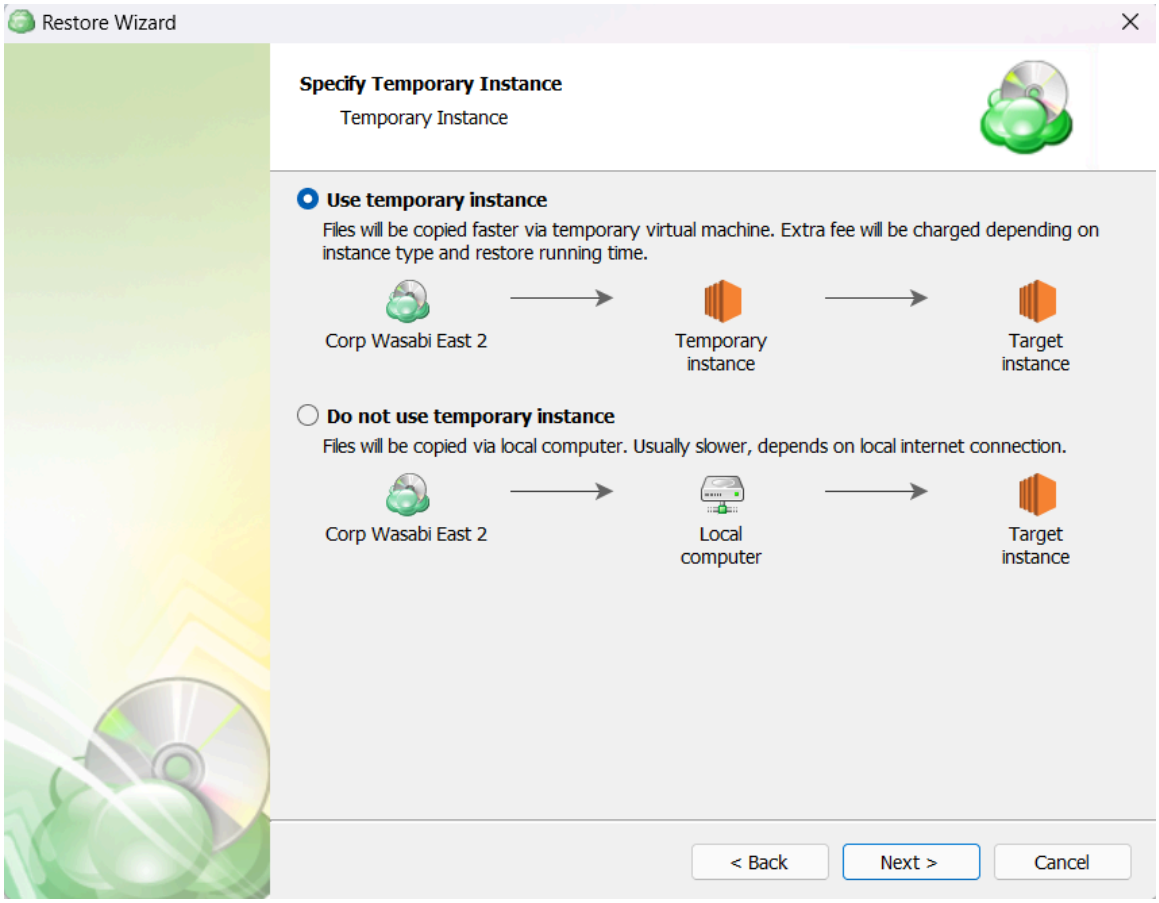


If you select “Reorganize partitions using advanced dialog” a new window will appear and allow you to resize the partitions and rearrange them on one or more virtual disks.



Click on any of the blue hyperlinks to open additional dialogue boxes allowing you greater control over the name and size of the virtual disk, as well as the ability to add additional virtual disks, and also exclude specific files or folders if desired.

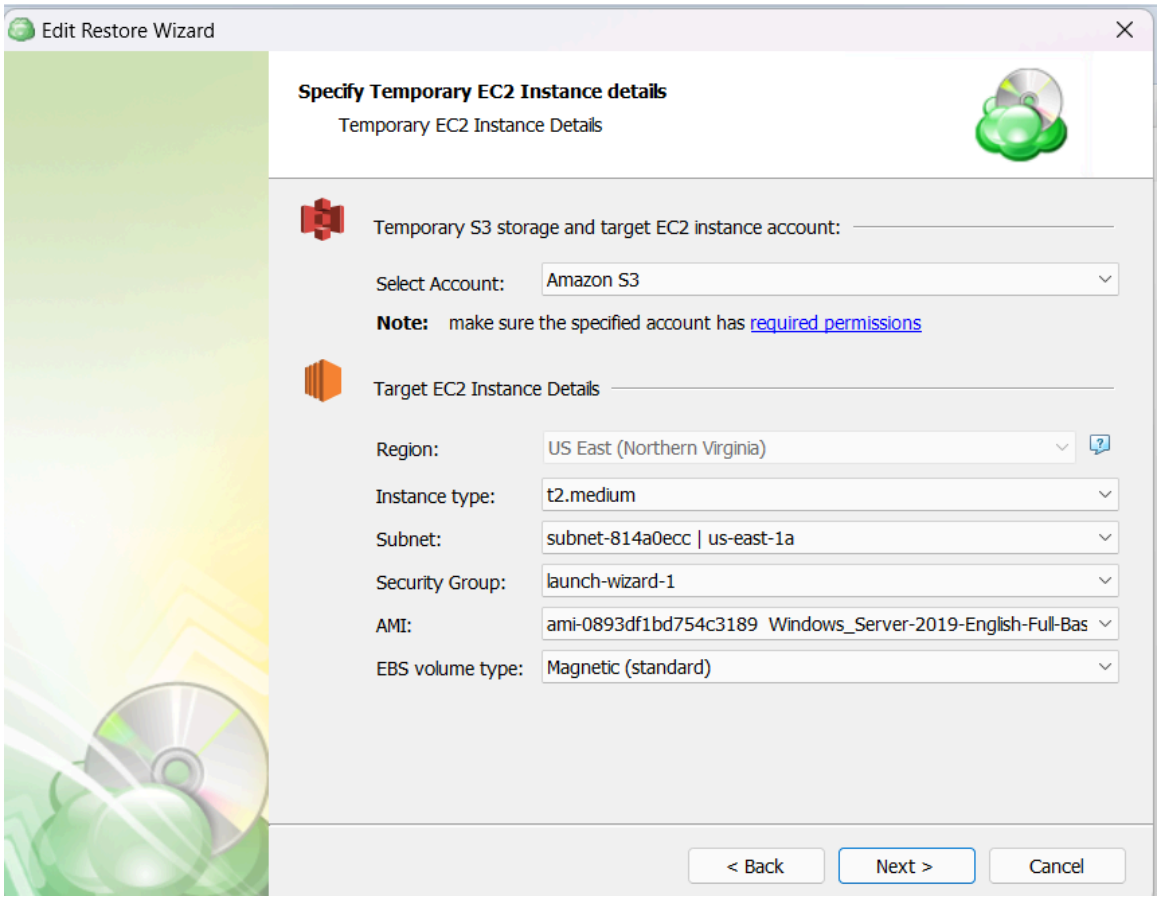
Step 12. After specifying the target EC2 instance details, you will need to choose between using a temporary EC2 instance or local computer for the restore operation.



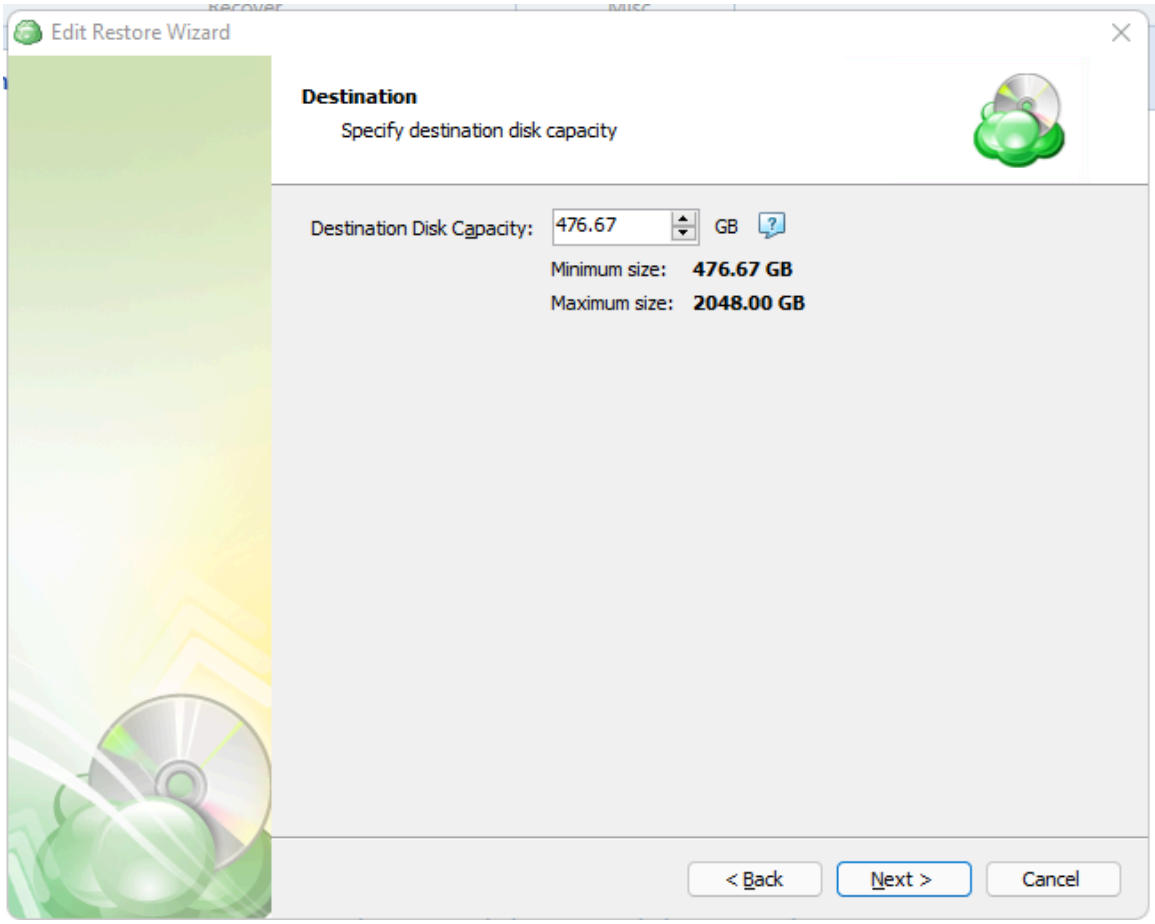
- **Use temporary instance:** This option creates a temporary EC2 instance in Amazon Web Services that will download backup data from the storage destination and restore it as a target instance. Usually, this method is faster as the temporary and target instance are located in the same AWS network.
- **Do not use temporary instance:** When selecting this option, the restore operation will be performed using the resources of local computer. Usually, this approach is slower, depending on the local internet connection.

> Enabling the "**Use temporary instance"** option will lead to additional charges in Amazon Web Services for running the temporary EC2 instance. Please check the AWS documentation on instance types and pricing for more information.

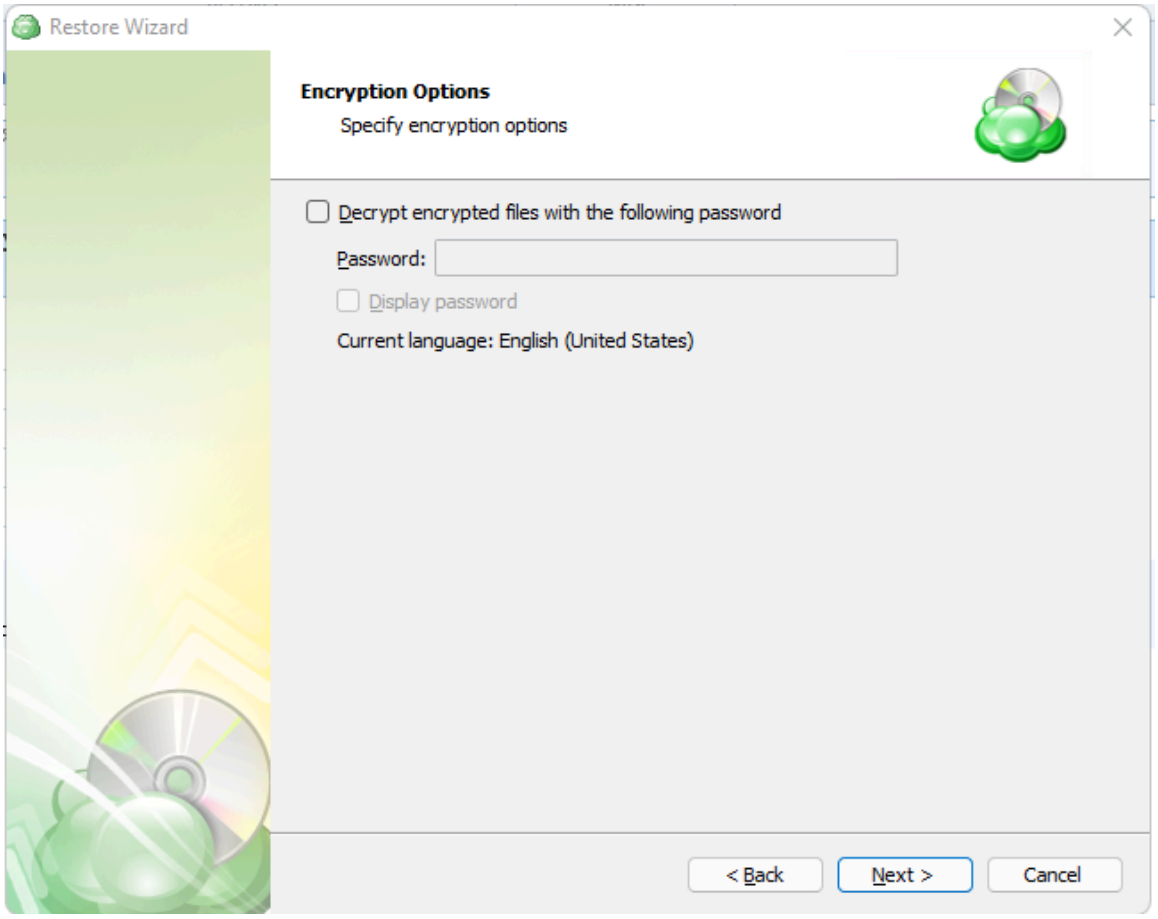
Step 13. If you have selected to use a temporary instance, the next page will allow you to select the Amazon account from the upper dropdown box, and specify the Temporary EC2 Instance details below.



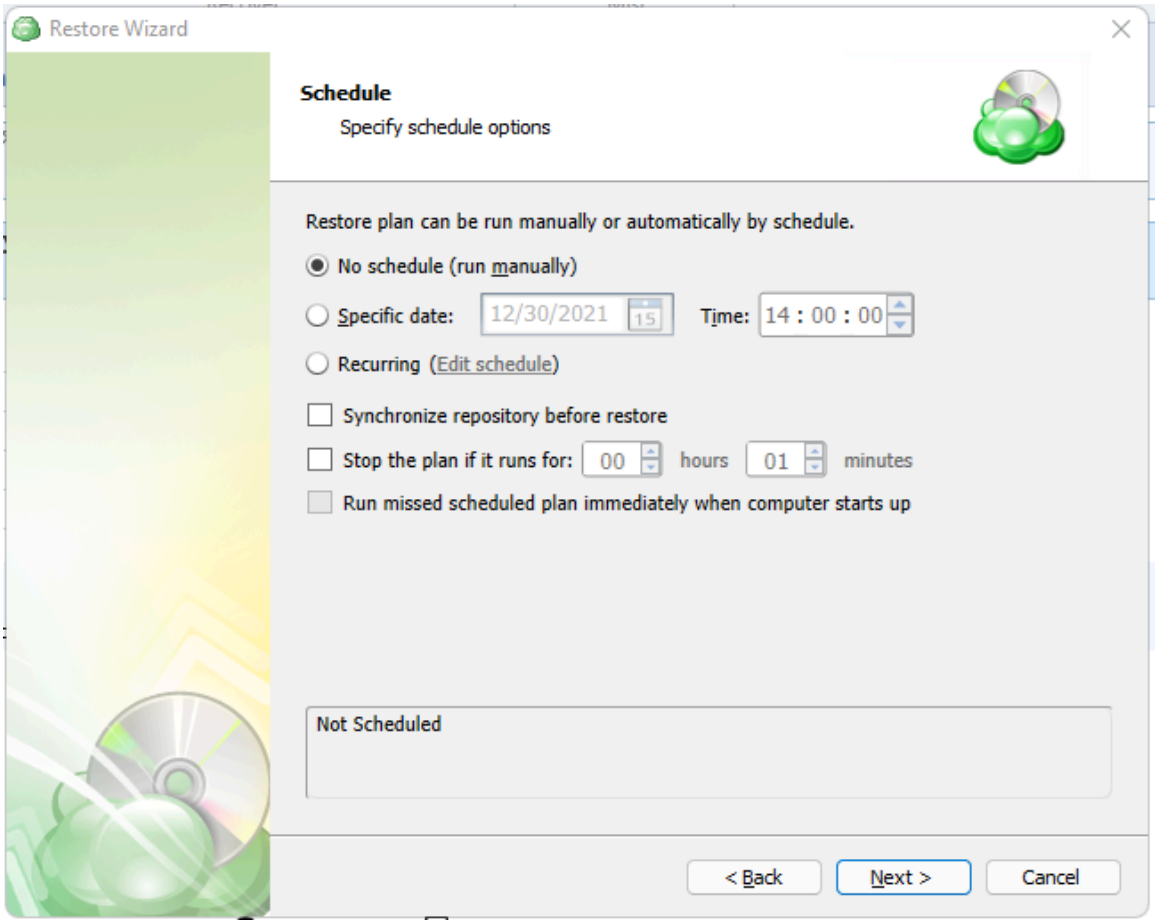
Step 14. Once the partitions are selected, the next step allows you to choose the size of the virtual disk used by the instance.



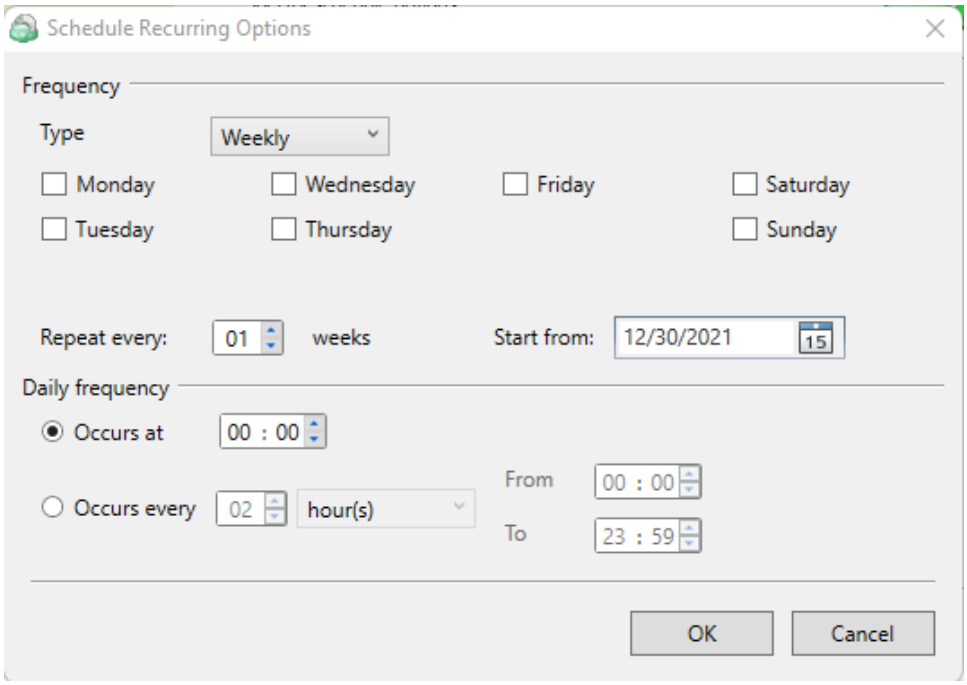
Step 15. If the backed up data was encrypted, the next step will be to enter the password for decryption. If the password is incorrect or missing, the restore plan will fail and you will need to edit the plan to input the correct password.



Step 16. If the restore plan is saved for later, next you will set the schedule for the plan, otherwise proceed to the next step.



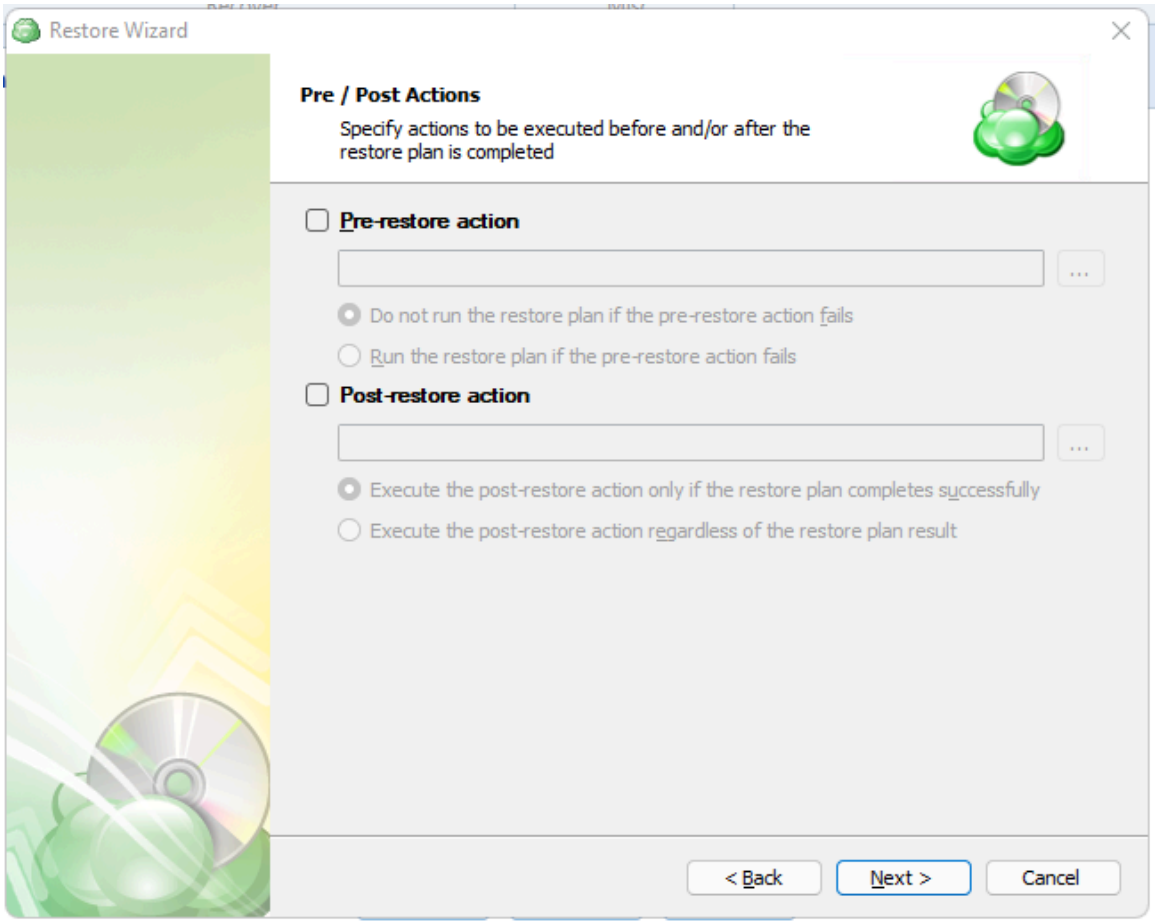
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria by clicking on the “Edit schedule” hyperlink to open this dialogue:



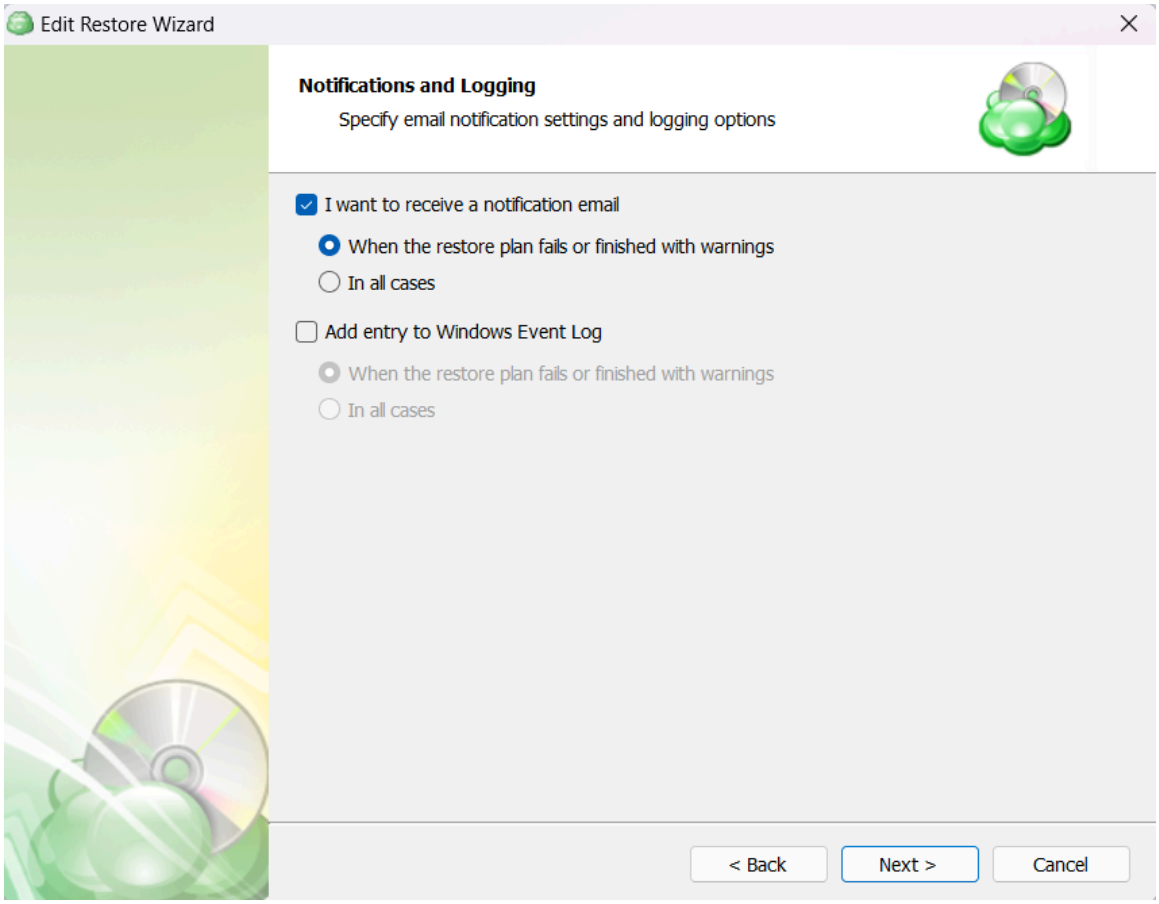
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

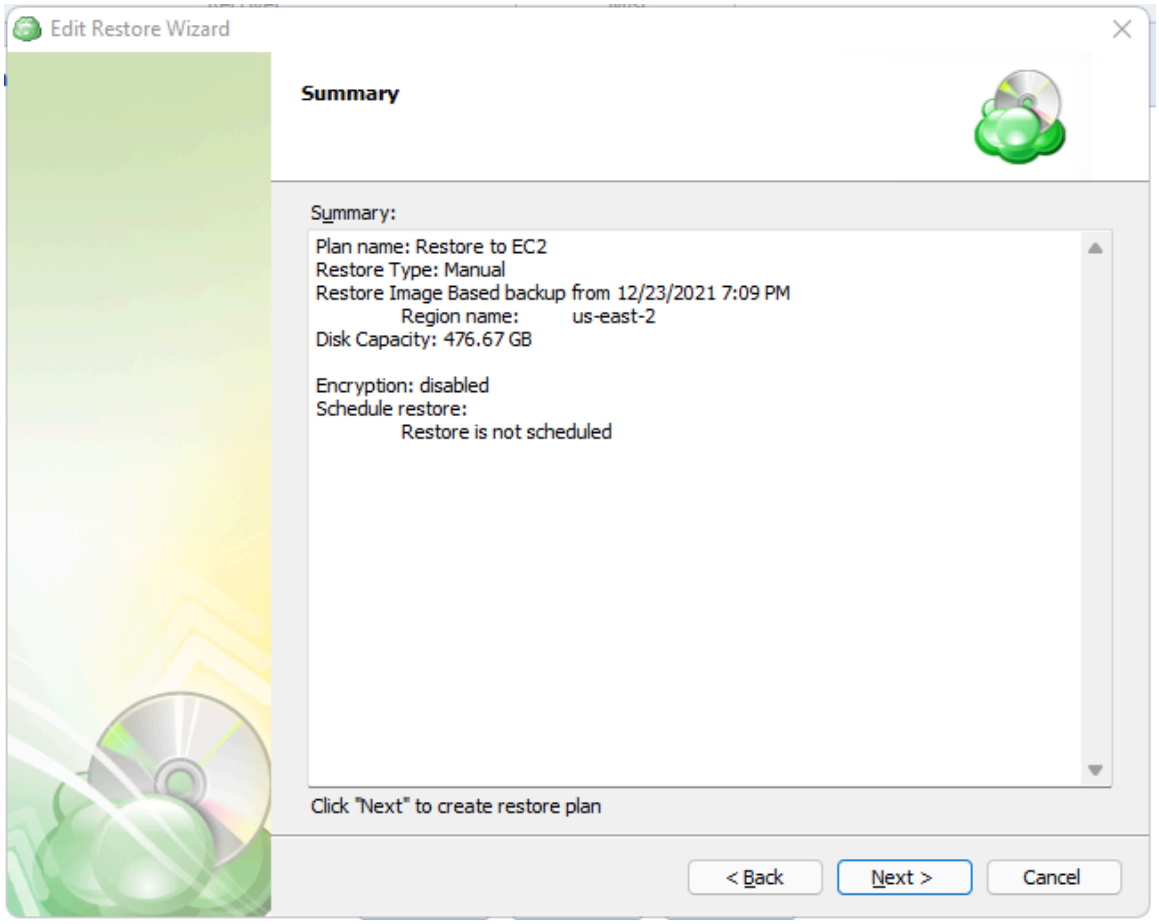
Step 17. The next step page allows the execution of custom scripts before and/or after the running of a Restore Plan.



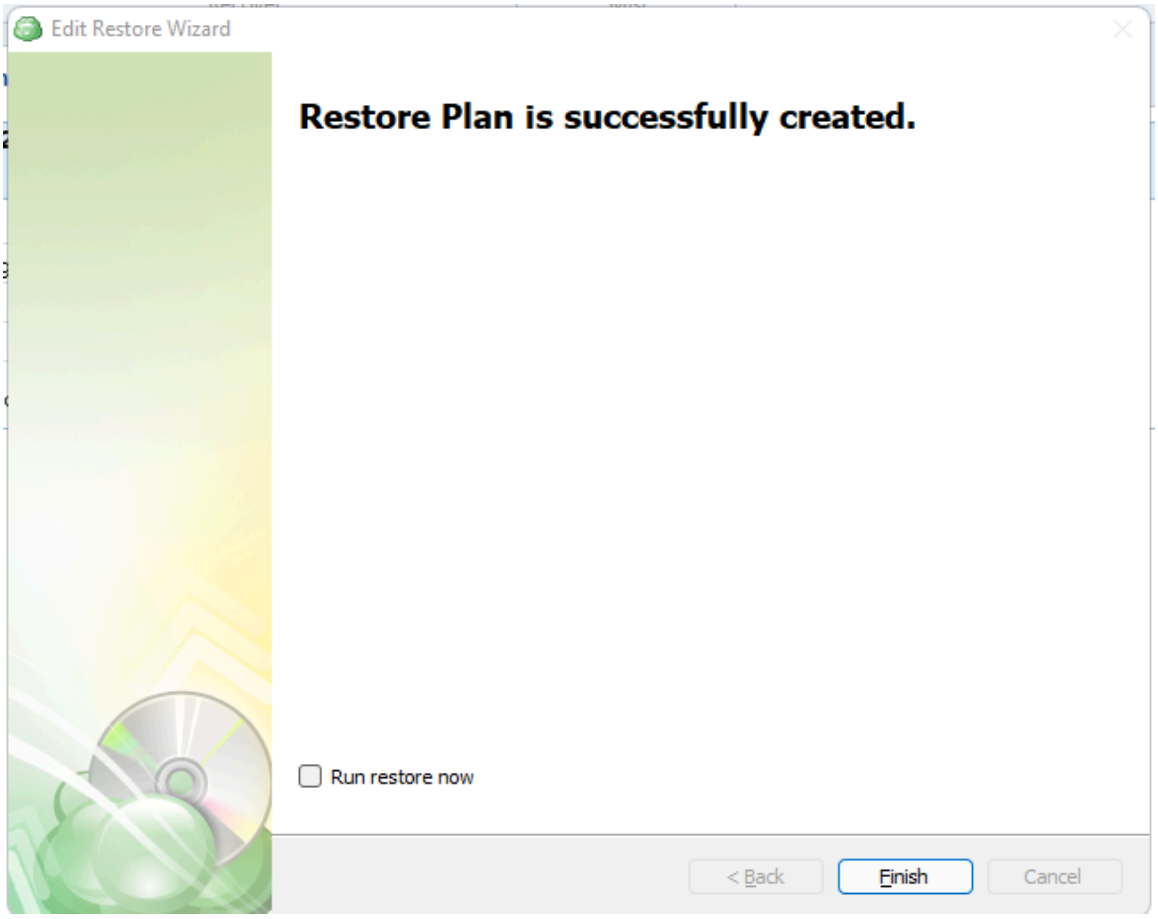
Step 18. The “Notifications and Logging” page allows you to enable notification email and add an entry to Windows Event Log upon restore plan completion or failure.



Step 19. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.



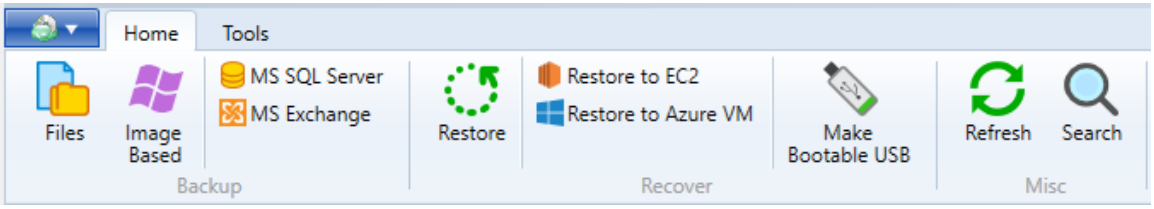
Step 20. The final step of the process is to select when the Restore Plan will start running. To have it start immediately, select the “Run Backup Now” option and click “Finish”. Otherwise, click “Finish” and the plan will begin at the next scheduled time.



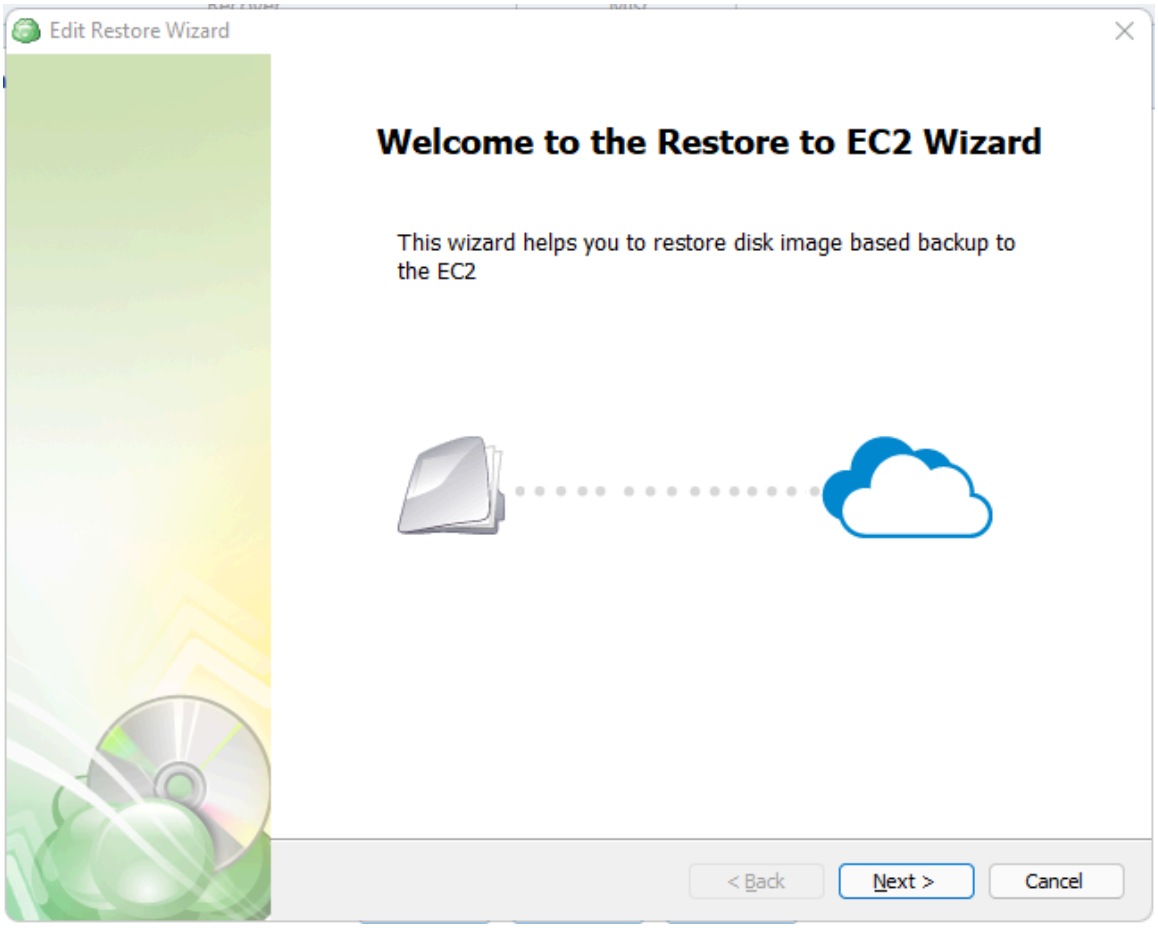
Restore to an EBS Volume using the Agent

> Please note that in order to enable restore to EC2 and EBS capabilities, the **vmimport** role must be created in advance. You can find more info in the help article below:
> https://help.mspbackups.com/billing-storage/storage-providers/amazon/required-permissions

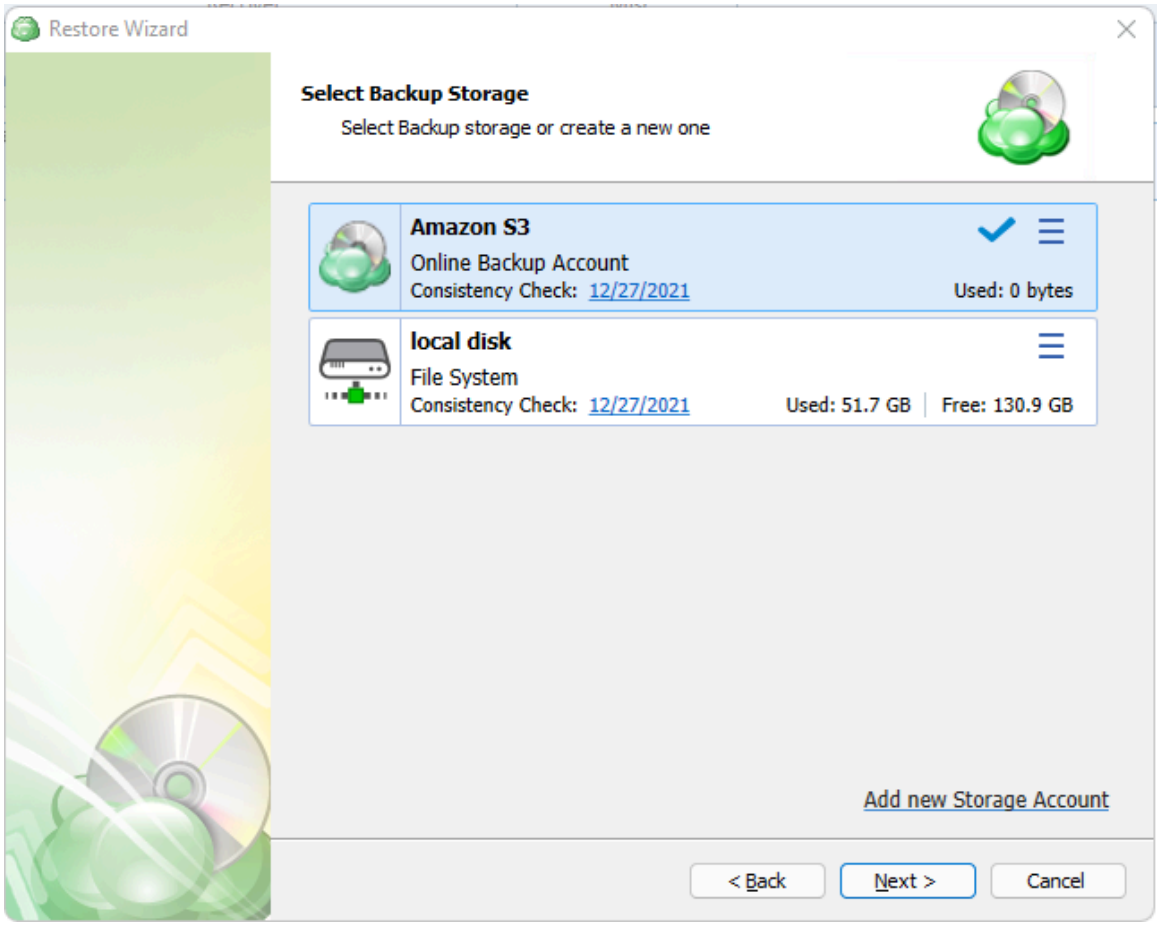
Step 1. After launching the Online Backup, click on “Restore to EC2” in the top menu



Step 2. The first step of the wizard indicates that you have started the wizard.

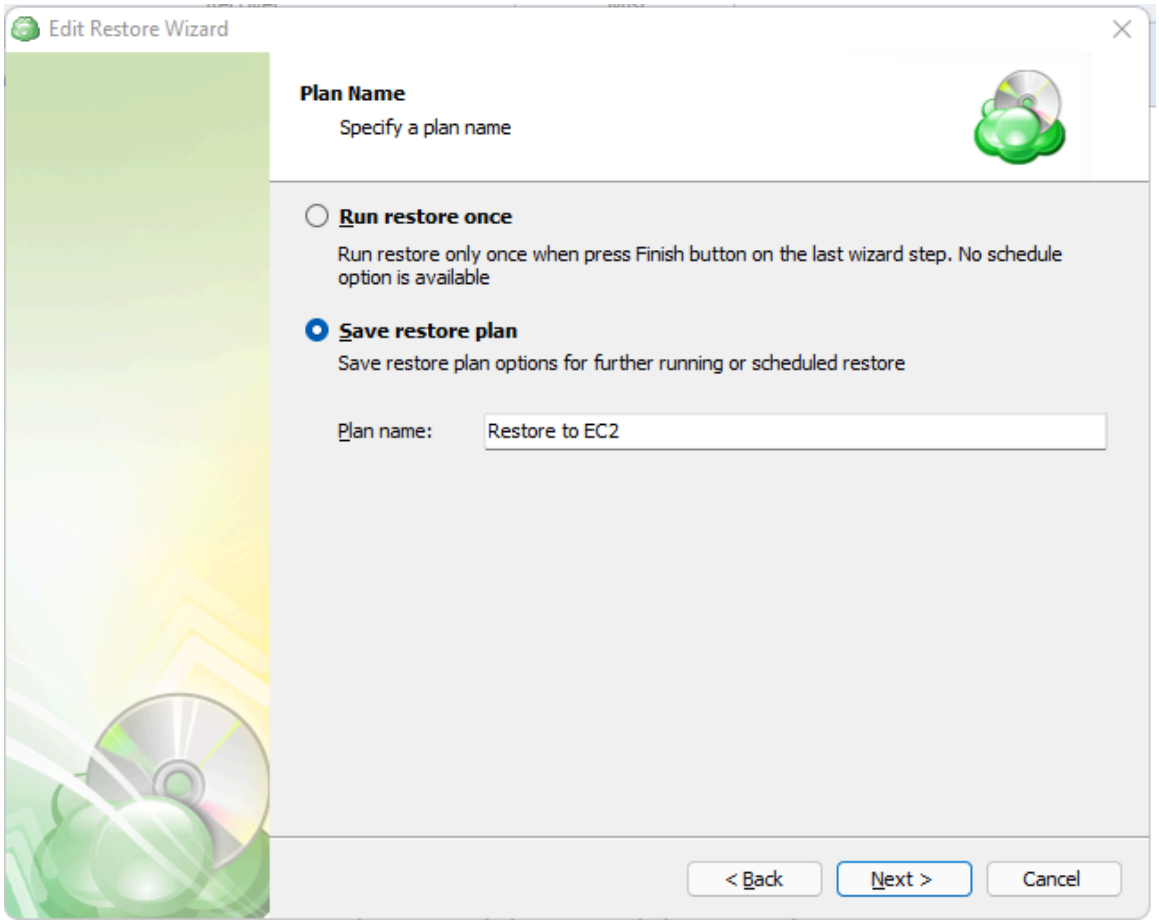


Step 3. The next step will prompt you to select the storage location for the source.

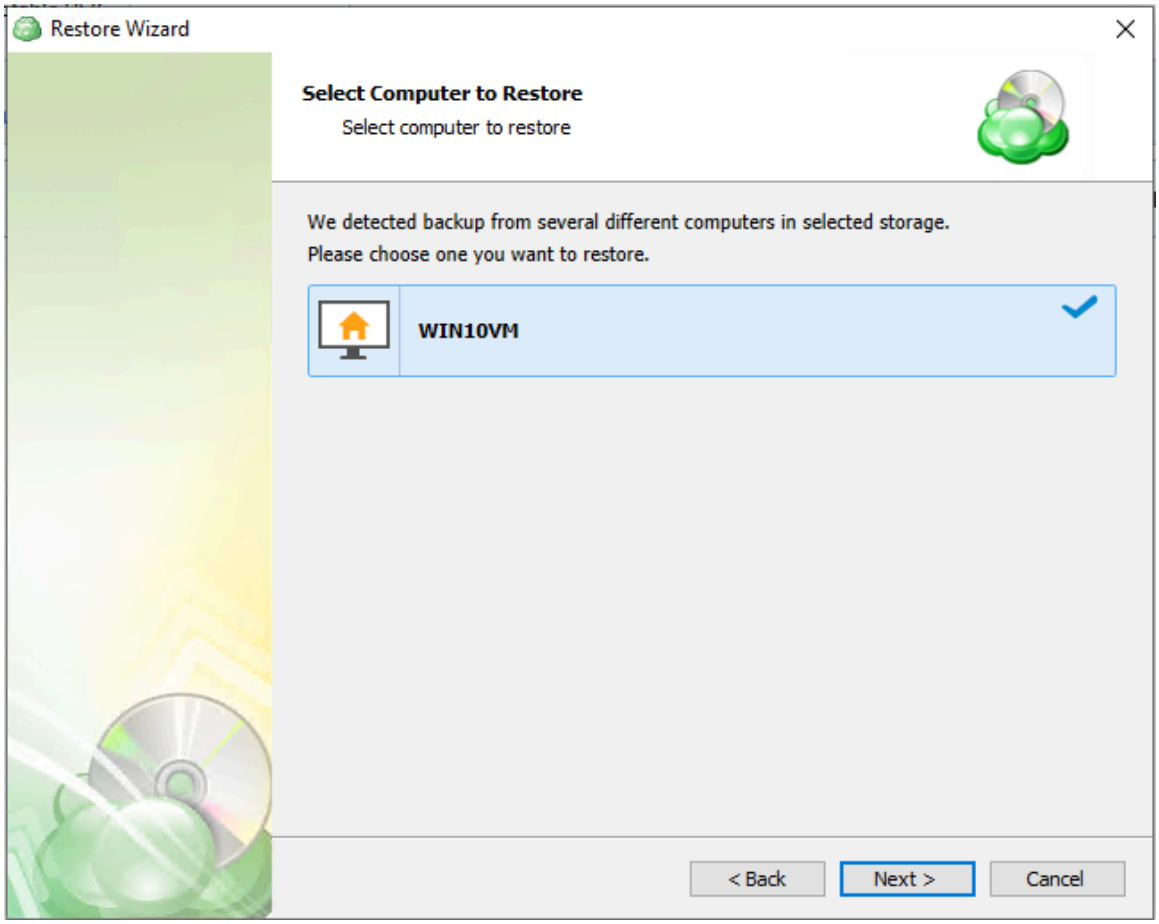


If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

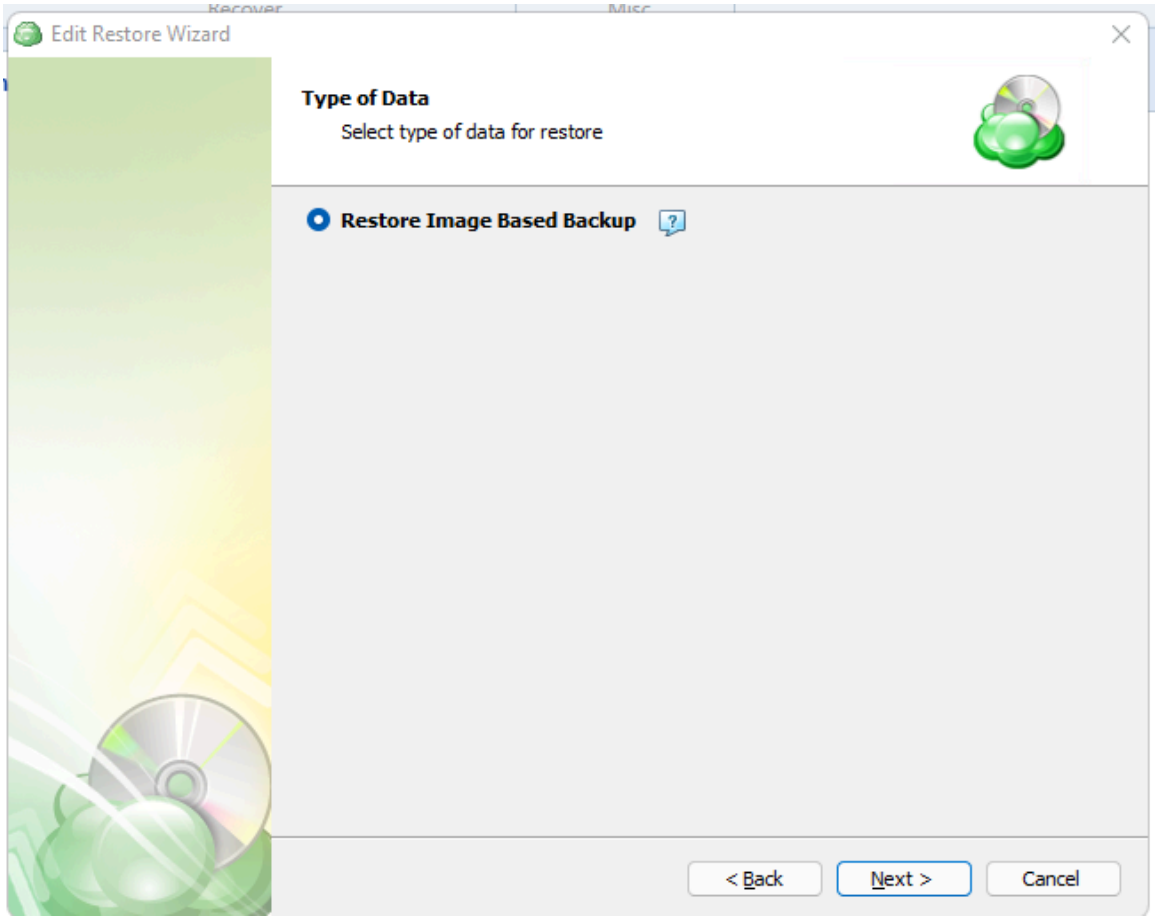
Step 4. Next you will choose whether to run the restore operation only once, or to save it for later use. The latter will allow you to name the plan.



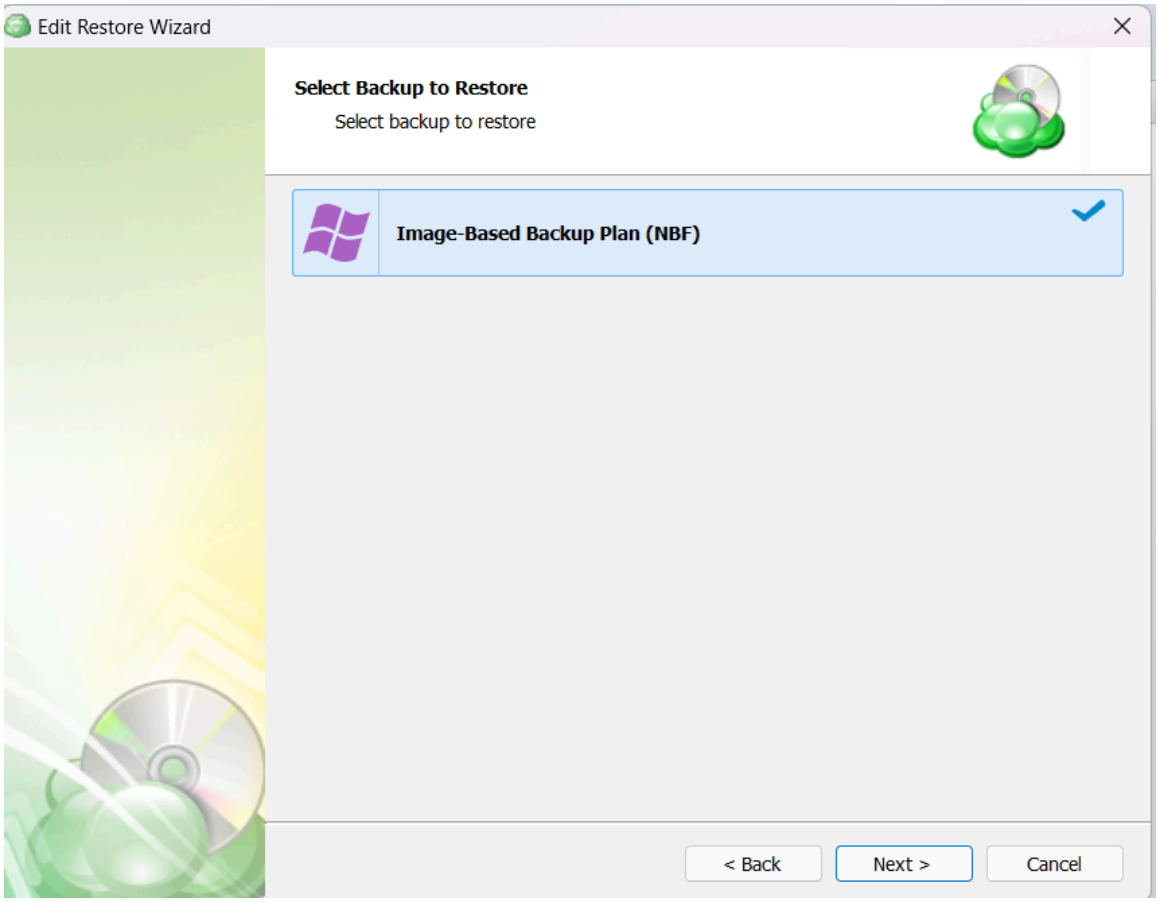
Step 5. Next you will be presented with a list of computers with the same prefix and associated "Backup User" as the computer on which the Agent is currently running. Click to select the desired computer then click on "Next".



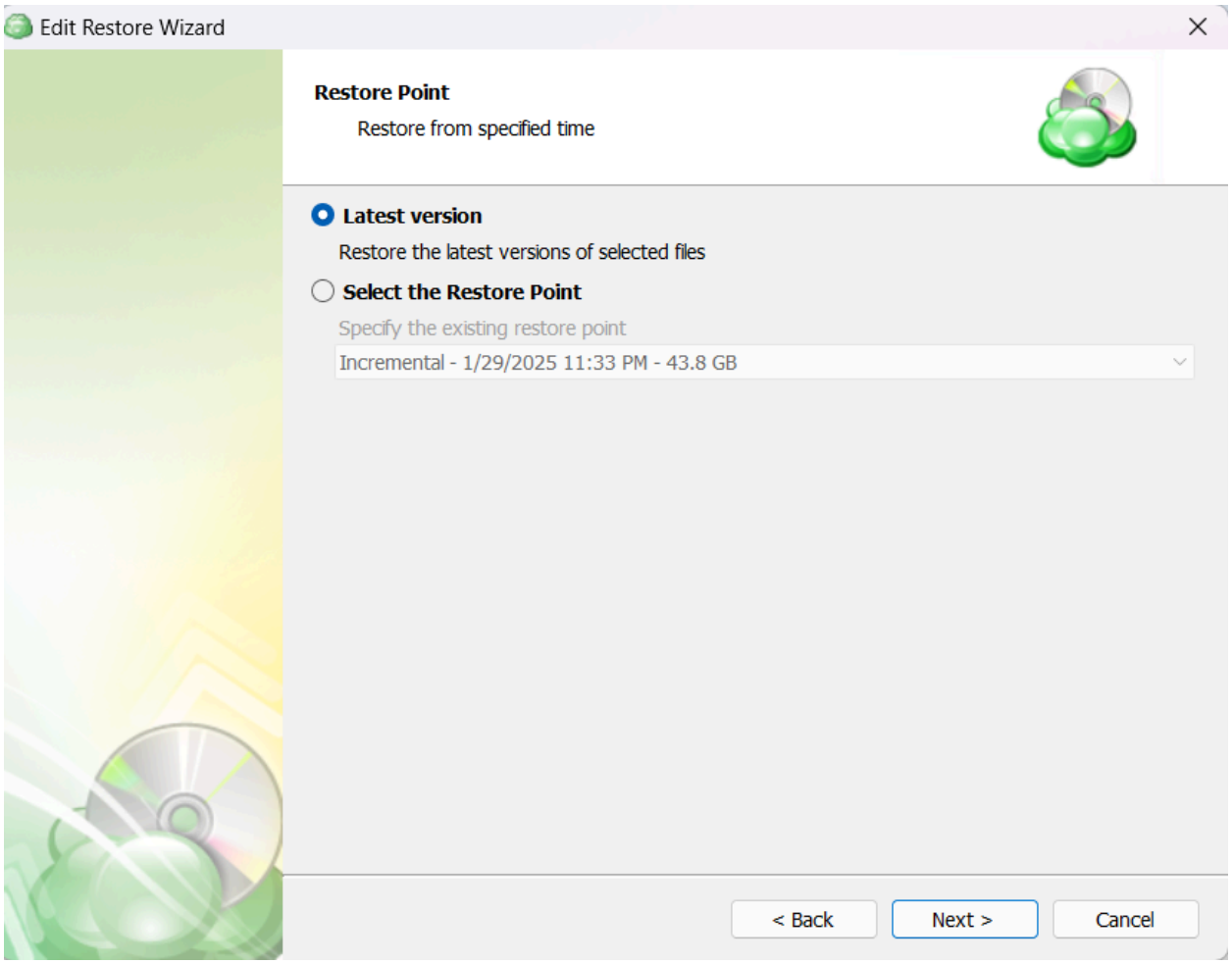
Step 6. Based on the contents of the selected source and computer, the next step is to choose the type of restore. Select “Restore Image Based Backup” then continue to the next step by clicking “Next”.



Step 7. With the correct type of restore selected, the application will generate a list of available backup plans.

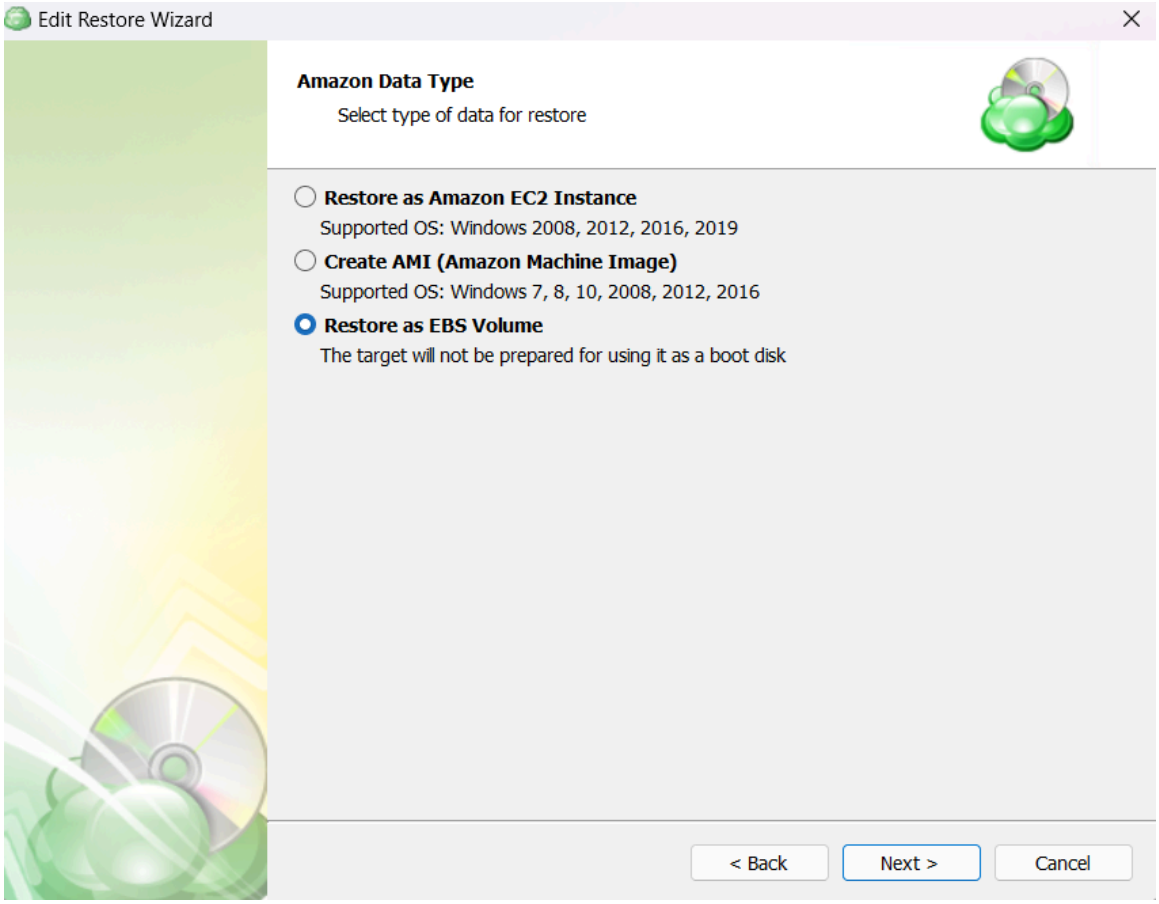


Step 8. The next step is to select the desired point in time to restore to.



- **Latest Version:** Automatically restores the most recent backup restore point.
- **Select the Restore Point:** Allows you to select a specific restore point (date) to restore.

Step 9. Next, select the desired target format for the restored data

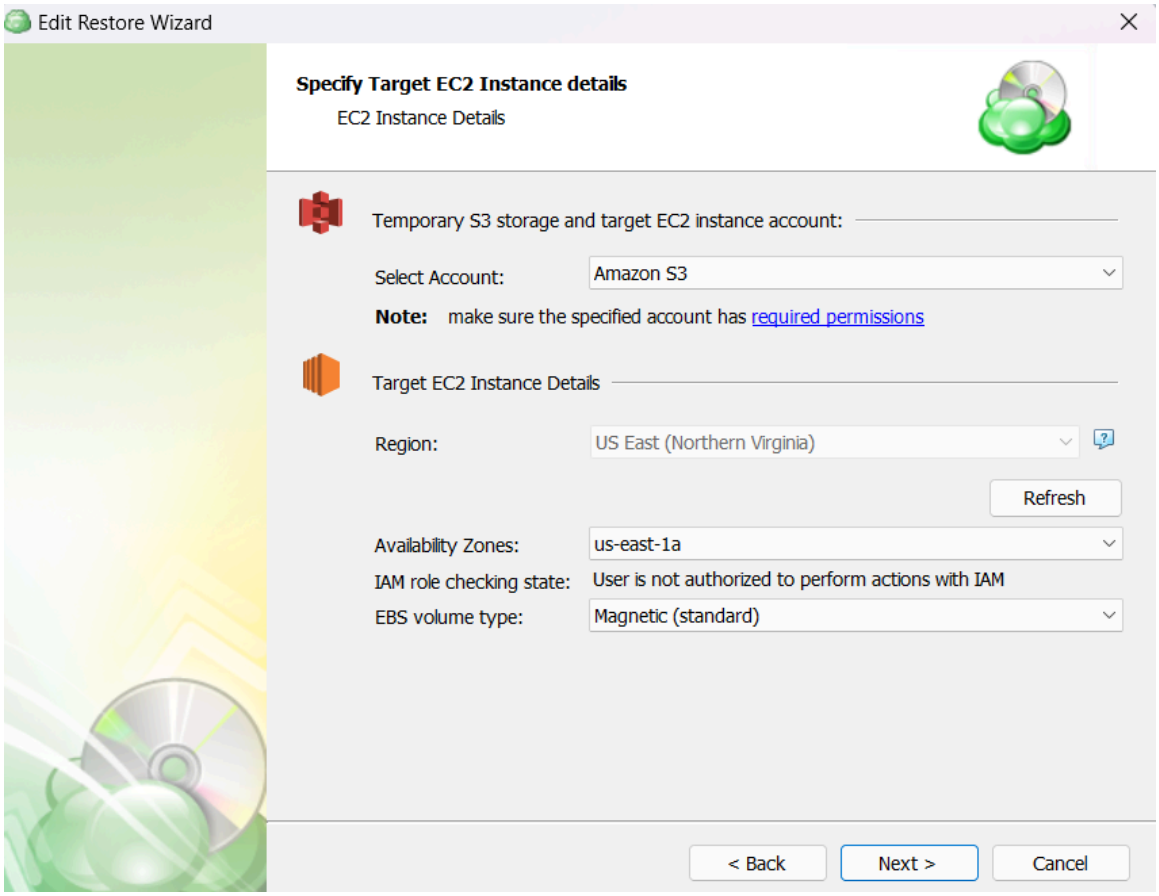


- **Restore as Amazon EC2 Instance:** Restores the partitions selected later to a physical disk.
- **Create AMI (Amazon Machine Image):** Restores the data as a virtual disk in multiple supported formats.
- **Restore as an EBS Volume:** Restores the data as either an EC2 machine, EBS volume, or Amazon Machine Image.

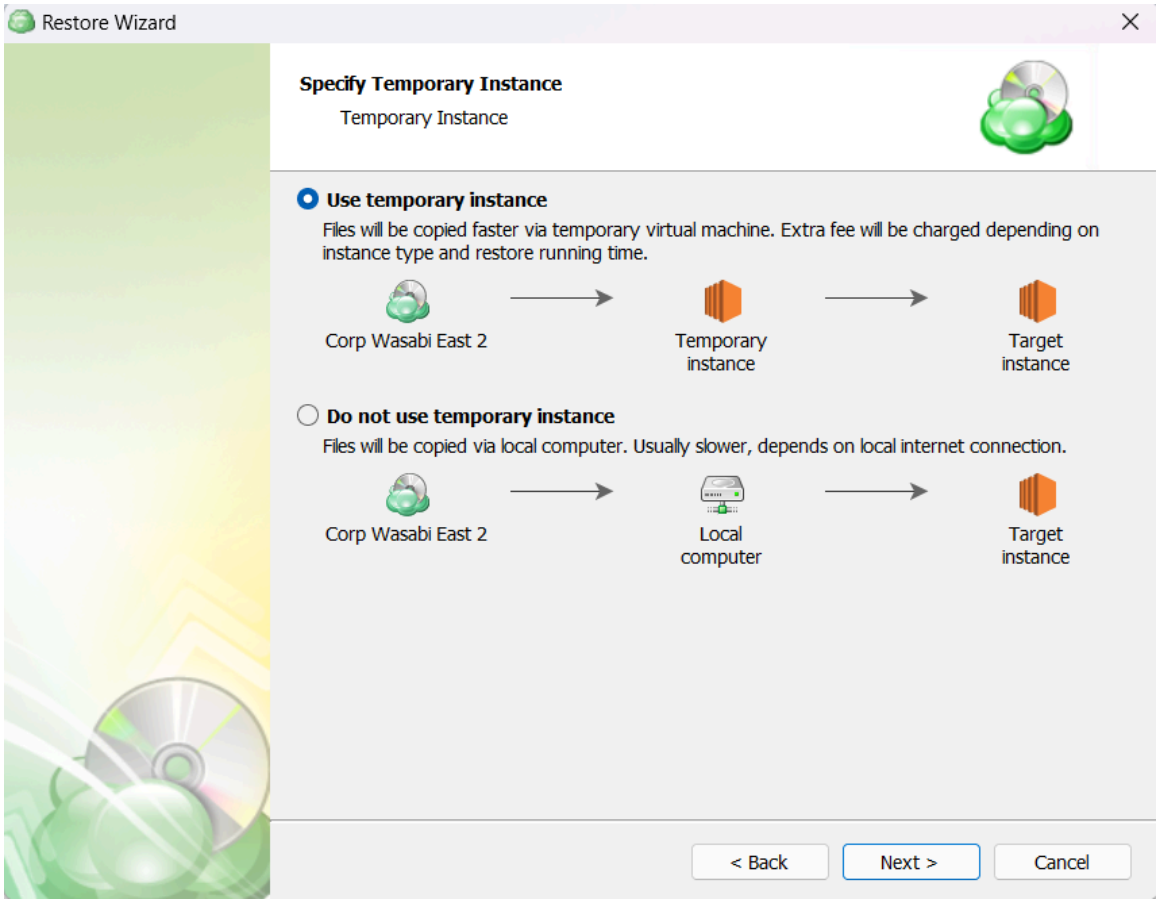
For AWS and Azure destinations, a storage account must already be specified through the MBS portal

Step 10. After selecting the type of restore target in the previous step, you are prompted to specify the parameters of the new EBS volume.

- **Select Account:** Please select the target AWS account.
- **Region:** Specify the geographic region for the target EBS volume.
- **Availability Zones**: Select one of the availability zones (depends on the region).
- **EBS volume type:** Specify the EBS volume type. The available options are: *Magnetic (standard), General Purpose SSD (gp2), Provisioned IOPS SSD (io1), Cold HDD (sc1), Throughput Optimized HDD (st1).* You can find more information about EBS volume types in AWS documentation.



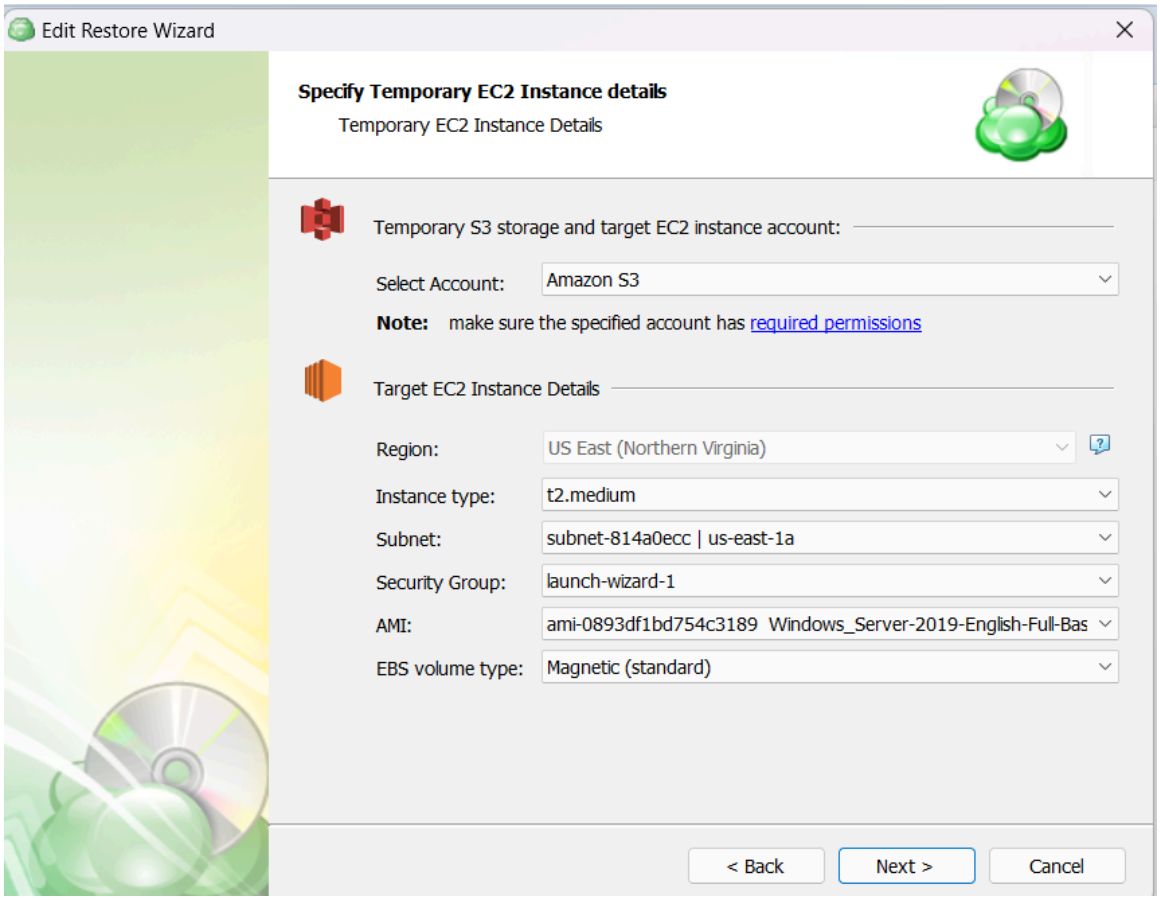
Step 11. After specifying the target EC2 instance details, you will need to choose between using a temporary EC2 instance or local computer for the restore operation.



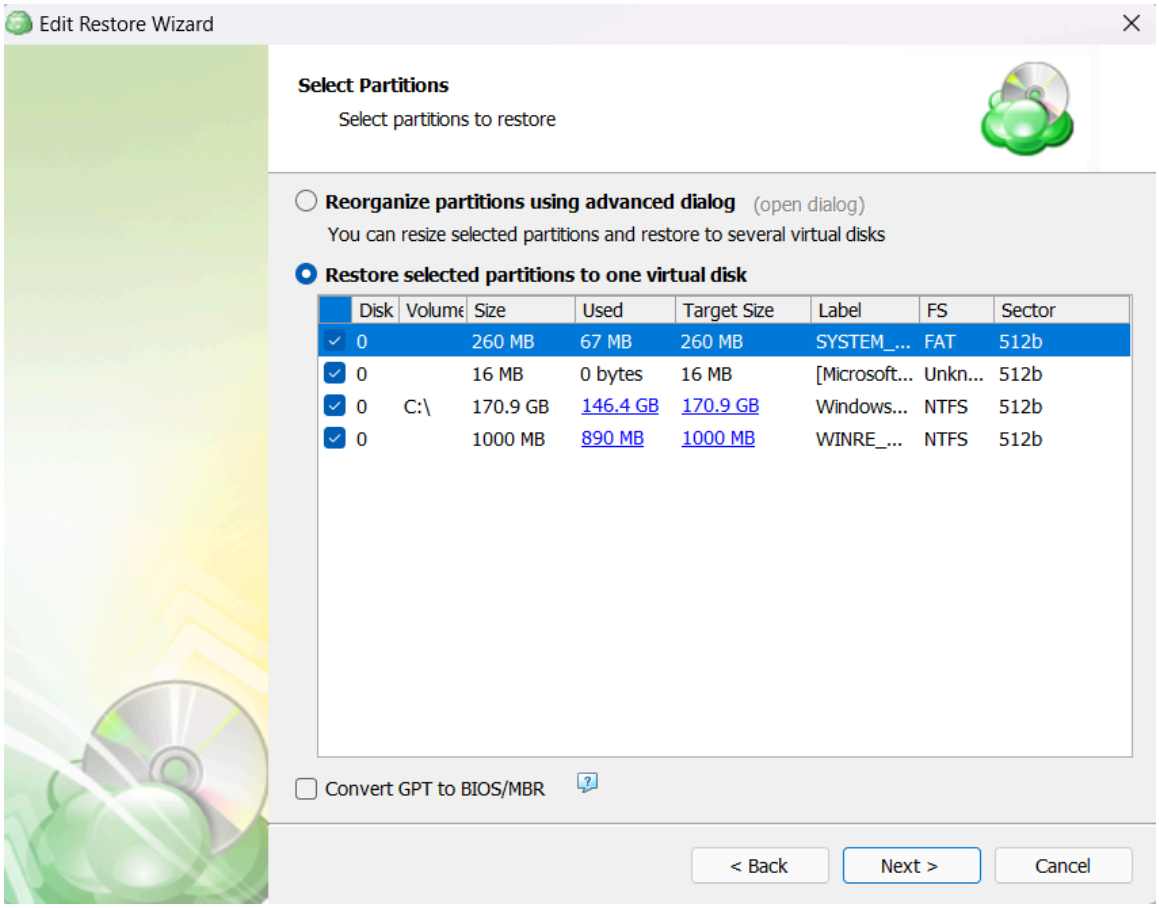
- **Use temporary instance:** This option creates a temporary EC2 instance in Amazon Web Services that will download backup data from the storage destination and restore it as a target instance. Usually, this method is faster as the temporary and target instance are located in the same AWS network.
- **Do not use temporary instance:** When selecting this option, the restore operation will be performed using the resources of local computer. Usually, this approach is slower, depending on the local internet connection.

> Enabling the "**Use temporary instance"** option will lead to additional charges in Amazon Web Services for running the temporary EC2 instance. Please check the AWS documentation on instance types and pricing for more information.

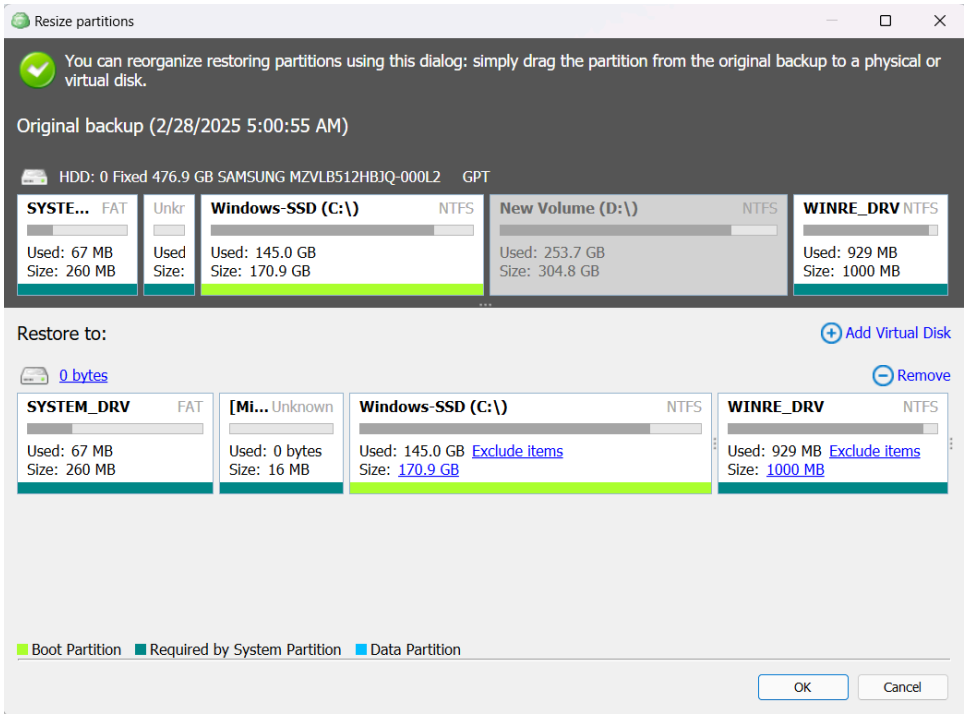
Step 12. If you have selected to use a temporary instance, the next page will allow you to select the Amazon account from the upper dropdown box, and specify the Temporary EC2 Instance details below.



Step 13. After selecting the type of restore target in the previous step, you can now choose to restore the partitions with their existing parameters or to reorganize and resize them.

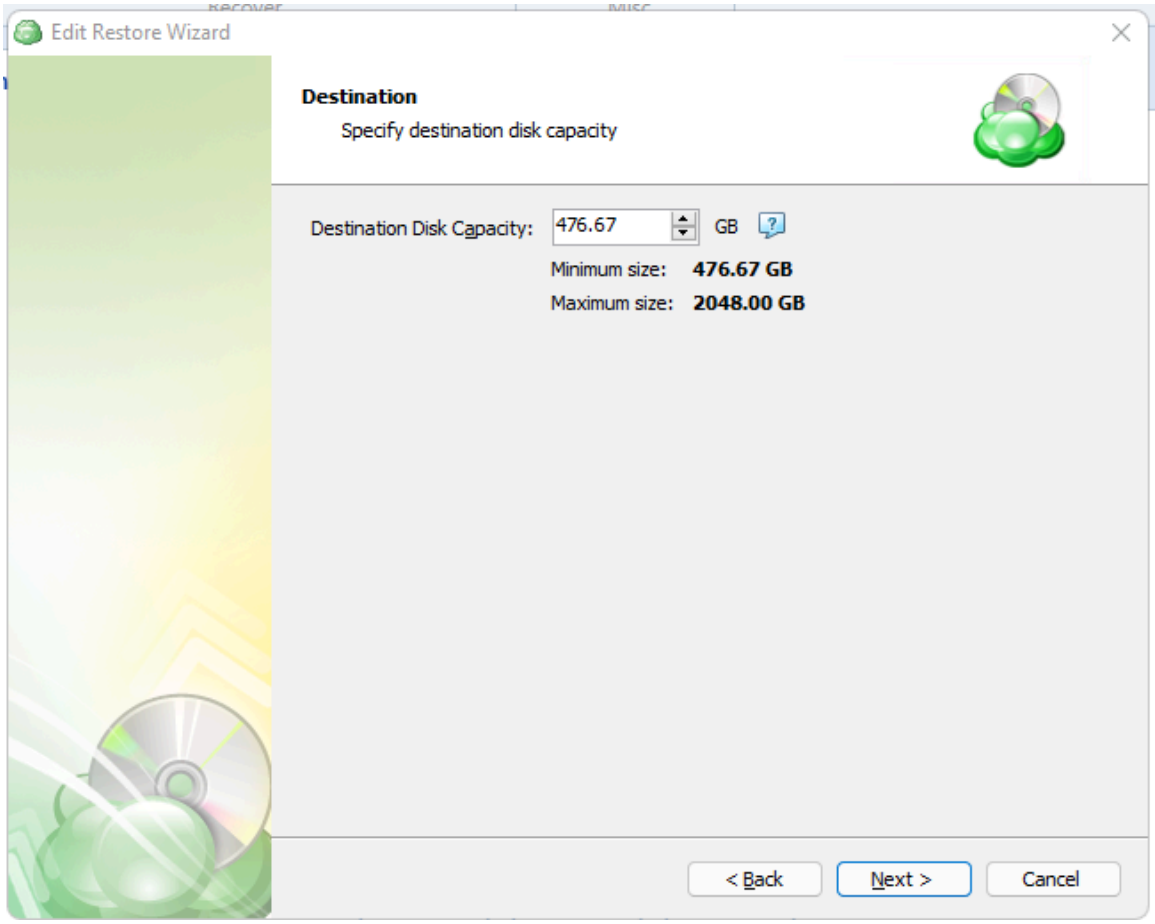


If you select “Reorganize partitions using advanced dialog” a new window will appear and allow you to resize the partitions and rearrange them on one or more virtual disks.

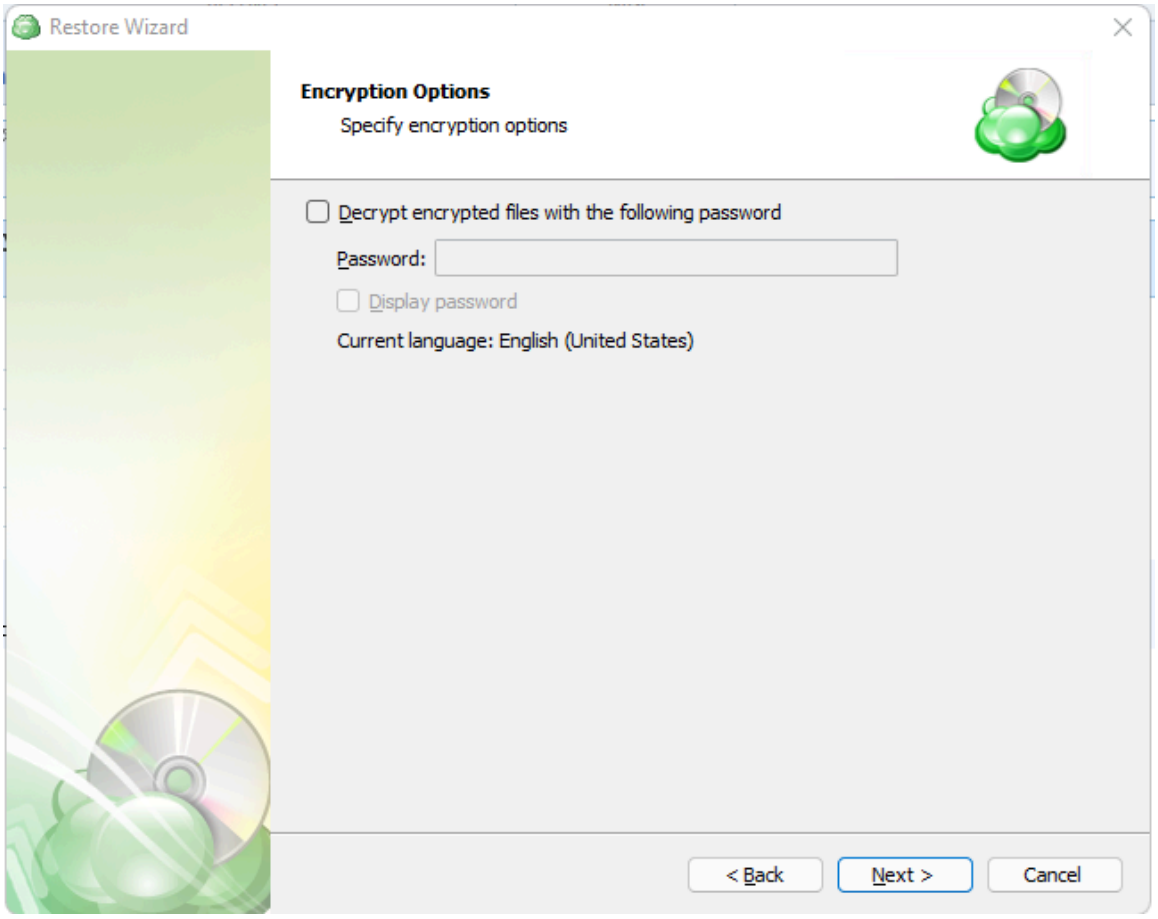


Click on any of the blue hyperlinks to open additional dialogue boxes allowing you greater control over the name and size of the virtual disk, as well as the ability to add additional virtual disks, and also exclude specific files or folders if desired.

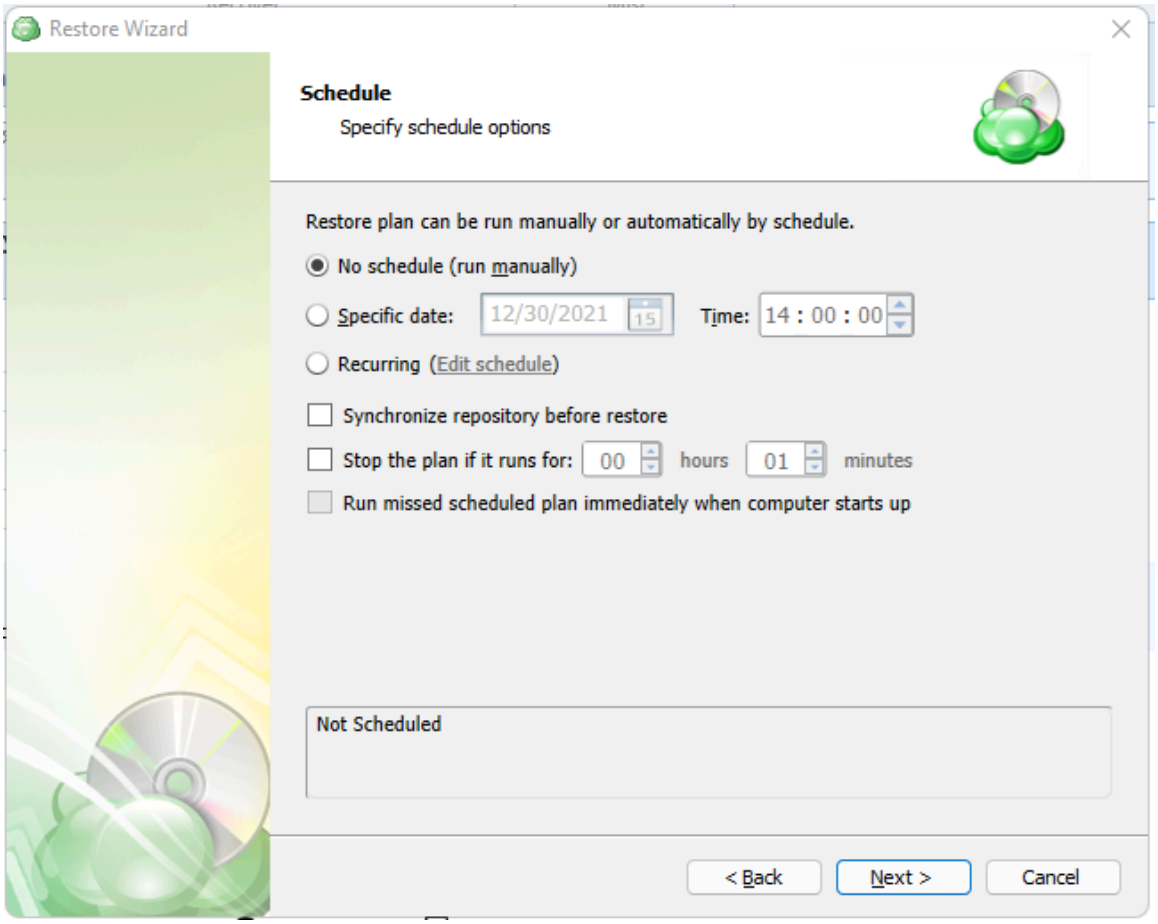
Step 14. Once the partitions are selected, the next step allows you to choose the size of the virtual disk used by the instance.



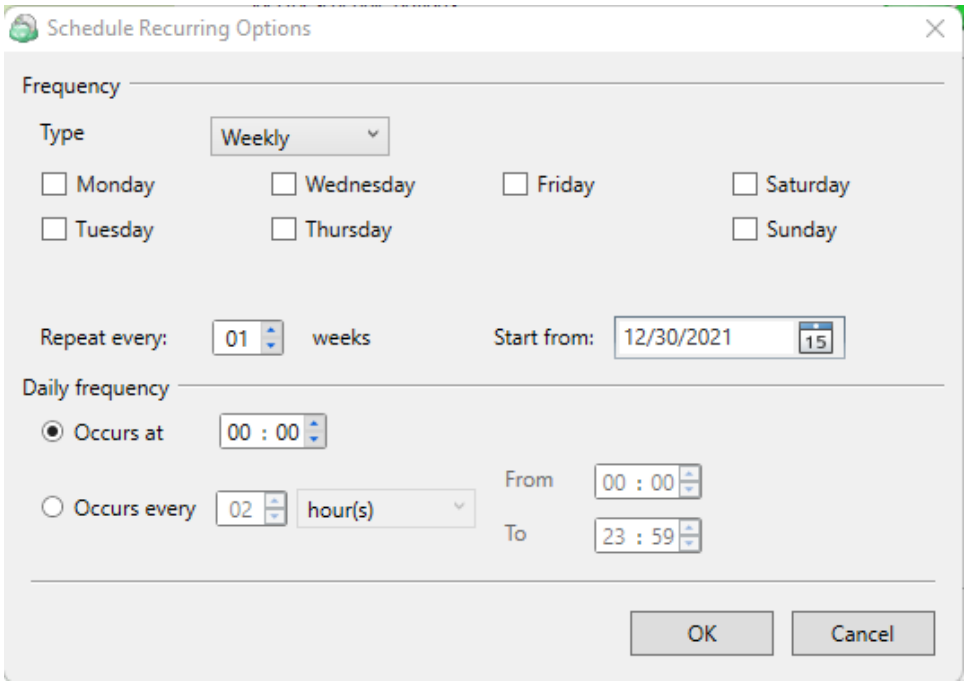
Step 15. If the backed up data was encrypted, the next step will be to enter the password for decryption. If the password is incorrect or missing, the restore plan will fail and you will need to edit the plan to input the correct password.



Step 16. If the restore plan is saved for later, next you will set the schedule for the plan, otherwise proceed to the next step.



- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria by clicking on the “Edit schedule” hyperlink to open this dialogue:

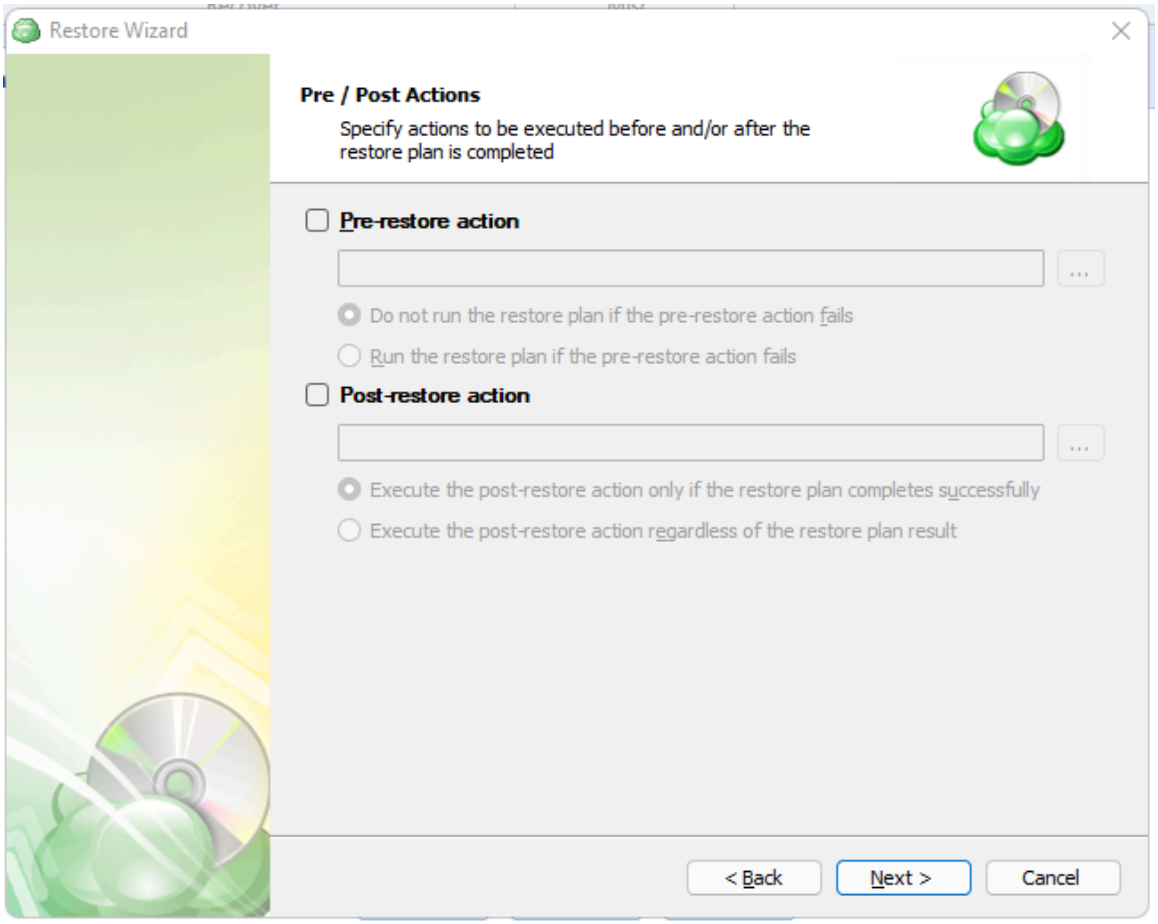


It is recommended to enable the "**Synchronize repository before restore"** if you are restoring on a computer different from the original or you are restoring data while logged in with a new or different backup user.

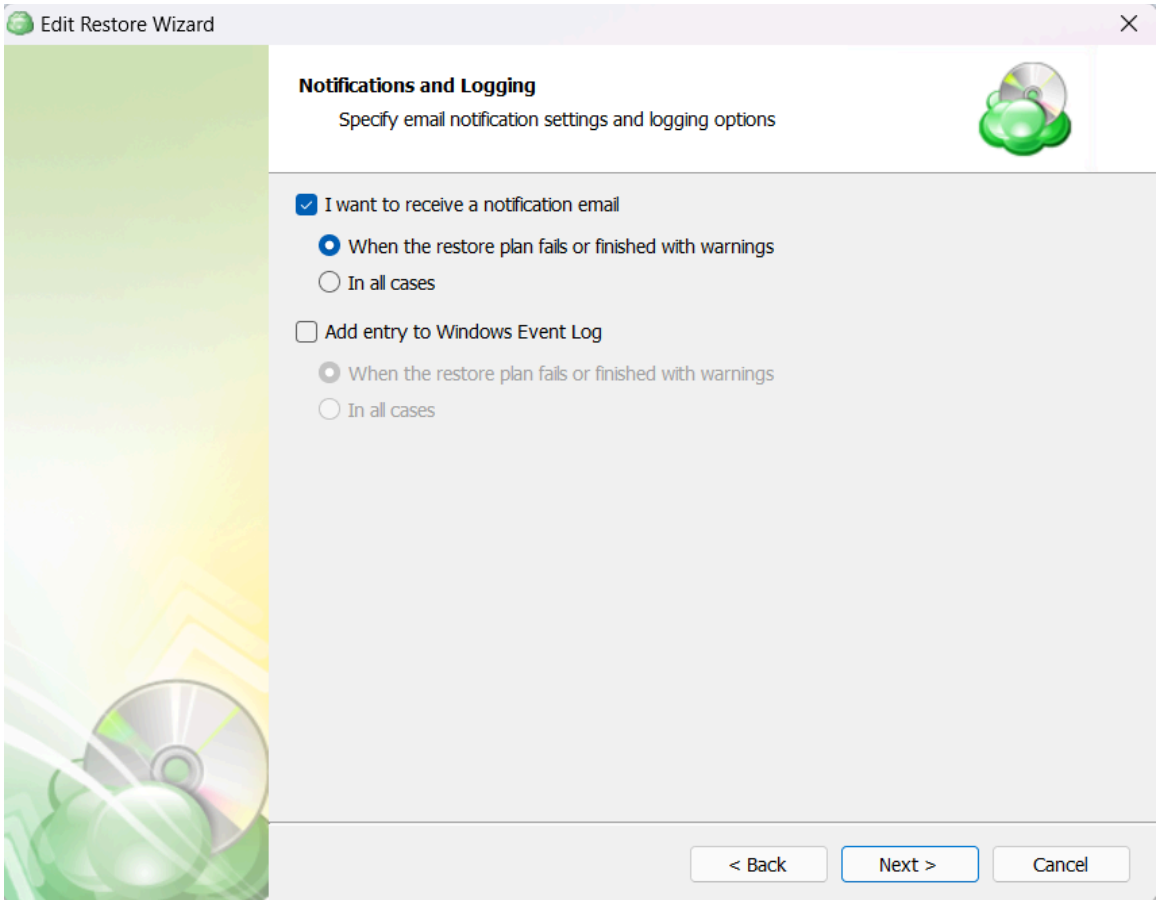
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

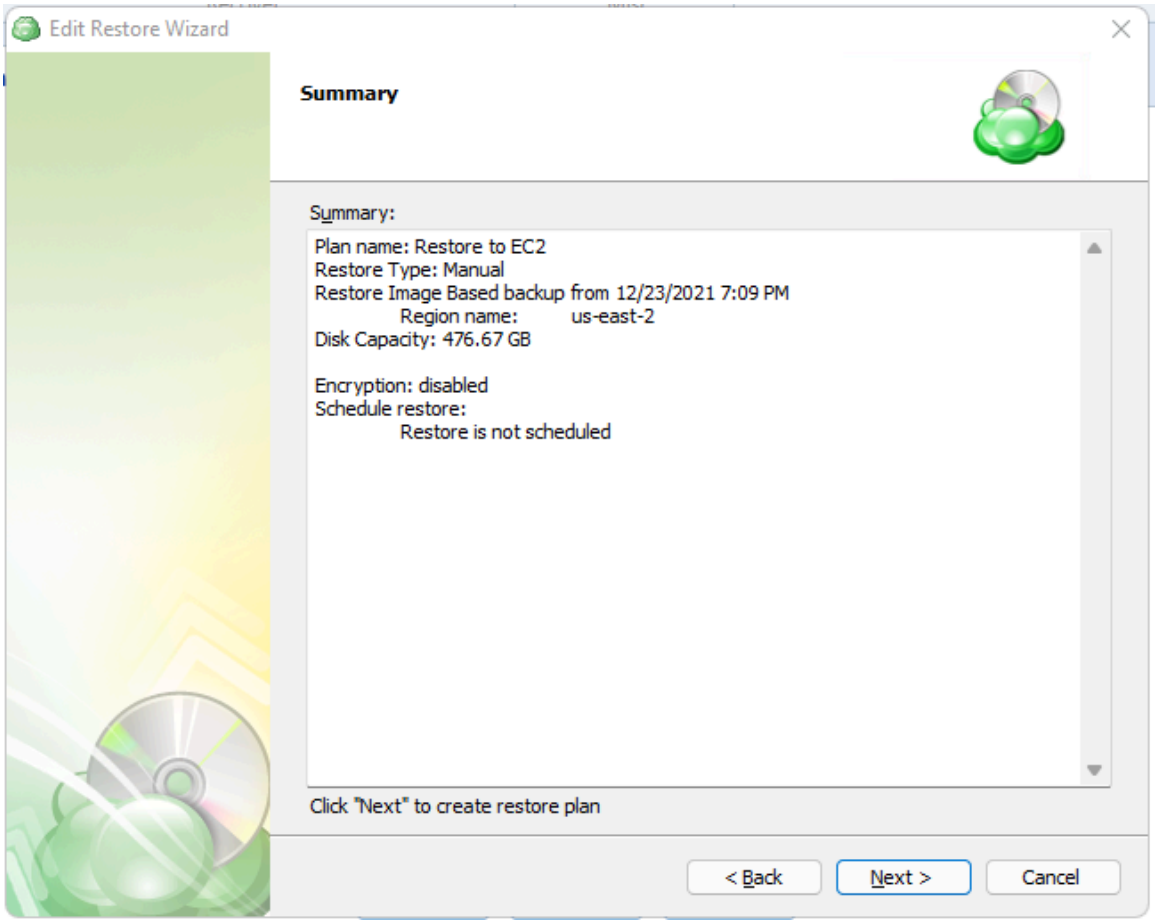
Step 17. The next step page allows the execution of custom scripts before and/or after the running of a Restore Plan.



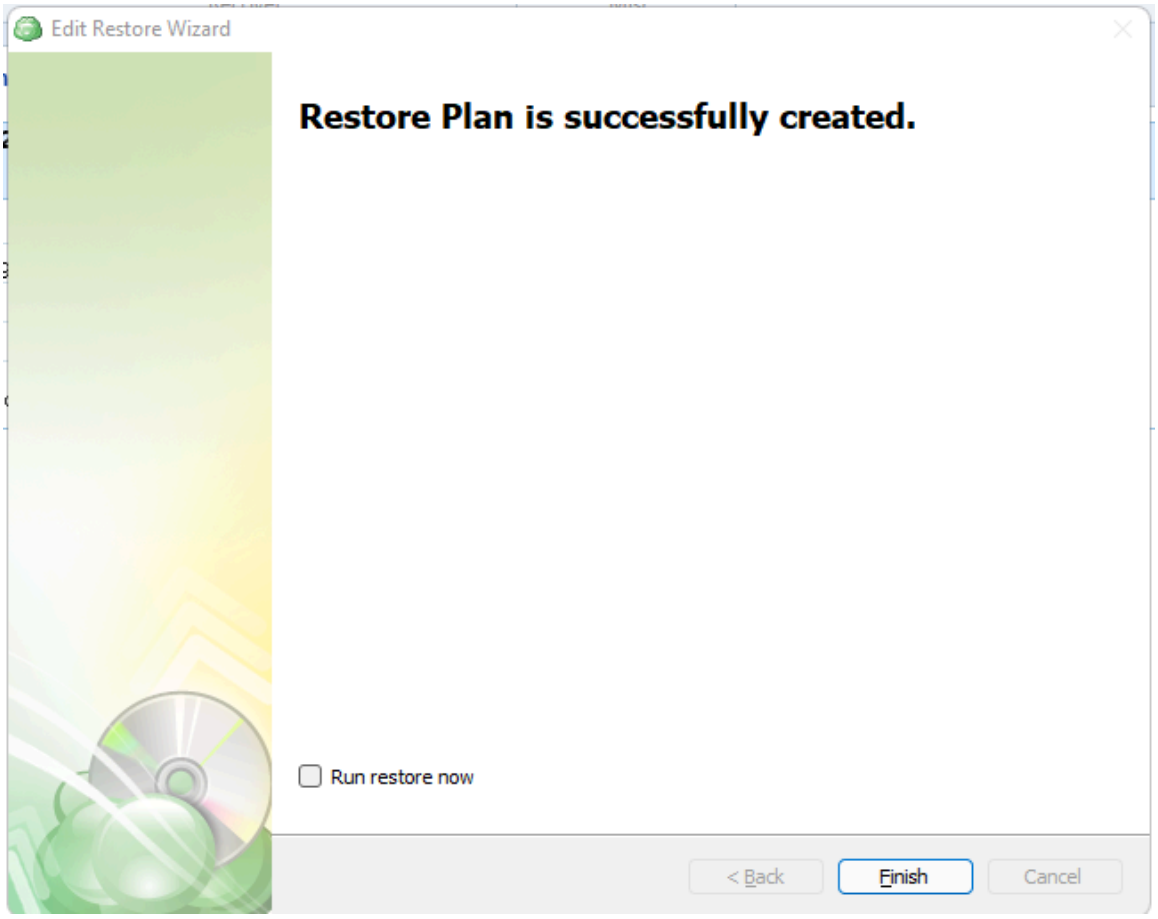
Step 18. The “Notifications and Logging” page allows you to enable notification email and add an entry to Windows Event Log upon restore plan completion or failure.



Step 19. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.



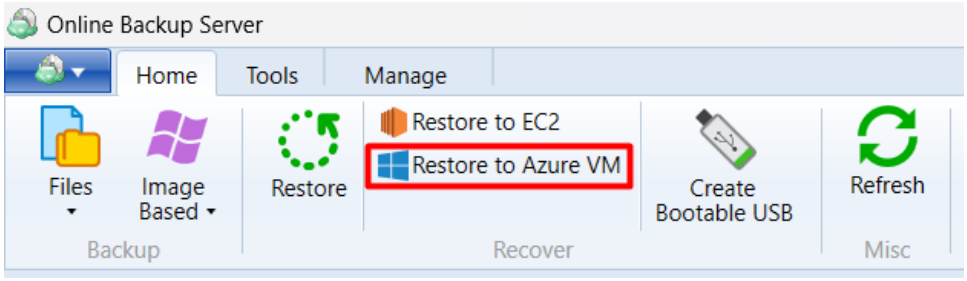
Step 20. The final step of the process is to select when the Restore Plan will start running. To have it start immediately, select the “Run Backup Now” option and click “Finish”. Otherwise, click “Finish” and the plan will begin at the next scheduled time.



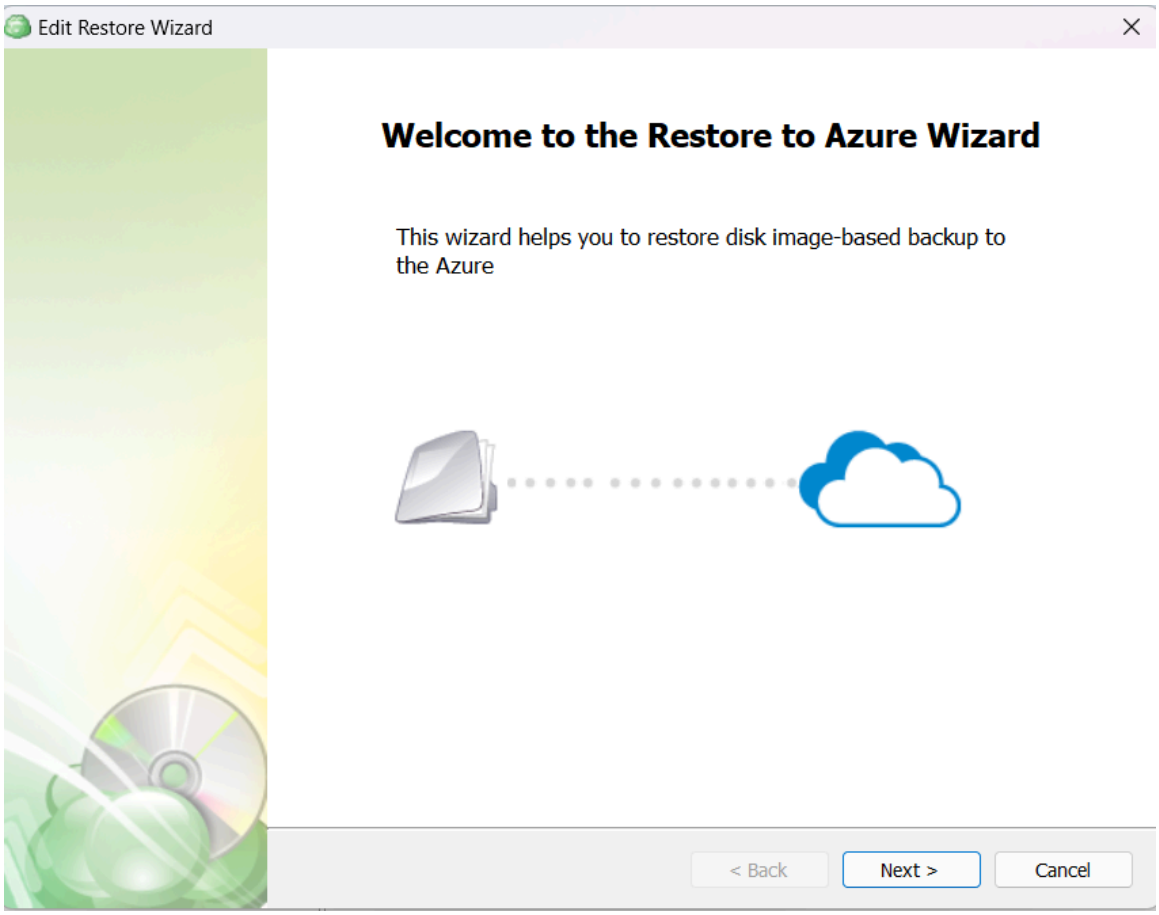
Restore to an Azure VM Instance - Agent

> Please note that in order to enable restore to AzureVM, you need to prepare your Azure environment (create a Resource Group, Storage Container, Virtual Network, Subnet, and Network Security Group). You can find more info in the help article below:
> https://help.mspbackups.com/restore/restore2cloud/restore-azurevm/prepare

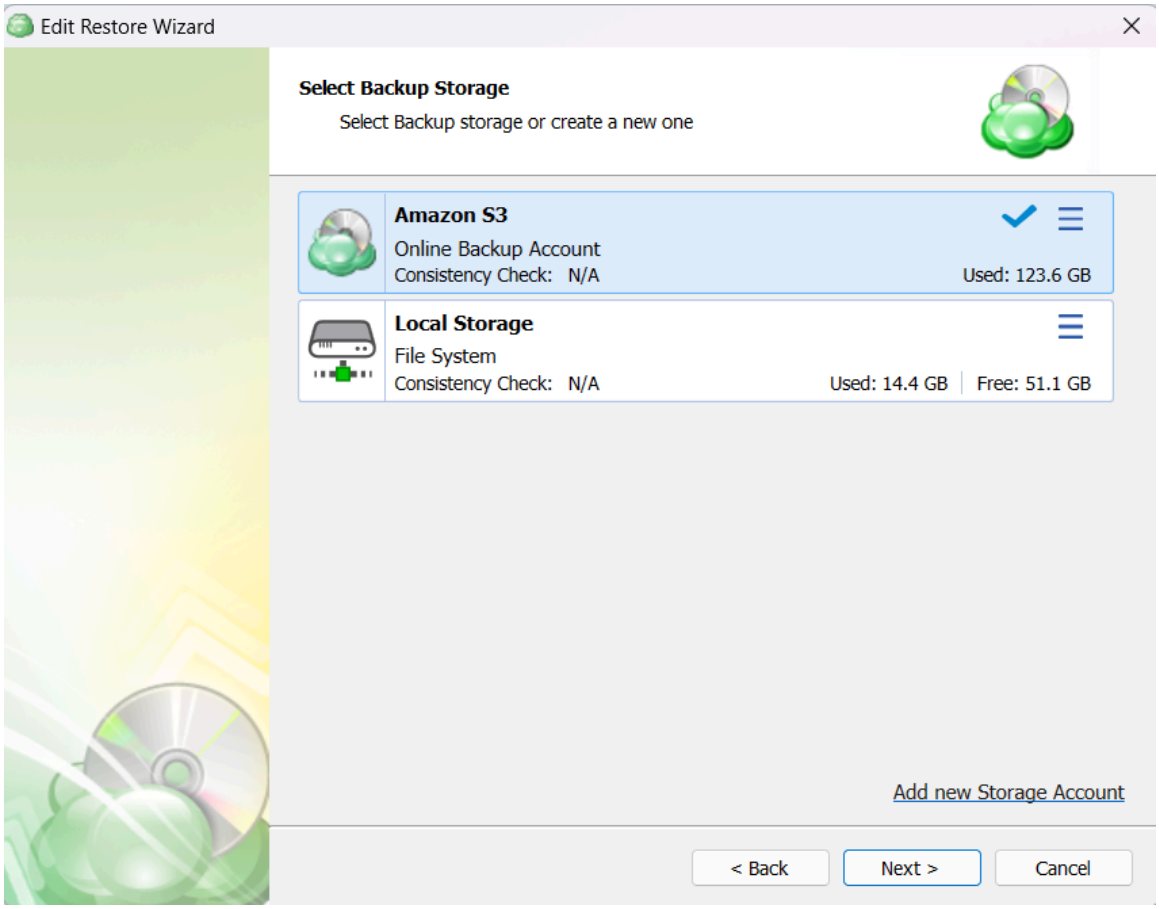
Step 1. After launching the Online Backup, please click on the “Restore to Azure VM” button.



Step 2. The first step of the wizard indicates that you have started the wizard.

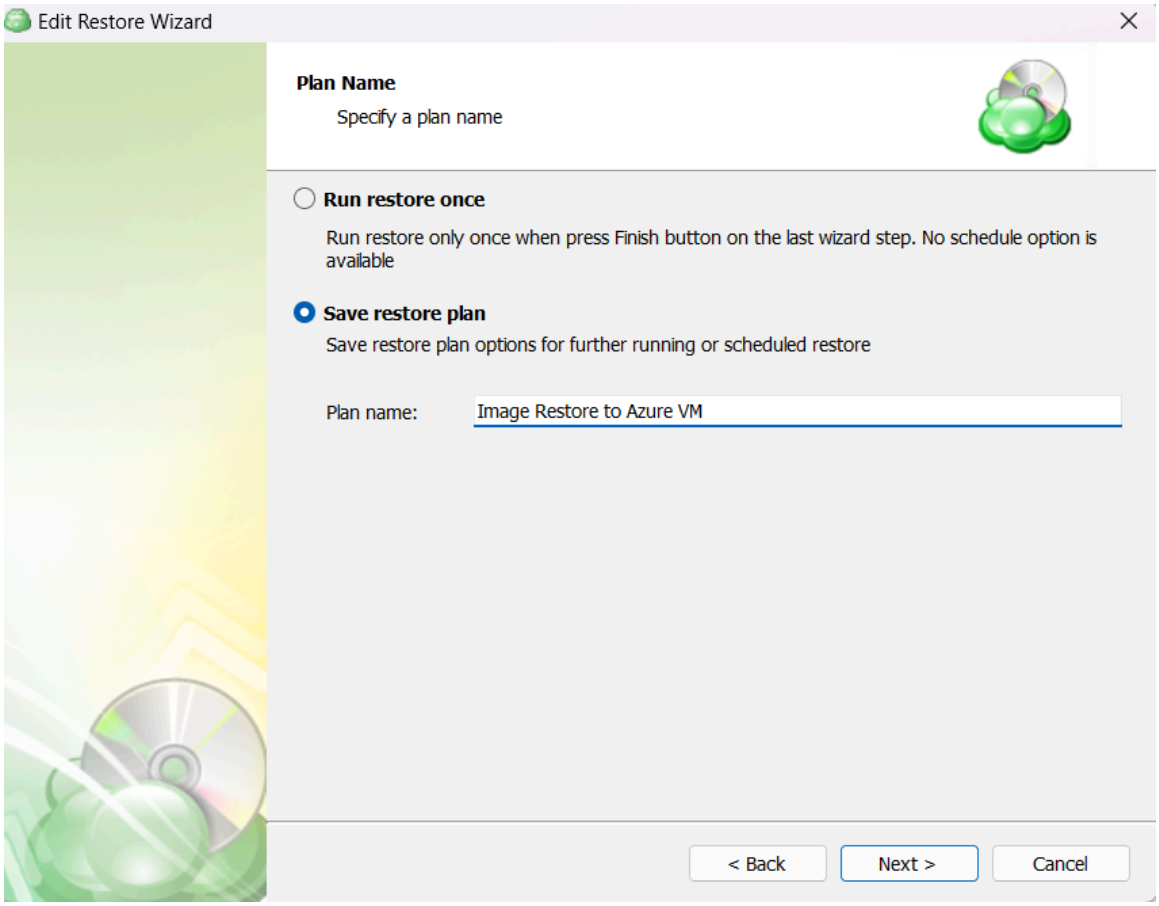


Step 3. The next step will prompt you to select the storage location for the source.

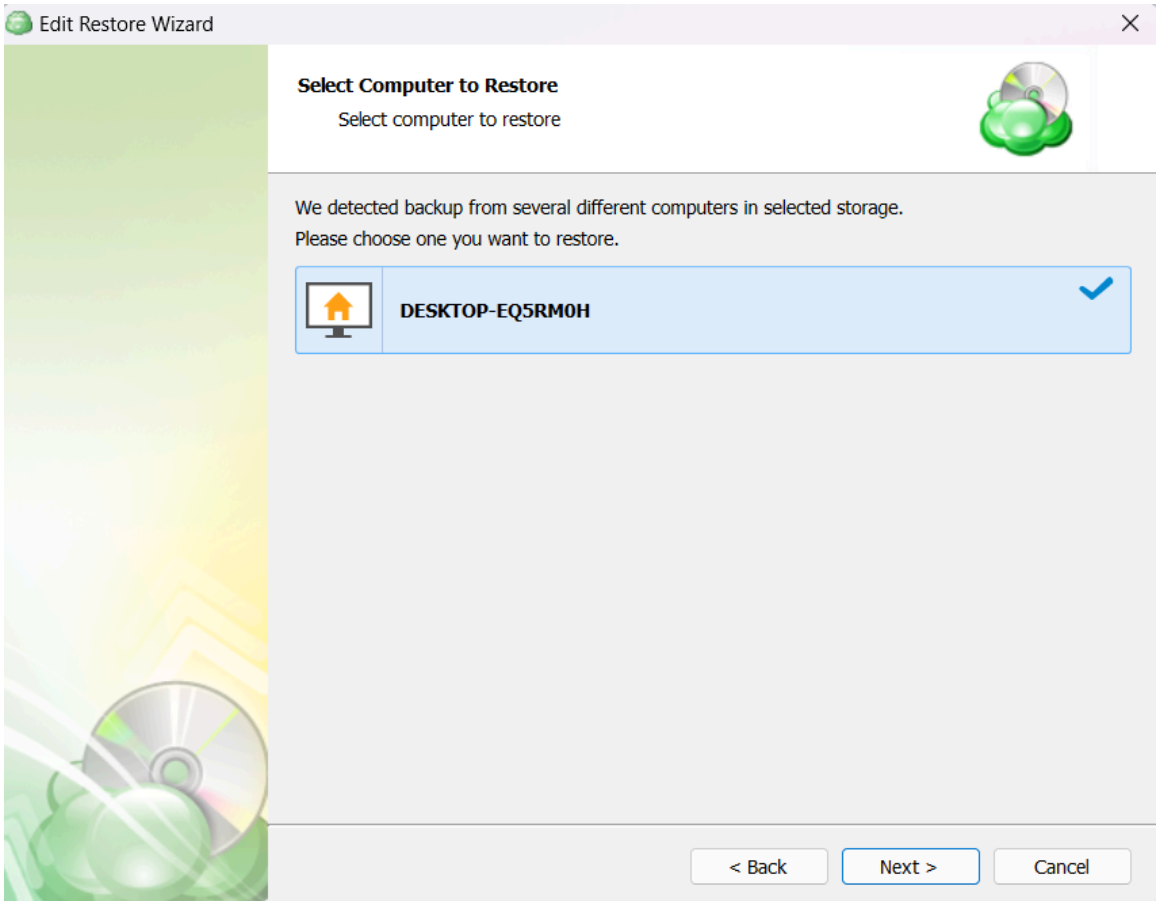


You can click “Add new Storage Account” to add a new local storage account. If you need to add a new cloud storage, this can be only done via the MBS portal, “Storage Accounts” page.

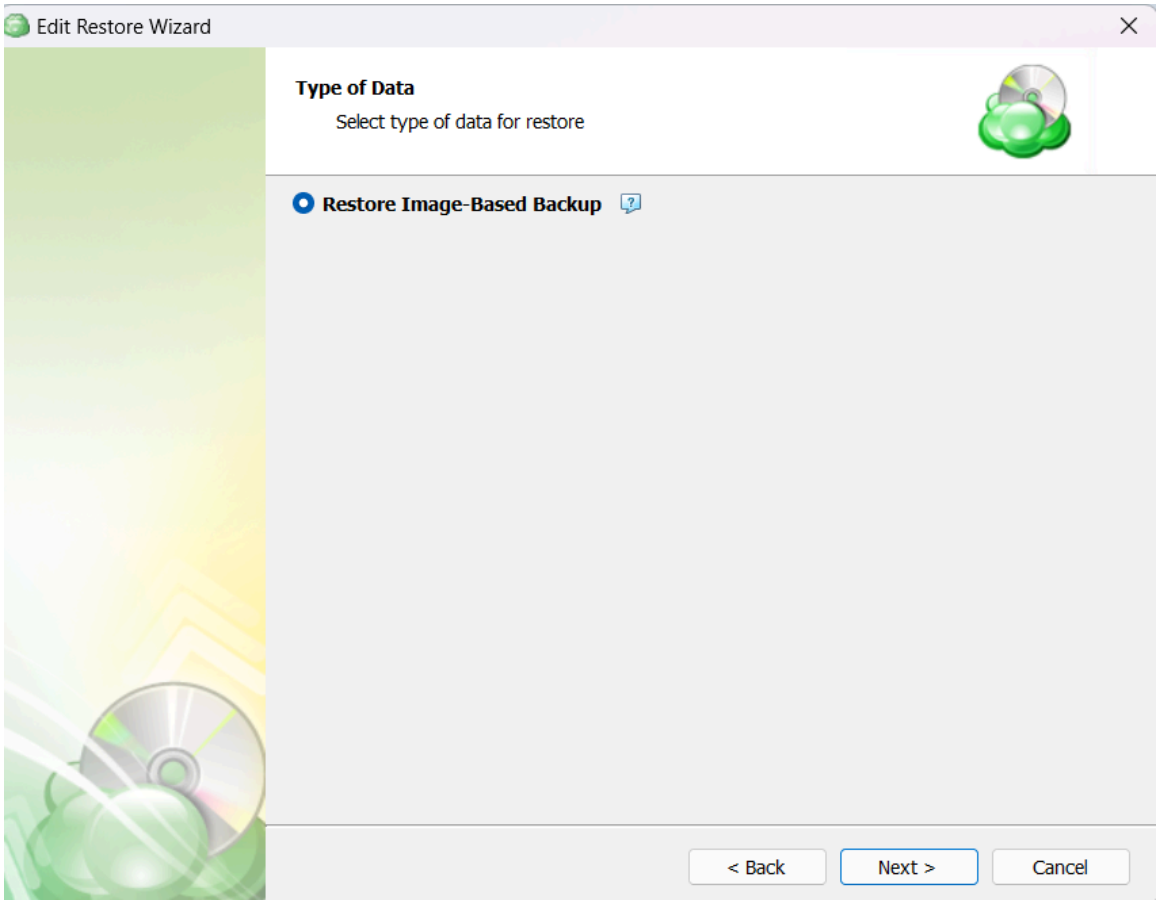
Step 4. Next you will choose whether to run the restore operation only once, or to save it for later use. The latter will allow you to name the plan.



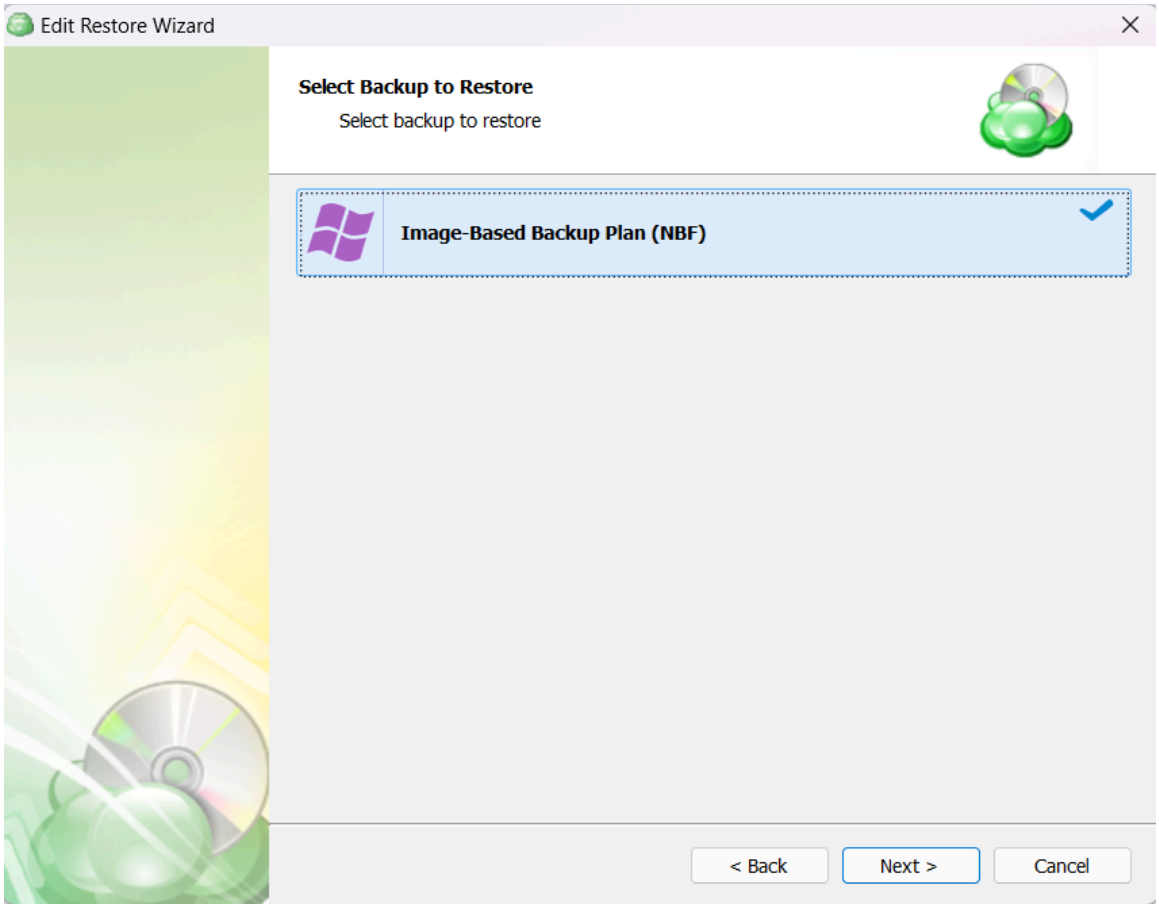
Step 5. Next you will be presented with a list of computers with the same prefix (computer name) and associated “Backup User” as the computer on which the Agent is currently running. Click to select the desired computer then click on “Next”.



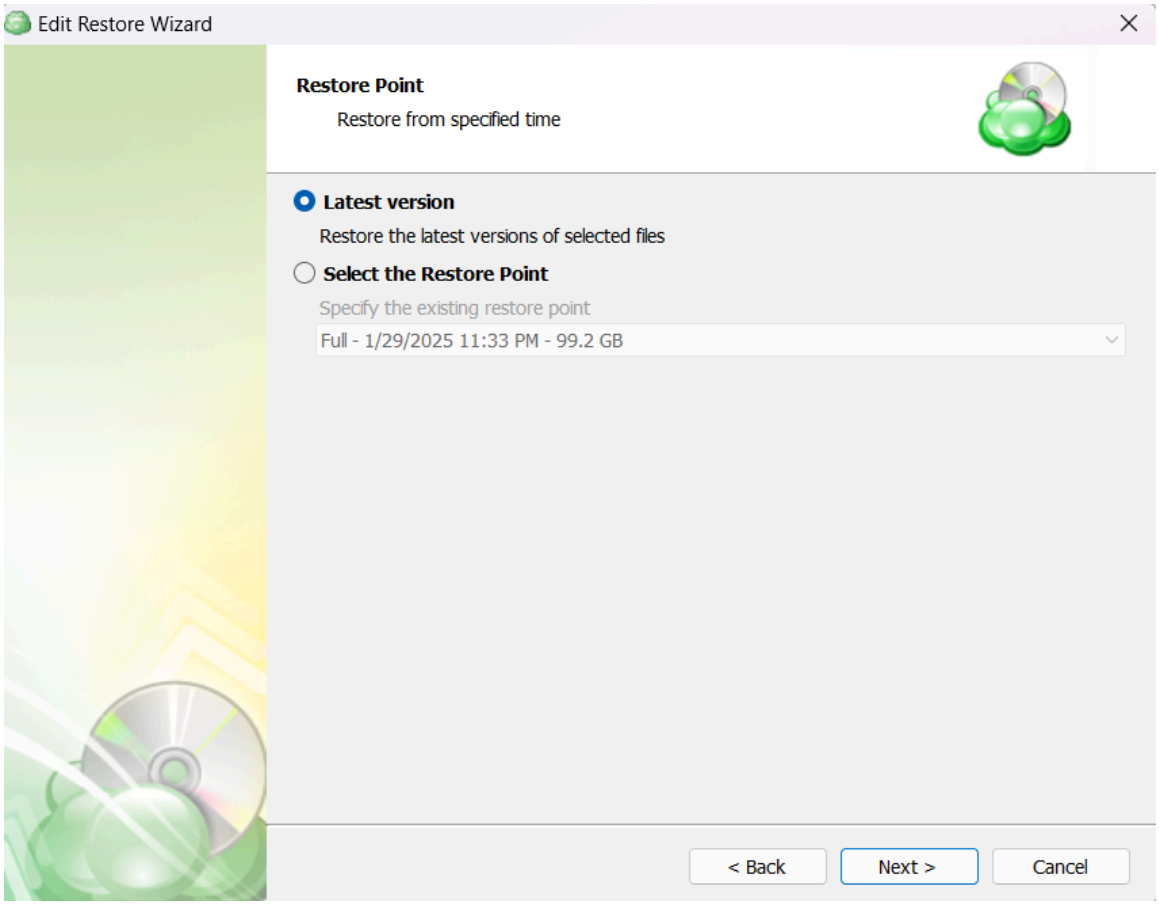
Step 6. Based on the contents of the selected source and computer, the next step is to choose the type of restore. Select “Restore Image Based Backup” then continue to the next step by clicking “Next”.



Step 7. With the correct type of restore selected, the application will generate a list of available backup plans.

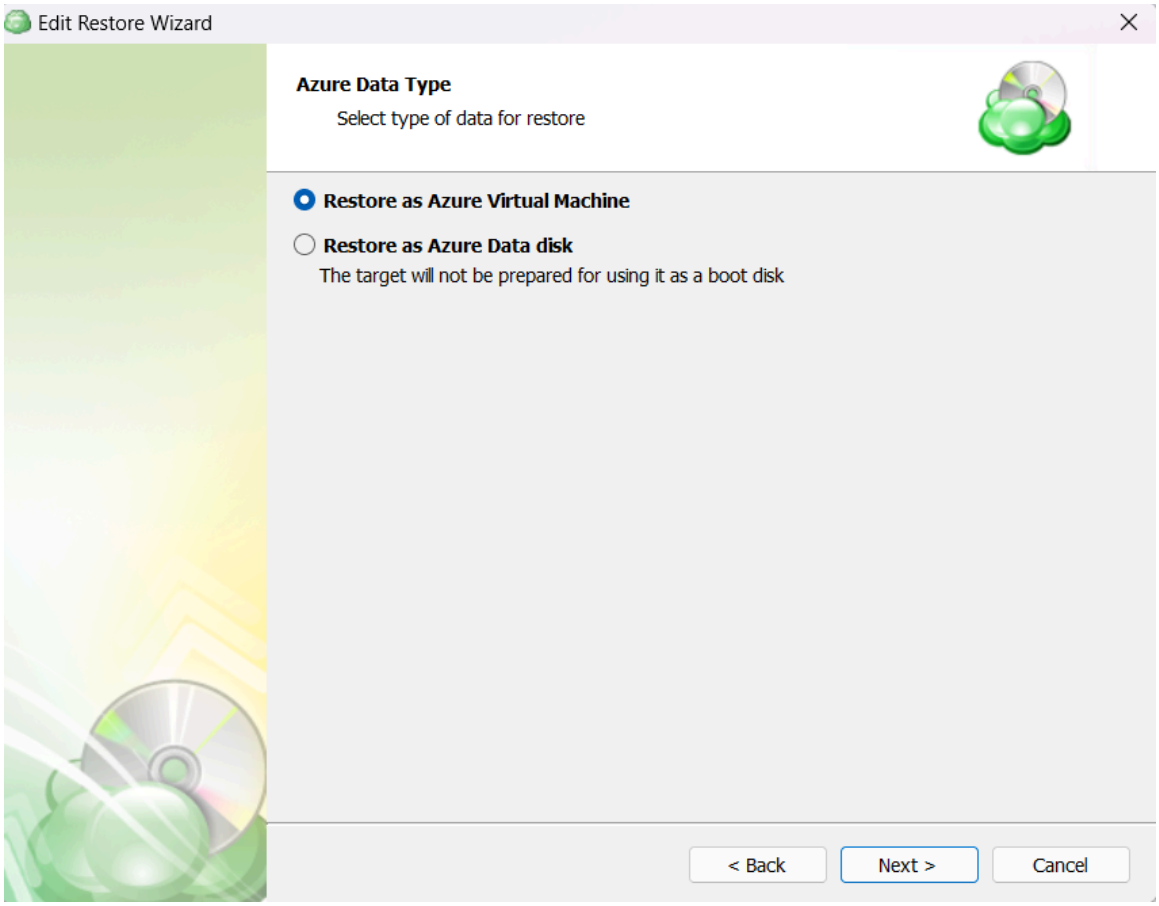


Step 8. The next step is to select the desired point in time to restore to.



- **Latest Version:** Automatically restores the most recent backup restore point.
- **Select the Restore Point:** Allows you to select a specific restore point (date) to restore.

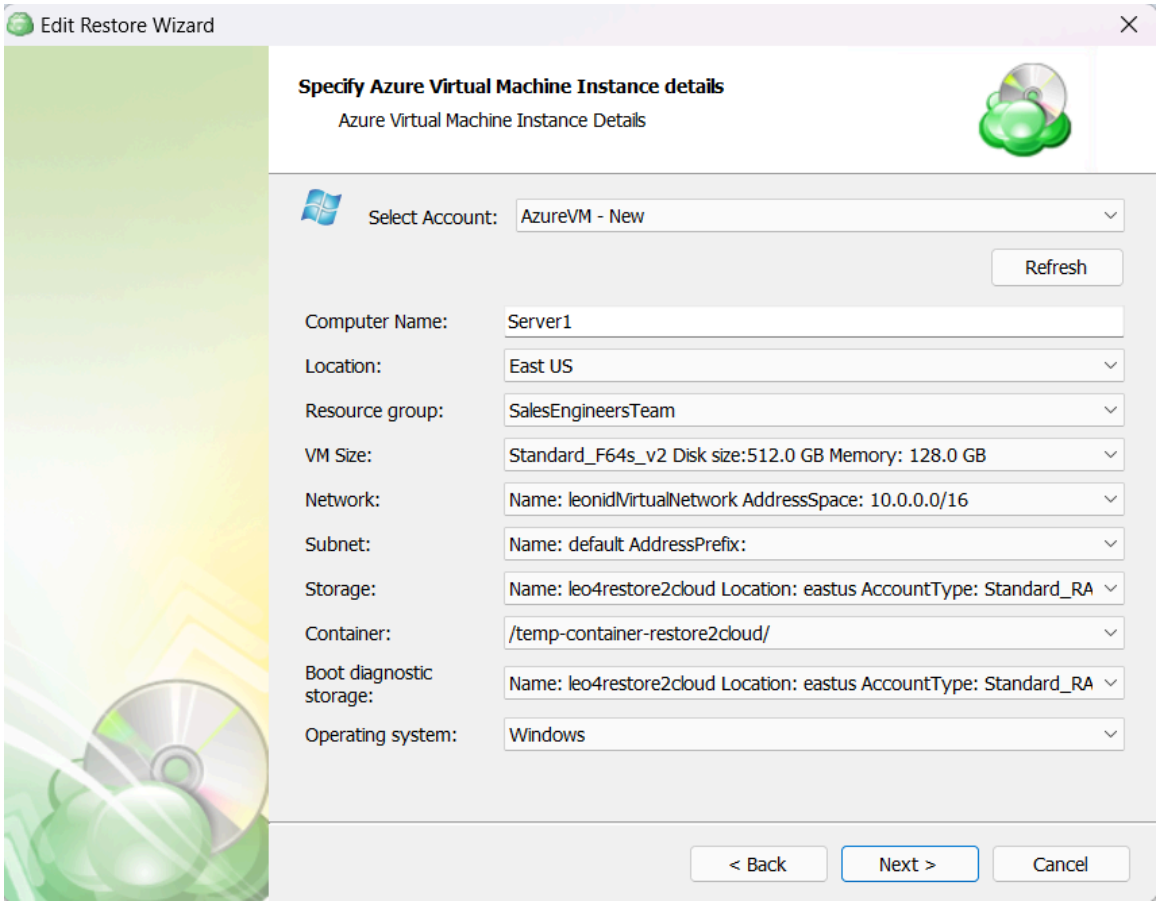
Step 9. Next, select the Azure Data Type.



- **Restore as Azure Virtual Machine:** Restores the image to an Azure VM
- **Restore as Azure Data Disk:** Restores the image as an Azure Data Disk

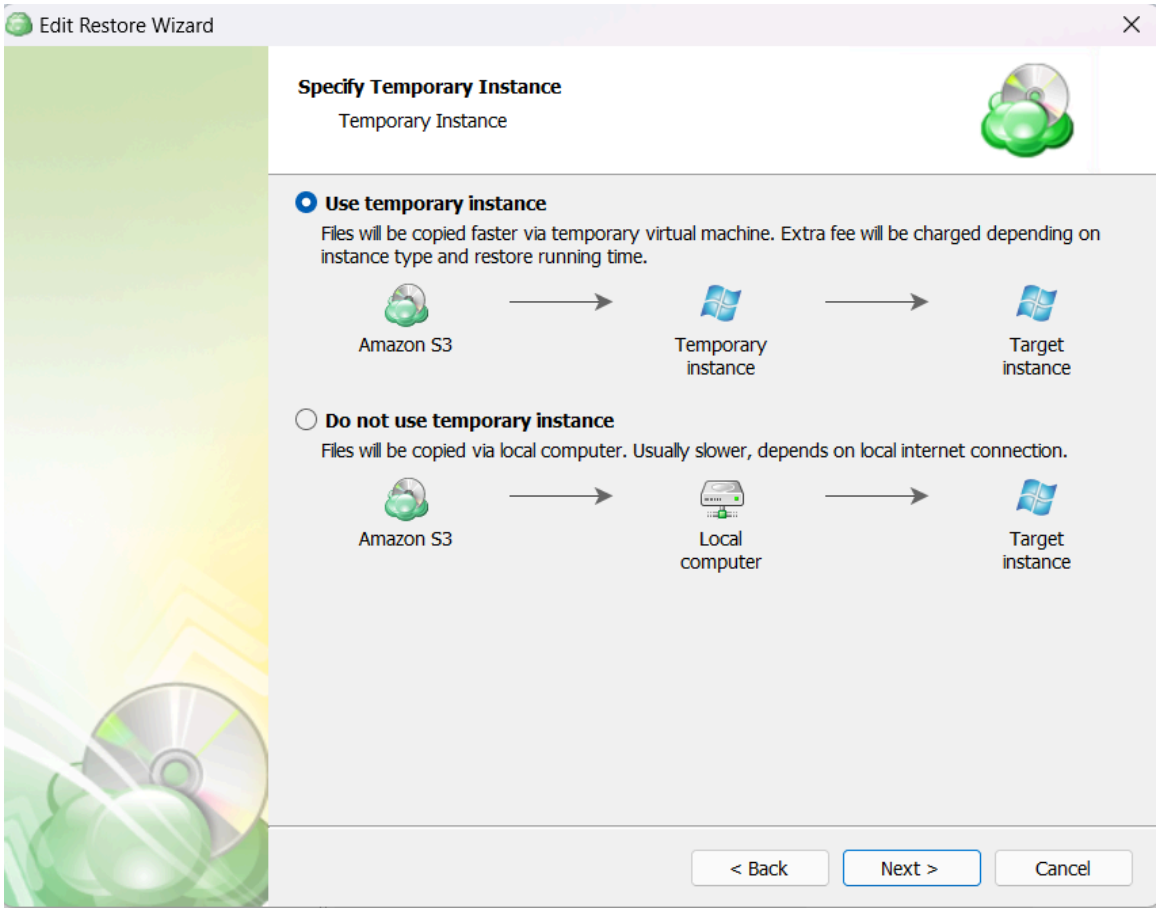
For AWS and Azure destinations, a storage account must already be specified through the MBS portal

Step 10. The next step is to specify the parameters for your target AzureVM instance:



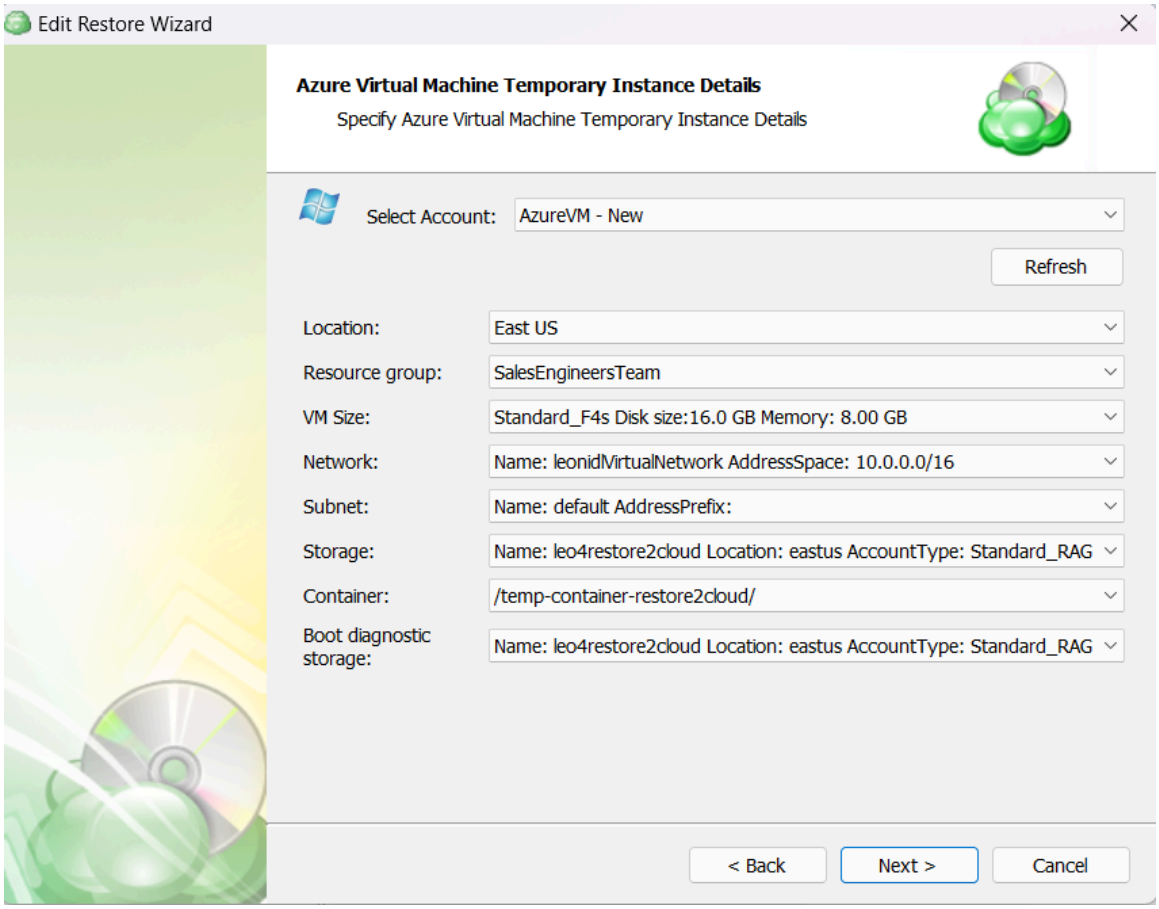
- **Azure Account:** The account under which a new Azure VM instance will be stored.
- **Computer Name:** Specify the computer name that will be given to the Azure VM.
- **Location:** The region that is to store the newly created Azure instance.
- **Resource Group:** Azure Resource Group. This has to be created in advance.
- **VM Size:** Select the required VM size that meets your requirements**.**
- **Network:** Select the correct Network. This has to be created in advance.
- **Subnet:** Specify one of the available subnets.
- **Storage**: Select your Azure storage.
- **Container:** Specify the Azure container is to store the temporary disk for VM import.
- **Boot Diagnostic Storage:** Select the storage where you would like to place diagnostic files. You can leave this option disabled.
- **Operating system:** Select the OS for the target instance.

Step 11. After specifying the target Azure VM instance details, you will need to choose between using a temporary instance or local computer for the restore operation.

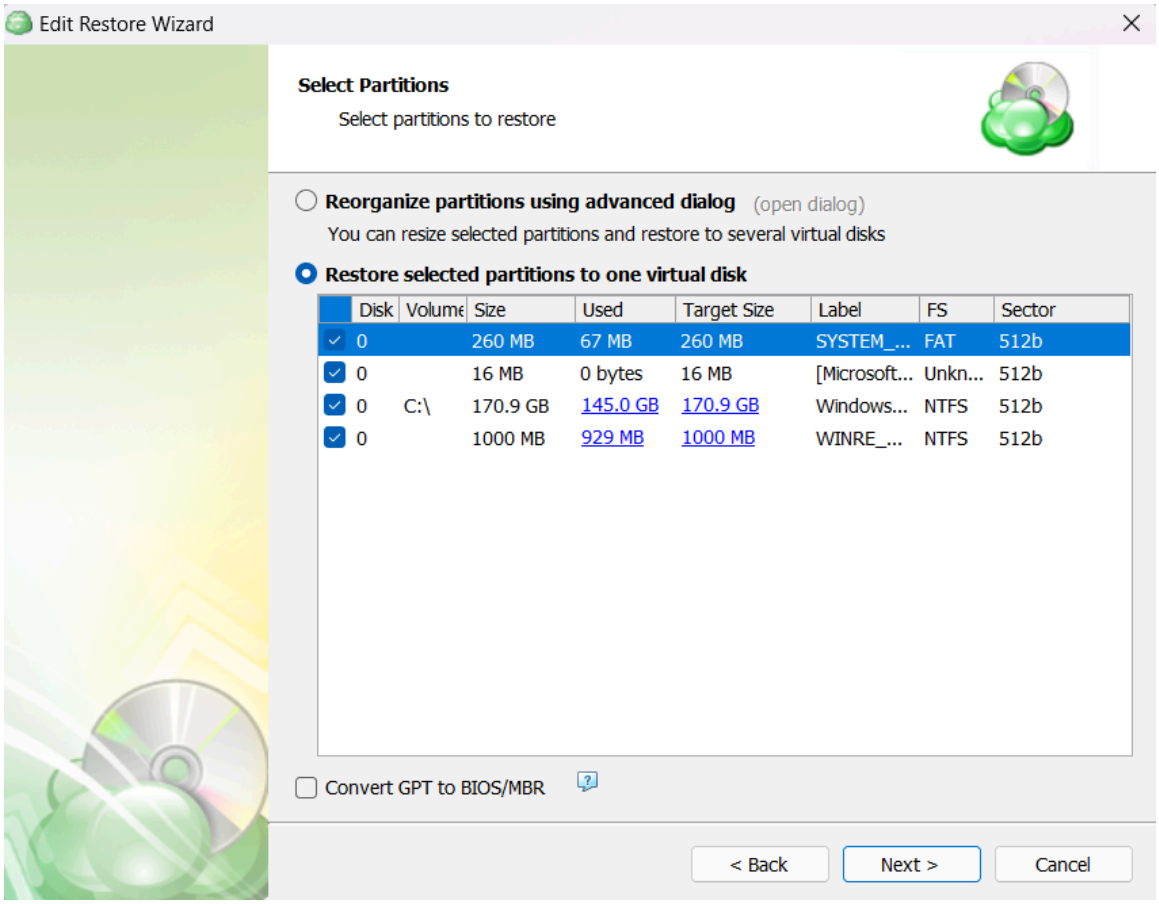


- **Use temporary instance**: This option creates a temporary Azure VM instance that will download backup data from the storage destination and restore it as a target instance. Usually, this method is faster as the temporary and target instance are located in the same Azure network.
- **Do not use temporary instance:** When selecting this option, the restore operation will be performed using the resources of the local computer. Usually, this approach is slower, depending on the local internet connection.

Step 12. If you have selected to use a temporary instance, the next page will allow you to select the Azure account from the upper dropdown box, and specify the Temporary Instance details below.



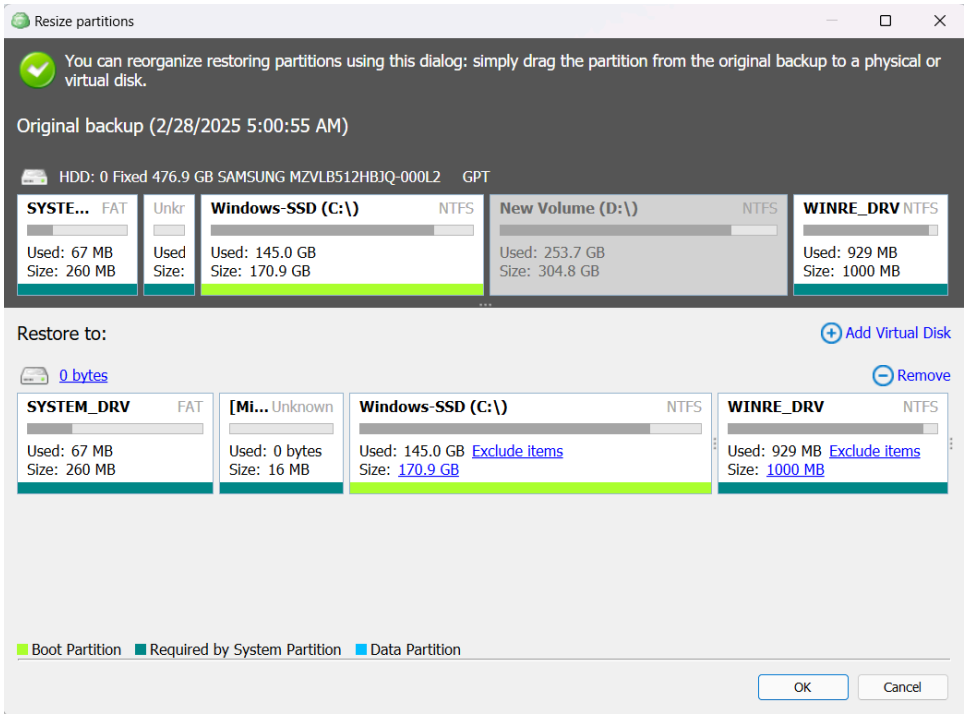
Step 13. After selecting the type of restore target in the previous step, you can now choose to restore the partitions with their existing parameters or to reorganize and resize them.



- **Convert GPT to BIOS/MBR:** Select this checkbox if the target instance or the target OS does not support UEFI boot and requires BIOS boot.

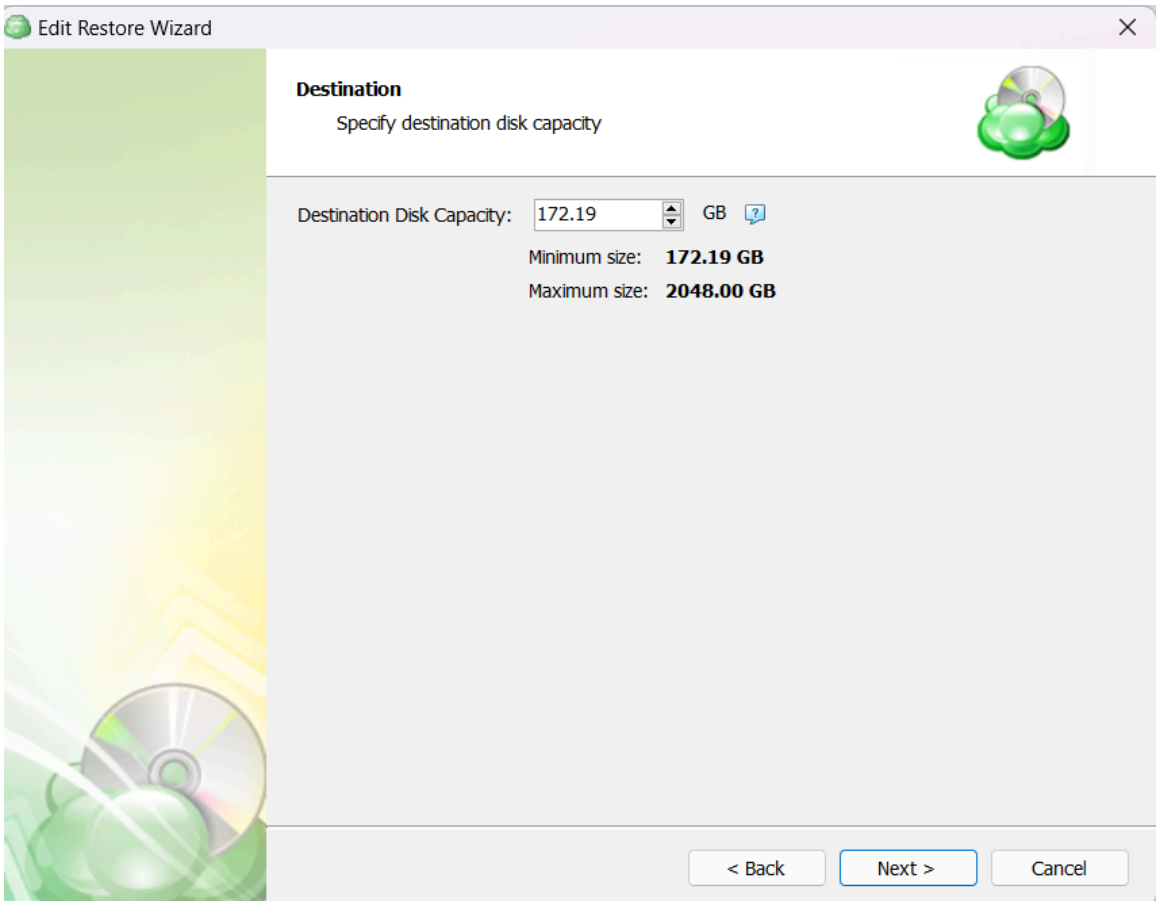
> Some instance types may not support some features such as UEFI boot or TPM. Refer to Azure Documentation to ensure selection of the appropriate type of instance.

If you select “Reorganize partitions using advanced dialog” a new window will appear and allow you to resize the partitions and rearrange them on one or more virtual disks.

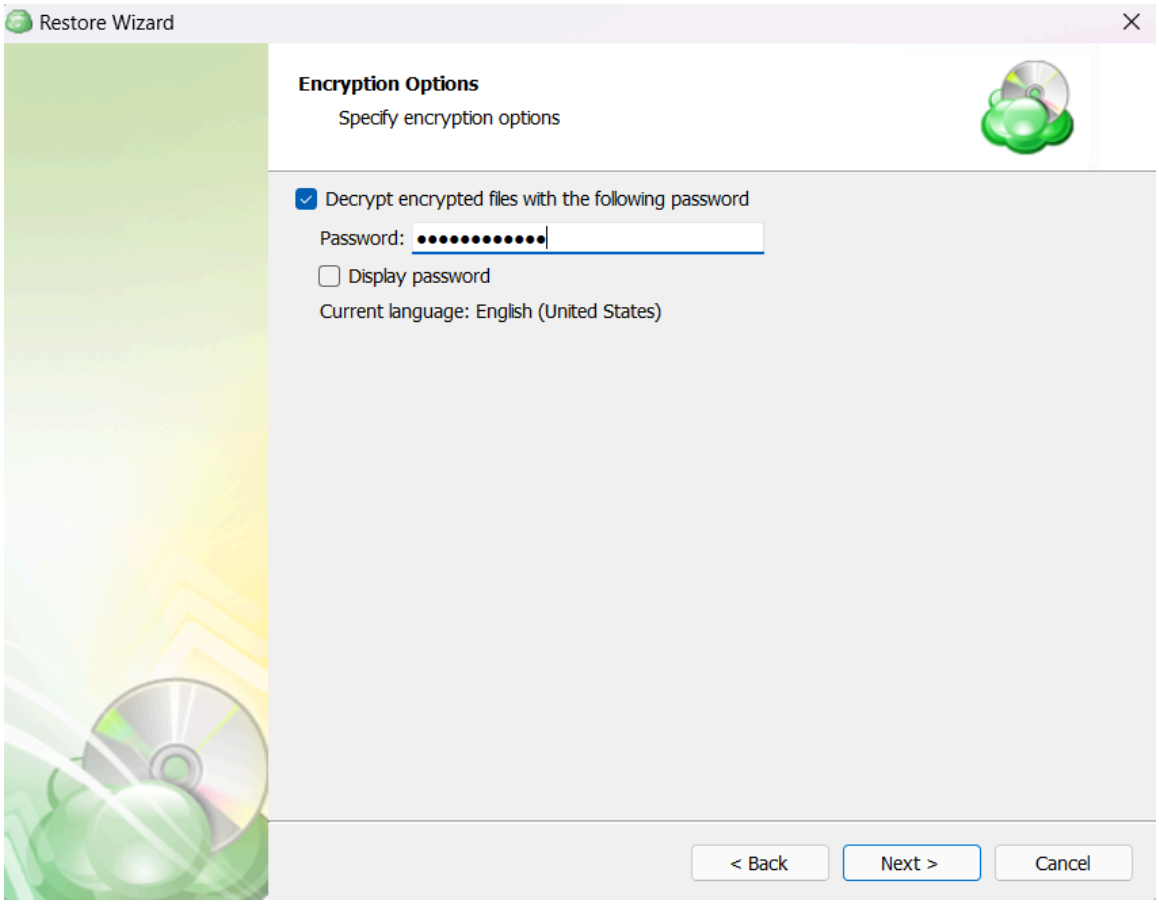


Click on any of the blue hyperlinks to open additional dialogue boxes allowing you greater control over the name and size of the virtual disk, as well as the ability to add additional virtual disks, and also exclude specific files or folders if desired.

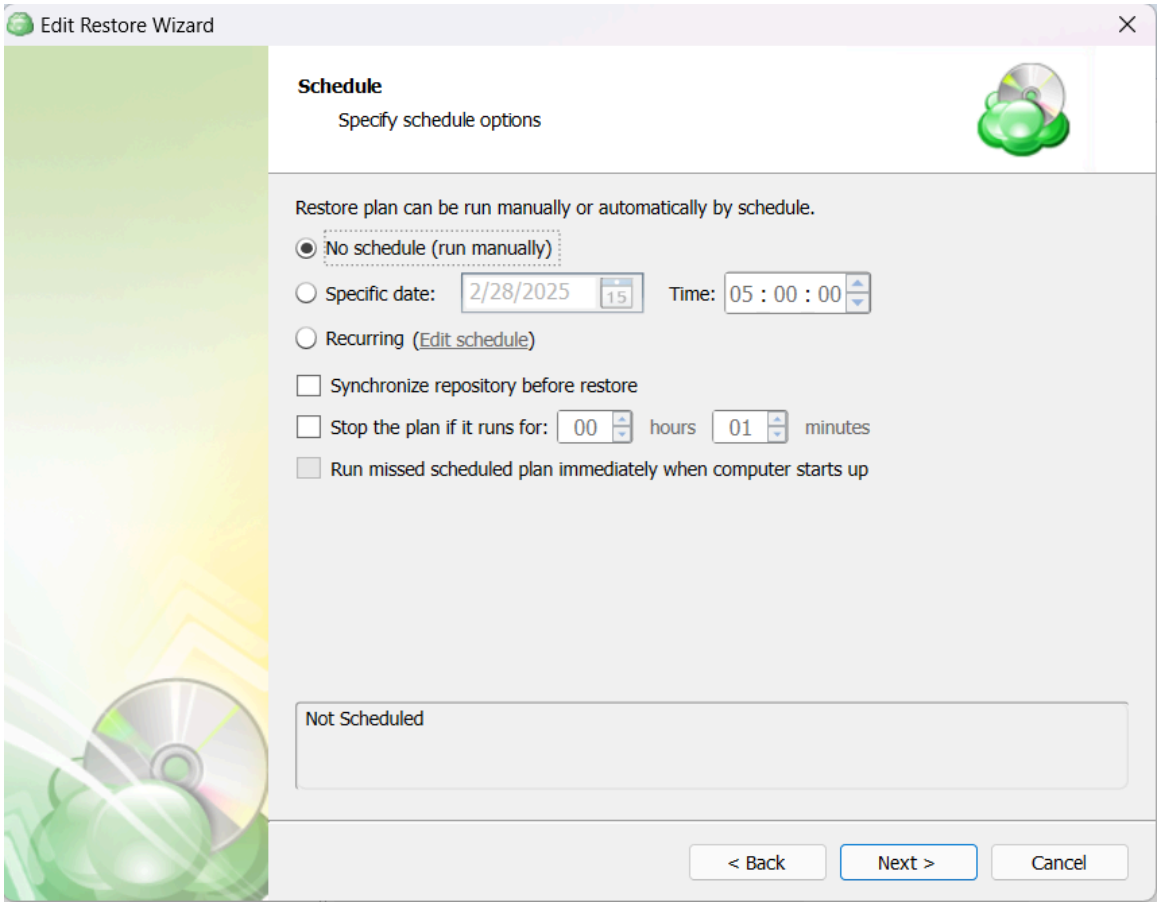
Step 14. Specify the destination disk capacity.



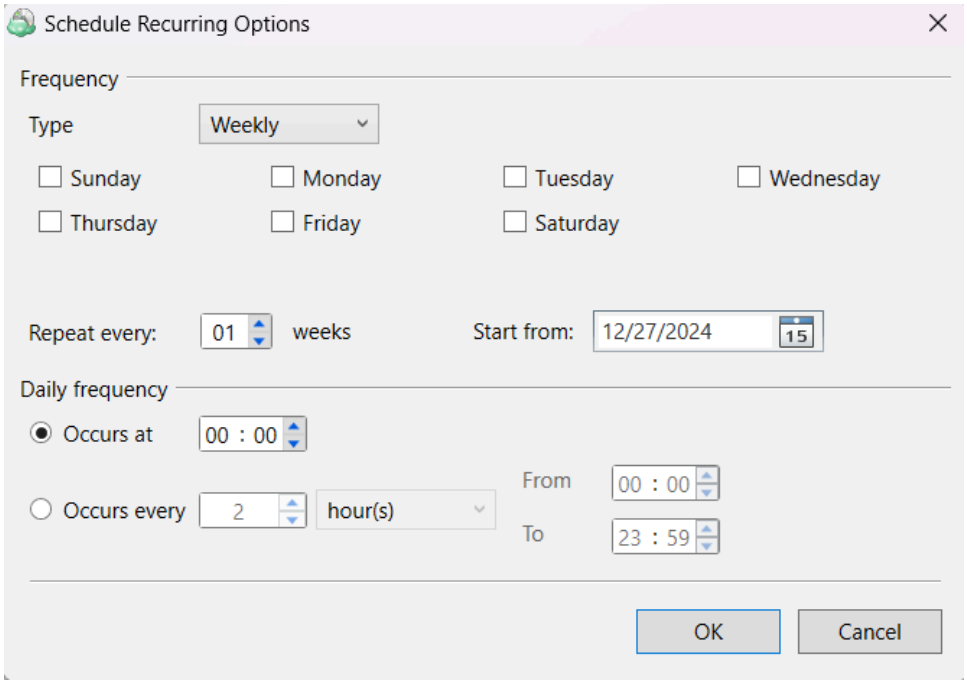
Step 15. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the Image.



Step 16. With the decryption password entered, the next step is setting the schedule for the restore plan.



- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

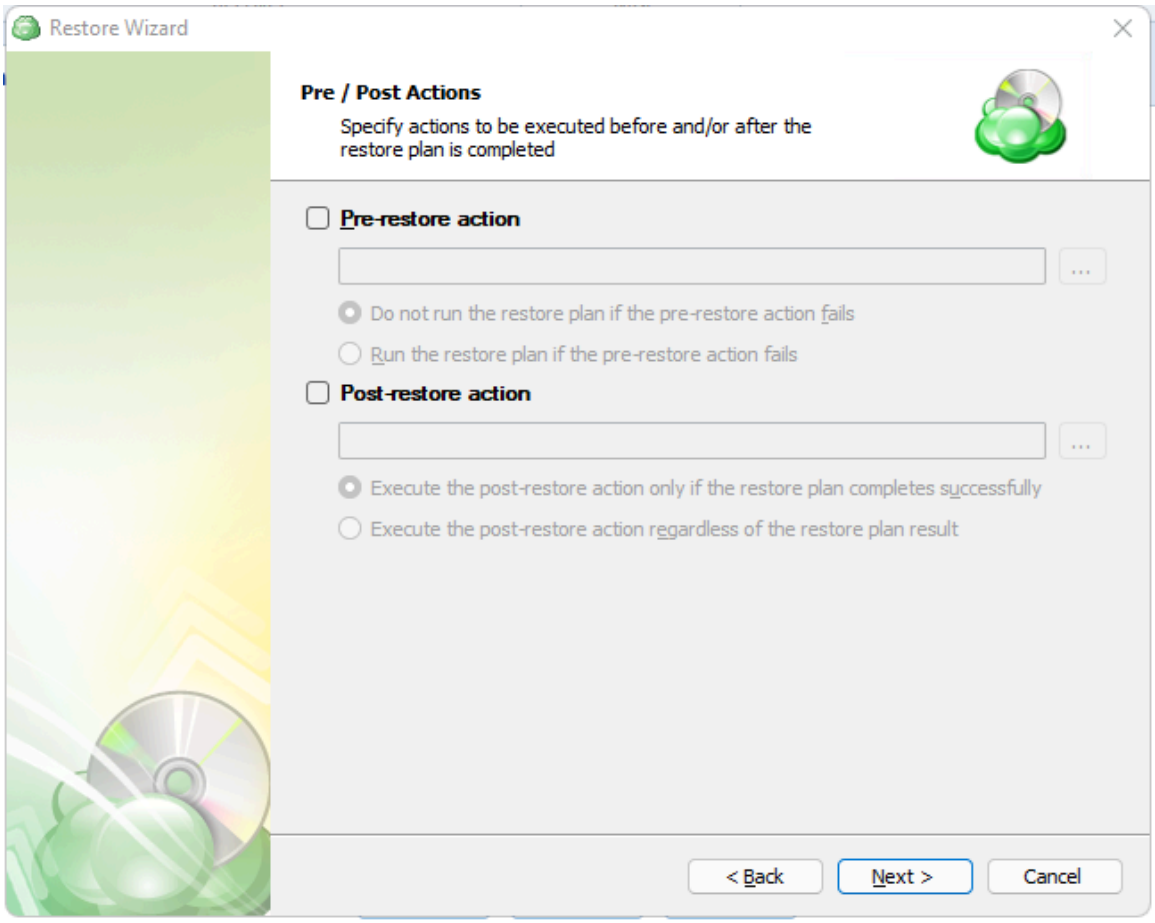


It is recommended to check the "**Synchronize repository before restore"** if the restore plan is created on a computer different from the original or if you are logged in with a different backup user account.

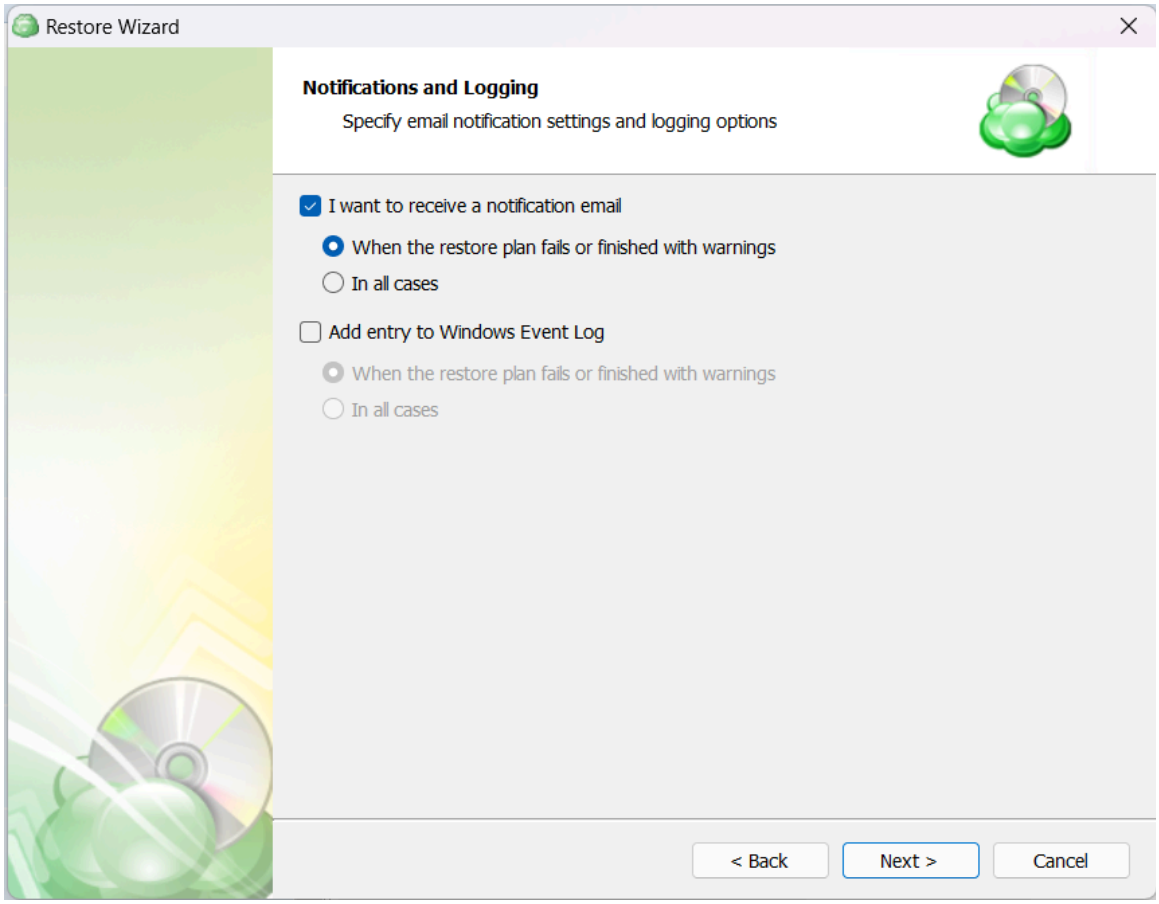
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

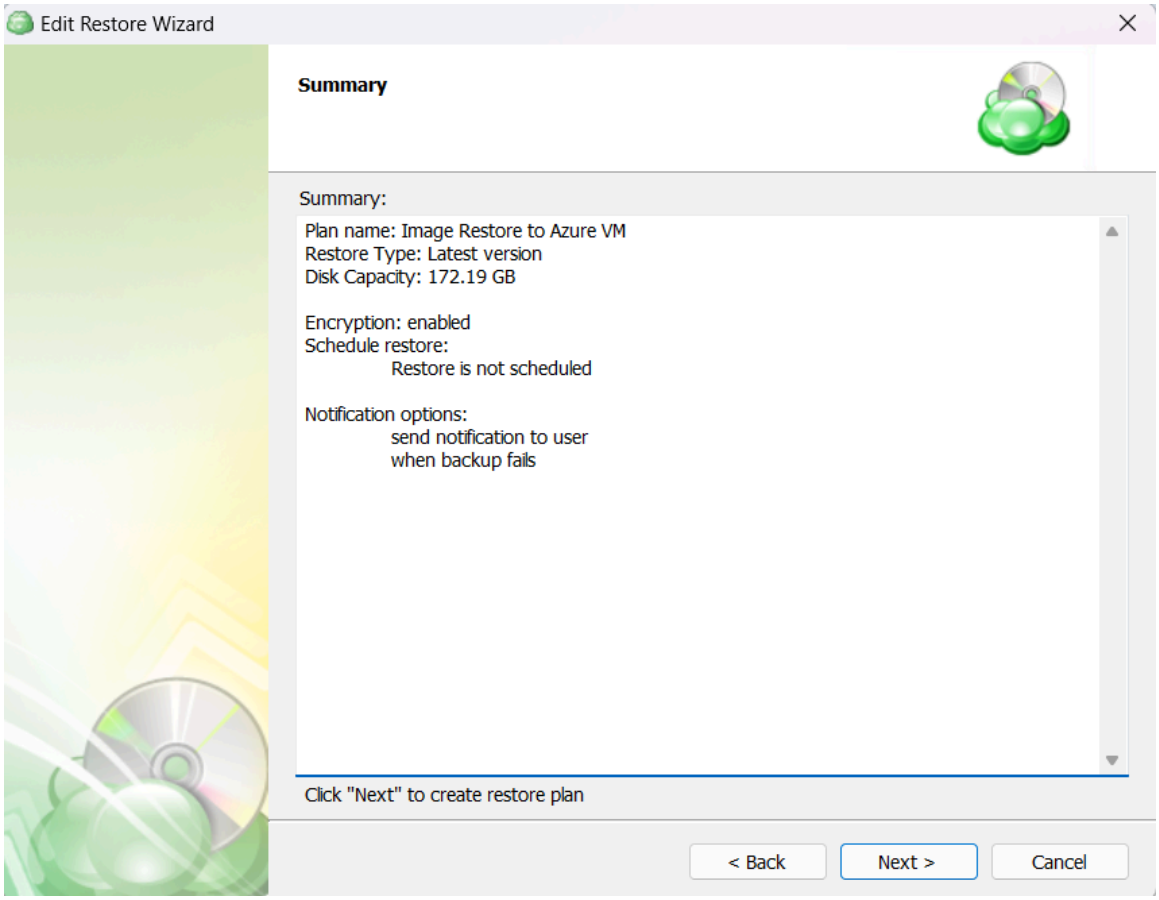
Step 17. After setting the schedule, the next step allows pre and post actions to be defined.



Step 18. Next, you can select options to receive notification email and/or add an entry to Windows Event Log.



Step 19. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.

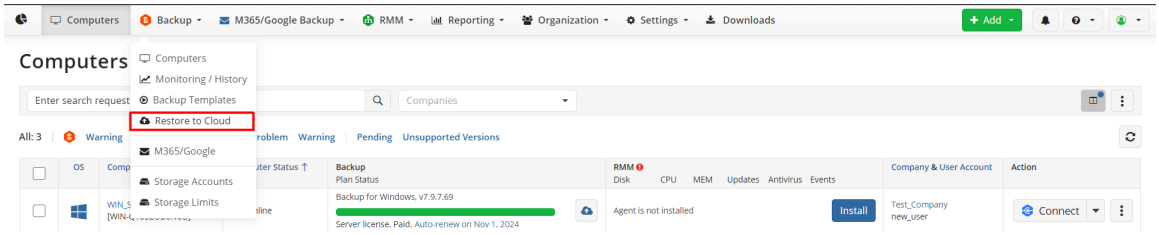


If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

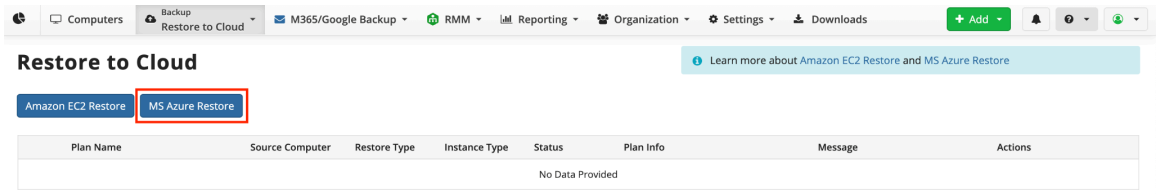
Restore to an Azure Virtual Machine using MBS

> Please note that in order to enable restore to AzureVM, you need to prepare your Azure environment (create a Resource Group, Storage Container, Virtual Network, Subnet, and Network Security Group). You can find more info in the help article below:
> https://help.mspbackups.com/restore/restore2cloud/restore-azurevm/prepare

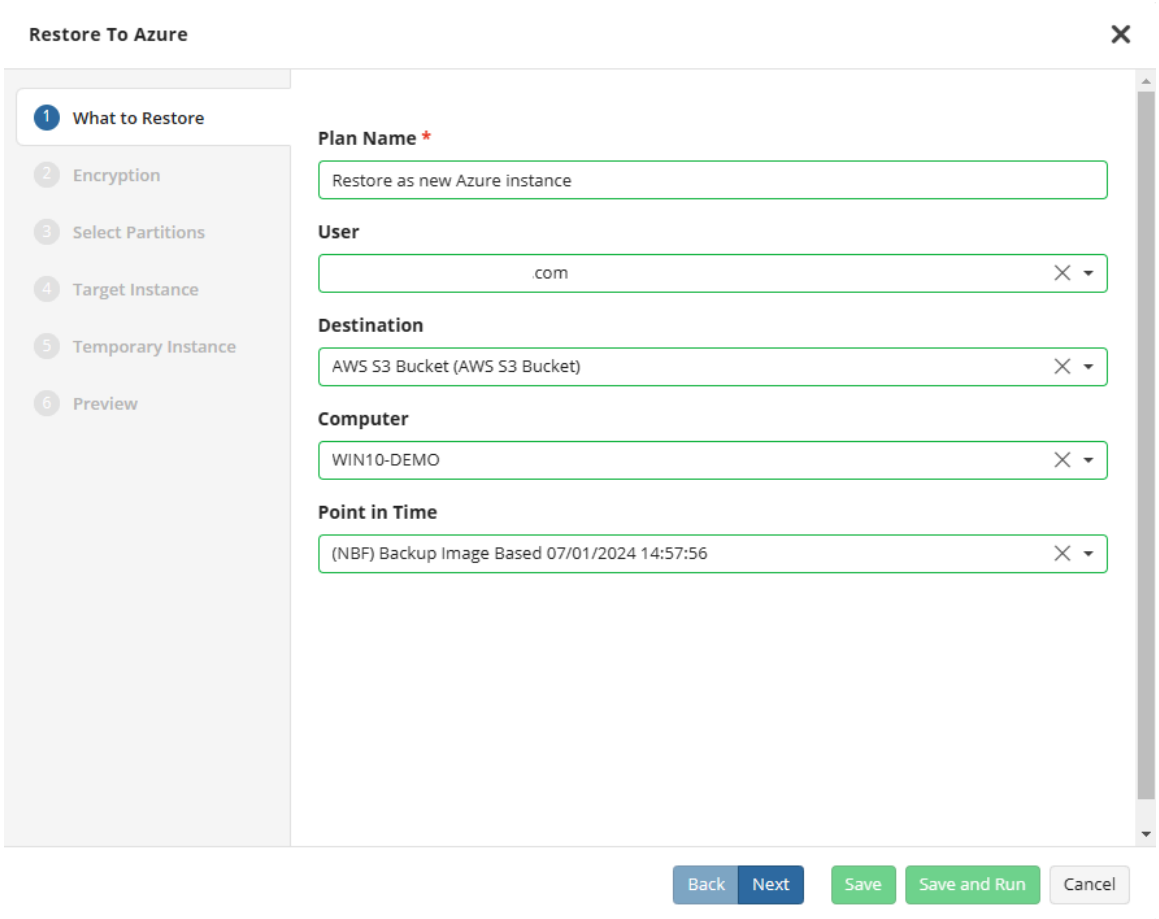
Step 1. Navigate to the MBS Portal and select “Backup” on the main menu, then click on “Restore to Cloud”:



Step 2. Next, please select the “MS Azure Restore” option.



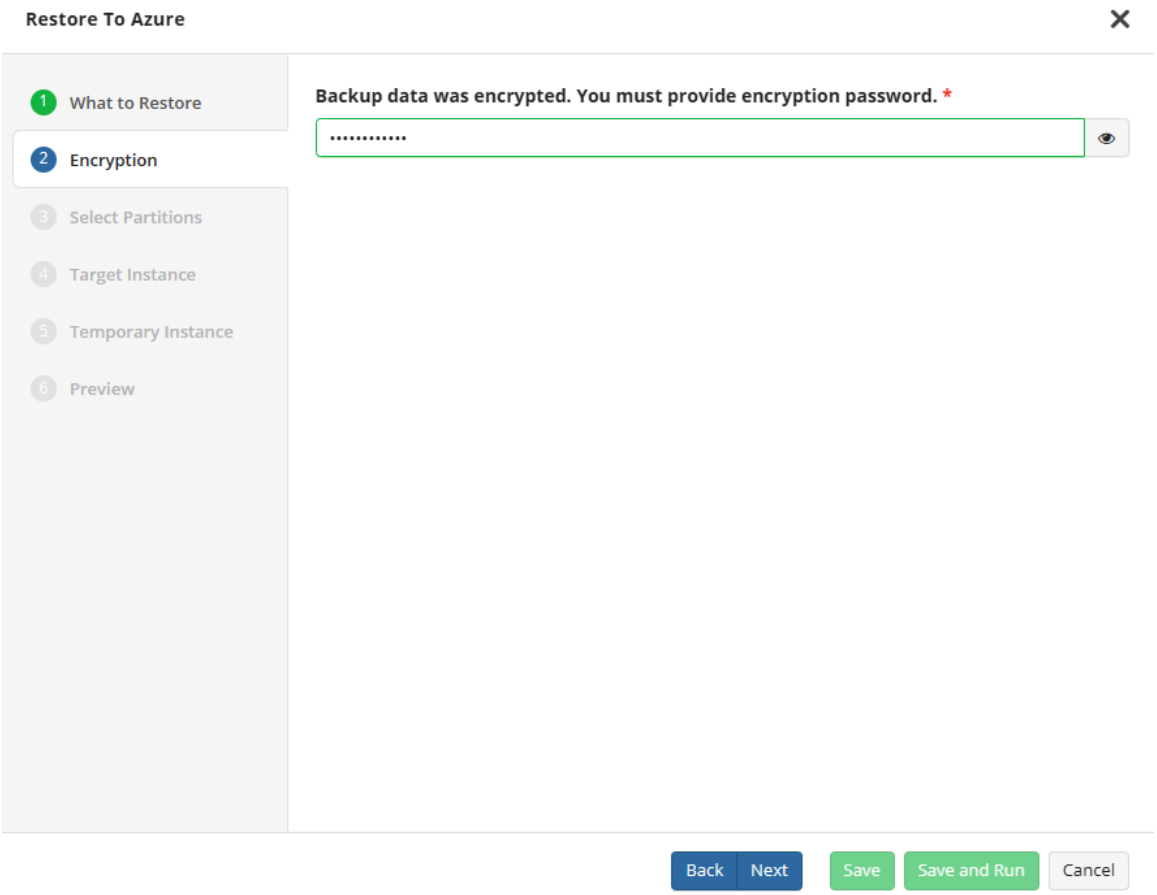
Step 3. The first page will prompt you to provide the restore plan name and select a backup dataset to restore.



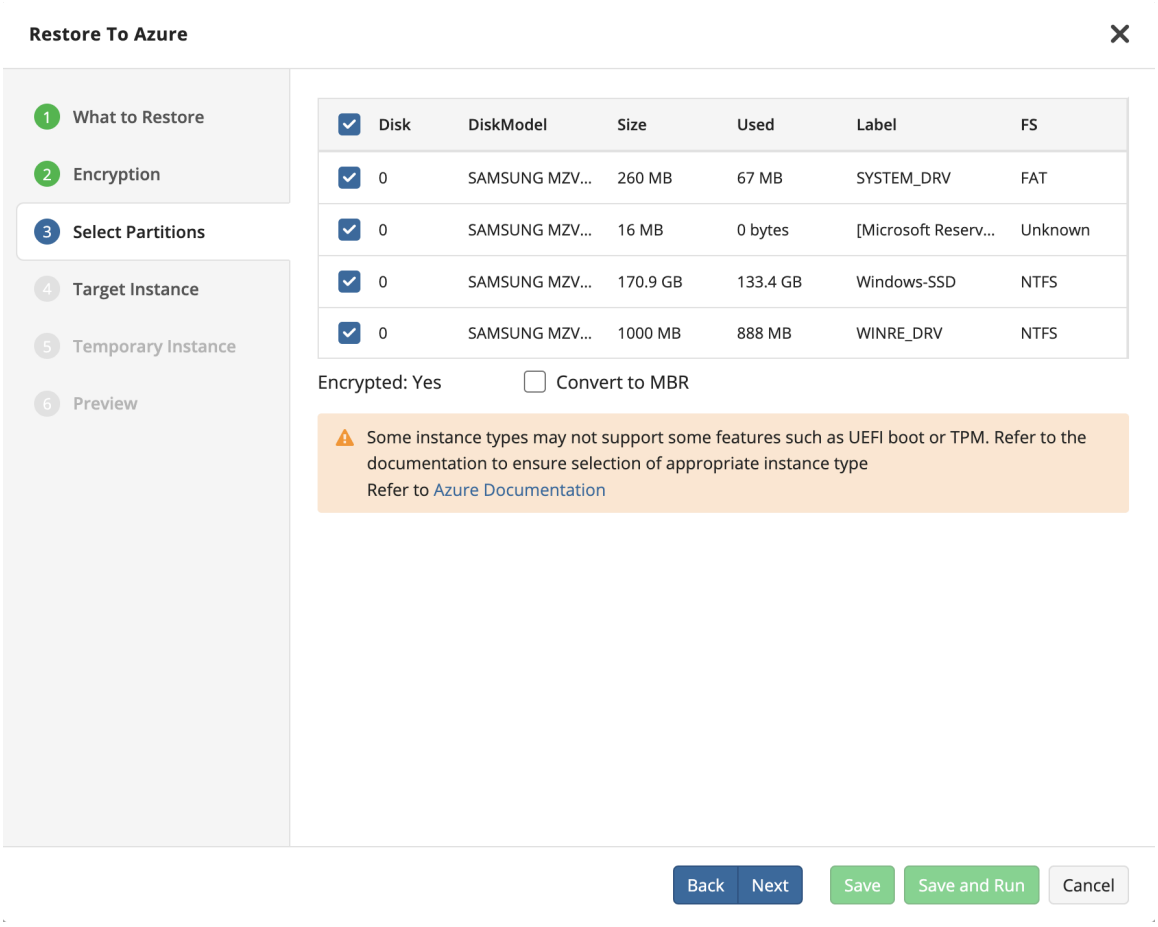
- **Plan Name:** The plan name is displayed on the **Restore to Cloud** dashboard
- **User:** Please select the user authorized during the creation of the backup dataset.
- **Destination:** Select the backup destination that contains the required backup data.
- **Computer:** Select the computer (prefix) containing the data to be restored.
- **Point in Time:** Pick the date/ backup version that is to be restored.

> Note that only cloud storage buckets can be used when restoring to EC2 from the MBS Console. Local storage can only be used when restoring from the Agent.

Step 4. If the backup dataset was encrypted, the next page will prompt for the encryption password.



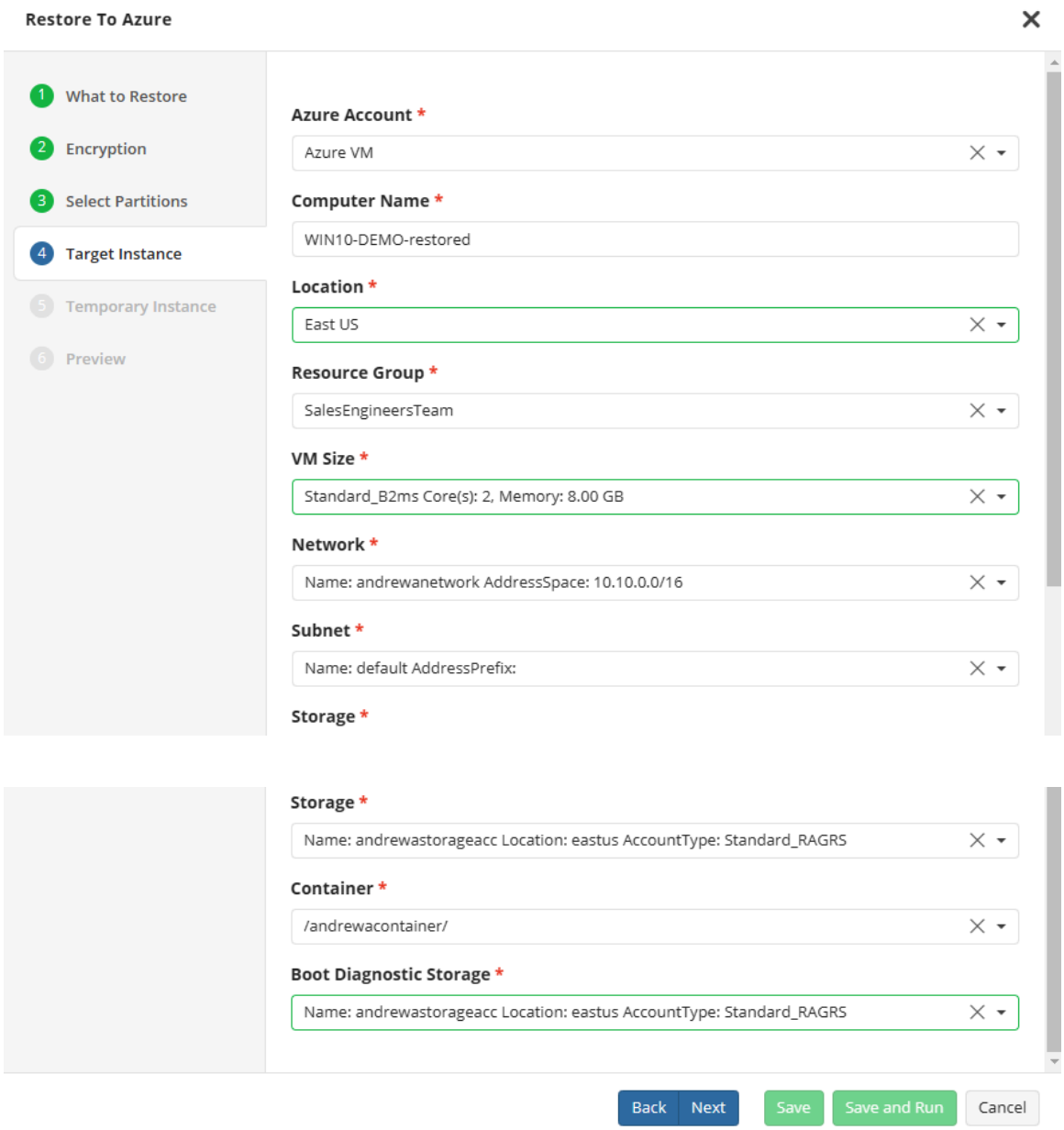
Step 5. Next you will need to select the partitions to restore.



- **Convert to MBR:** Please select this option if the system does not support GPT (GUID Partition Table) and requires conversion to the Master Boot Record.

> Some instance types may not support some features such as UEFI boot or TPM. Refer to the documentation to ensure selection of appropriate instance type. Refer to Azure Documentation

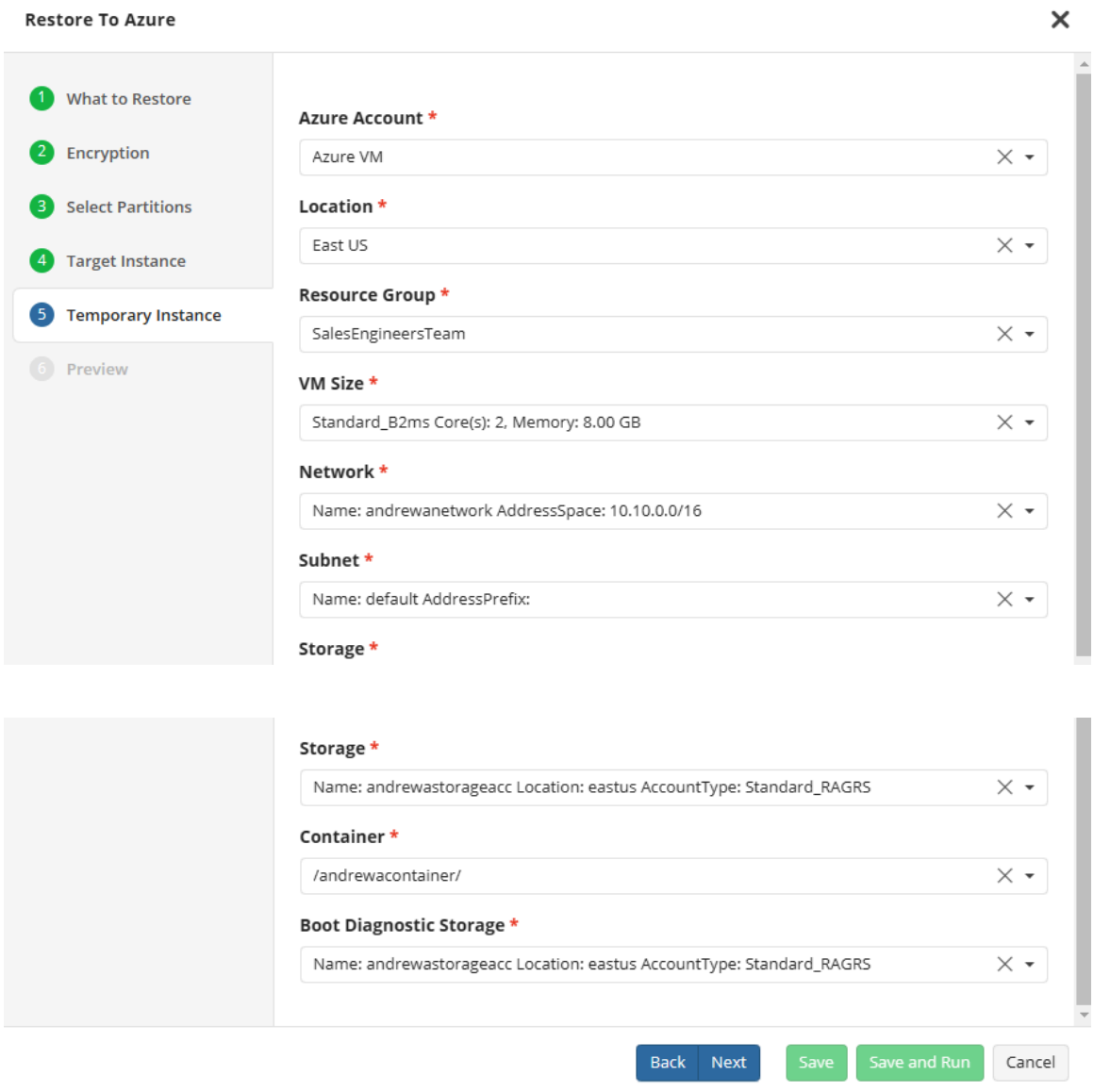
Step 6. The next step is to specify the parameters for your **target AzureVM instance**:



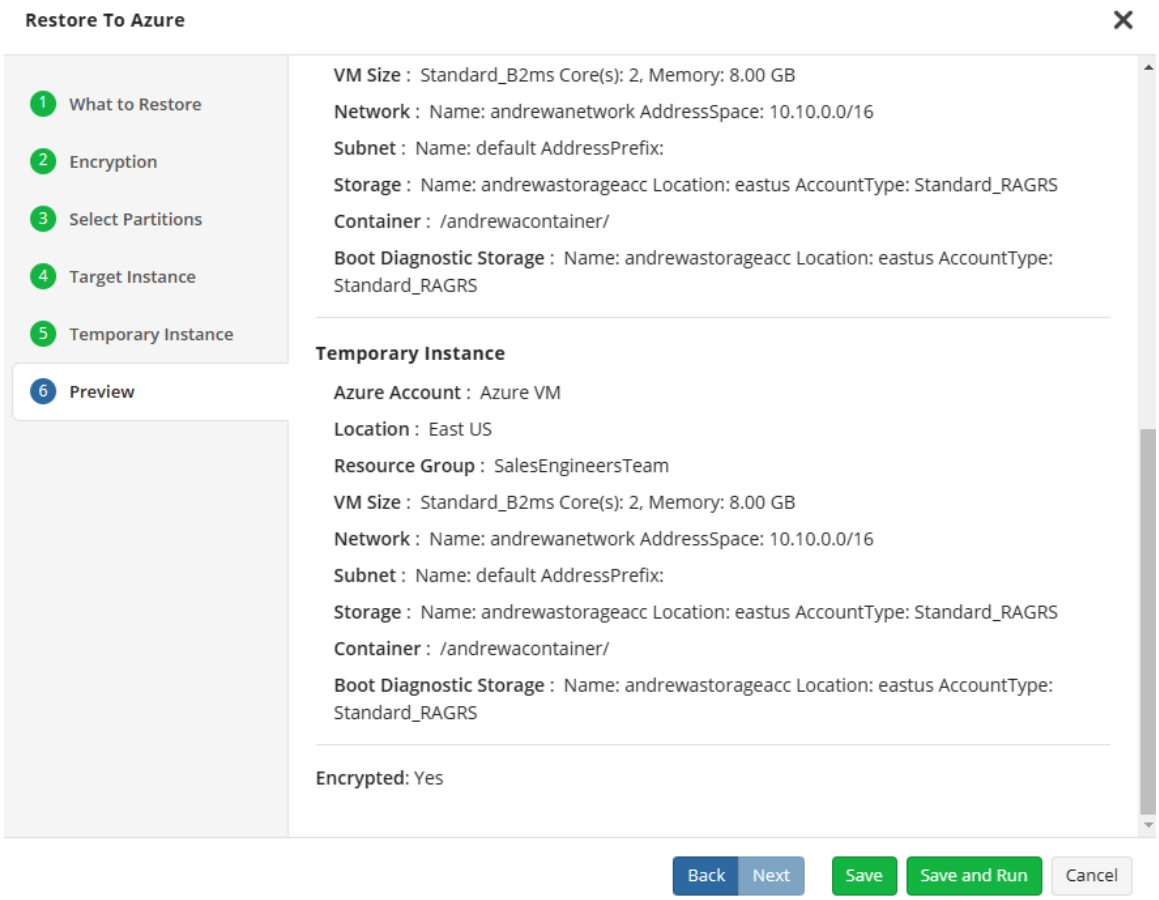
- **Azure Account:** The account under which a new Azure VM instance will be stored.
- **Computer Name:** Select the computer (prefix) containing the data to be restored.
- **Location:** The region that is to store the newly created Azure instance.
- **Resource Group:** Azure Resource Group. This has to be created in advance.
- **VM Size:** Select the required VM size that meets your requirements in terms of cores and RAM.

- **Network:** Select the correct Network. This has to be created in advance.
- **Subnet:** Specify one of the available subnets.
- **Storage**: Select your Azure storage.
- **Container:** Specify the Azure container is to store the temporary disk for VM import.
- **Boot Diagnostic Storage:** Select the storage where you would like to place diagnostic files. You can leave this option disabled.

Step 7. Next, please specify the **Temporary Instance** parameters:



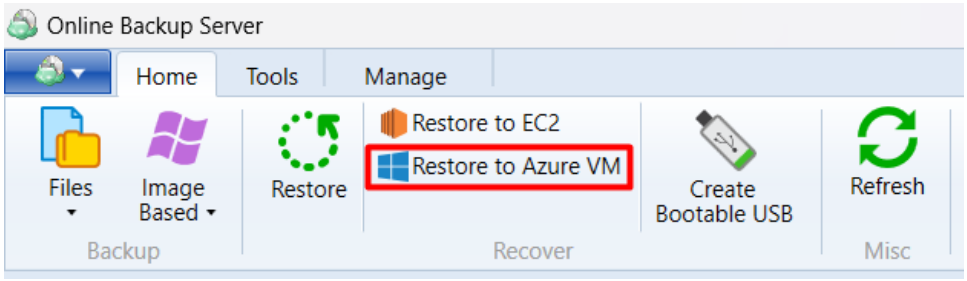
Step 8. Review all settings specified across the restore wizard and ensure that they are accurate. Click **Save and Run** to execute the restore to an AzureVM instance.



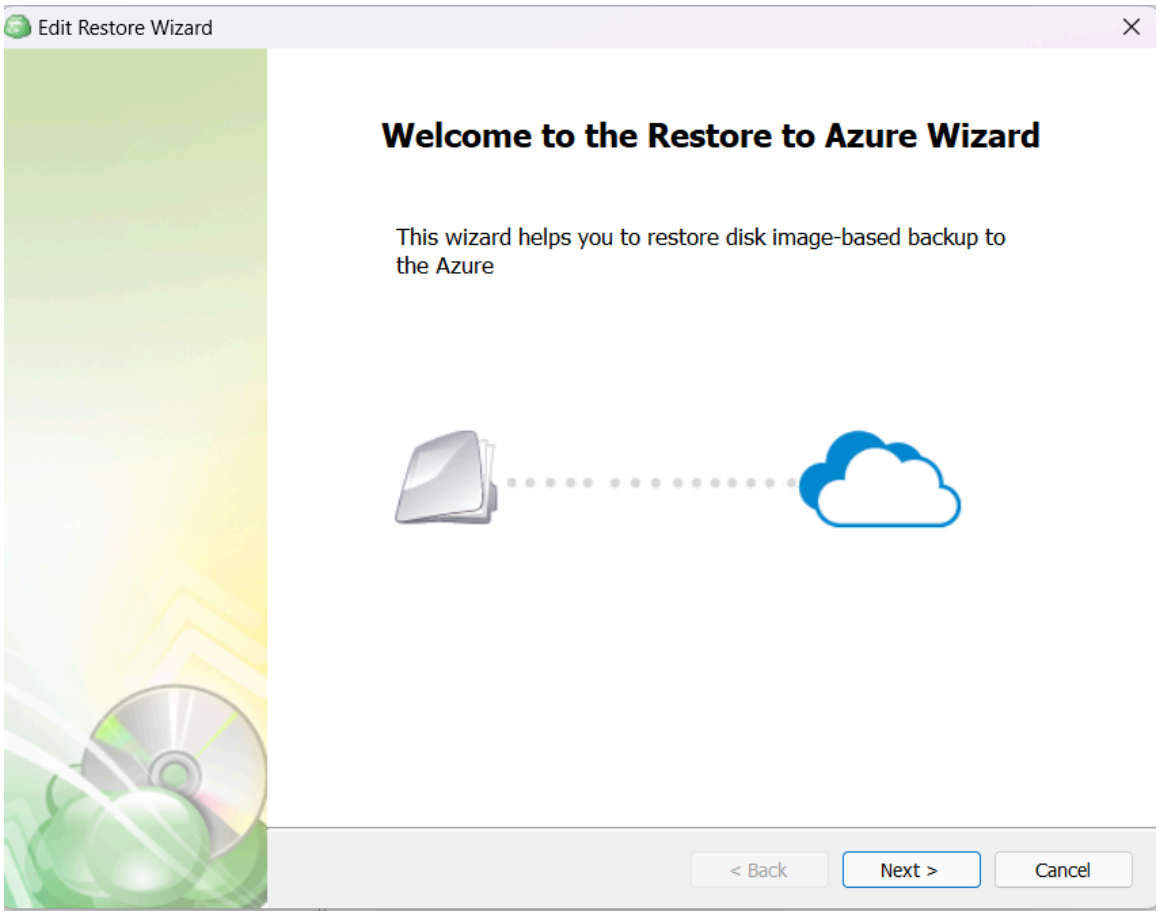
Restore to an Azure Data Disk using the Agent

> Please note that in order to enable restore to AzureVM, you need to prepare your Azure environment (create a Resource Group, Storage Container, Virtual Network, Subnet, and Network Security Group). You can find more info in the help article below:
> https://help.mspbackups.com/restore/restore2cloud/restore-azurevm/prepare

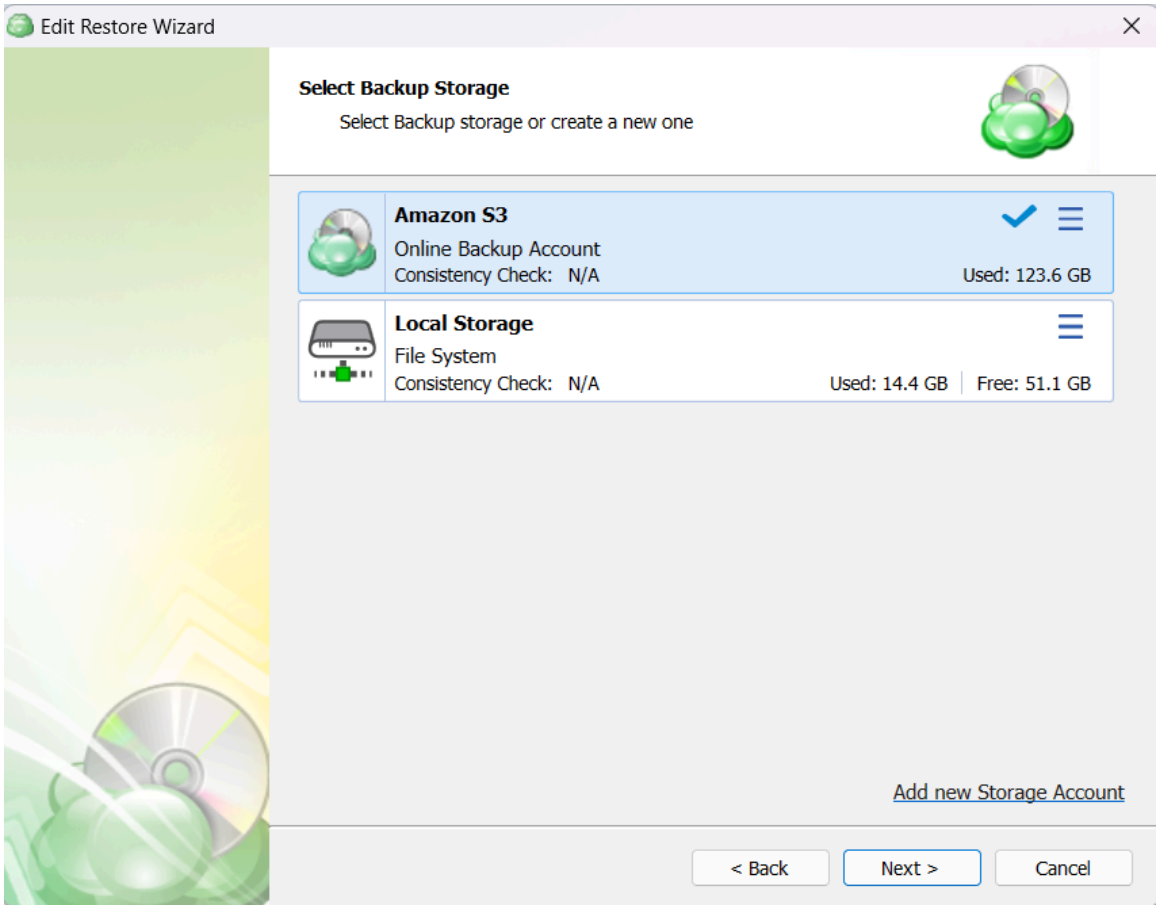
Step 1. After launching the Online Backup, please click on the “Restore to Azure VM” button.



Step 2. The first step of the wizard indicates that you have started the wizard.

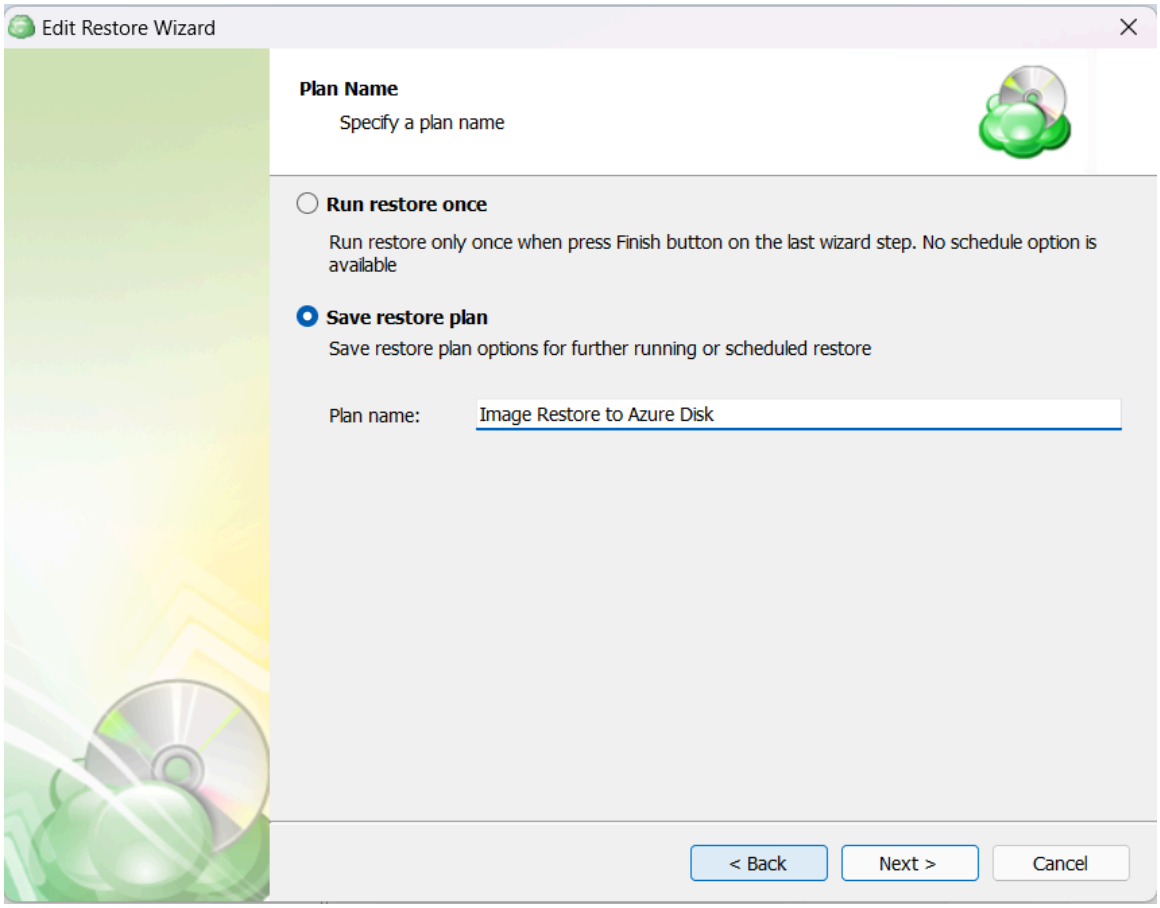


Step 3. The next step will prompt you to select the storage location for the source.

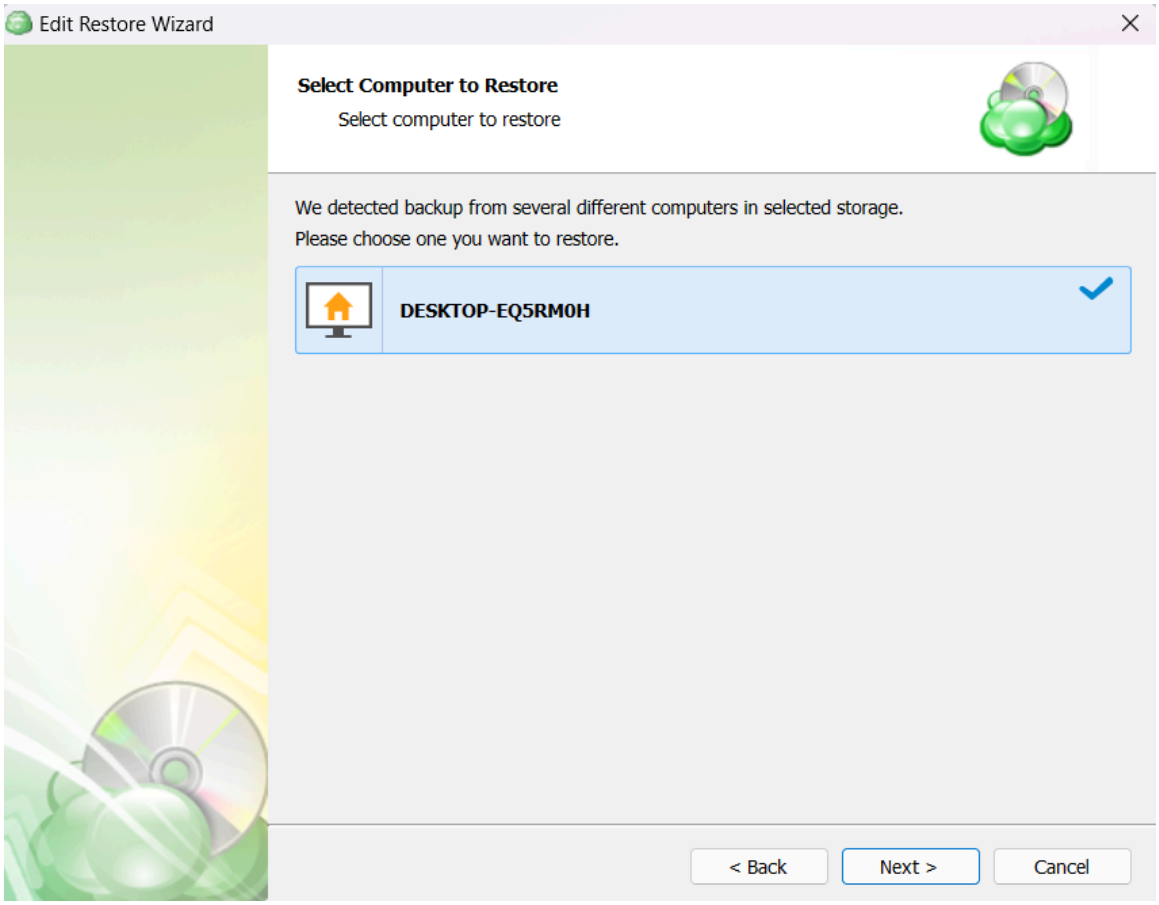


You can click “Add new Storage Account” to add a new local storage account. If you need to add a new cloud storage, this can be only done via the MBS portal, “Storage Accounts” page.

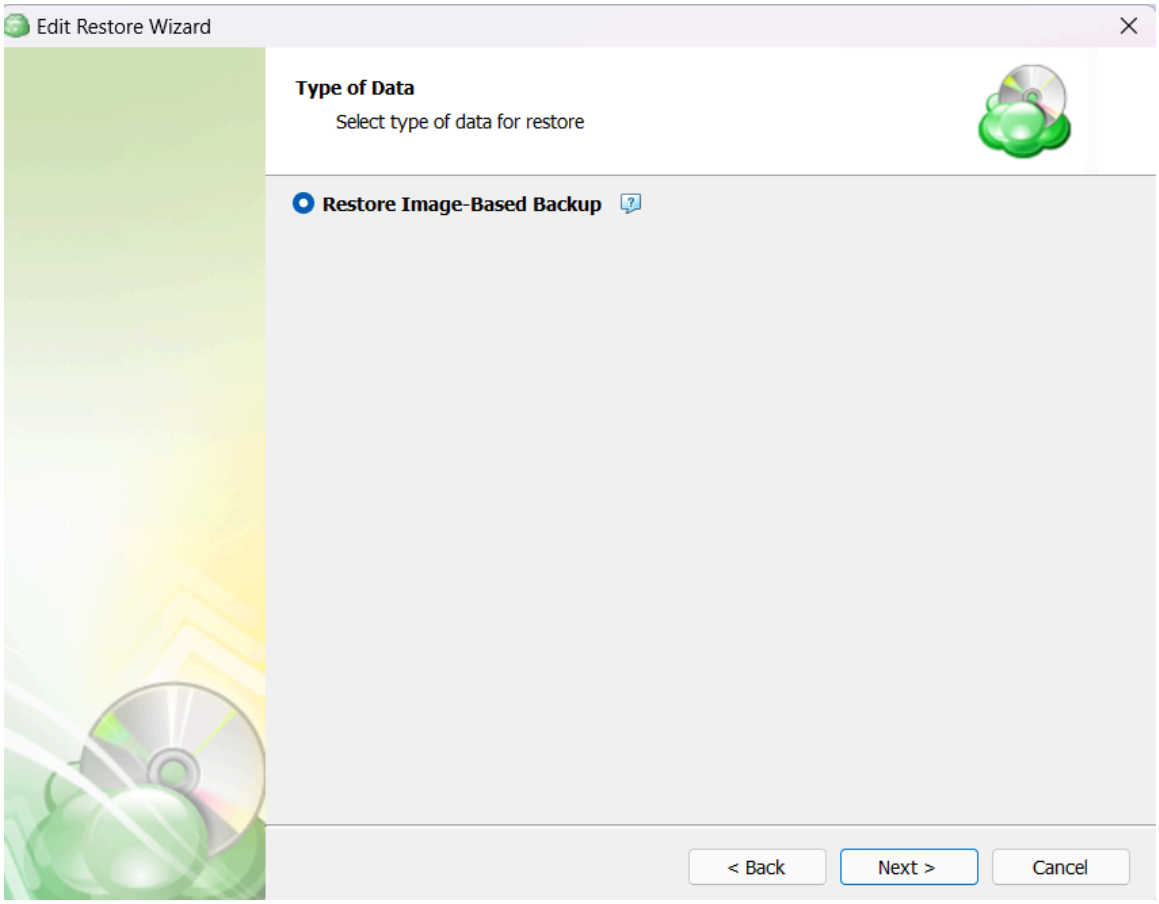
Step 4. Next you will choose whether to run the restore operation only once, or to save it for later use. The latter will allow you to name the plan.



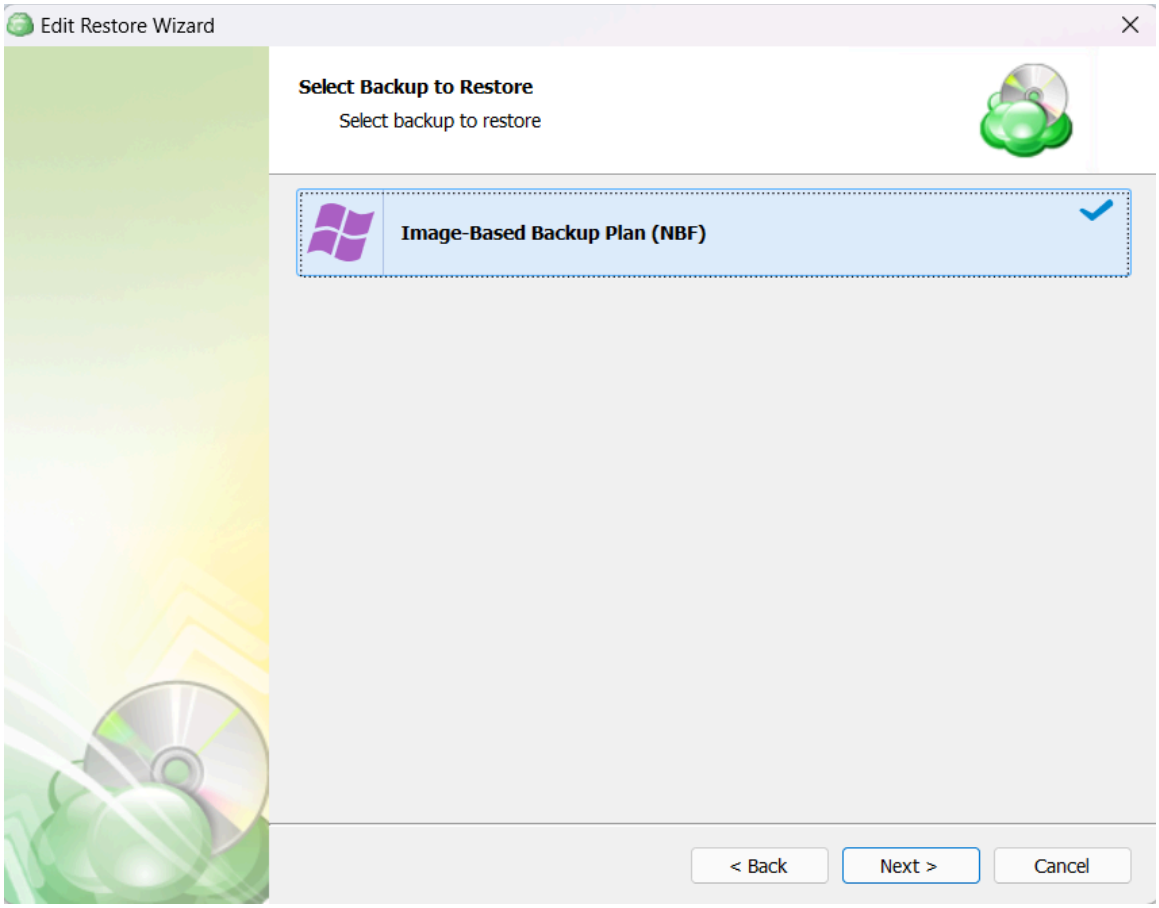
Step 5. Next you will be presented with a list of computers with the same prefix (computer name) and associated “Backup User” as the computer on which the Agent is currently running. Click to select the desired computer then click on “Next”.



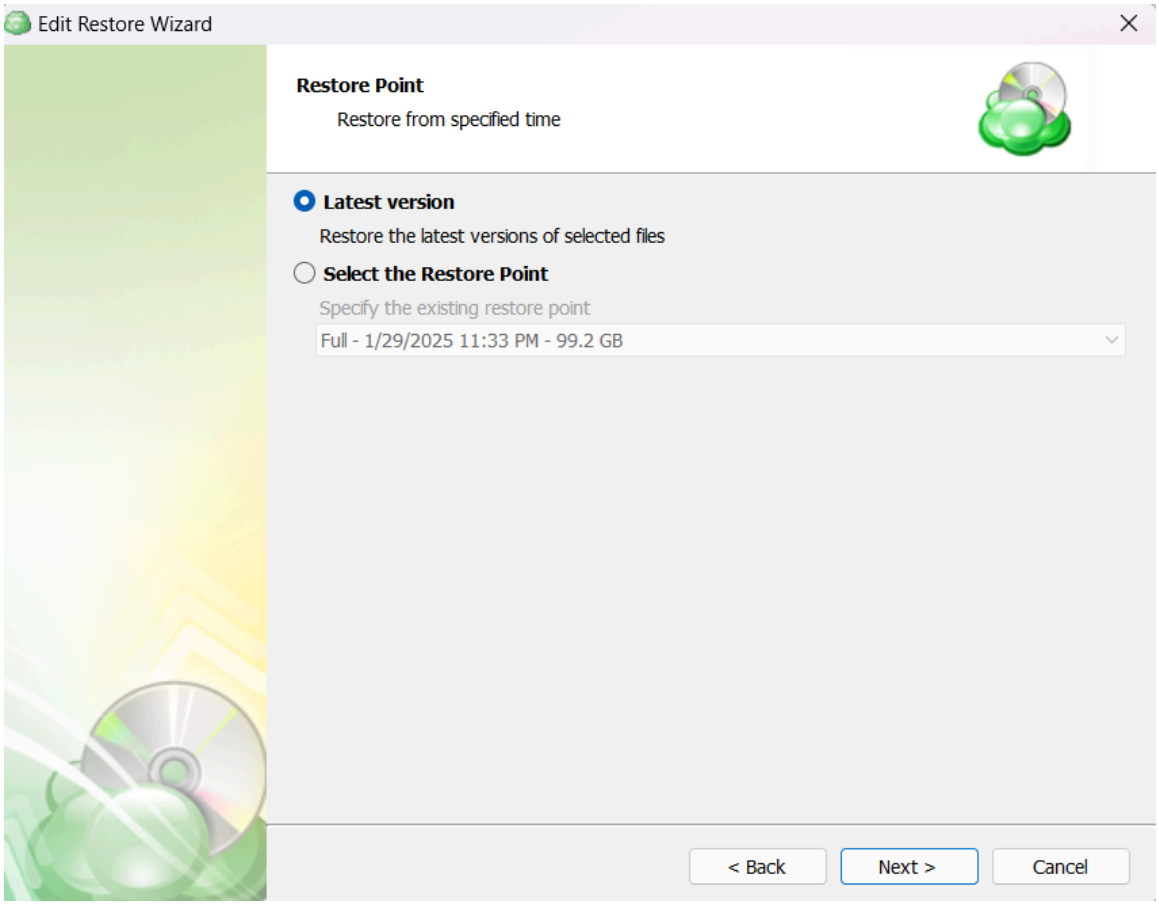
Step 6. Based on the contents of the selected source and computer, the next step is to choose the type of restore. Select “Restore Image Based Backup” then continue to the next step by clicking “Next”.



Step 7. With the correct type of restore selected, the application will generate a list of available backup plans.

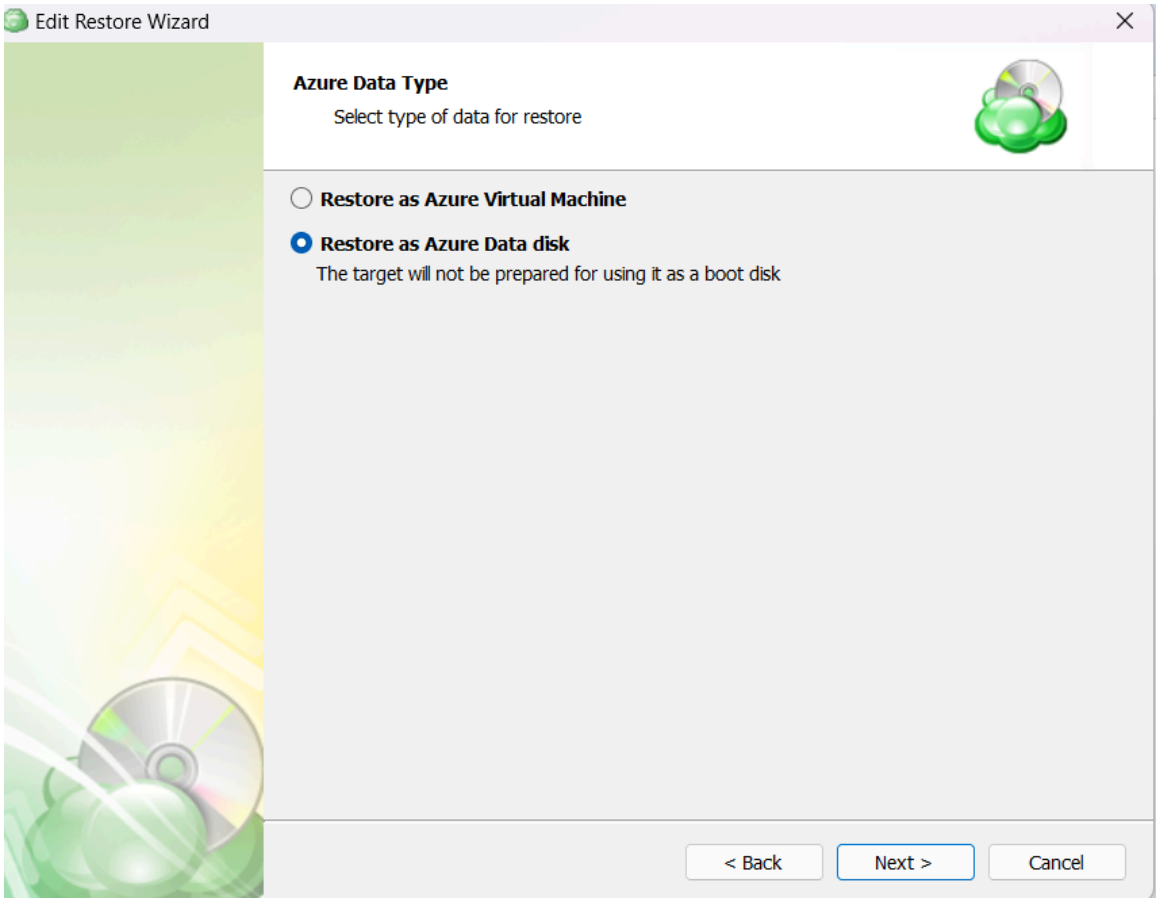


Step 8. The next step is to select the desired point in time to restore to.



- **Latest Version:** Automatically restores the most recent backup restore point.
- **Select the Restore Point:** Allows you to select a specific restore point (date) to restore.

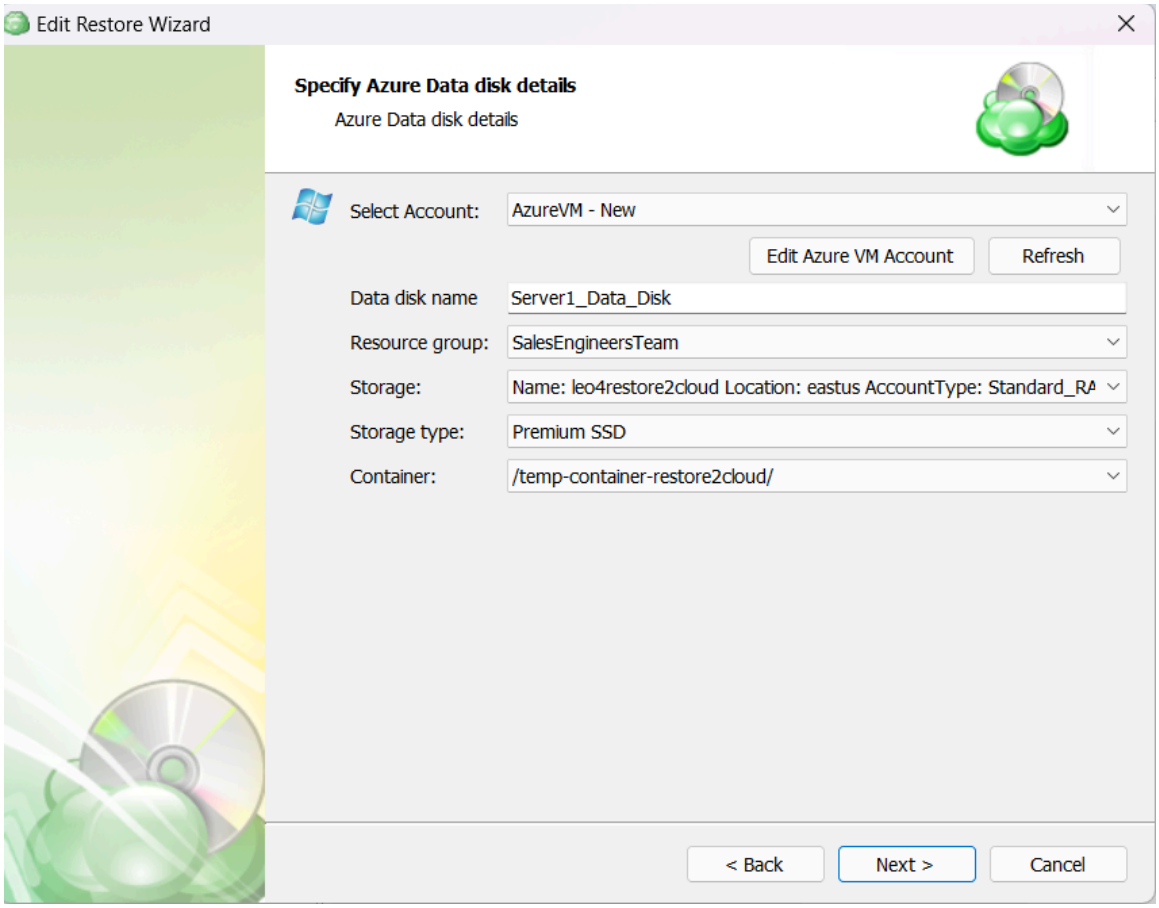
Step 9. Next, select the Azure Data Type.



- **Restore as Azure Virtual Machine:** Restores the image to an Azure VM
- **Restore as Azure Data Disk:** Restores the image as an Azure Data Disk

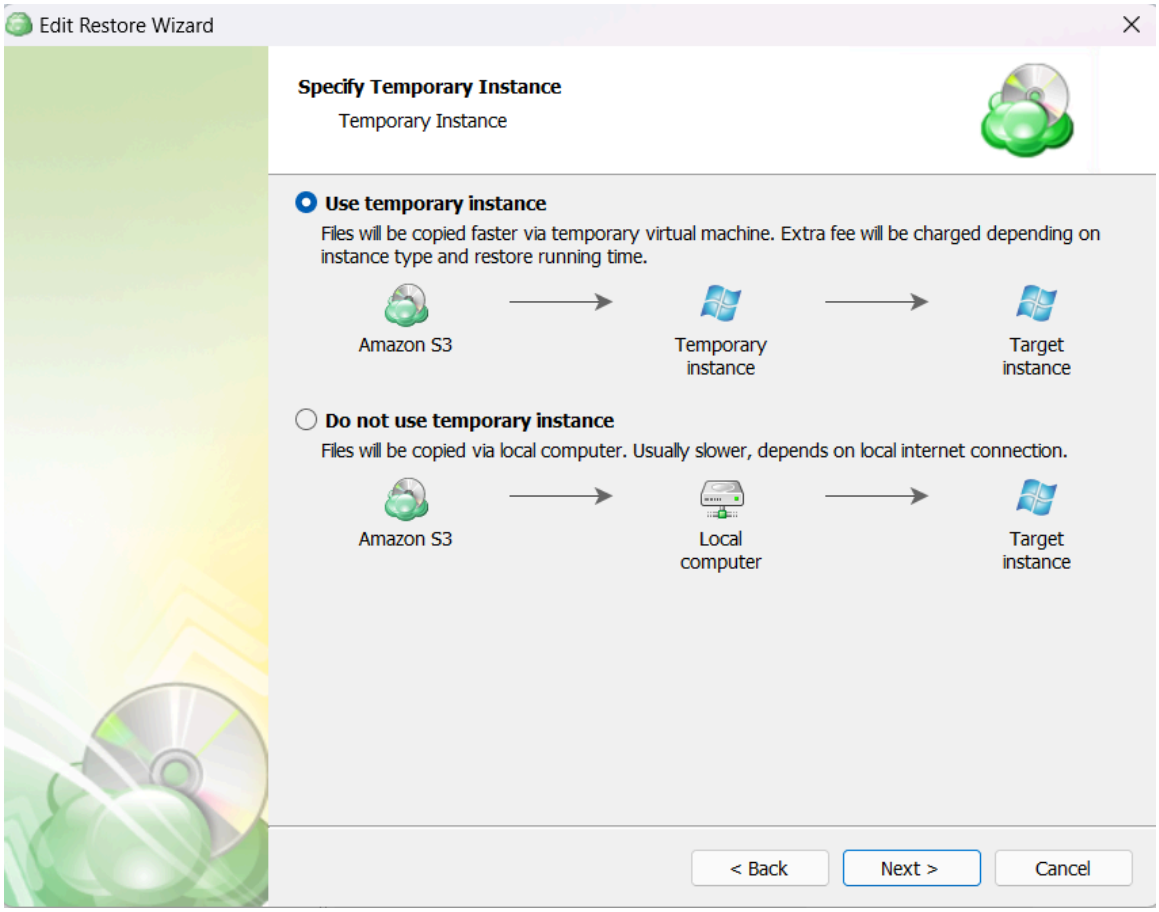
For AWS and Azure destinations, a storage account must already be specified through the MBS portal

Step 10. The next step is to specify the parameters for your target AzureVM instance:



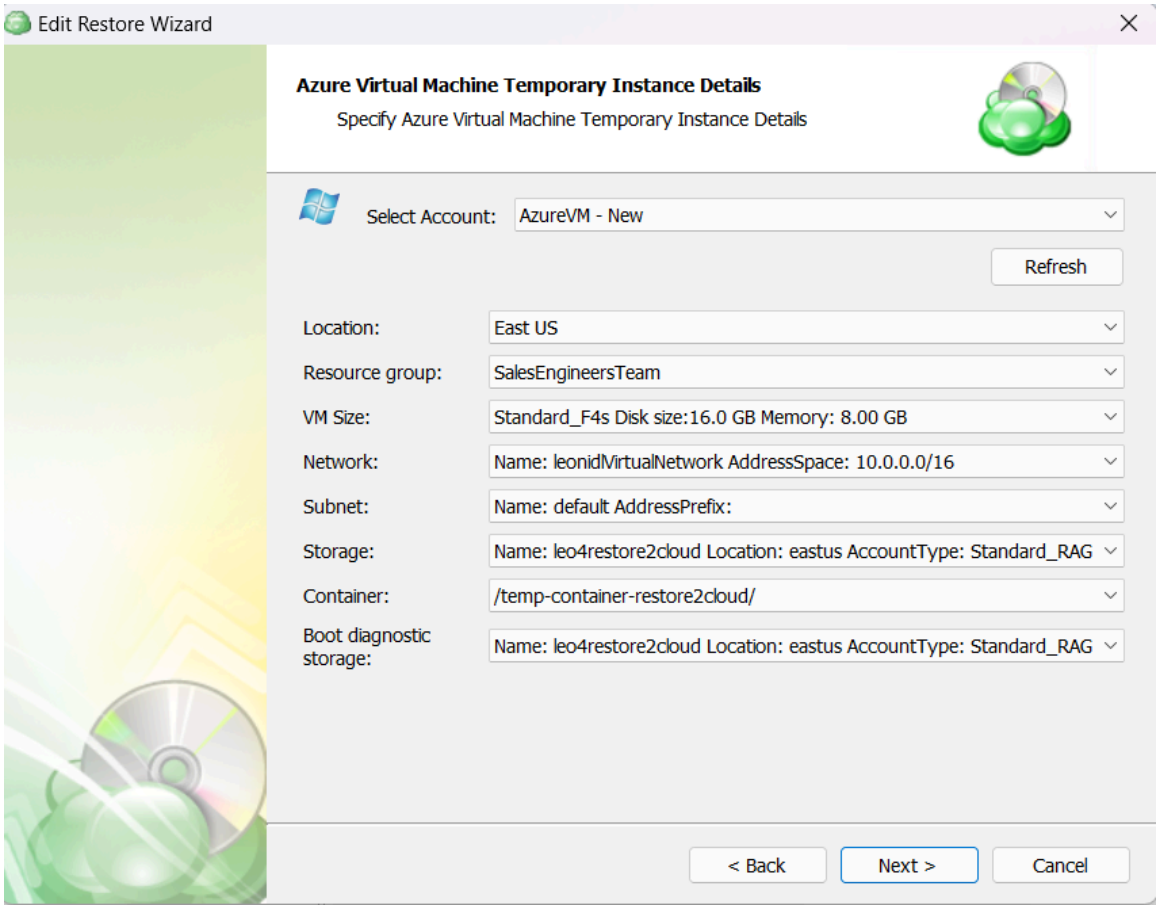
- **Azure Account:** The account under which a new Azure Data Disk will be stored.
- **Data disk name:** Specify the name for the Azure data disk.
- **Resource Group:** Azure Resource Group. This has to be created in advance.
- **Storage**: Select your Azure storage.
- **Storage type:** select between the *Premium SSD, Standard SSD, and Standard HDD.*
- **Container:** Specify the Azure container is to store the temporary disk for VM import.

Step 11. After specifying the target Azure VM instance details, you will need to choose between using a temporary instance or local computer for the restore operation.

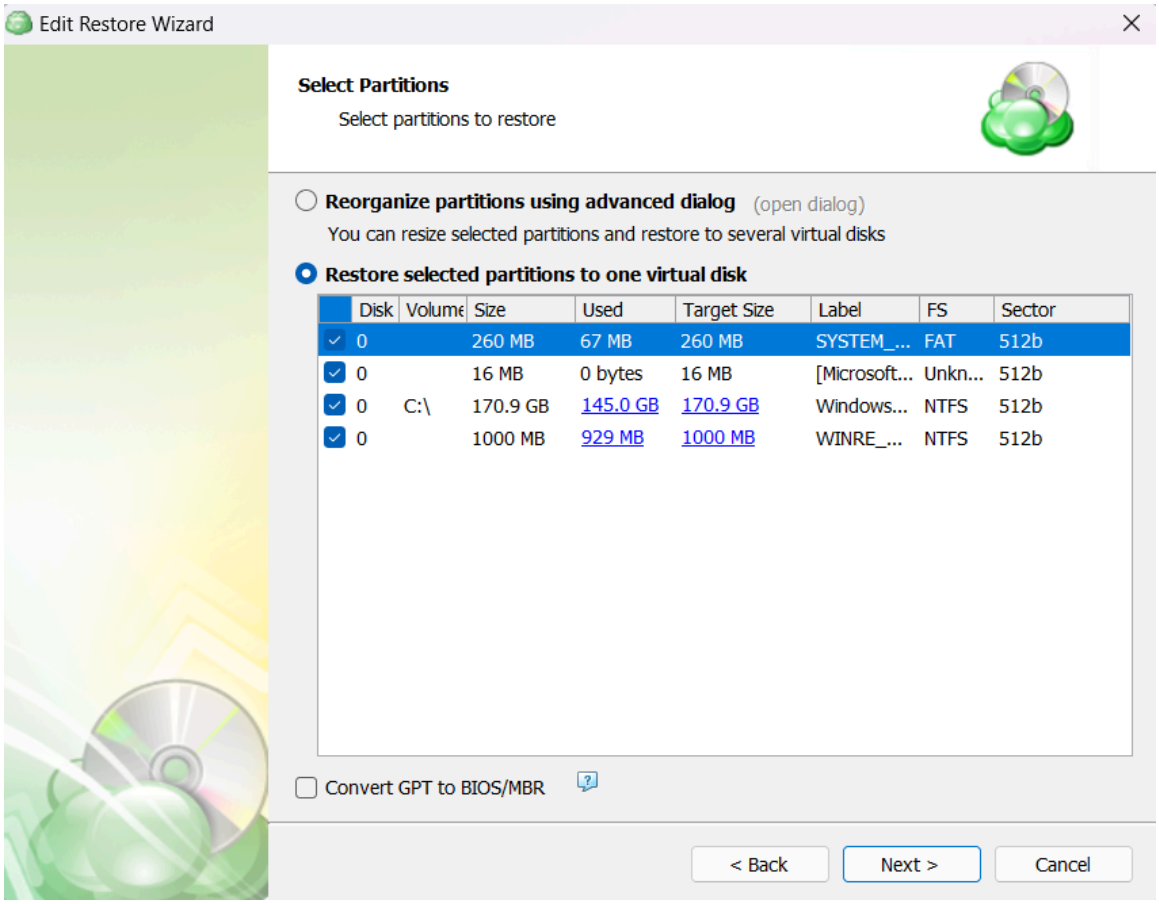


- **Use temporary instance**: This option creates a temporary Azure VM instance that will download backup data from the storage destination and restore it as a target instance. Usually, this method is faster as the temporary and target instance are located in the same Azure network.
- **Do not use temporary instance:** When selecting this option, the restore operation will be performed using the resources of the local computer. Usually, this approach is slower, depending on the local internet connection.

Step 12. If you have selected to use a temporary instance, the next page will allow you to select the Azure account from the upper dropdown box, and specify the Temporary Instance details below.



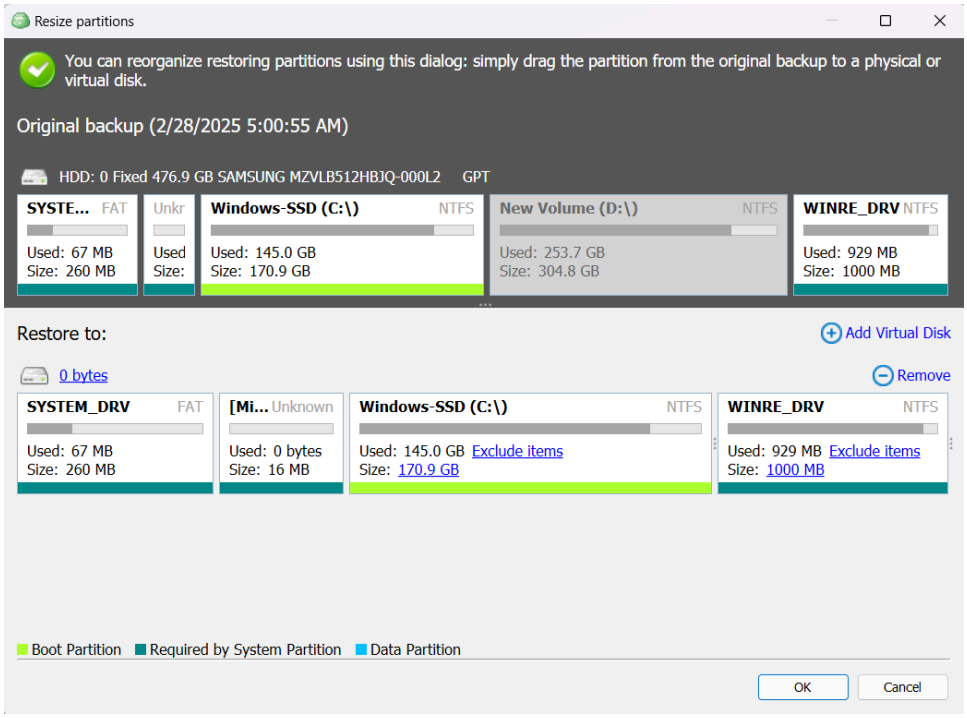
Step 13. After selecting the type of restore target in the previous step, you can now choose to restore the partitions with their existing parameters or to reorganize and resize them.



- **Convert GPT to BIOS/MBR:** Select this checkbox if the target instance or the target OS does not support UEFI boot and requires BIOS boot.

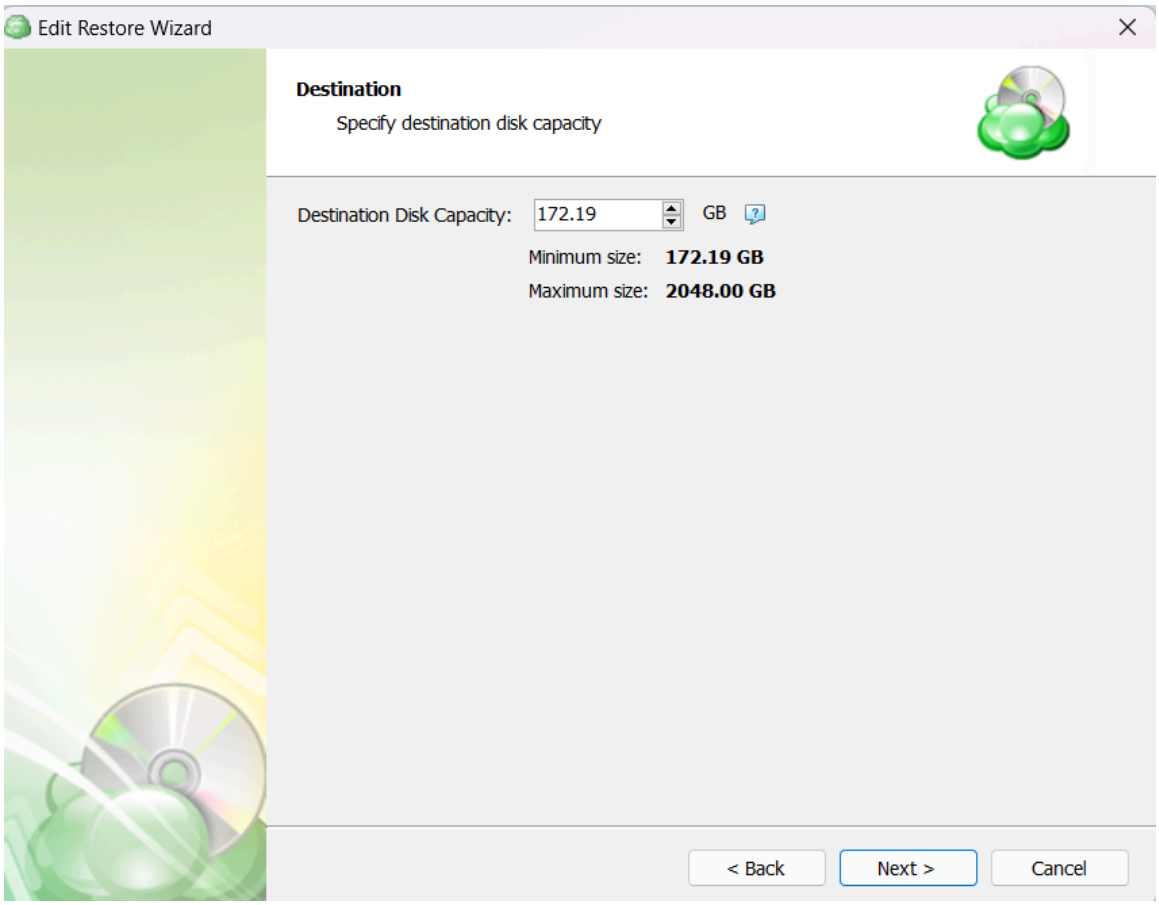
> Some instance types may not support some features such as UEFI boot or TPM. Refer to Azure Documentation to ensure selection of appropriate type of instance.

If you select “Reorganize partitions using advanced dialog” a new window will appear and allow you to resize the partitions and rearrange them on one or more virtual disks.

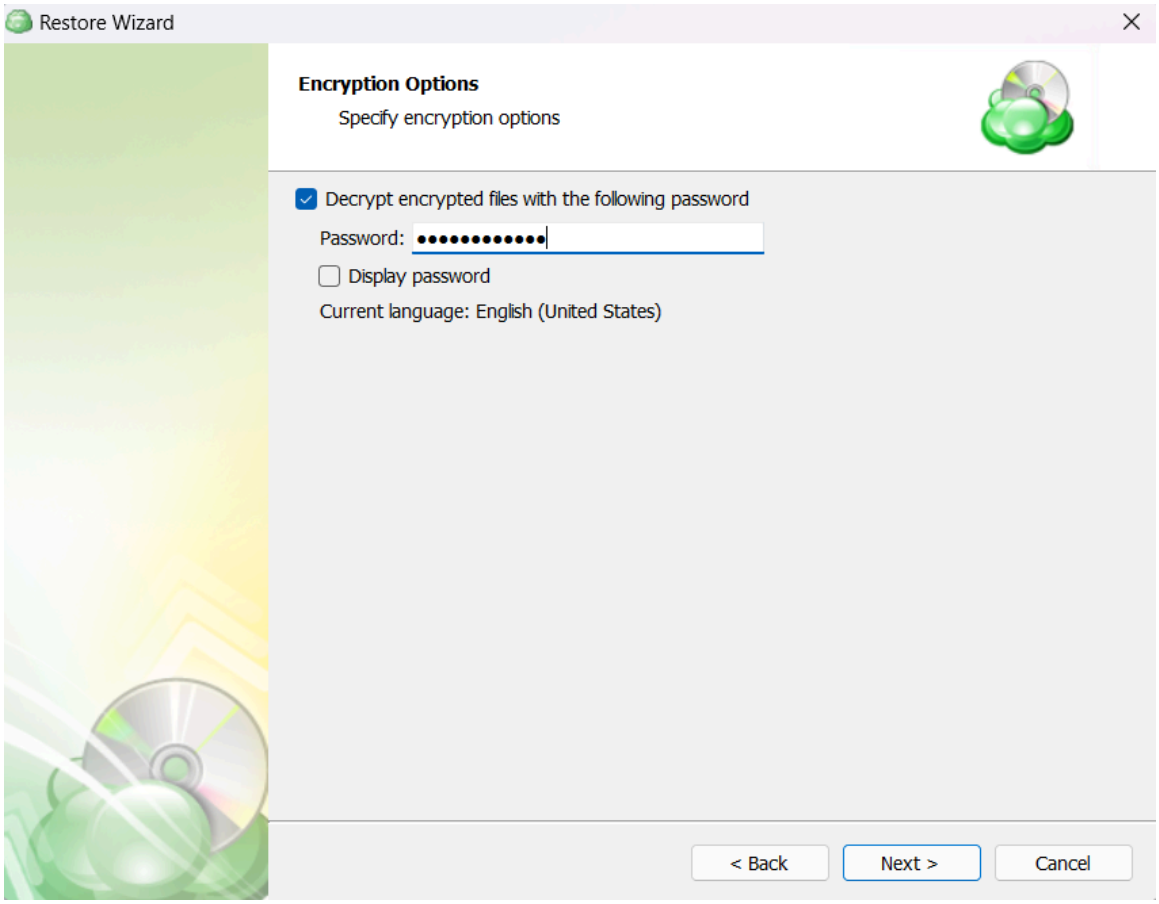


Click on any of the blue hyperlinks to open additional dialogue boxes allowing you greater control over the name and size of the virtual disk, as well as the ability to add additional virtual disks, and also exclude specific files or folders if desired.

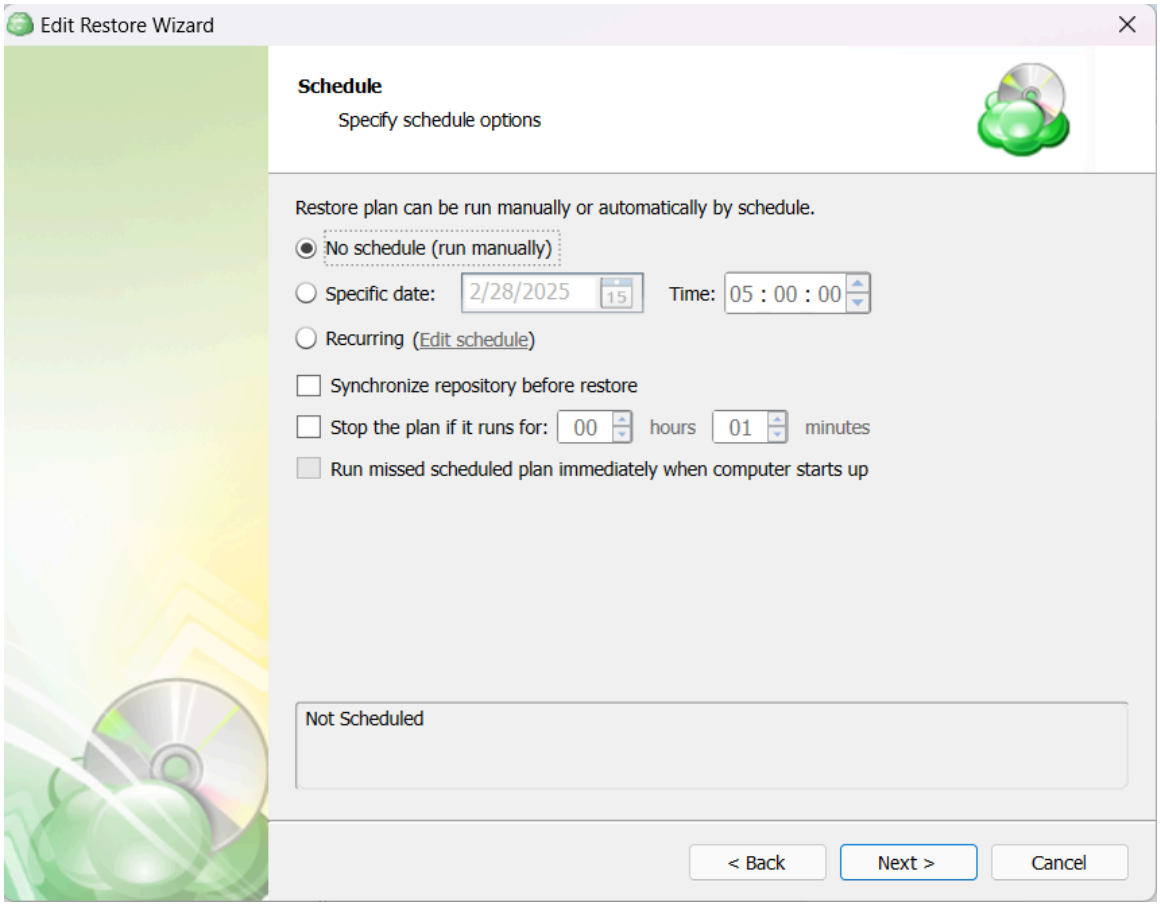
Step 14. Specify the destination disk capacity.



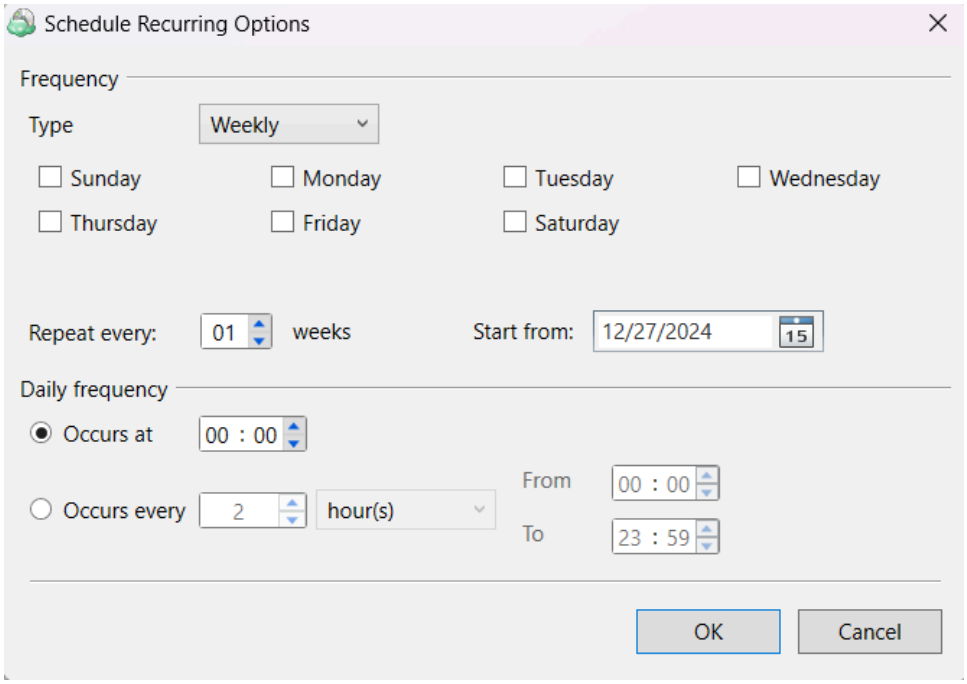
Step 15. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the Image.



Step 16. With the decryption password entered, the next step is setting the schedule for the restore plan.



- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

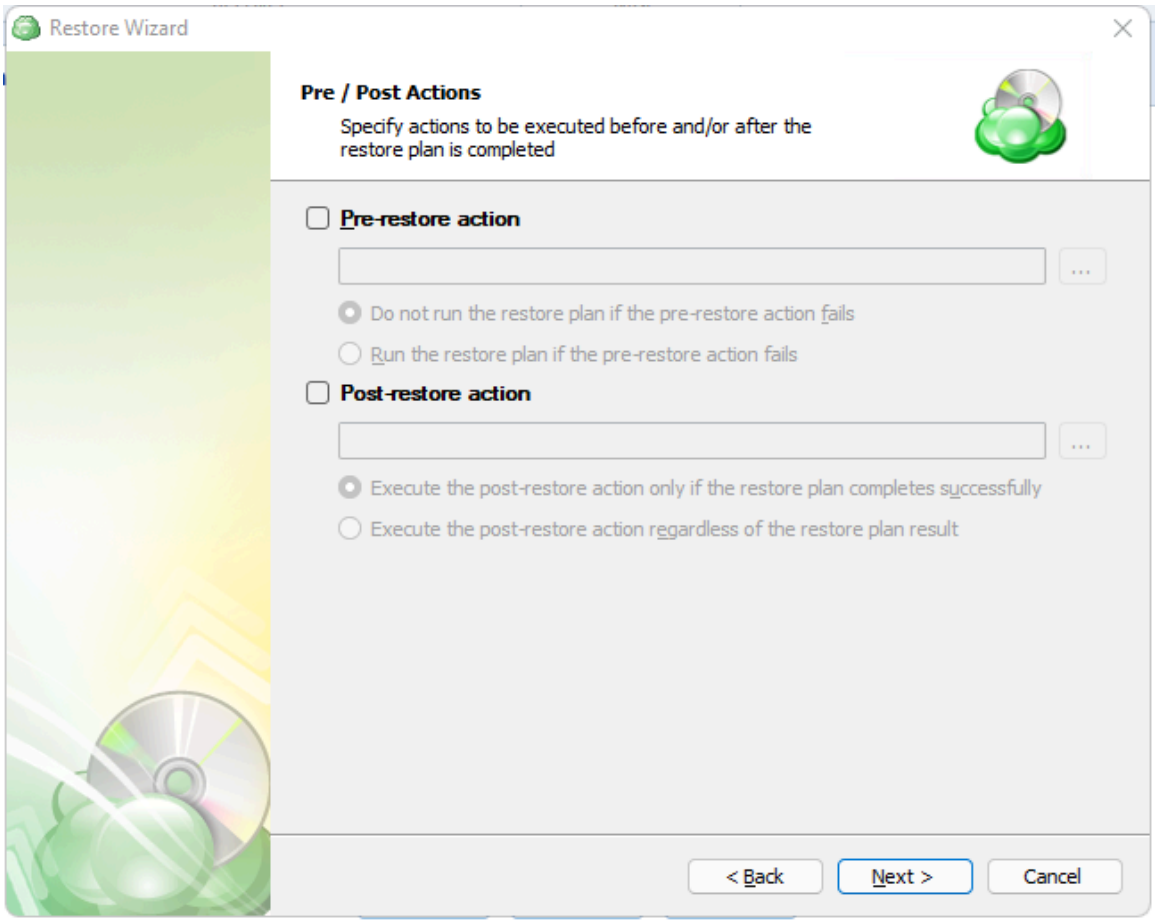


It is recommended to check the "**Synchronize repository before restore"** if the restore plan is created on a computer different from the original or if you are logged in with a different backup user account.

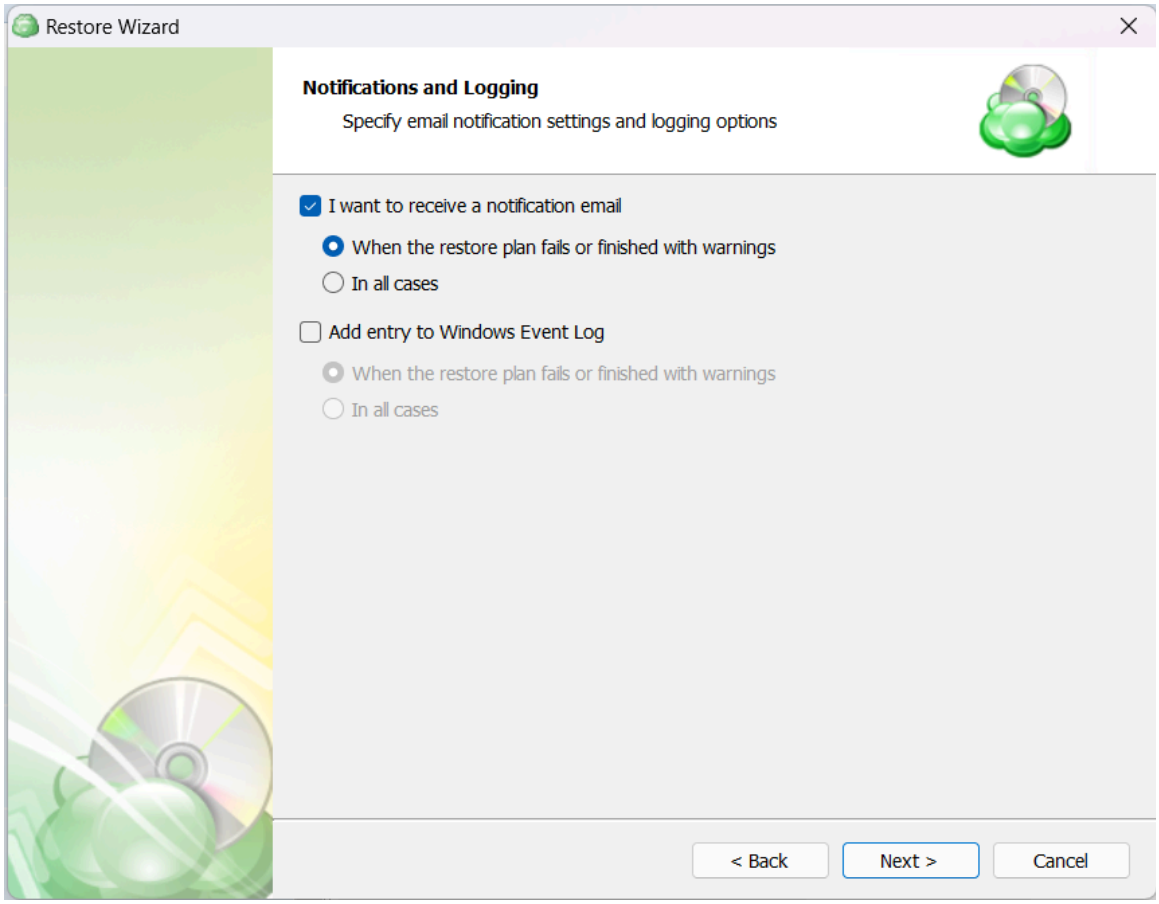
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

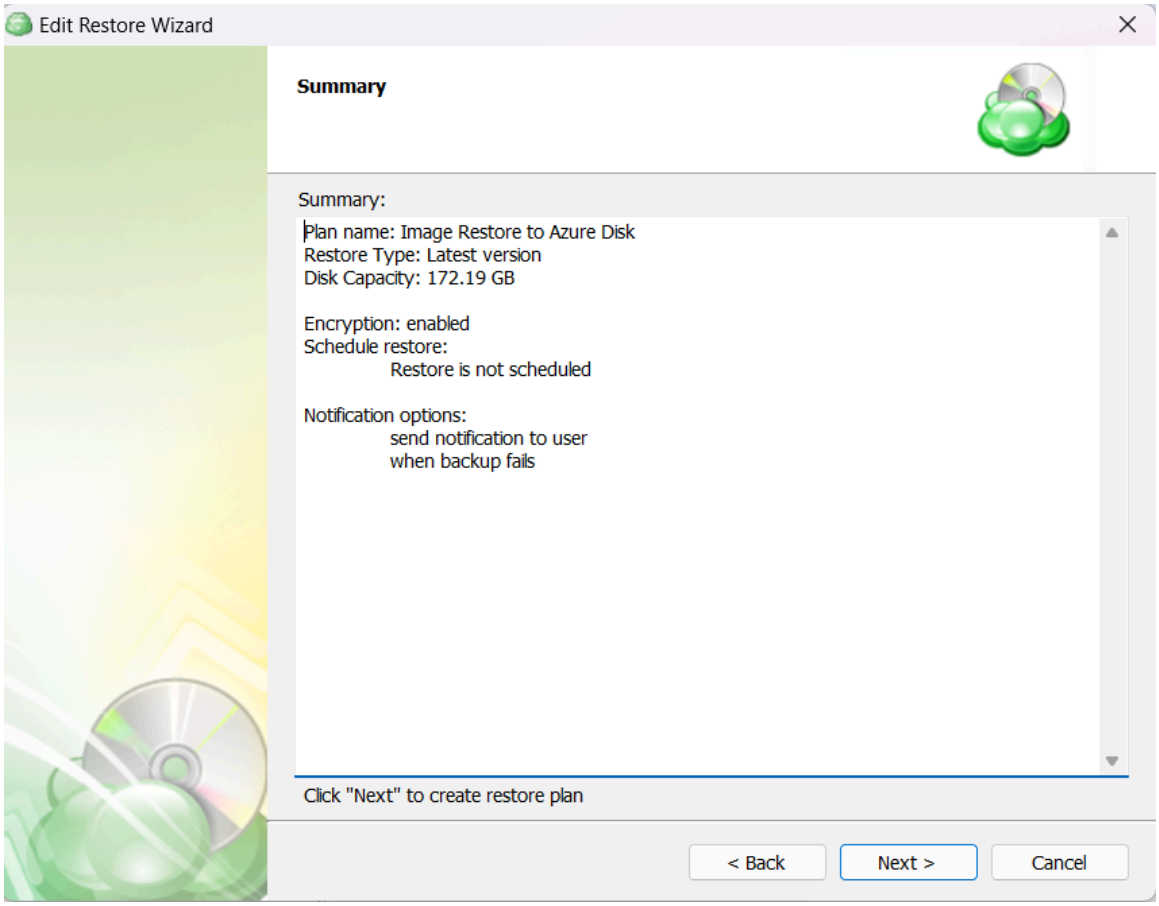
Step 17. After setting the schedule, the next step allows pre and post actions to be defined.



Step 18. Next, you can select options to receive notification email and/or add an entry to Windows Event Log.



Step 19. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.

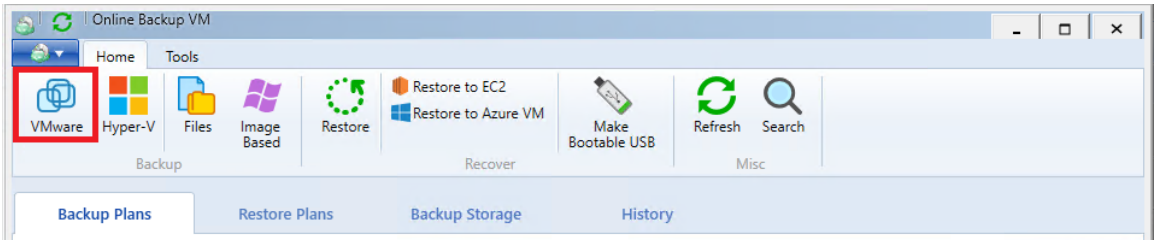


If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

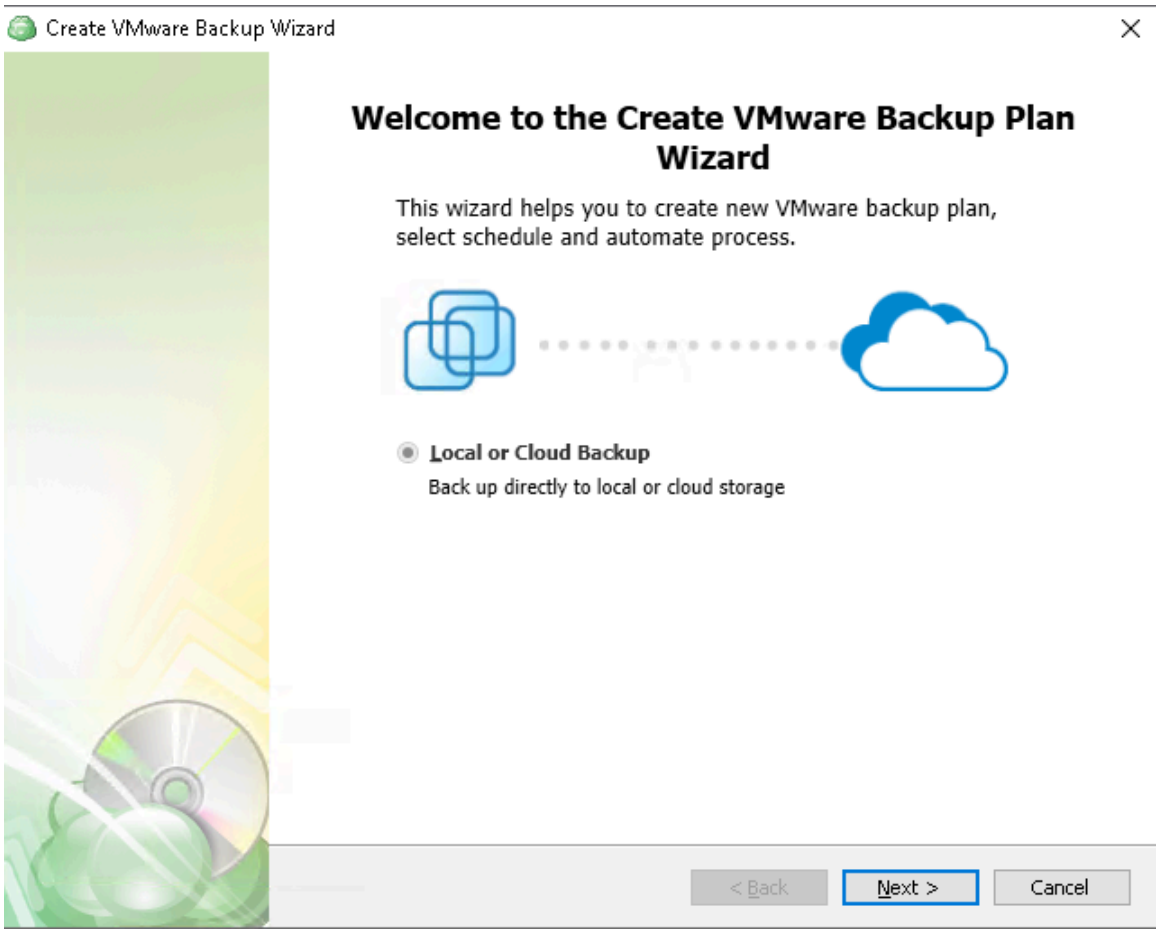
VMWare Backup Plans

Backing up VMs using the Agent

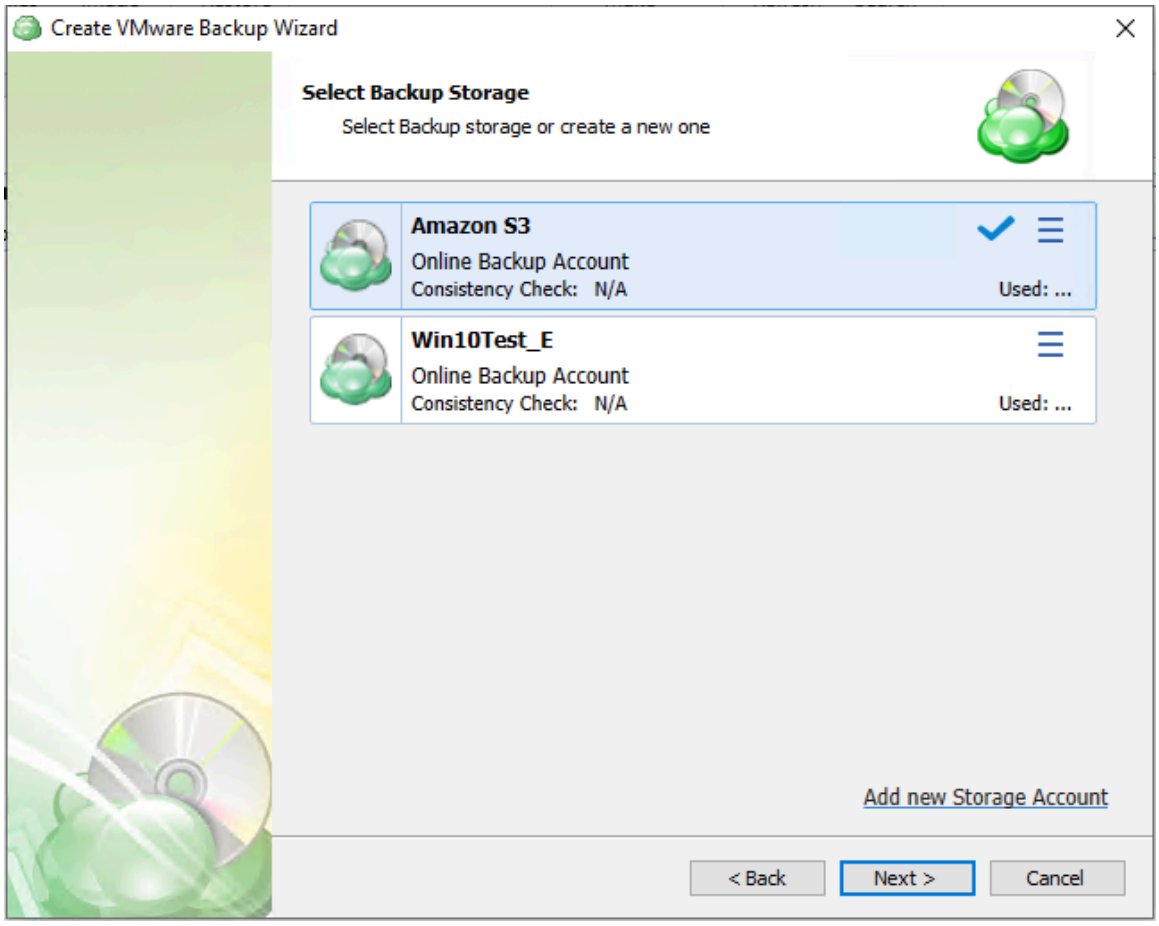
Step 1. Within the Online Backup Agent, click on “VMware”



Step 2. You will then be prompted with a list of available backup types.

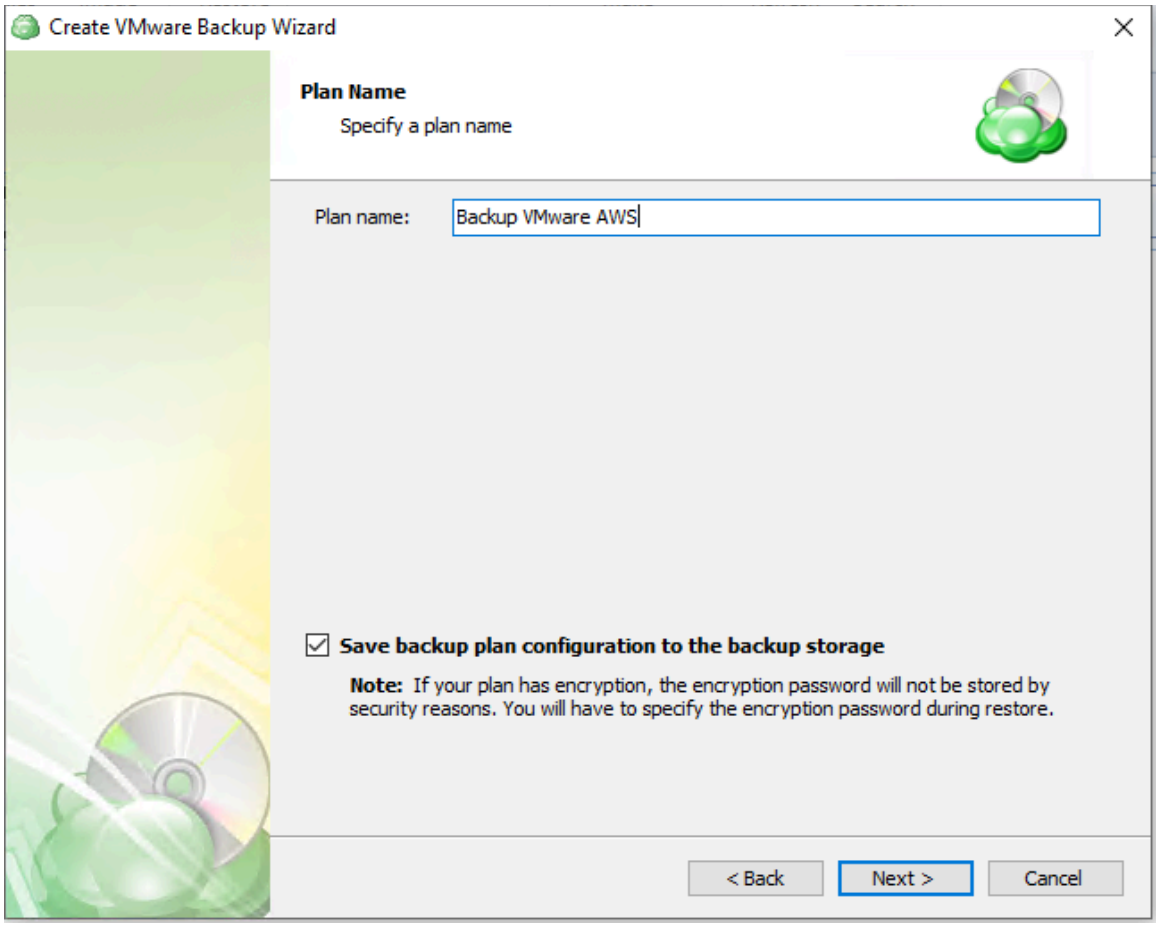


Step 3. The next step will prompt you to select the destination for the backup.



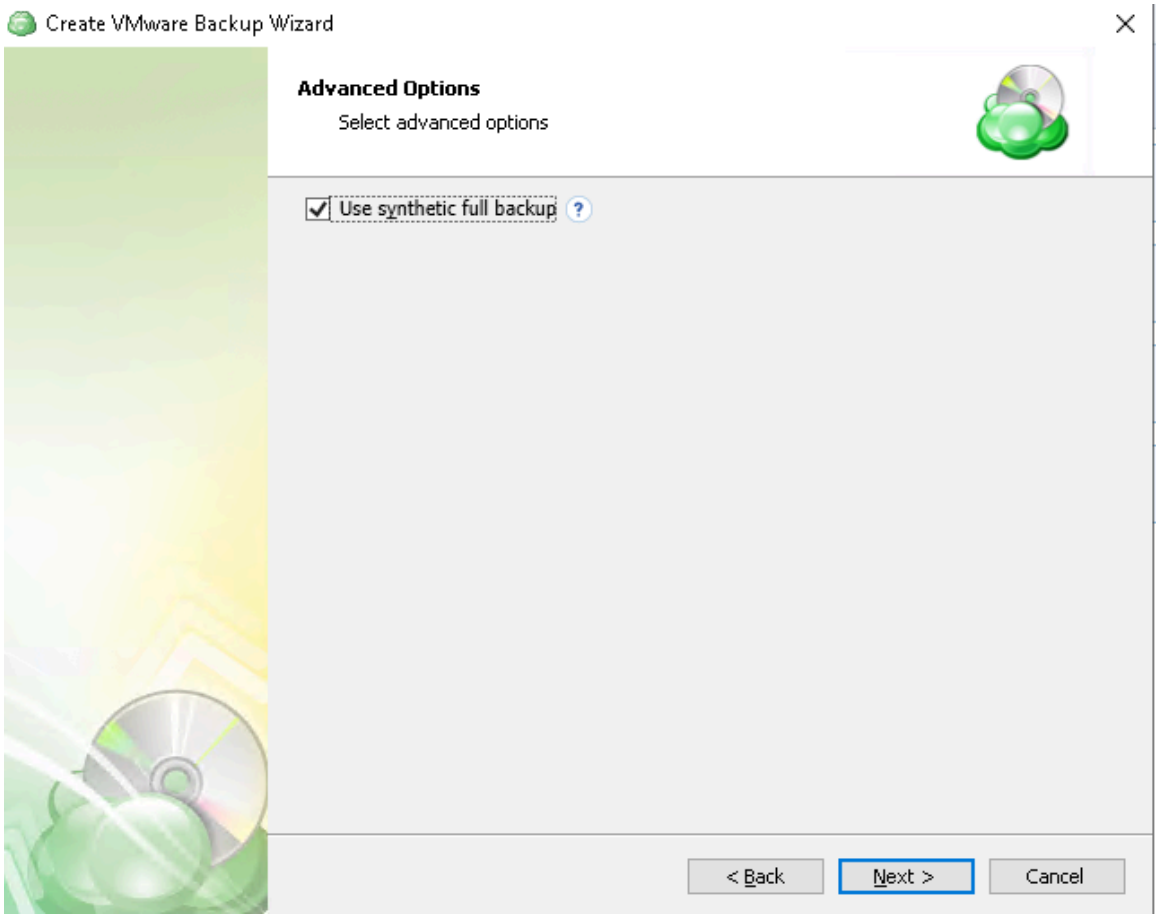
If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

Step 4. Next, you will be prompted to name the plan.



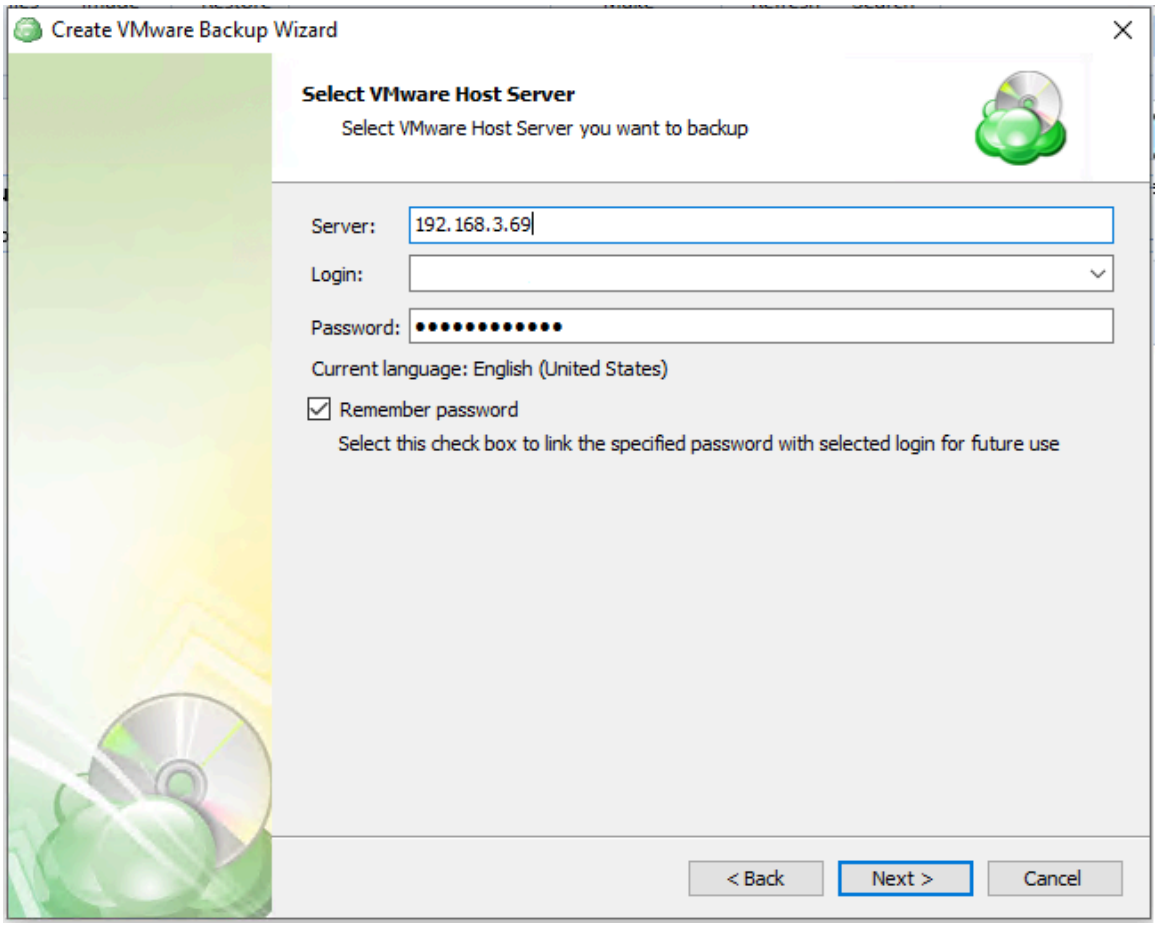
It is recommended to use a descriptive name which will distinguish the backup from others.

Step 5. The next step will give you a list of available Advanced Options. It is recommended to leave these in their default configuration.



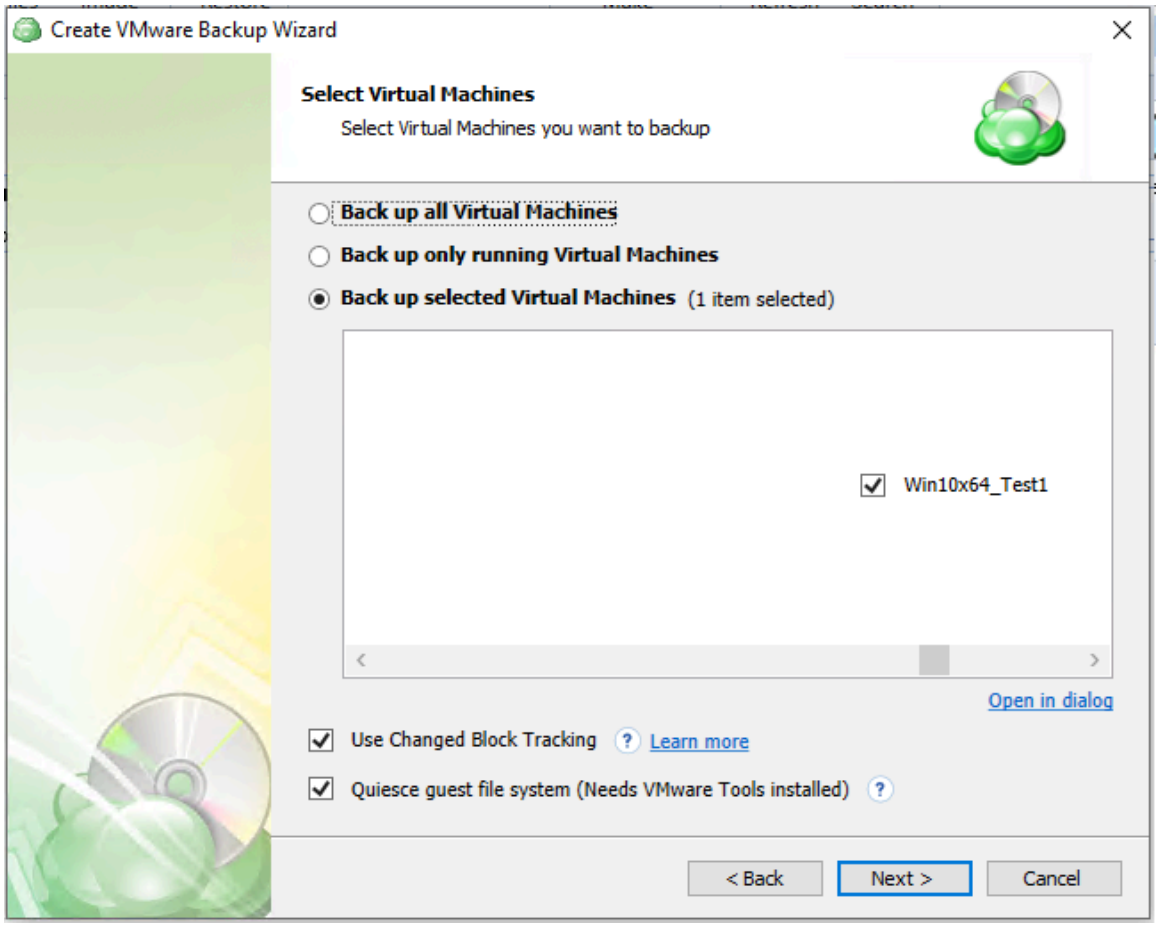
Synthetic Full Backup reduces the amount of transmitted data and backup time. A new Backup revision is assembled on the target storage by combining already existing blocks from previous revisions with newly uploaded blocks

Step 6. Connect to the vCenter or ESXi by using the FQDN or IP address.



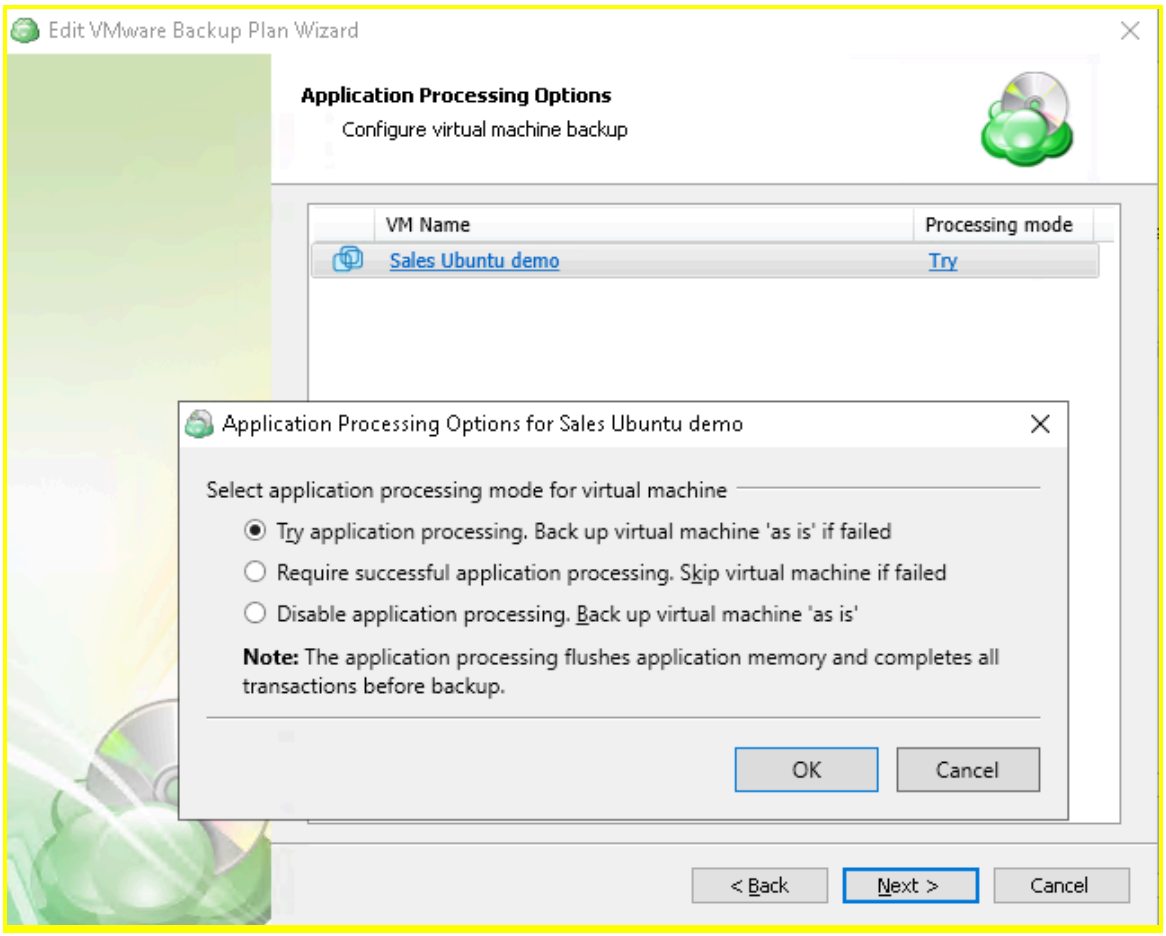
It is important to determine whether FQDN or IP addresses will be used for all future plan configurations. The application will consider each to be unique hosts, even if the target machine is the same.

Step 7. Next, select the Virtual Machines you wish to back up.



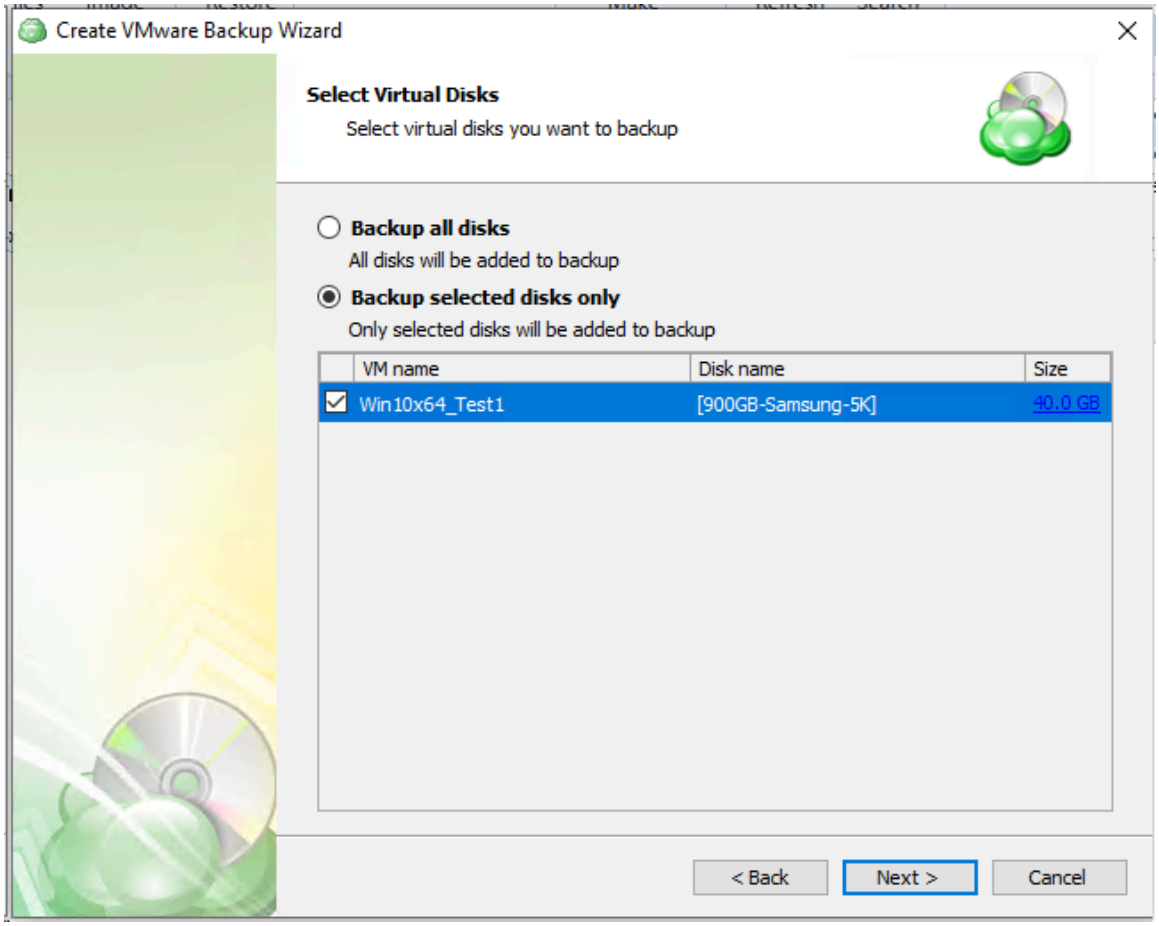
- **Back up all Virtual Machines:** will backup all VMs regardless of current state. This is recommended only for small environments.
- **Back up only running Virtual Machines**: Only backs up VMs currently in "Running" status and is recommended for clustered environments where backup servers planned for failover procedures are not required to be selected.
- **Backup up selected Virtual Machines:** Allows you to backup a group of VMs by selecting them from the list below. This allows for greater control of mixed status VMs and for larger environments where it is beneficial to split the backup into multiple plans.

Step 8. Select the processing mode

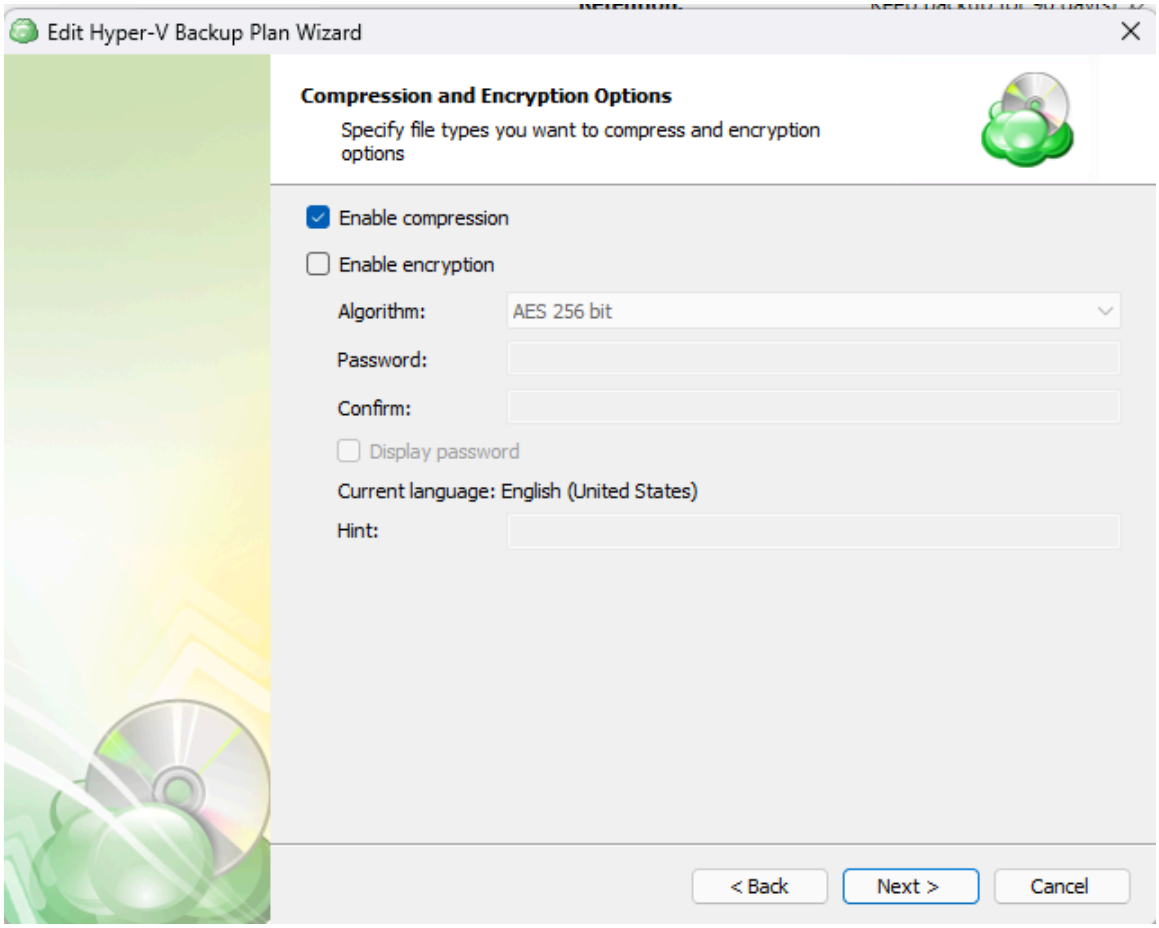


- **Try application processing**. Backup will perform whether or not the application-concistent process fails. If the processing fails, the backup will be done “as is”, but data consistency is not guaranteed.
- **Require successful application processing**. Skip virtual the machine if processing fails. If processing is successful, it ensures that applications running in the VM, such as databases, are taken into consideration and the backup will ensure data consistency is maintained.
- **Disable application processing**. Backup virtual machine “as is” and does not perform any application processing. The VM is backed up in its current state, which may cause data inconsistencies.

Step 9. Once you have selected which VMs to backup, the application allows you to then choose whether to backup all virtual disks on the selected VMs or to only backup selected virtual disks.



Step 10. After you have selected which VMs and disks to backup, the next step is to set the compression or encryption options.



Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

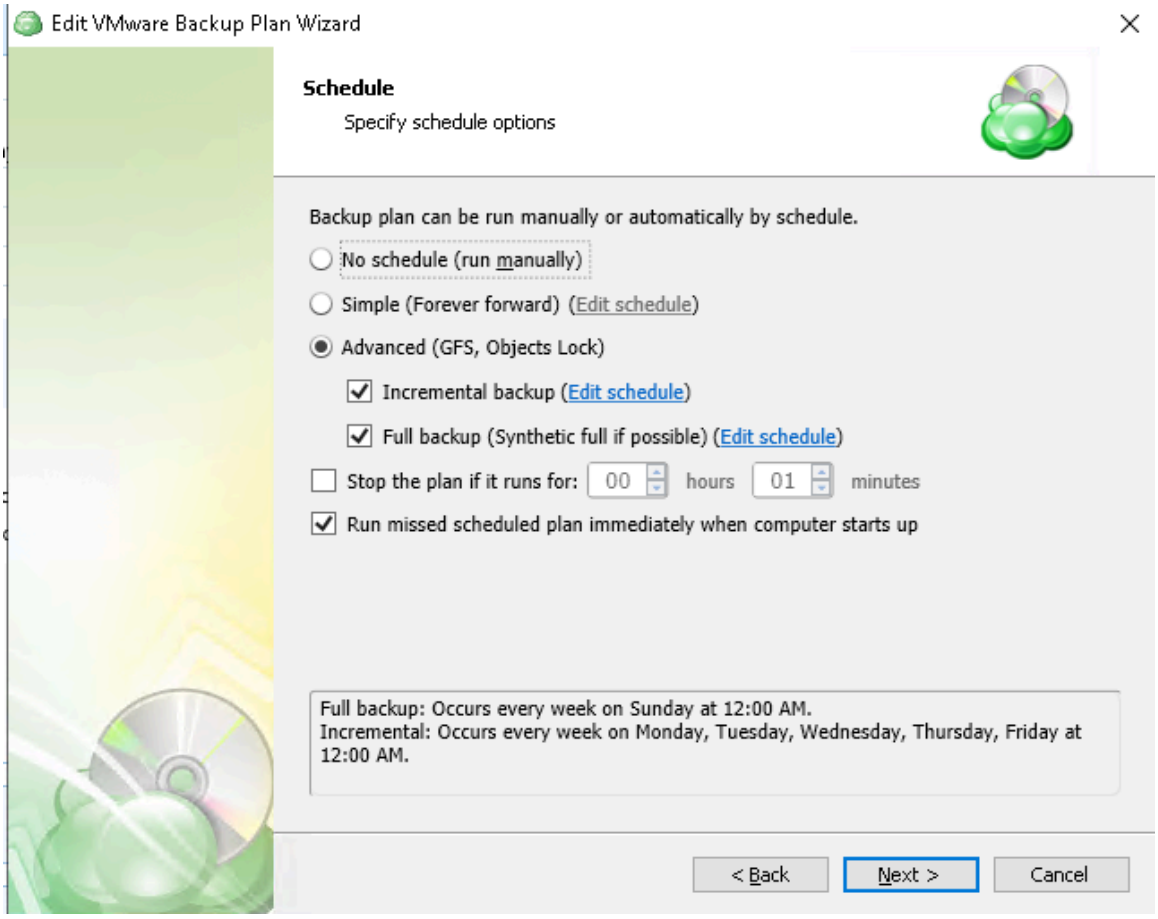
Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place and enable the Password Recovery Service.

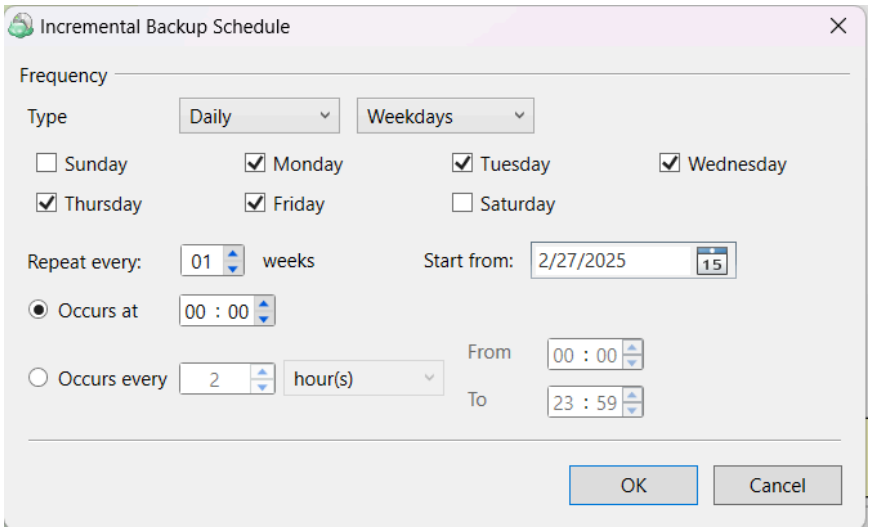
Step 11. Next you are able to choose whether or not to enable the Full Consistency Check.

It is recommended that you leave "**Enable Full Consistency Check**" enabled.

Step 12. Next you are prompted to set the schedule for your backup plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.



- **Simple (Forever forward):** Select the Simple (Forever Forward) option to use the Forever Forward Incremental (FFI). This schedule offers one full backup followed by a limited number of incrementals. Once the limit is exceeded, a new full backup is created using the synthetic full capabilities.



Forever Forward backups are only supported by a limited number of cloud storage providers. For more information, refer to Forever Forward Incremental.

The Simple (Forever forward) schedule is recommended for retention up to 100 restore points which do not require Object Lock for legal compliance.

It is not recommended to select the Simple (Forever forward) schedule for long-term storage and archival purposes. The Advanced Schedule is recommended for all storage needs over 100 restore points.

- **Advanced (GFS, Object Lock):** Select the Advanced option to set up a flexible, recurring schedule with generations. Every generation contains one full backup followed by incrementals.
    - Clicking on “Edit Schedule” next to Incremental and Full backups allow you to configure the frequency they will be created. If both a Full and Incremental are scheduled for the same day, the application will perform the Full only.

It is recommended to use the Advanced (GFS, Object Lock) option and regularly scheduled full backups for long-term storage (longer than 6 months) or backups that must comply with legal or industry requirements.

Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

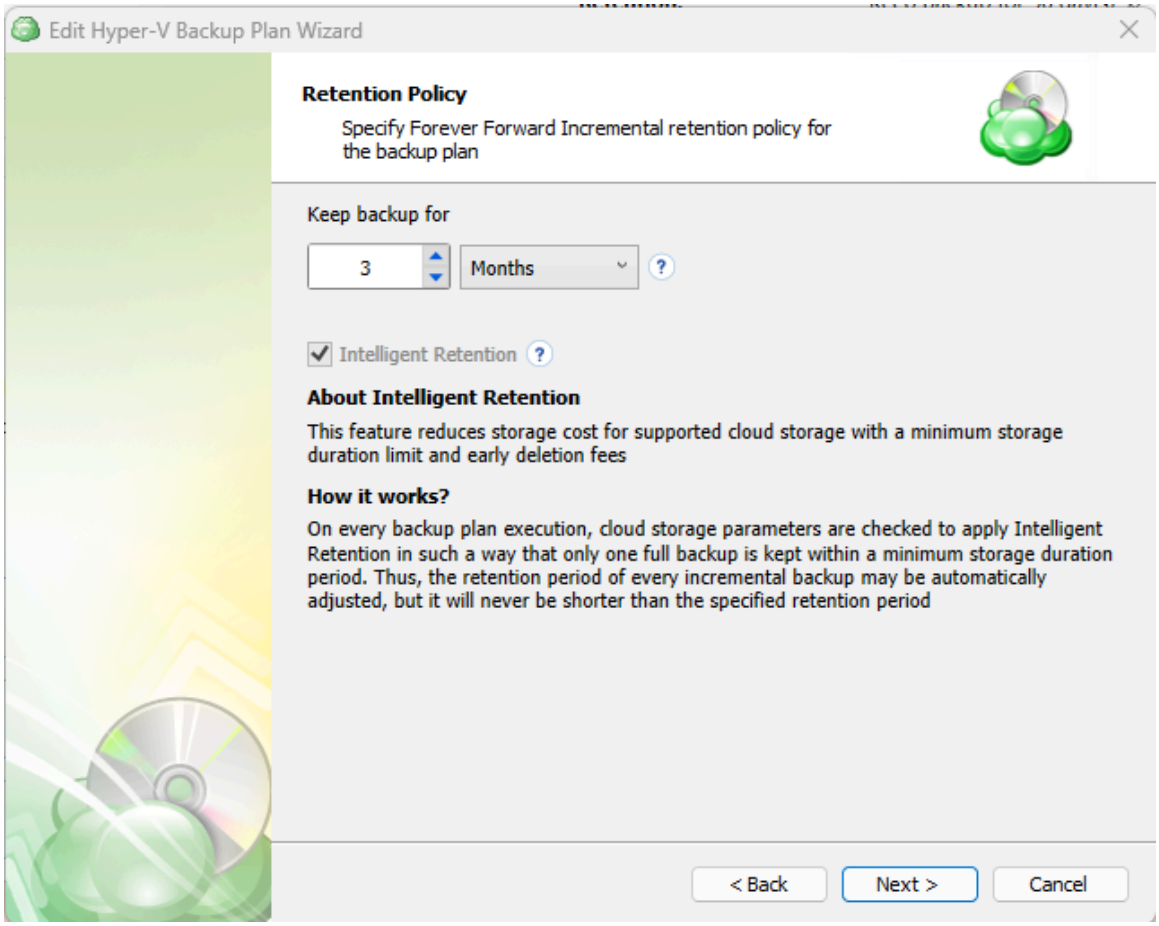
Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

Synthetic Full Backups allow the system to merge a series of incremental backups together to form a new full backup, greatly reducing the time and bandwidth needed to perform full backups after the initial full. If the storage destination does not support Synthetic full, then a traditional full will be made instead.

The Advanced Schedule and GFS retention policies will only perform properly with regularly scheduled full backups.

Step 13. On the “Retention Policy" step, you can set the policies the application will use to determine which data to purge at regular intervals.

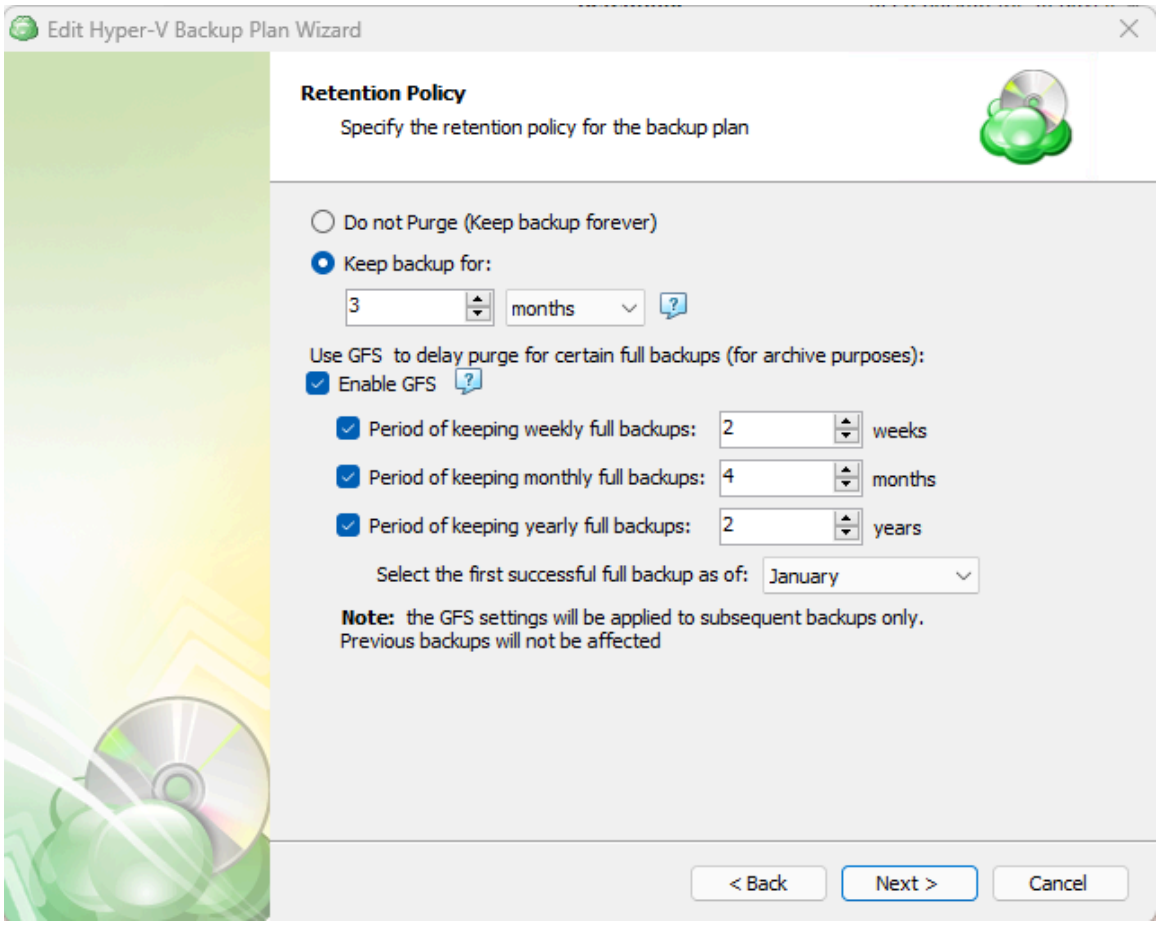
If you have selected the Simple (Forever forward) schedule you will be presented with the following options:



- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.

If you have selected the Advanced (GFS, Object Lock) schedule, you will also have an option to define the multigenerational Grandfather-Father-Son (GFS) parameters if required.

This allows you to retain full backups for longer periods while purging the incremental backups after a shorter period.

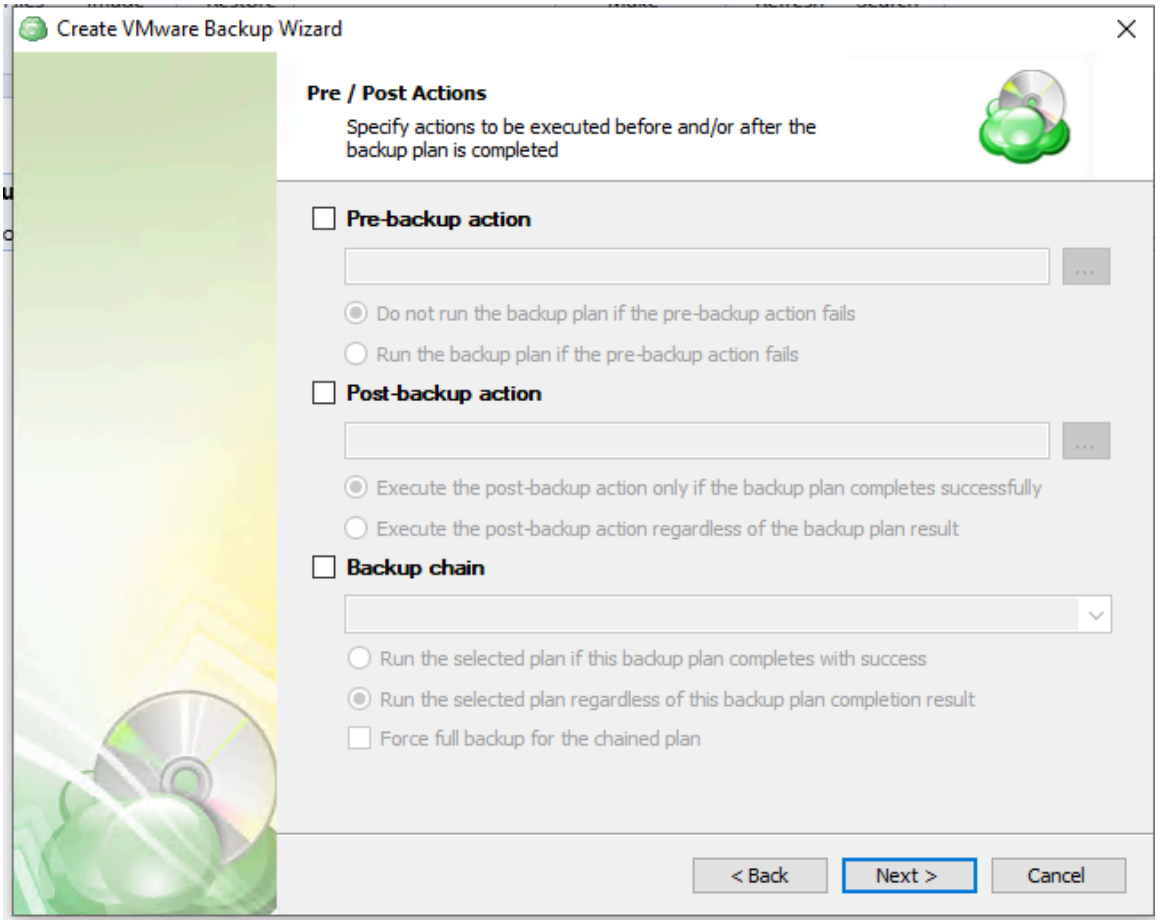


- **Enable GFS**: Select this option if you want to keep Full Backups for archival purposes at the selected intervals.
- **Period of keeping weekly full backups**: Set the number of Weekly Full Backups to retain. This is determined separately from the “Keep backup for” value and relies on Full Backups to be scheduled on at least a weekly basis in the previous step.
- **Period of keeping monthly full backups:** Number of Monthly Full Backups to retain. A Full Backup can be flagged as both a Weekly and Monthly backup, but once the number of Weekly Full Backups has exceeded their retention setting, only those also flagged as a Monthly will be retained.
- **Period of keeping yearly full backups:** Set the number of Yearly Full Backups to retain. A Full Backup can be flagged as a Weekly, Monthly, and Yearly Backup. Once the number of Monthly Full Backups has exceeded their retention setting, only those also flagged as a Yearly will be retained.
    - **Select the first successful full backup as of**: Select the first Monthly Full Backup you would like to flag and retain as the first Yearly Full Backup.

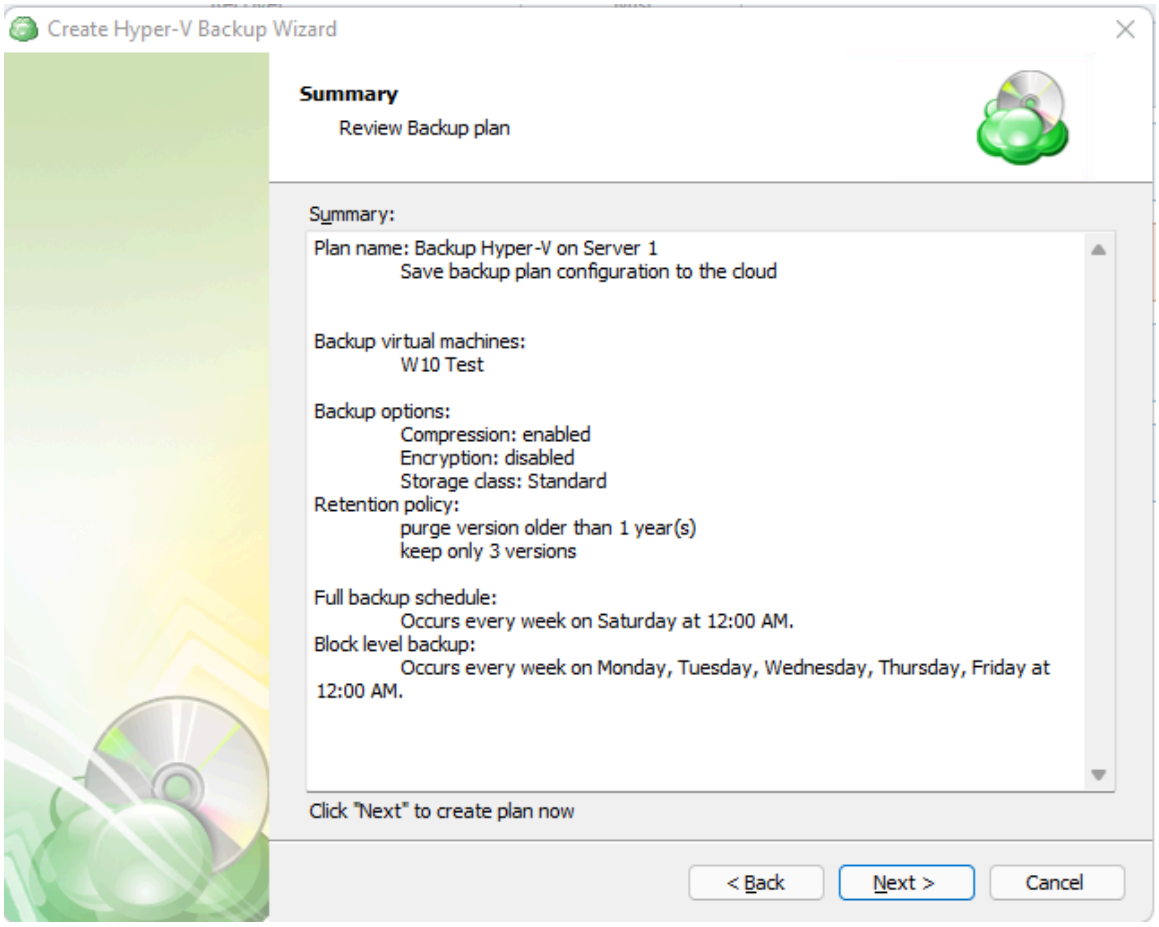
Generations will not be deleted until the youngest point in the chain has met the retention criteria.

GFS Retention provides an excellent way to efficiently archive data for compliance. Additional information can be found in GFS Policy topics in the MBS Documentation

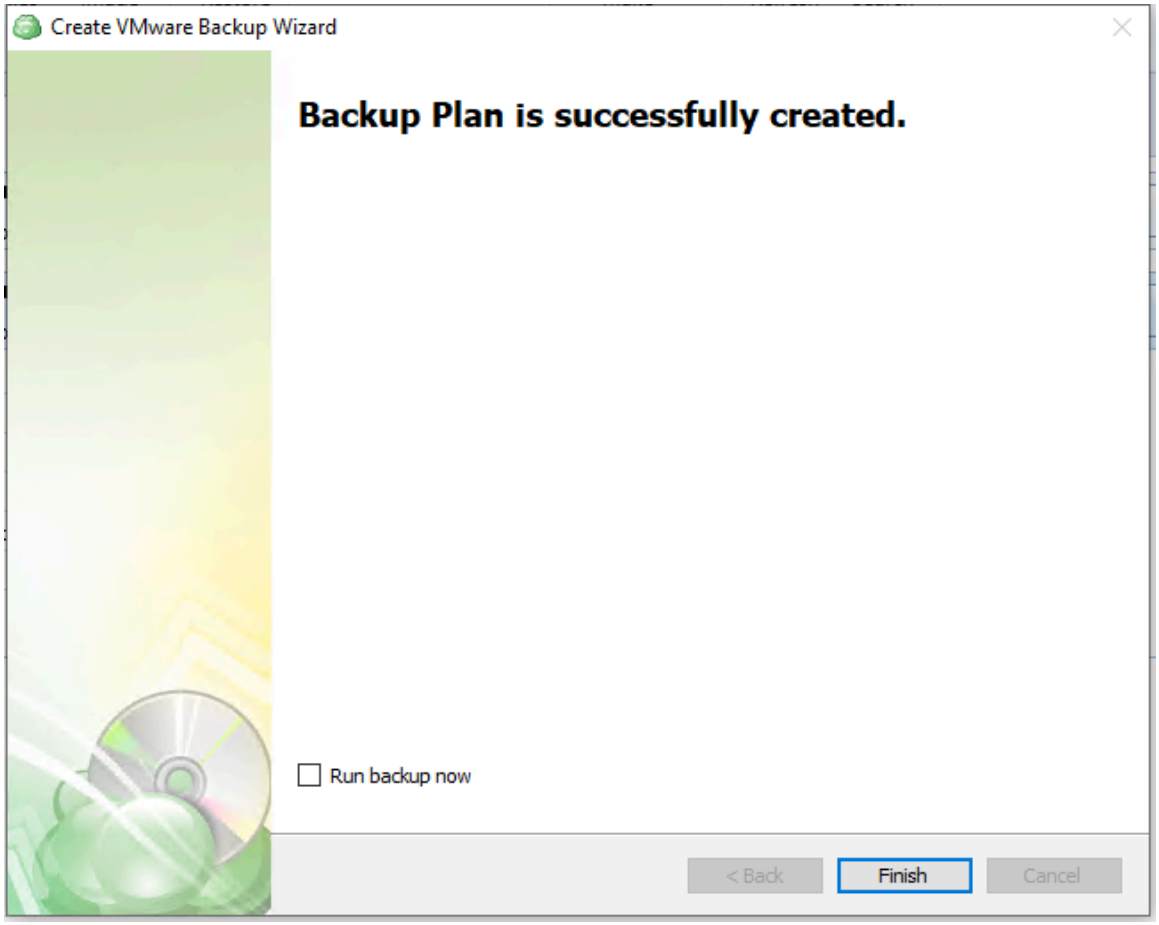
Step 14. After the schedule is set, the next section is used to set the “Pre” and “Post” Actions



Step 15. After the schedule is set, you will be shown a summary of the selected options.

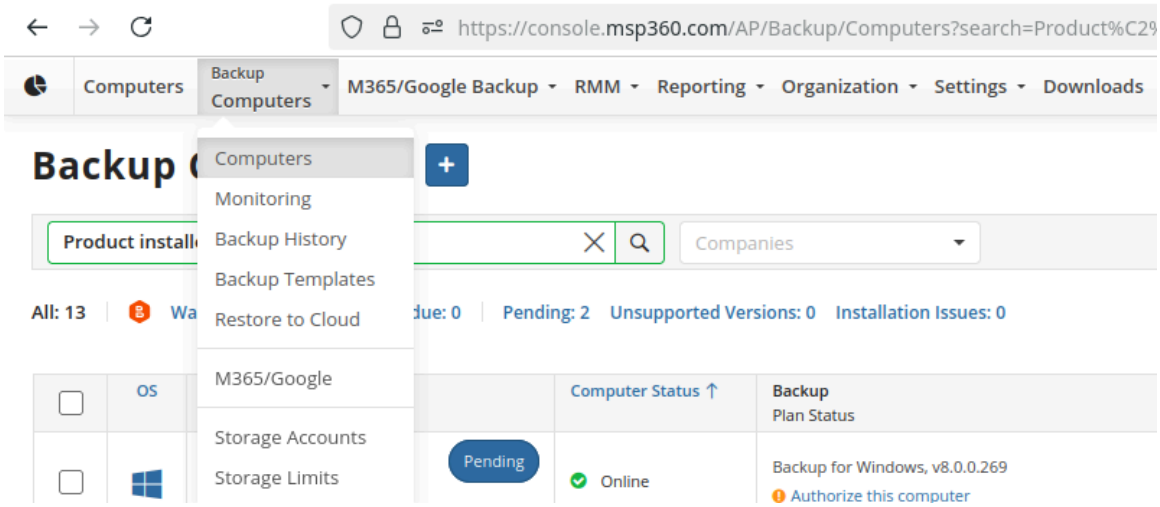


Step 16. The final step of the wizard will confirm that the Backup Plan was successfully created. If you select the “Run backup now” box, the application will initiate it immediately upon exiting the wizard, otherwise it will run at the next scheduled time.

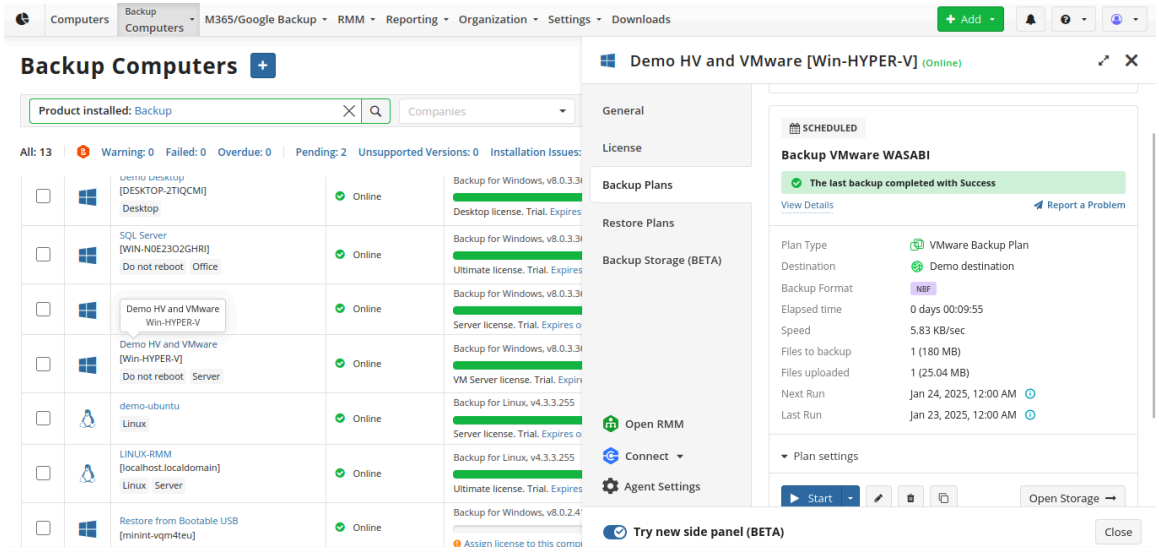


Backing up VMs using MBS

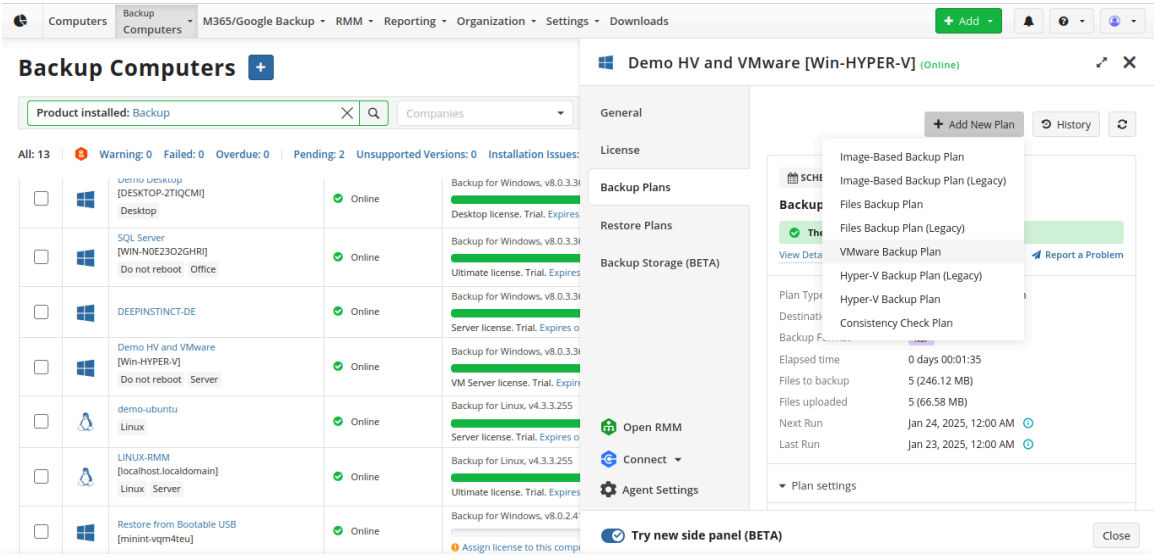
Step 1. From the MBS Portal, left-click Backup > Computers



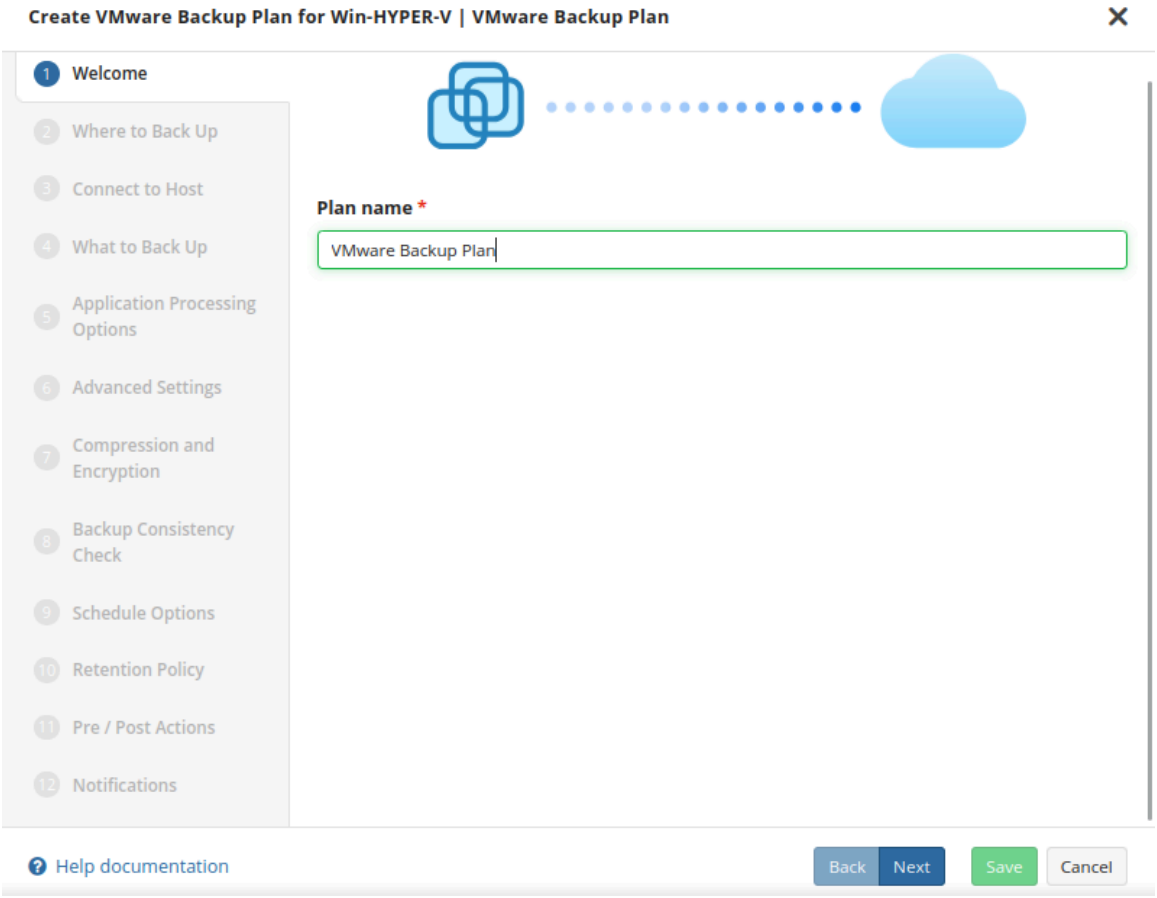
Step 2. Locate the computer you wish to backup from the list and open the current list of plans by either clicking on the name of the computer, or by selecting “Show Plans” from the three dots menu.



Step 3. To create a new VMWare Backup Plan, click on “Add New Plan” then click on “VMWare Backup Plan”

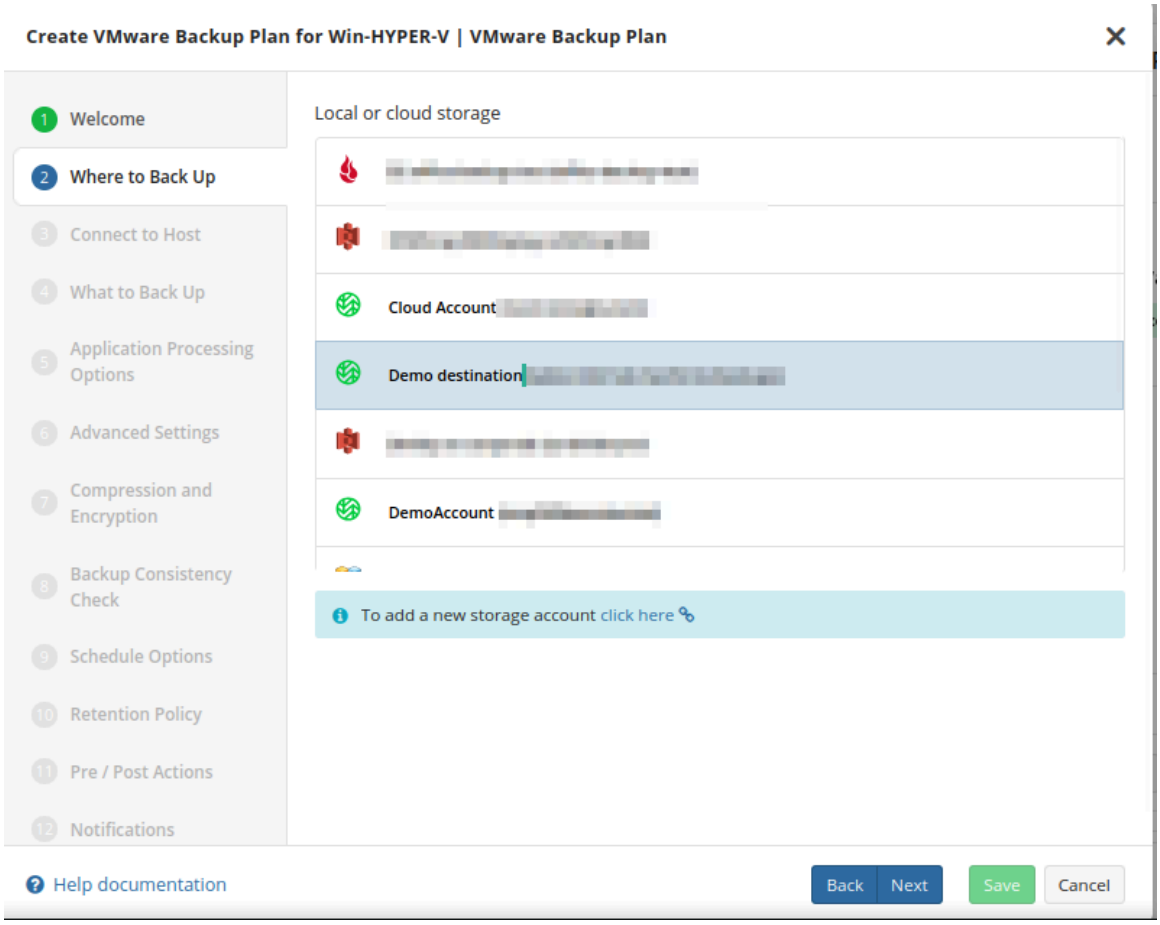


Step 4. The first step when creating a new VMware backup plan is to give the plan a name.

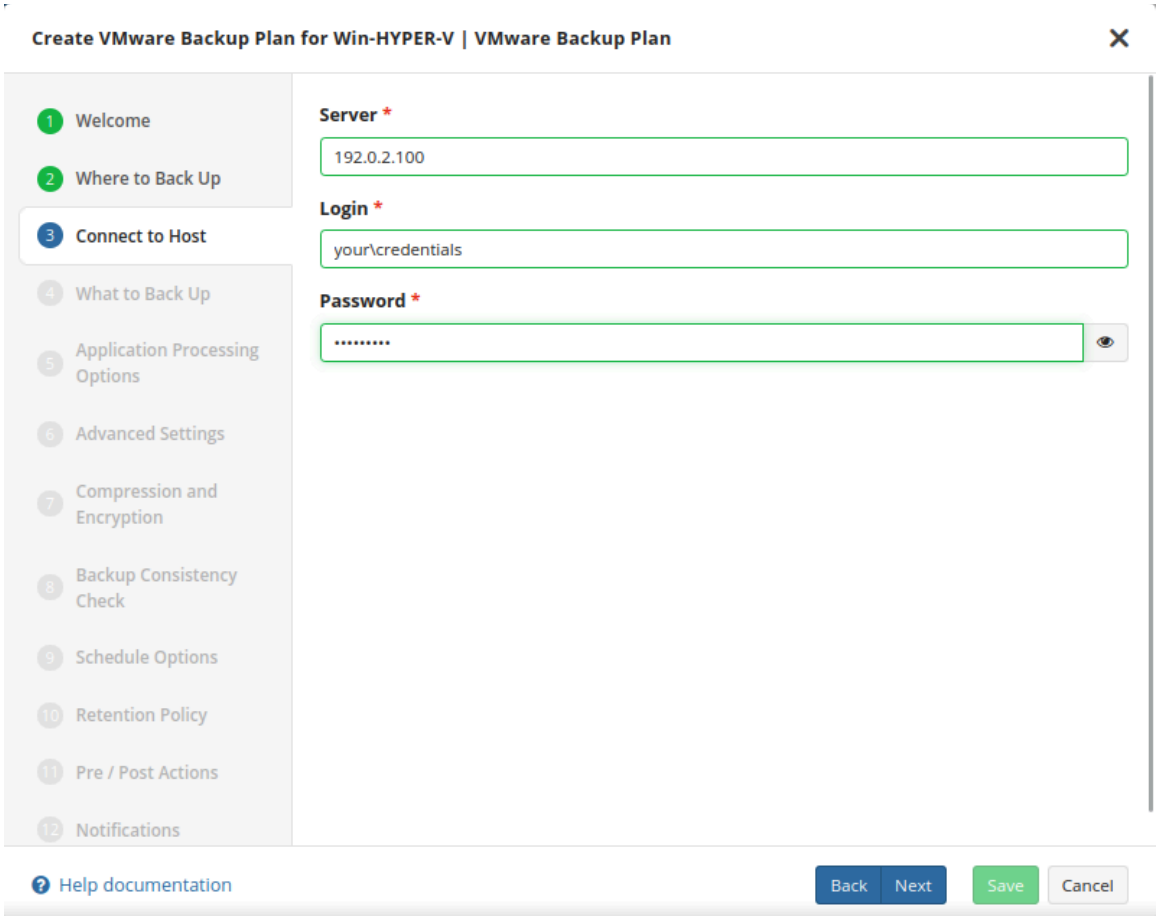


It is recommended to use a descriptive name which will distinguish the backup from others.

Step 5. In the next section, you are prompted to select the backup destination.

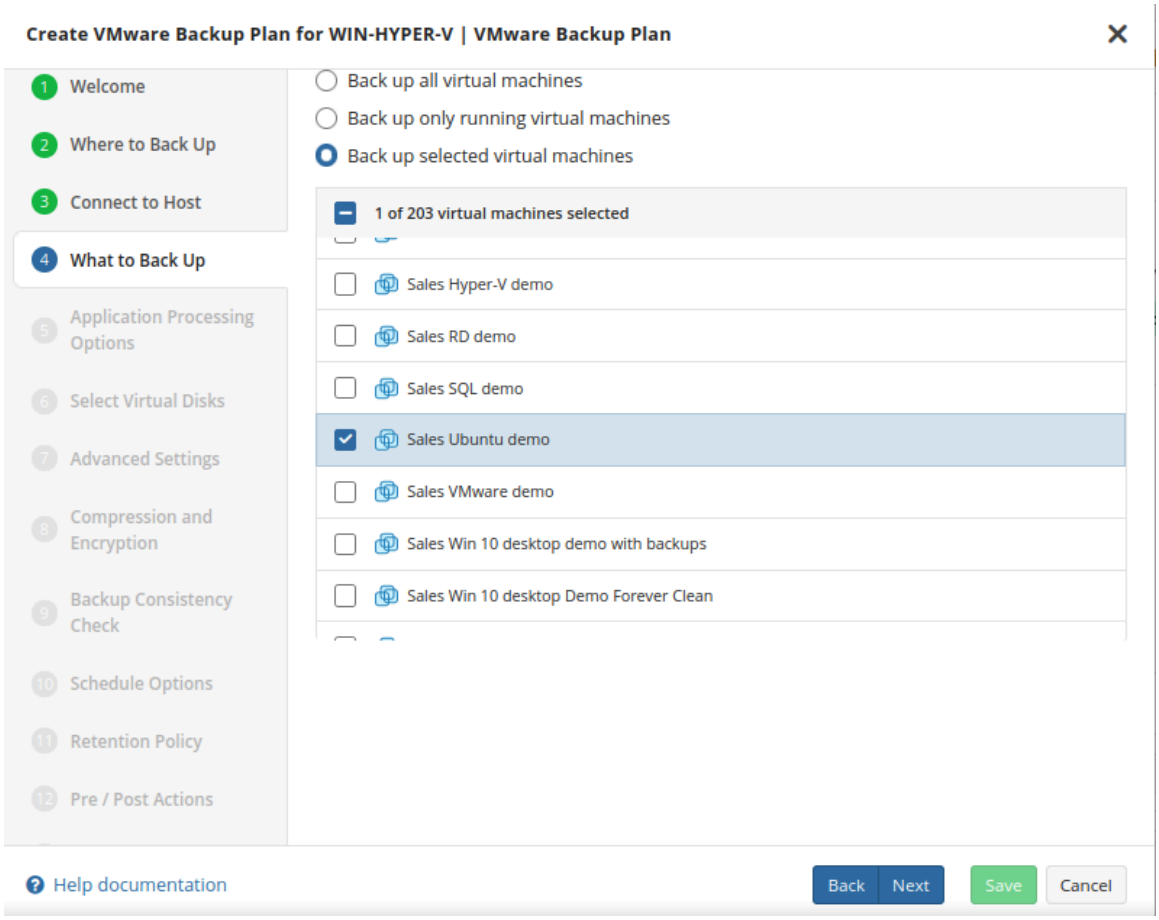


Step 6. Connect to the vCenter or ESXi by using the FQDN or IP address.



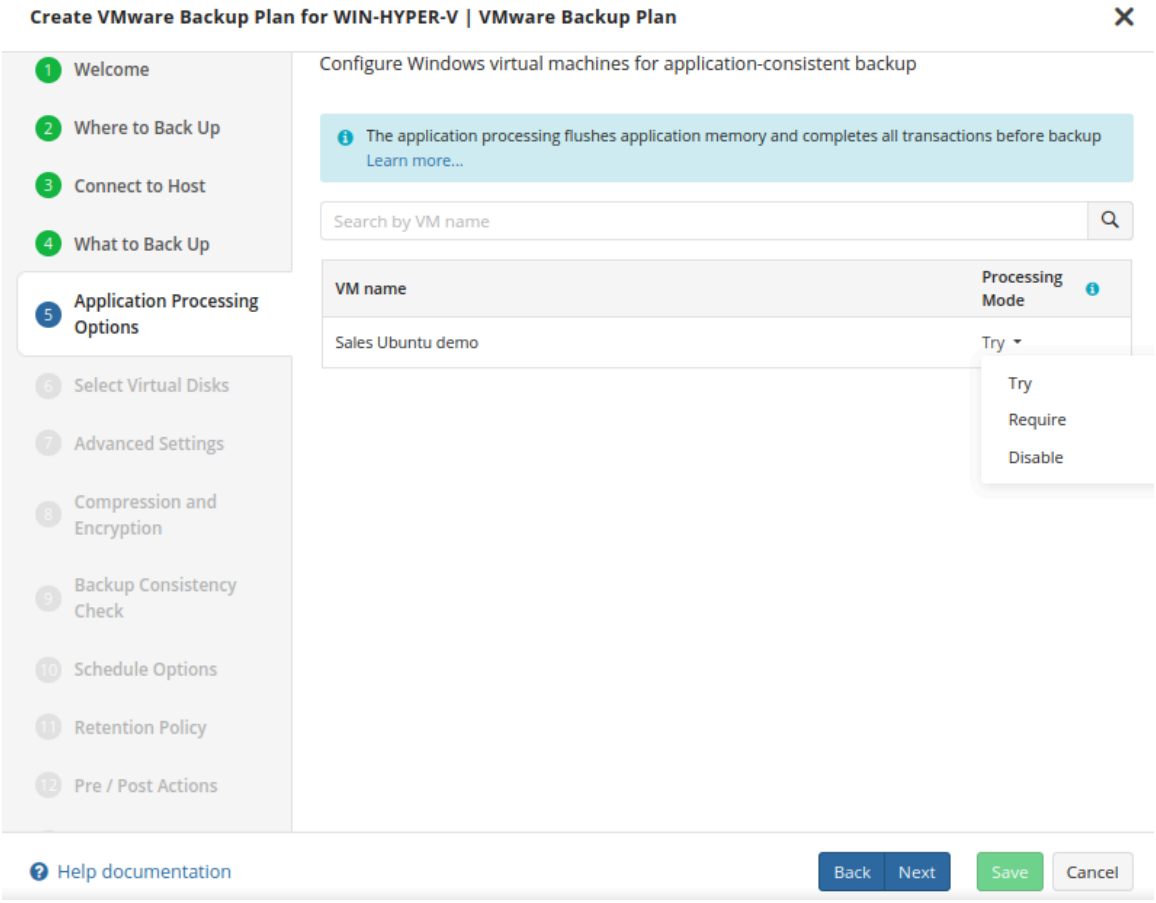
It is important to determine whether FQDN or IP addresses will be used for all future plan configurations. The application will consider each to be unique hosts, even if the target machine is the same.

Step 7. Next, select the Virtual Machines you wish to back up.



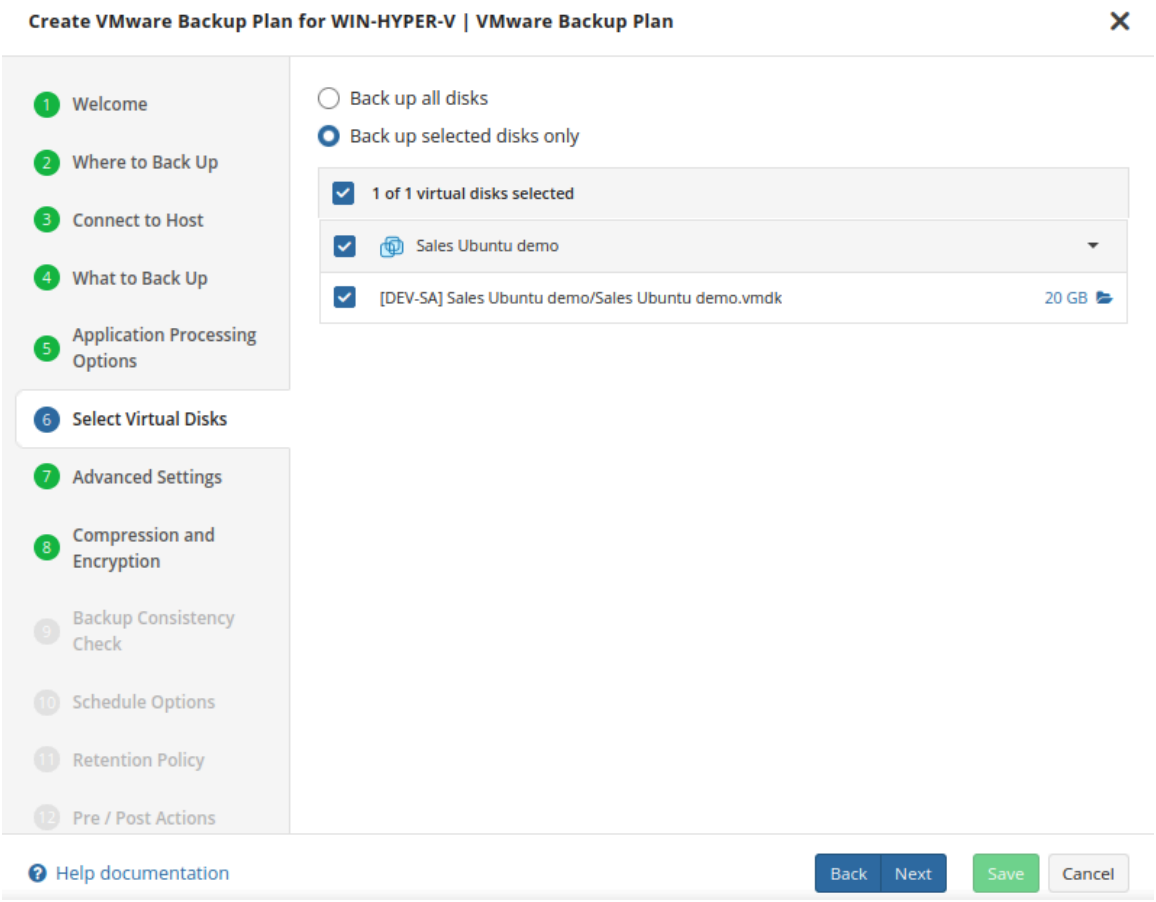
- **Back up all Virtual Machines:** will backup all VMs regardless of current state. This is recommended only for small environments.
- **Back up only running Virtual Machines**: Only backs up VMs currently in "Running" status and is recommended for clustered environments where backup servers planned for failover procedures are not required to be selected.
- **Backup up selected Virtual Machines:** Select which VMs to include with this plan. This allows for greater control of mixed status VMs and for larger environments where it is beneficial to split the backup into multiple plans.

Step 8. Next, you are able to configure the Application Processing options.

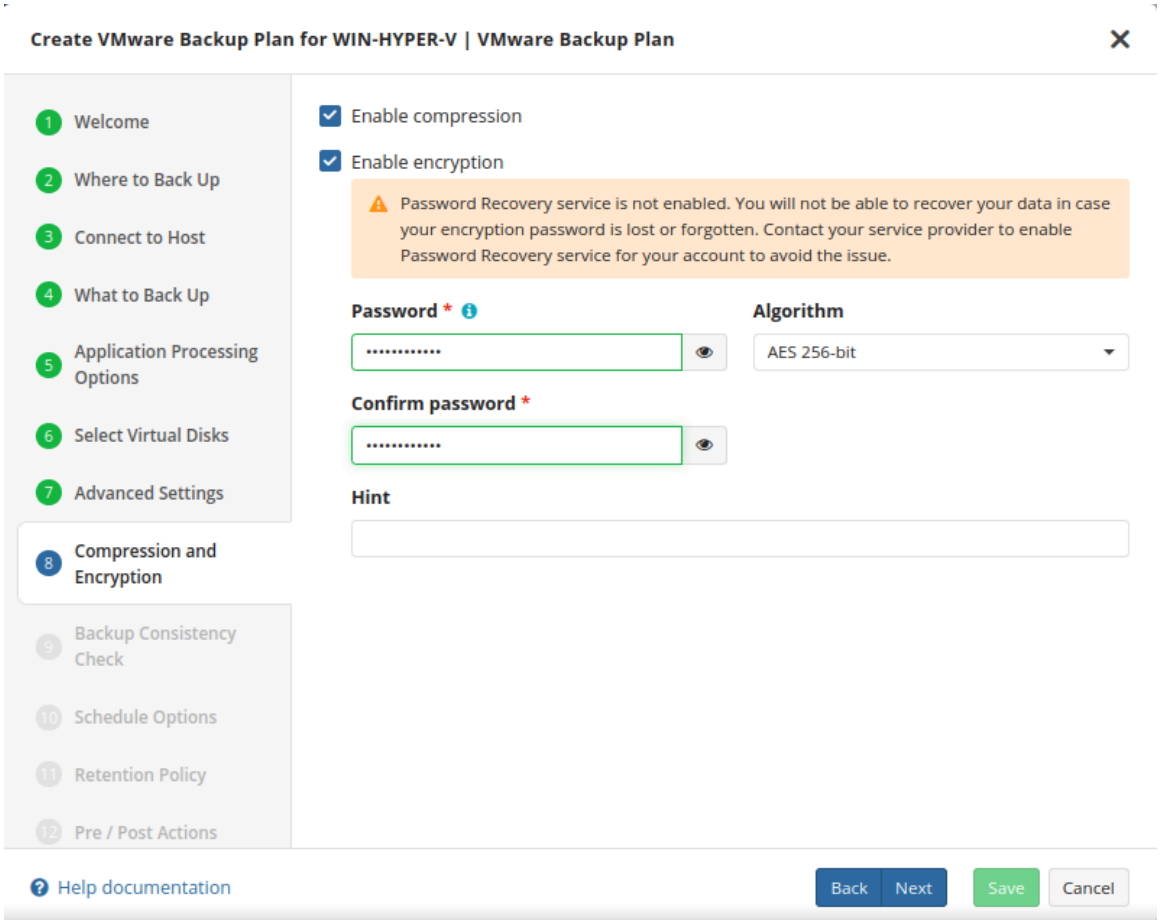


- **Try application processing**. Backup will perform whether or not the application-concistent process fails. If the processing fails, the backup will be done “as is”, but data consistency is not guaranteed.
- **Require successful application processing**. Skip virtual the machine if processing fails. If processing is successful, it ensures that applications running in the VM, such as databases, are taken into consideration and the backup will ensure data consistency is maintained.
- **Disable application processing**. Backup virtual machine “as is” and does not perform any application processing. The VM is backed up in its current state, which may cause data inconsistencies.

Step 9. Next you are prompted to select which virtual disks should be backed up in each VM.



Step 10. After configuring the parameters for what and how to perform the backup, you are able to set the encryption and compression options.

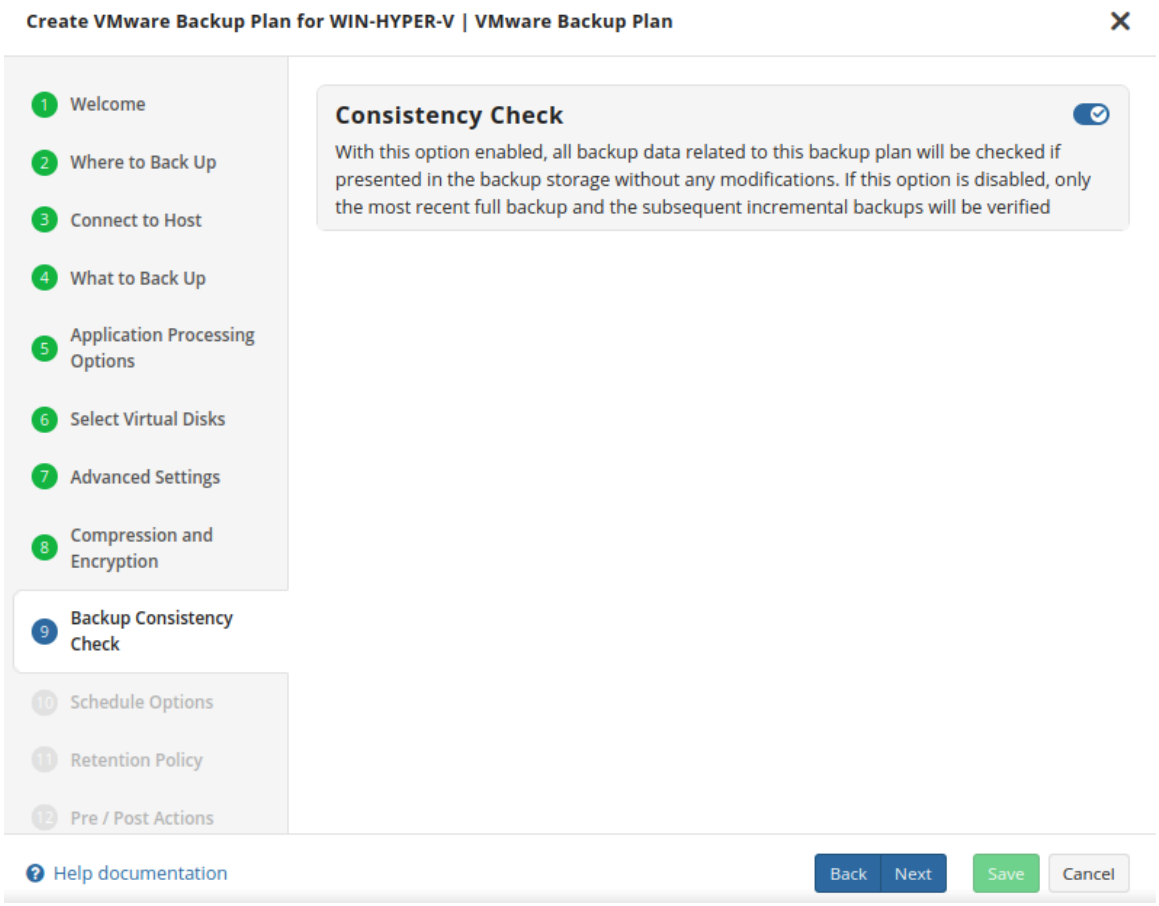


Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

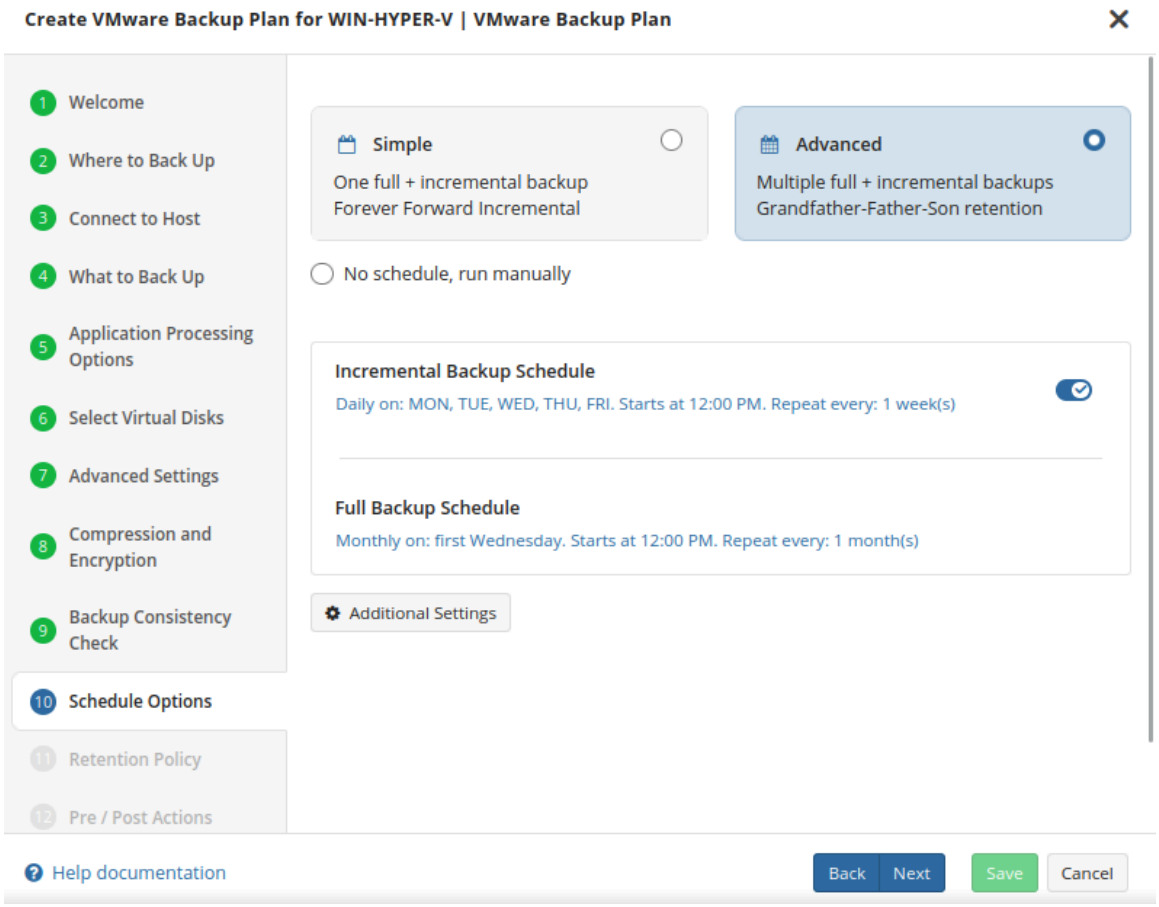
It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place and enable the Password Recovery Service.

Step 11: Select if you're going to use the full consistency check

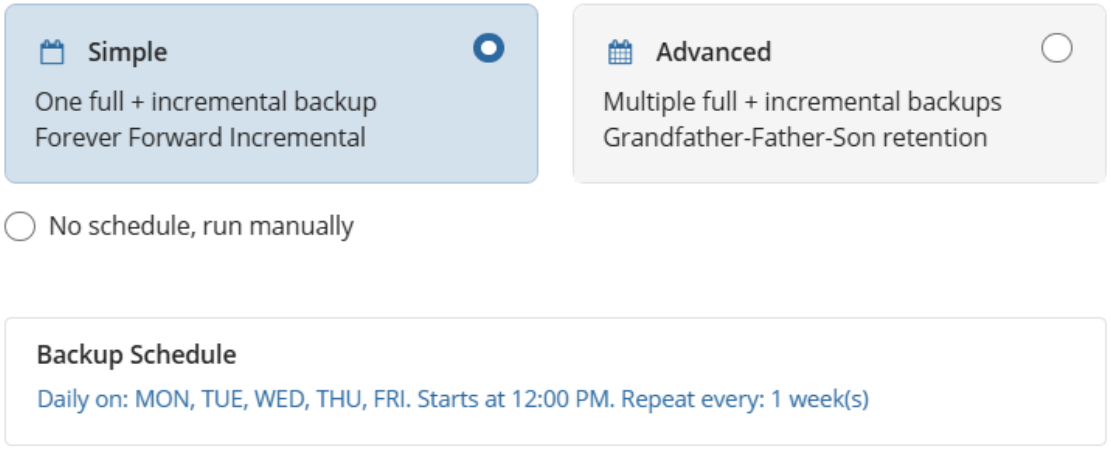


It is recommended that you leave "**Enable Full Consistency Check**" enabled.

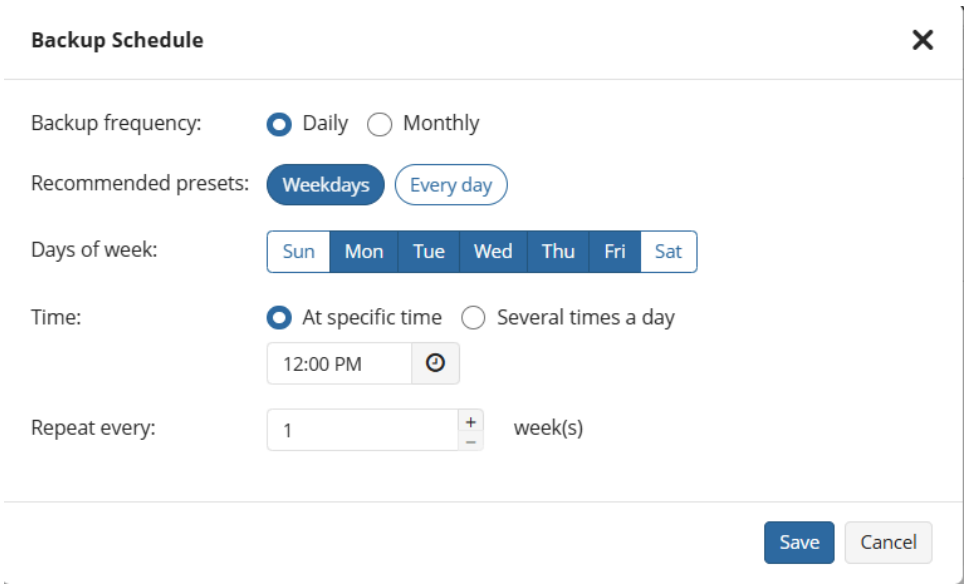
Step 12: The next section allows you to specify the preferred backup Schedule and the additional settings.



- **Simple (Forever forward):** Select the Simple (Forever Forward) option to use the Forever Forward Incremental (FFI). This schedule offers one full backup followed by a limited number of incrementals. Once the limit is exceeded, a new full backup is created using in-cloud copying (synthetic full backup).
  The simple schedule is unavailable if the selected storage account does not support synthetic full backups. To find more information about the supported storage providers and storage classes, please refer to the Forever Forward Incremental article.



You can modify the “Backup Schedule” by clicking on the section as displayed below:

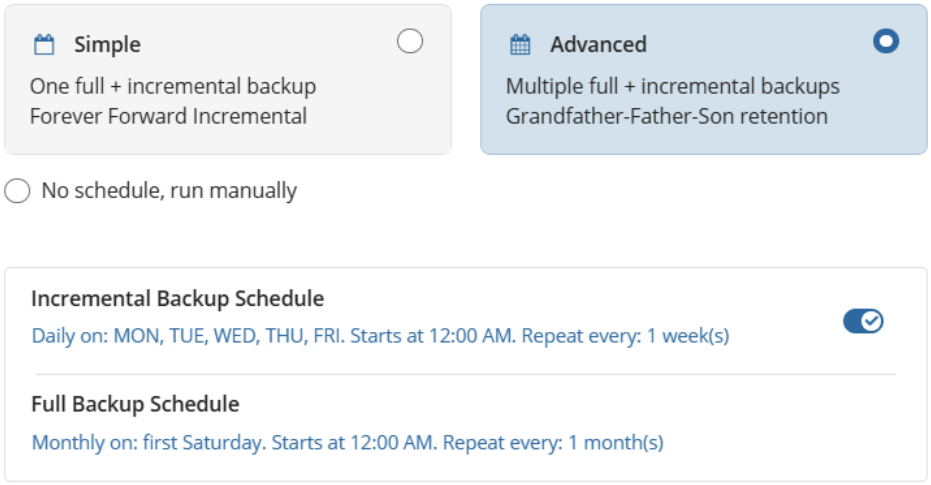


The Simple (Forever forward) schedule is a good option to use for the short-term retention policy such as 30 days (1 months) or 90 days (3 months).

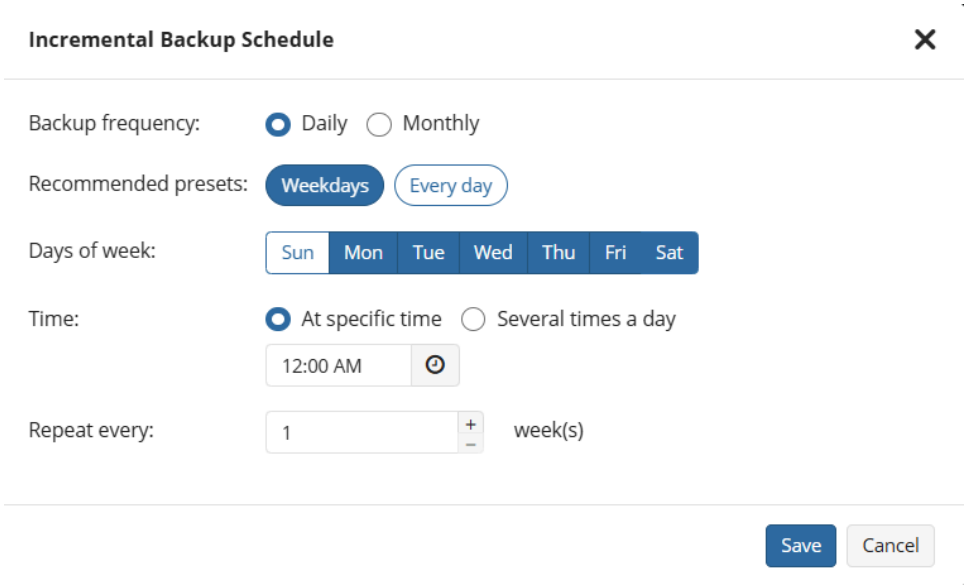
It is not recommended to select the Simple (Forever forward) schedule for long-term storage and archival purposes. If you are planning to retain more than 100 restore points (days), please consider using the Advanced schedule.

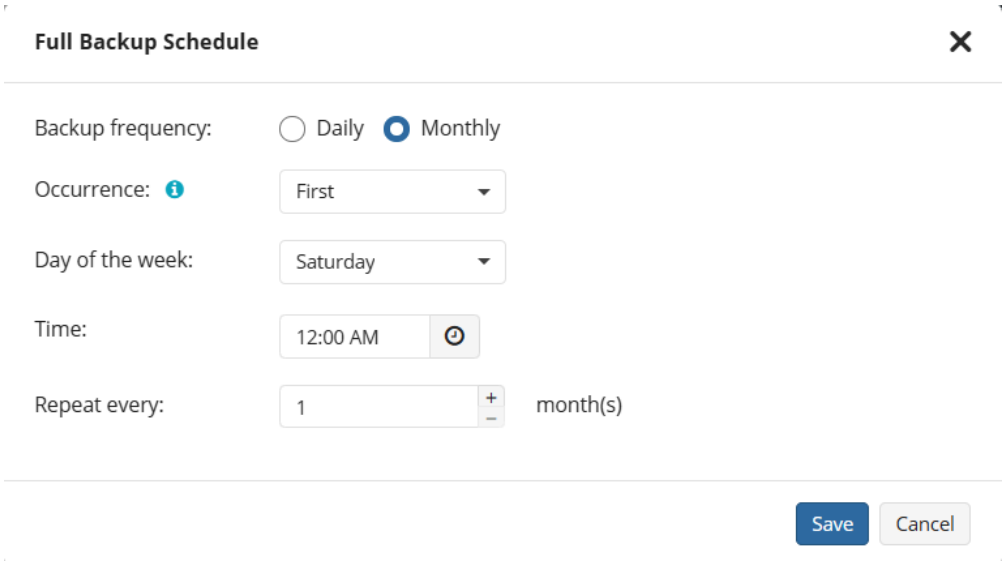
> Synthetic Full Backups allow the system to merge a series of incremental backups together to form a new full backup, greatly reducing the time and bandwidth needed to perform full backups after the initial full. If the storage destination does not support Synthetic full, then a traditional full will be made instead.

- **Advanced (GFS, Object Lock):** Select the Advanced option to set up a flexible, recurring schedule with generations. Every generation contains one full backup followed by incrementals.



The “Advanced” option allows you to configure different schedules for your Incremental and Full backups:



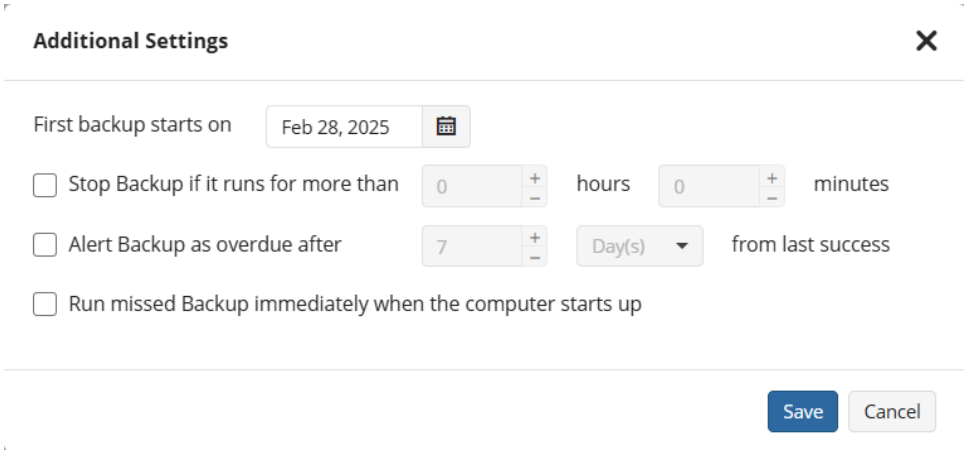


It is recommended to use the Advanced (GFS, Object Lock) option and regularly scheduled full backups for long-term storage (longer than 6 months), archival, and legal purposes.

The most common setup for the Advanced Schedule is daily Incremental backups with either weekly or monthly Full backups.

The retention policy will only perform properly with regular scheduled full backups.

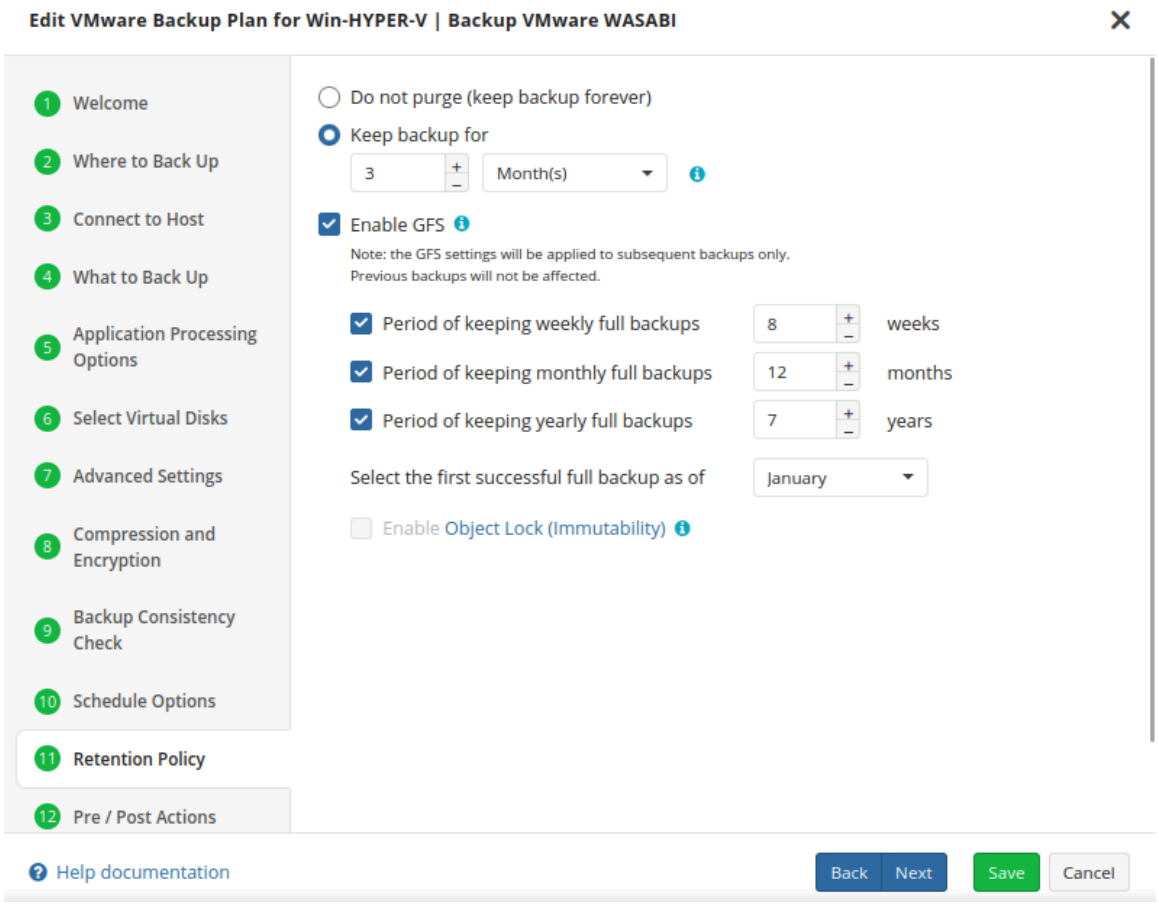
By clicking on the **Additional Settings** button, you can see the options below:



Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

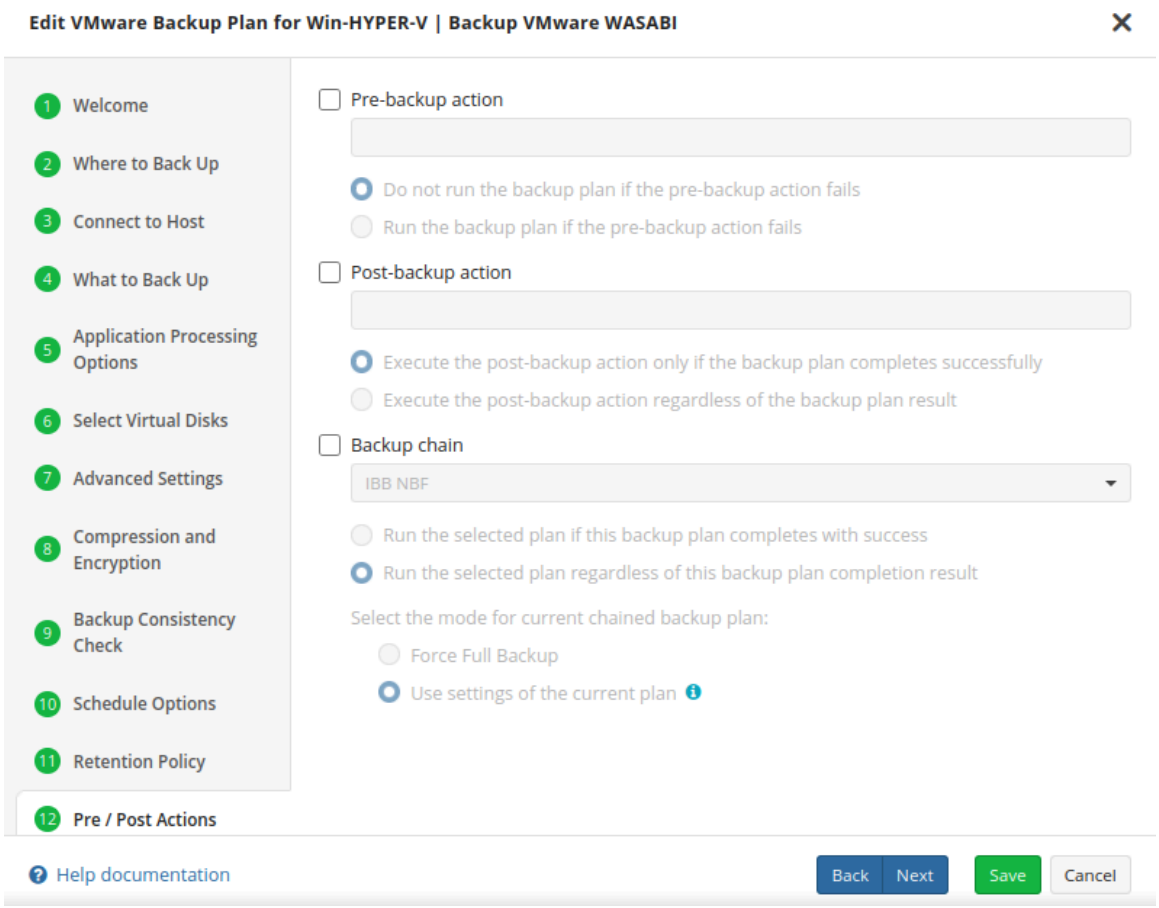
Step 13: On the “Retention Policy" step, you can set the policies the application will use to determine which data to purge at regular intervals.



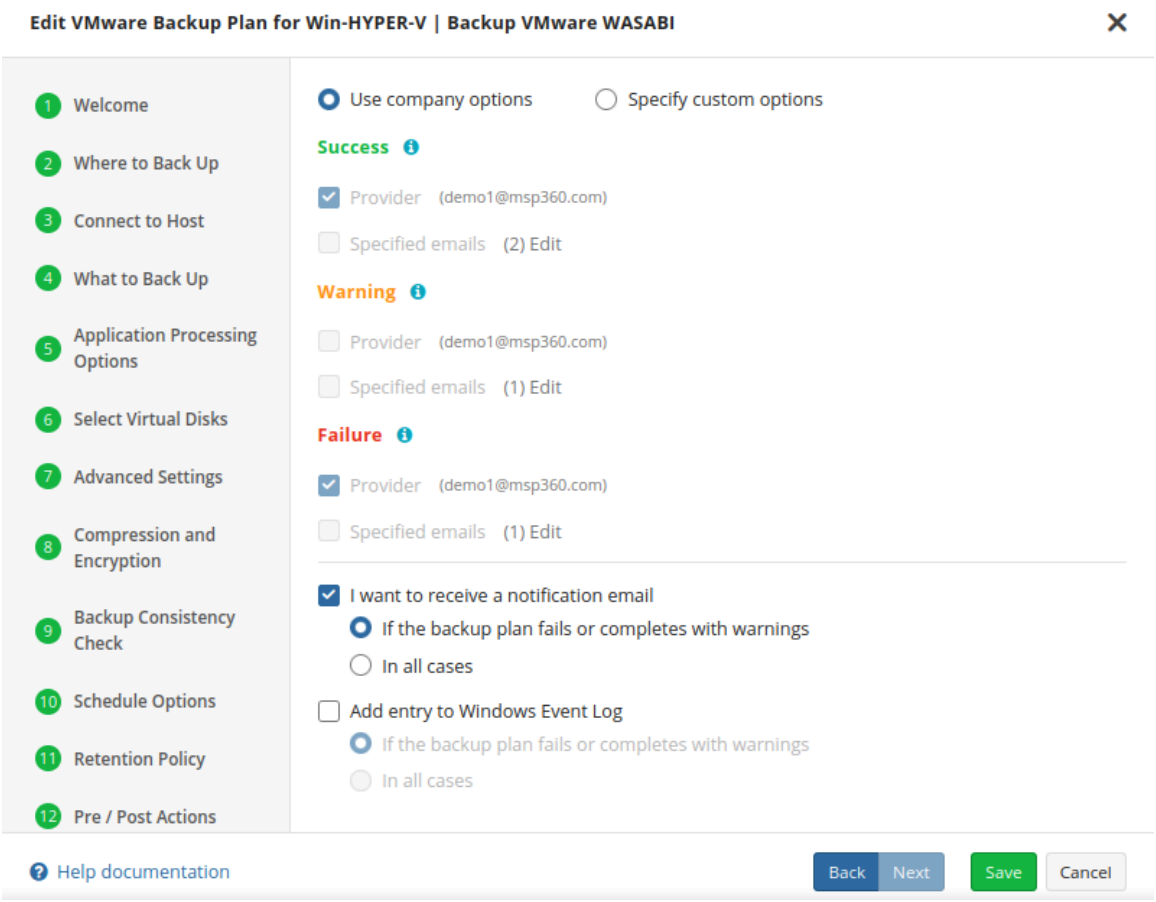
- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.
- **Enable GFS**: Select this option if you want to keep Full Backups for archival purposes at the selected intervals.
- **Period of keeping weekly full backups**: Set the number of Weekly Full Backups to retain. This is determined separately from the “Keep backup for” value and relies on Full Backups to be scheduled on at least a weekly basis in the previous step.
- **Period of keeping monthly full backups:** Number of Monthly Full Backups to retain. A Full Backup can be flagged as both a Weekly and Monthly backup, but once the number of Weekly Full Backups has exceeded their retention setting, only those also flagged as a Monthly will be retained.

- **Period of keeping yearly full backups:** Set the number of Yearly Full Backups to retain. A Full Backup can be flagged as a Weekly, Monthly, and Yearly Backup. Once the number of Monthly Full Backups has exceeded their retention setting, only those also flagged as a Yearly will be retained.
    - **Select the first successful full backup as of**: Select the first Monthly Full Backup you would like to flag and retain as the first Yearly Full Backup.
- **Enable Object Lock (Immutability):** Activates immutability, preventing modifications or deletions of backups. It is applied to GFS Full Backups and remains in effect until the defined retention policy expires

Step 14: After the retention policy is set. Next you are prompted to set pre and post actions



Step 15. After pre-post actions, you can configure the notifications for this backup plan.

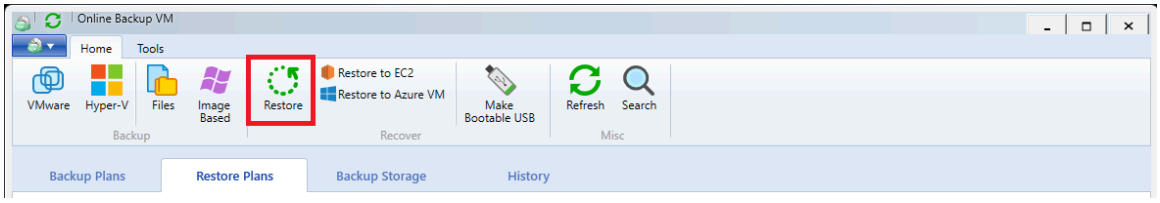


Step 16. Once you are satisfied with the plan configuration, click on “Save” to finish.

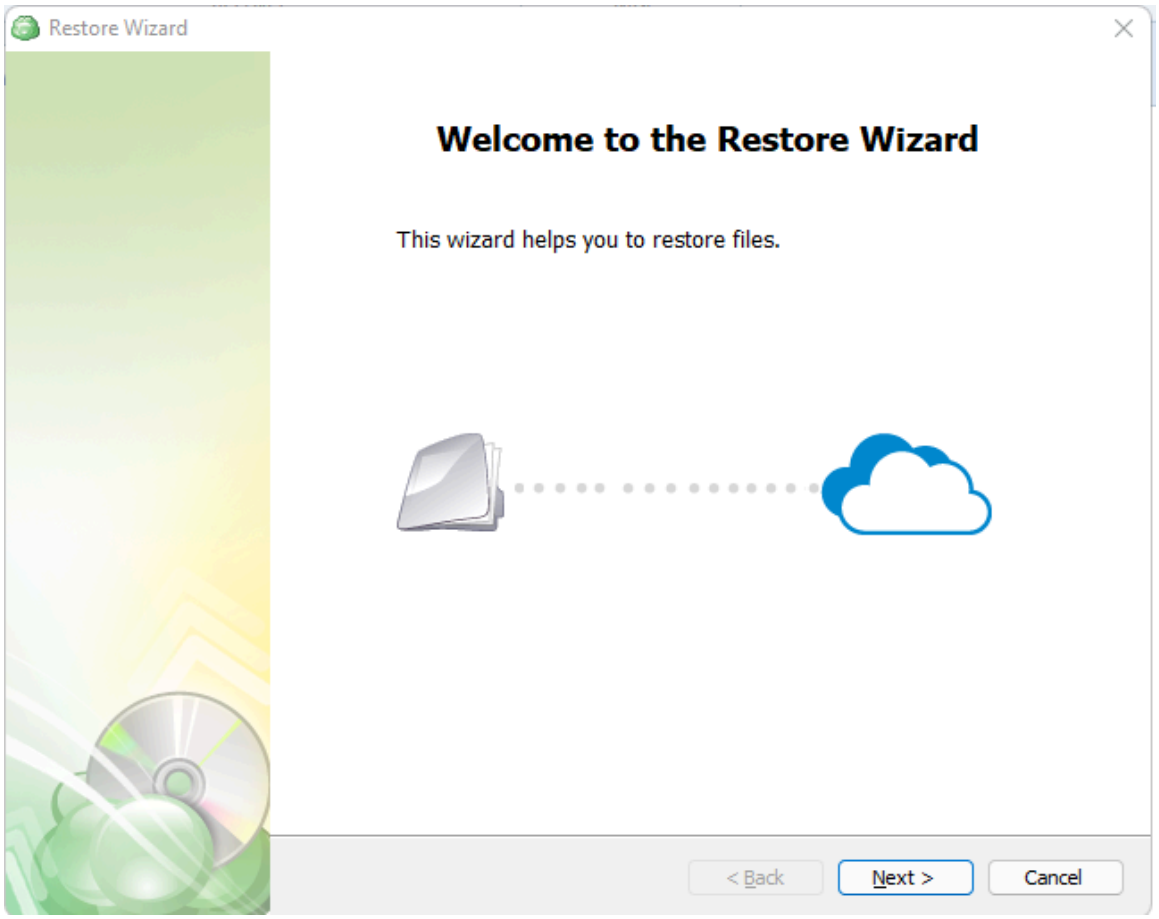
VMWare Restore Plans

Restore as a VM using the Agent

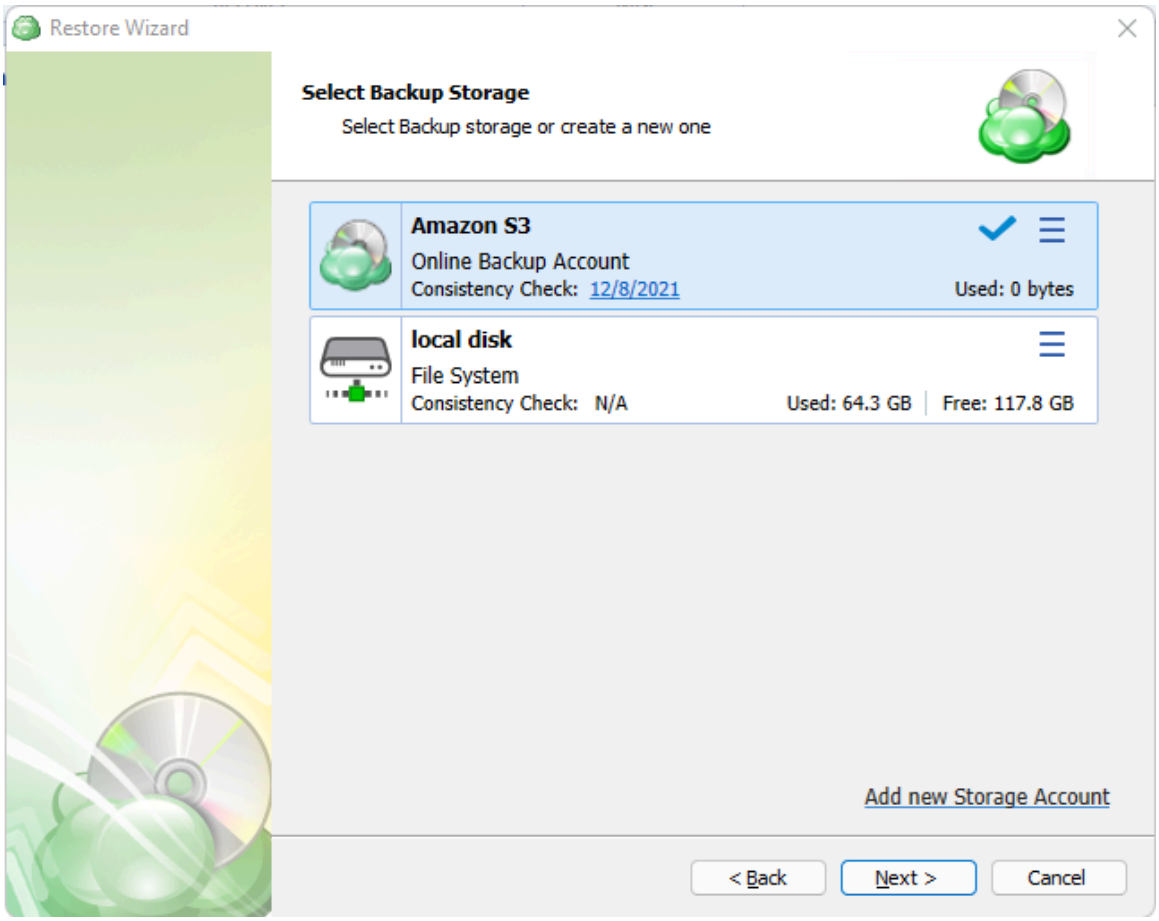
Step 1. Within the Online Backup Agent, click on “Restore”



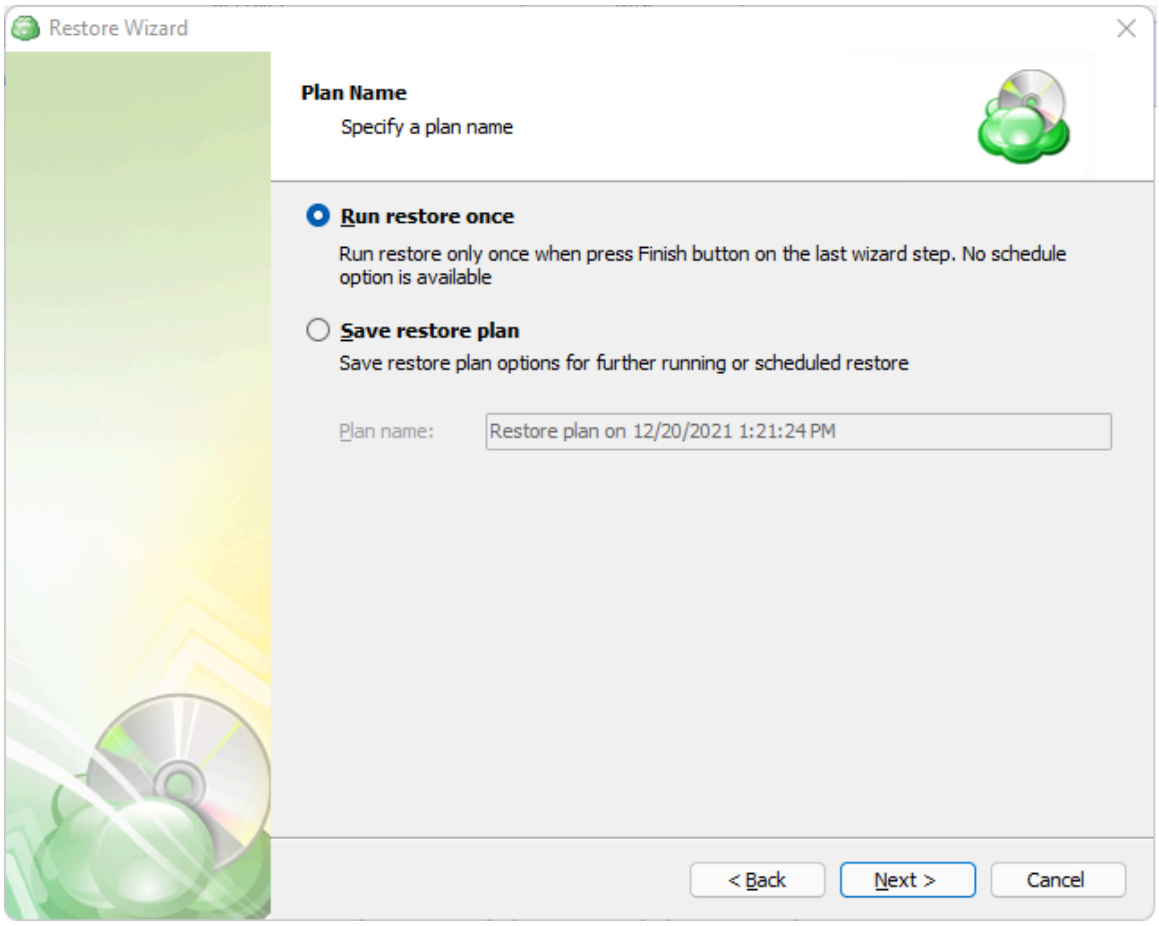
Step 2. Once the wizard starts, click on Next to advance to the next step.



Step 3. The next step will prompt you to select the source for the restore point.



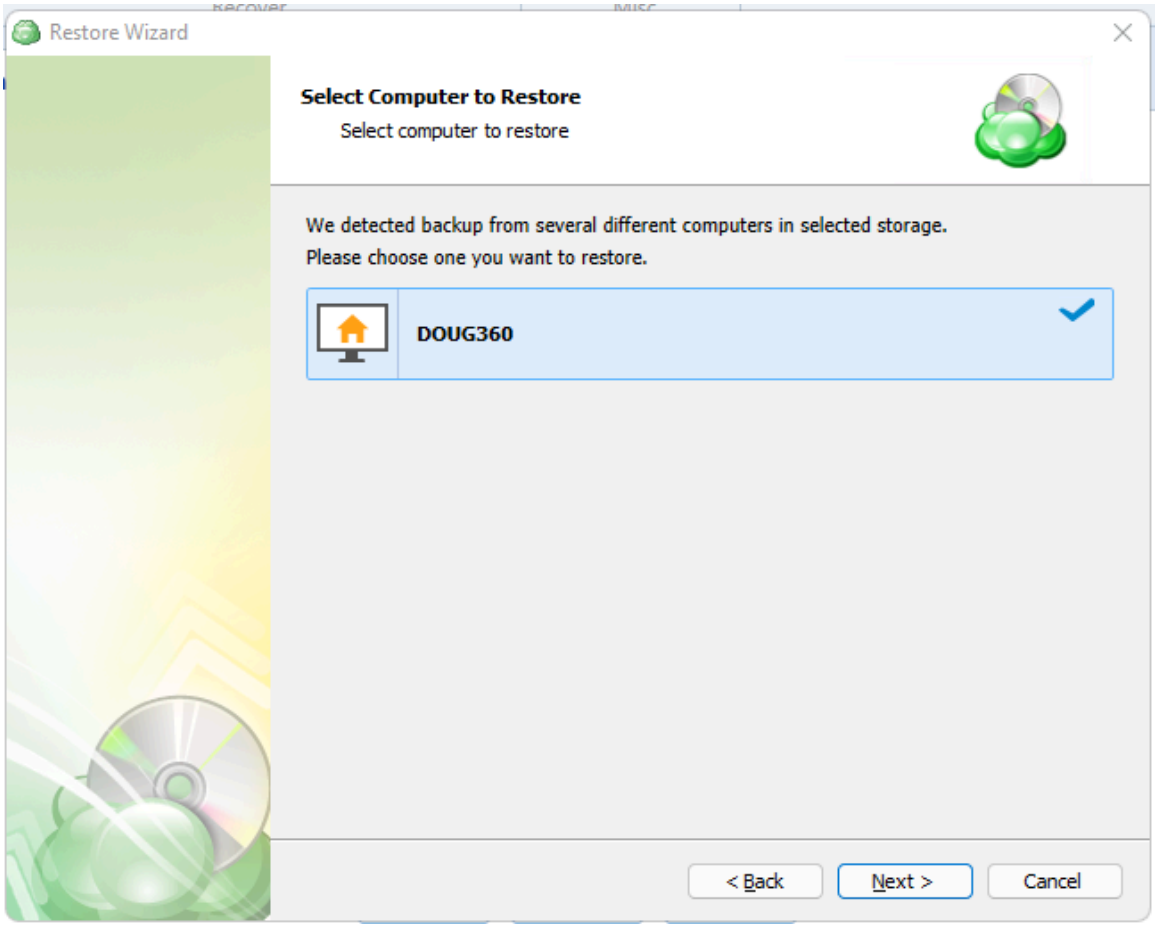
Step 4. Next, you will be given the option to either run the restore once or to save it to run later.



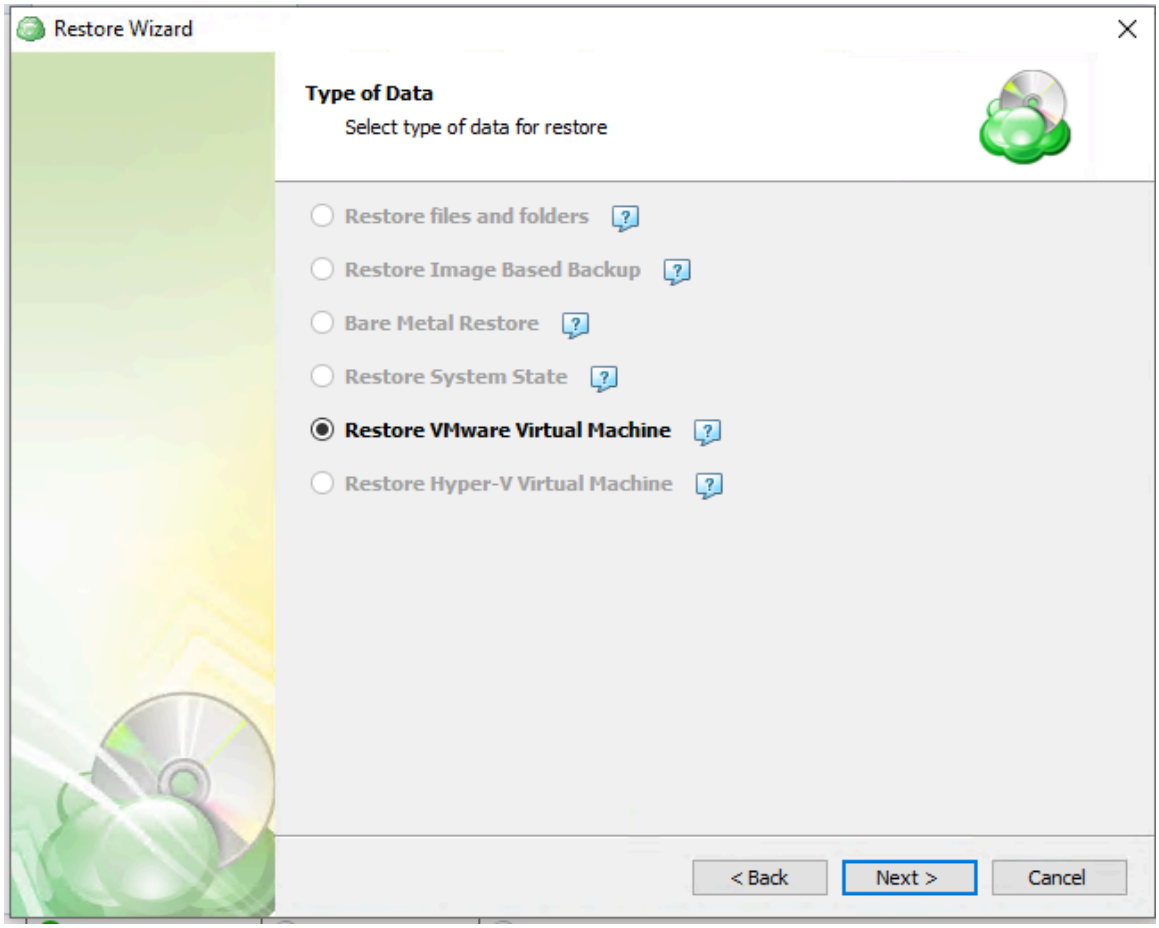
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

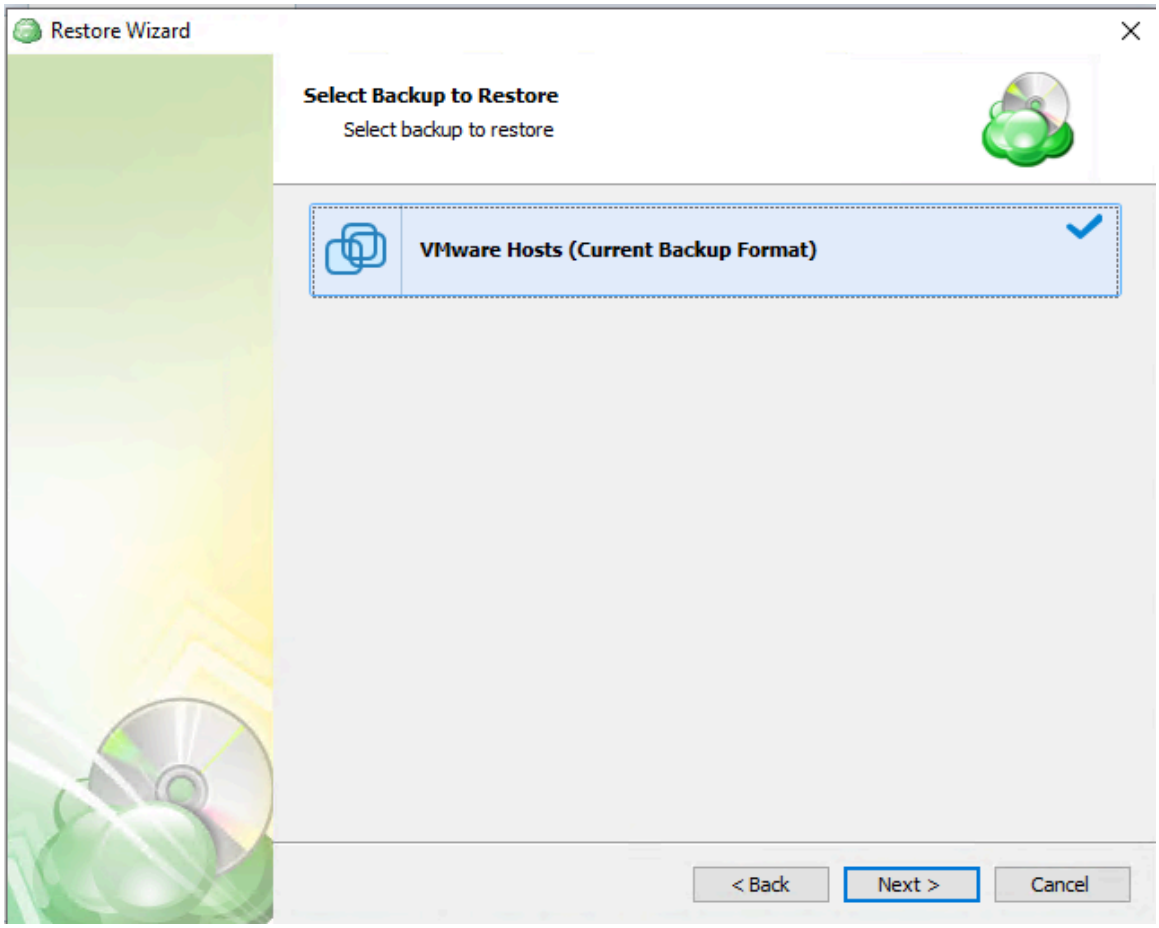
Step 5. With the type of restore selected, the next step is to select the correct Host server which the VM resides on.



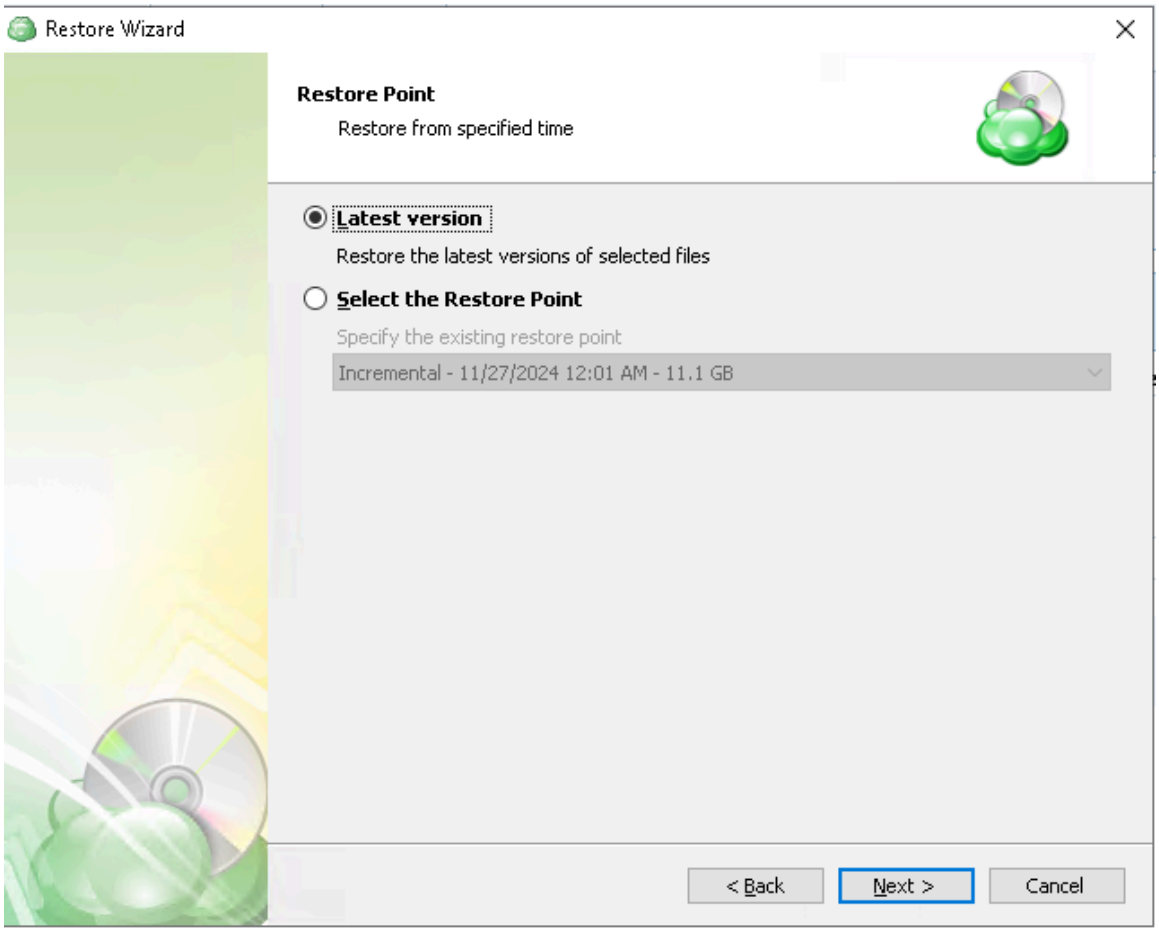
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore VMware Virtual Machine” option to continue.



Step 7. With the correct type of data selected, the application will generate a list of available VM backup plans.

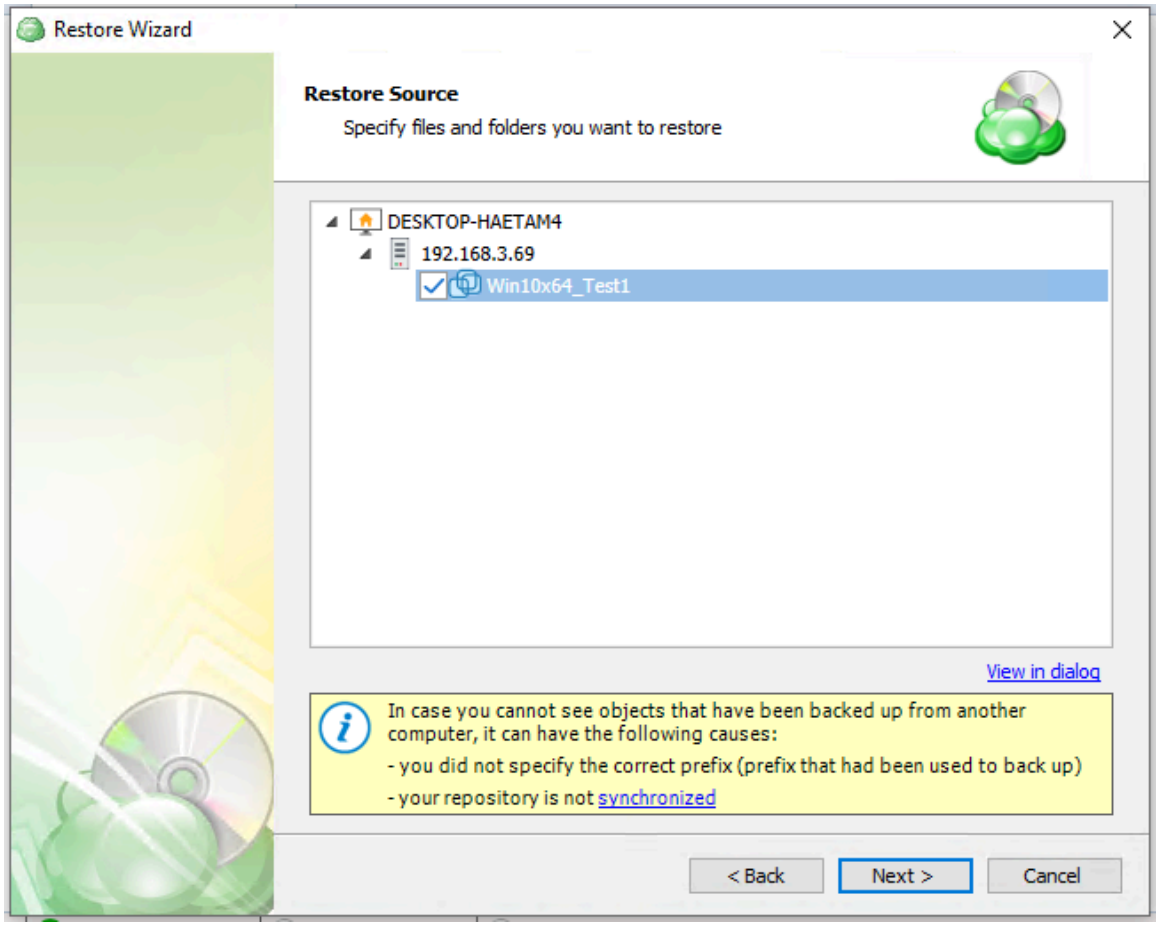


Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.

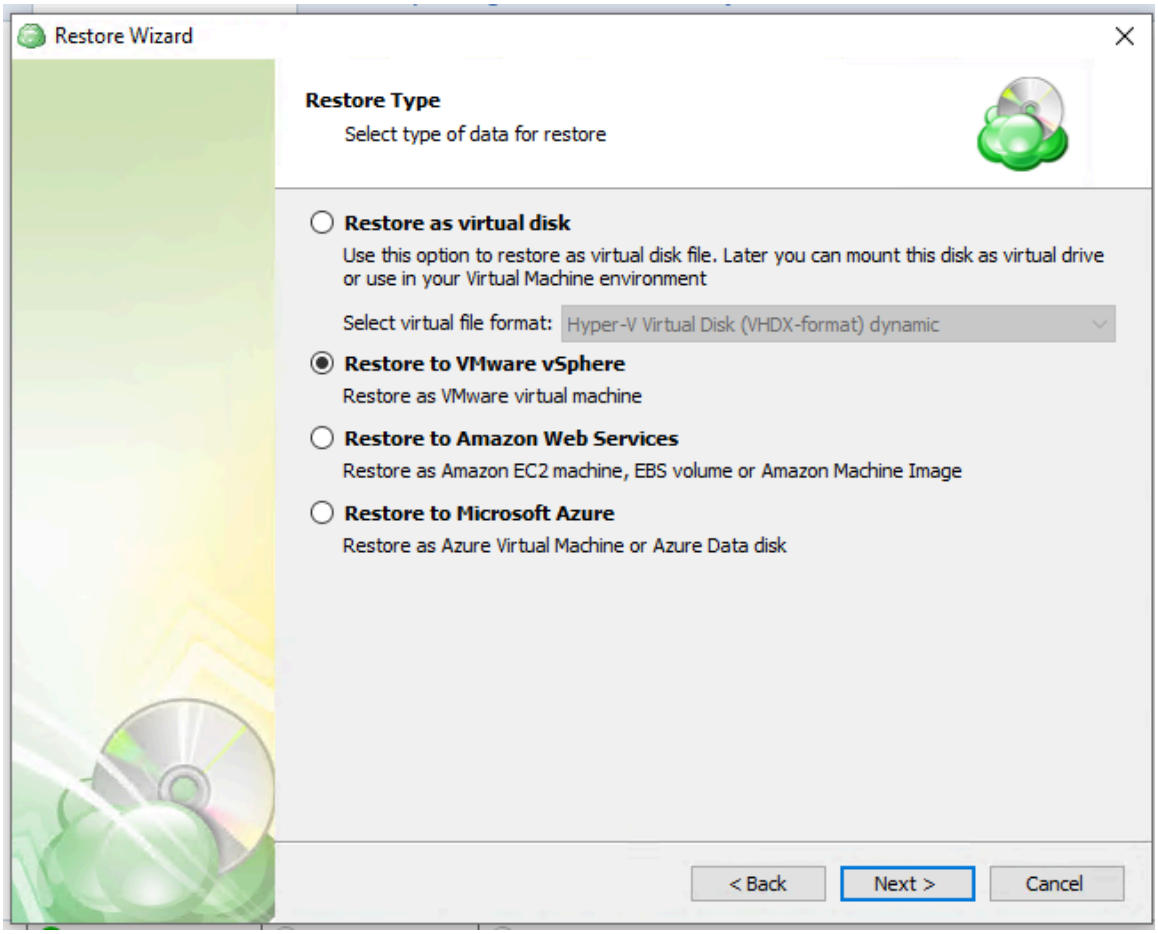


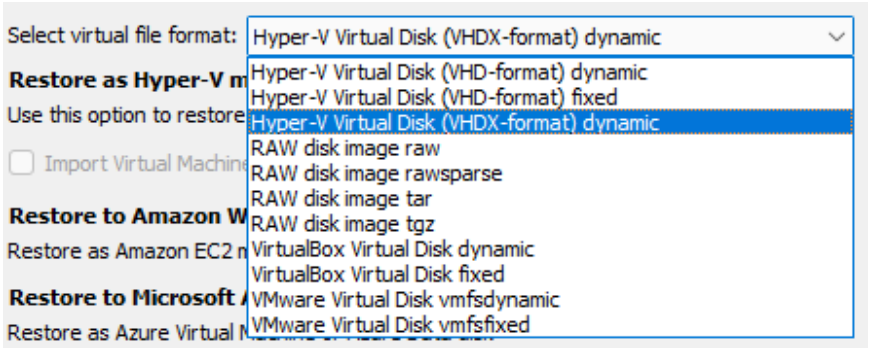
If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which to restore.



Step 10. The next step of the wizard allows you to choose how the VM data should be restored.

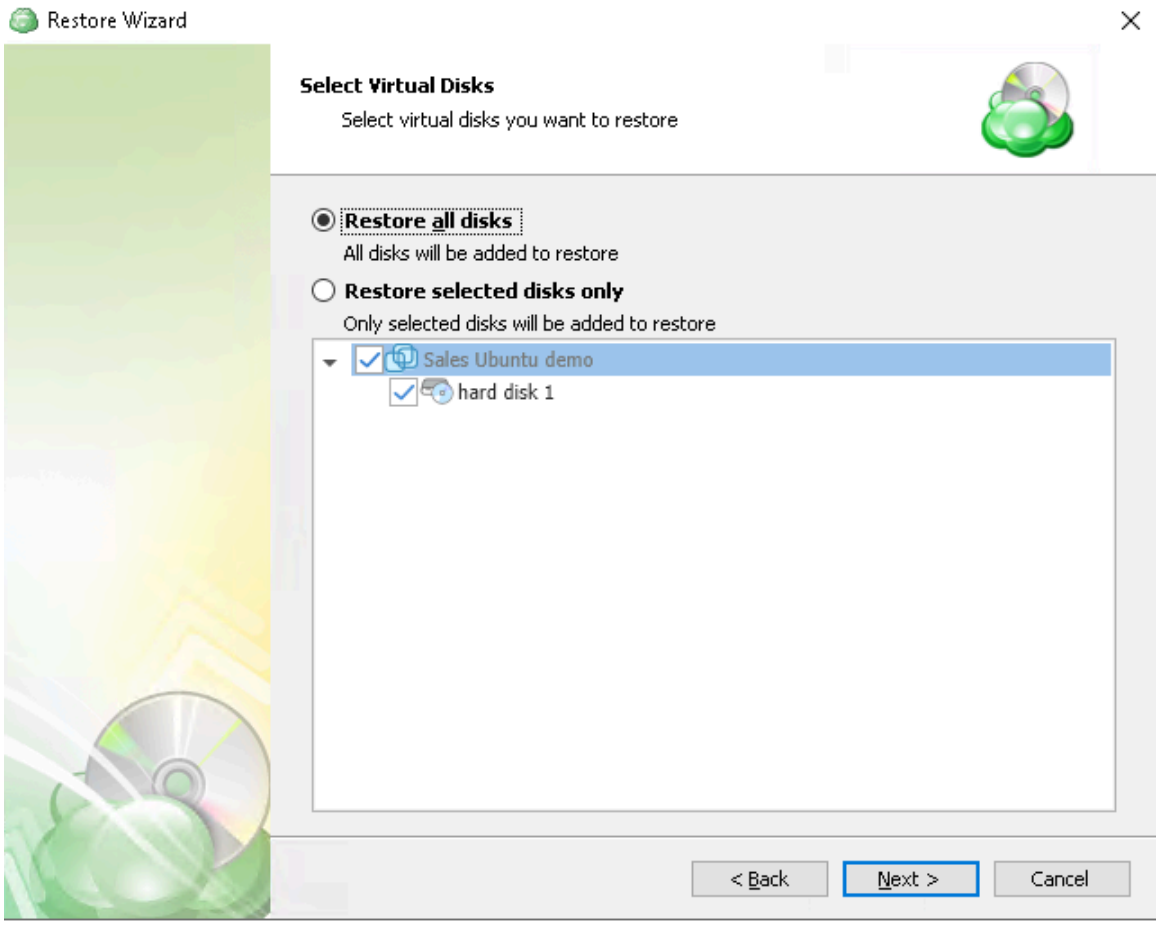


- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:
  - 

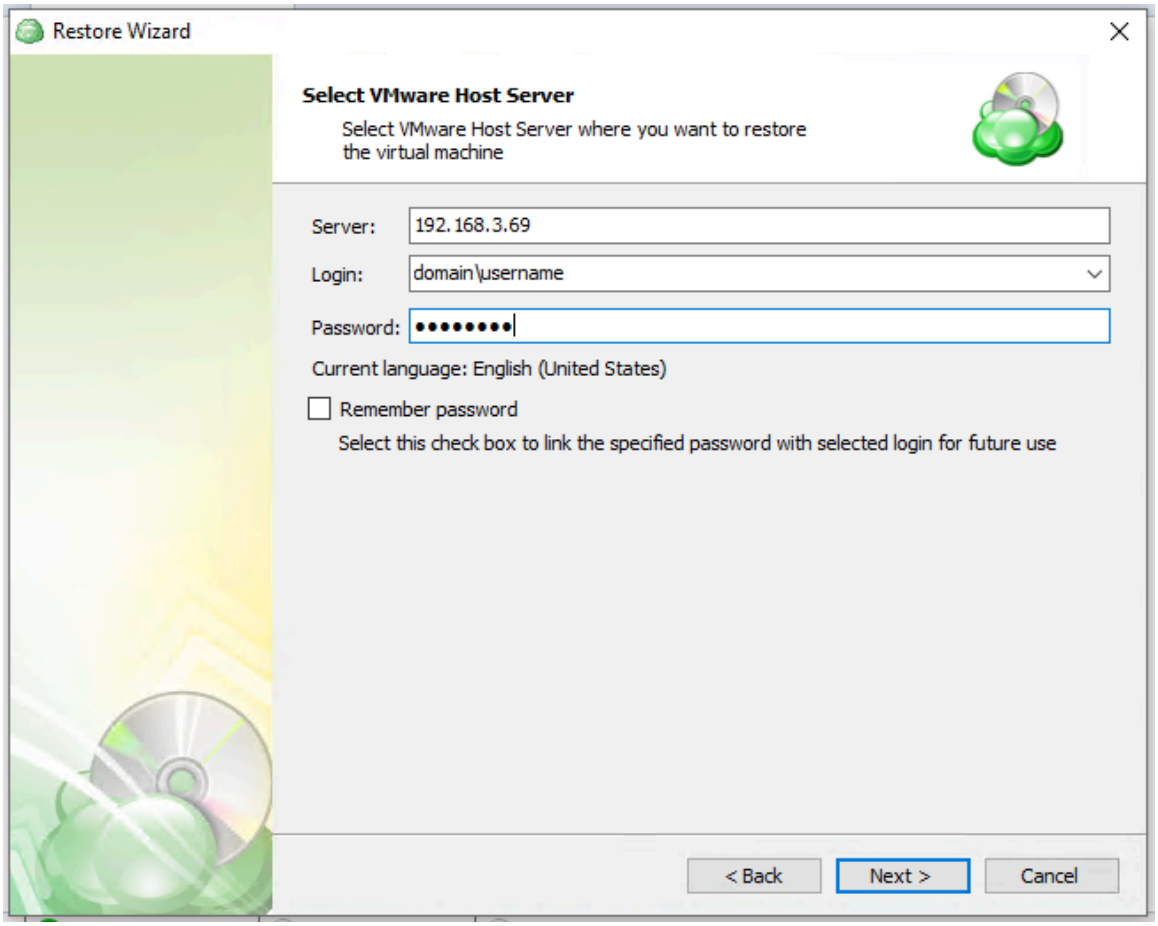
- **Restore to VMware VSphere:** Selecting this option restores the virtual machine configuration as well as the virtual disks to VSphere as a VM.

- **Restore to Amazon Web Services:** If enabled, this will restore the selected VM directly to AWS Cloud either as an EC2 instance, EBS volume, or AMI.
- **Restore to Microsoft Azure:** This will restore the VM directly to Azure as either an Azure Virtual Machine or Azure Data disk.

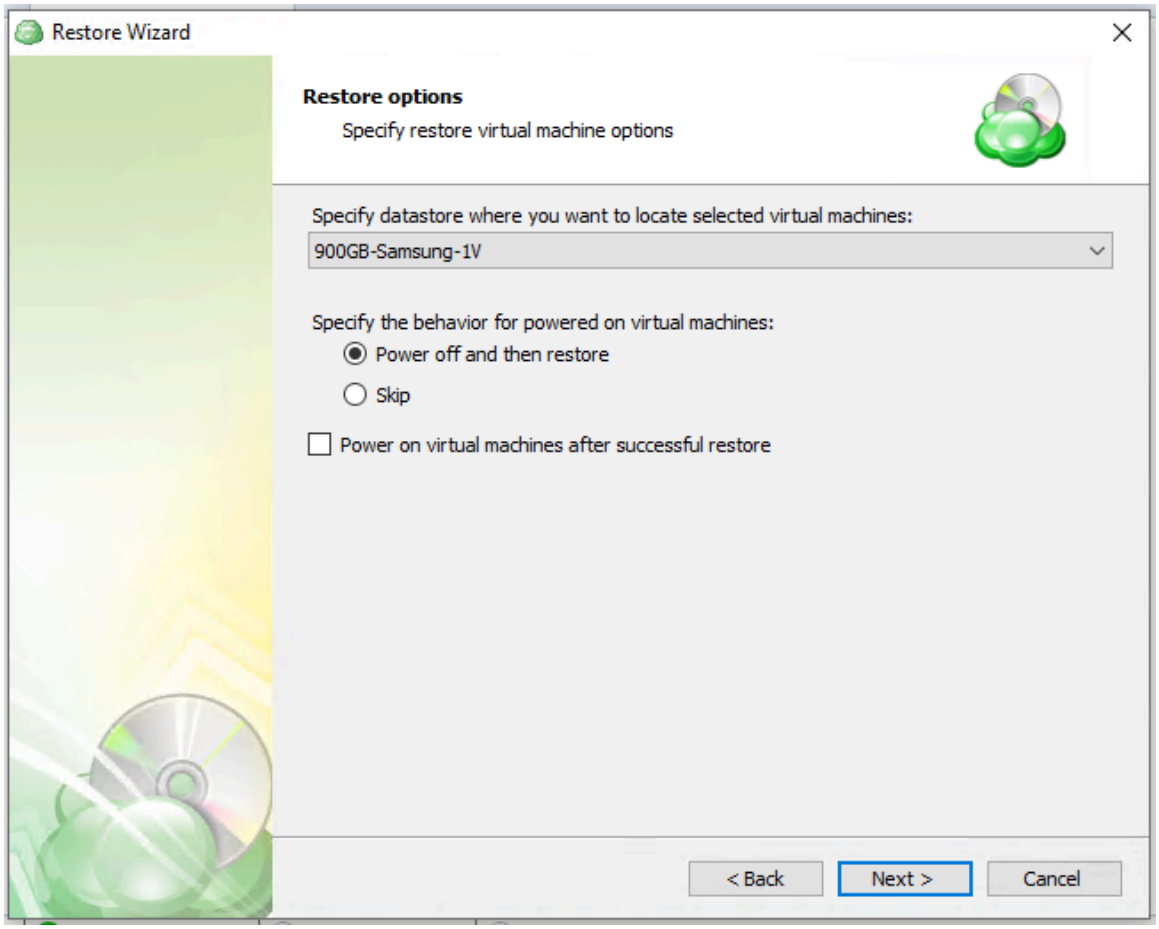
Step 11. The next step is to select the disks to be restored



Step 12. The next step is to choose a destination for the restored VM or virtual disk.

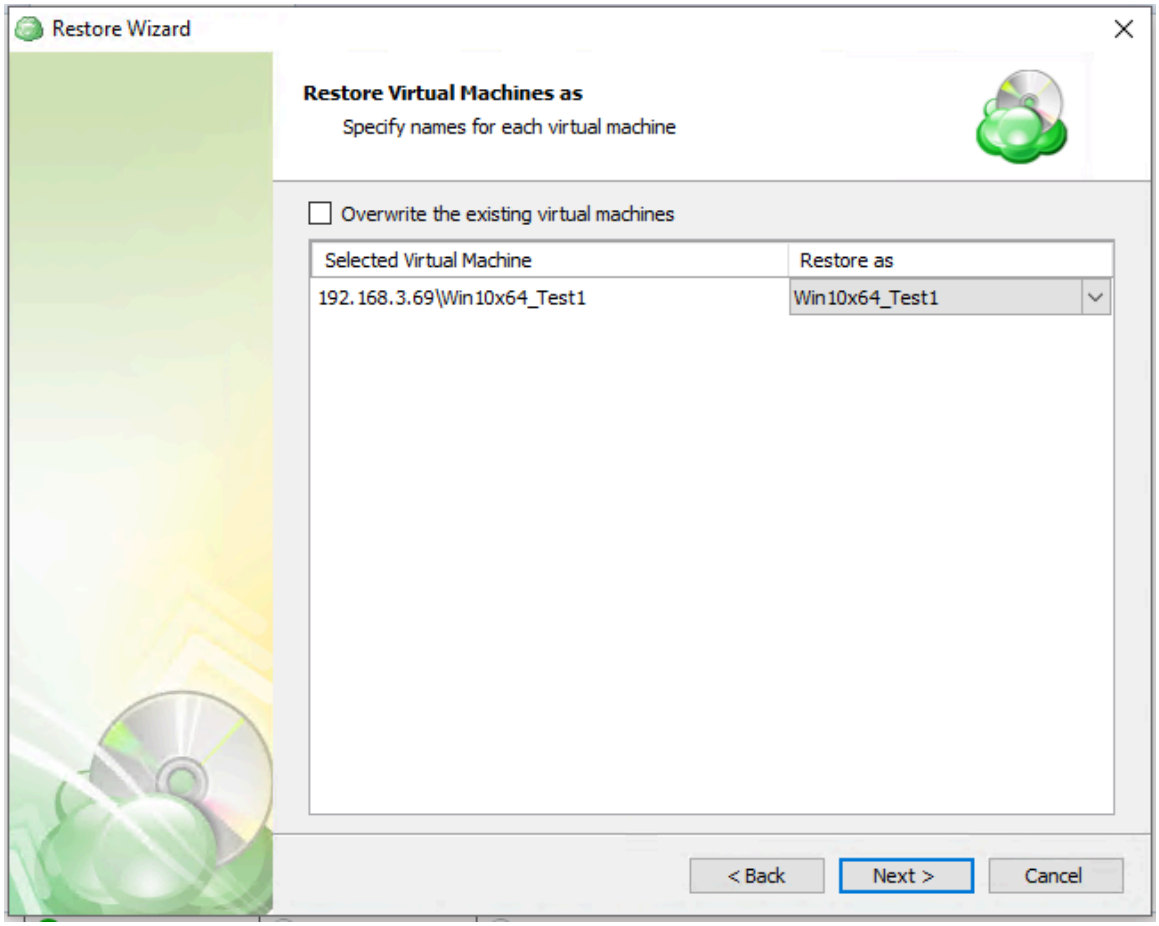


Step 13. Once the destination is selected, you are presented with additional options for importing the restored VM.



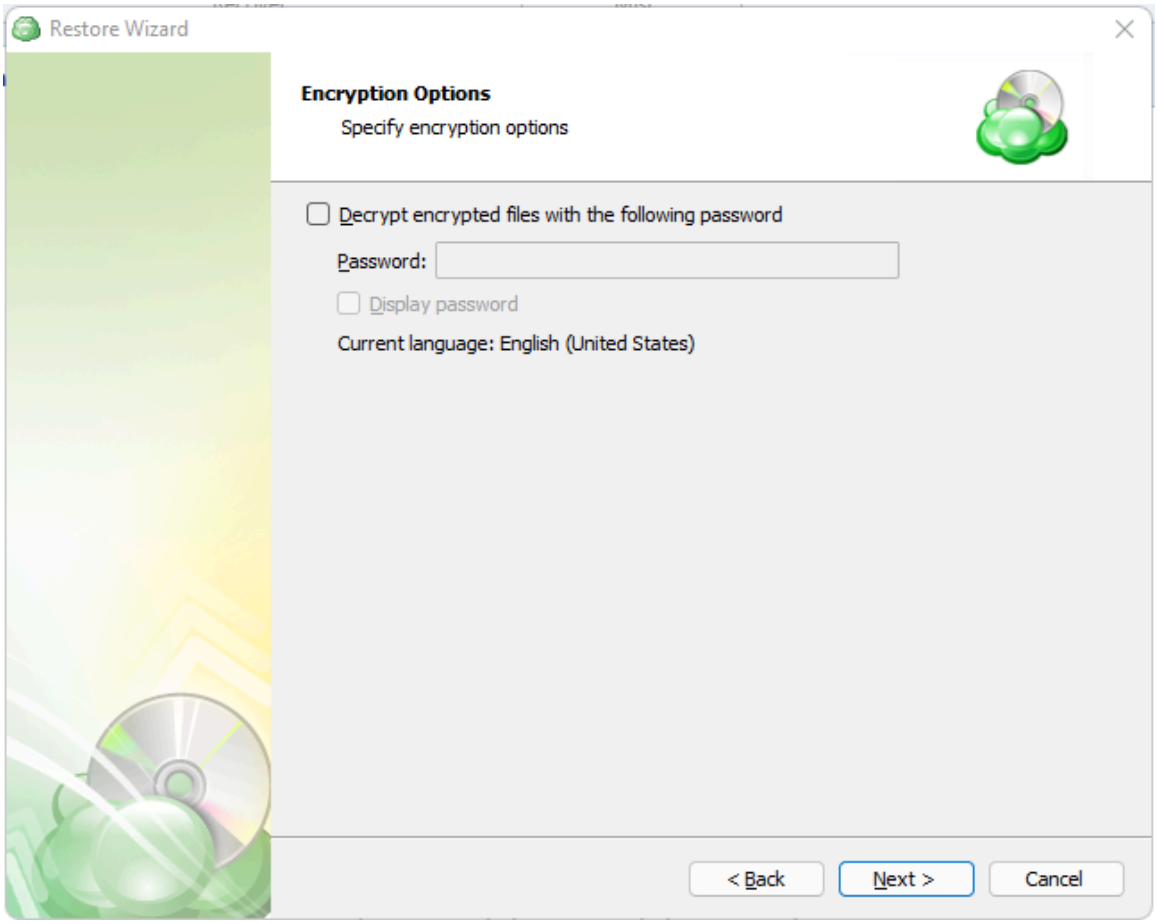
- **Specify datastore…:** Select the destination disk on the VMware host where the VM should be restored to.
- **Specify the behavior…:** Choose the action to take if the target VM being overwritten is currently powered on. If you select “Skip” then any powered on VMs will be ignored during the restore process.

Step 14. Next, you will be prompted to select which VM you would like to overwrite. If you wish to restore it as a different name or target VM, select or type over the value in the “Restore as” list.

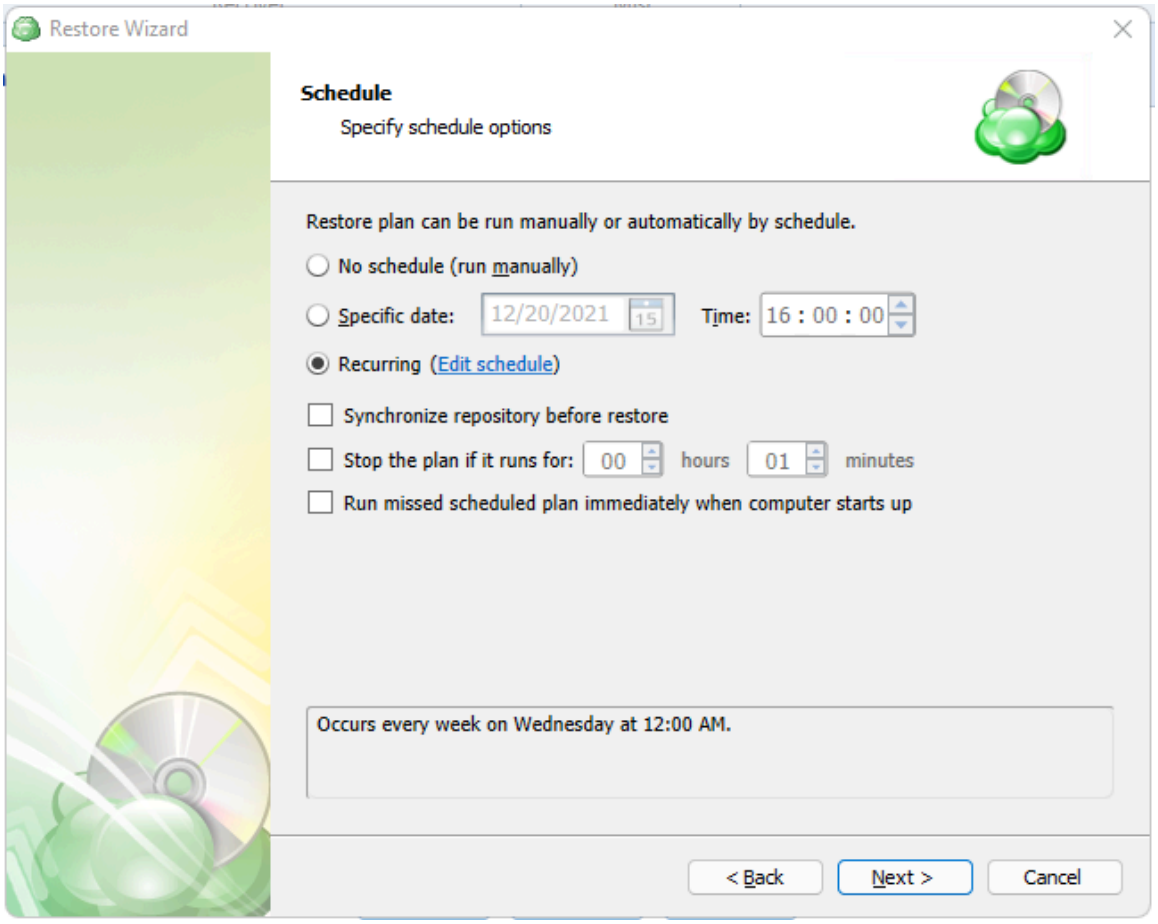


- **Restore As:** Enter a new name in this field to restore the VM with a new or different name.

Step 15. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the VM.



Step 16. With the decryption password entered, the next step is setting the schedule for the restore plan.

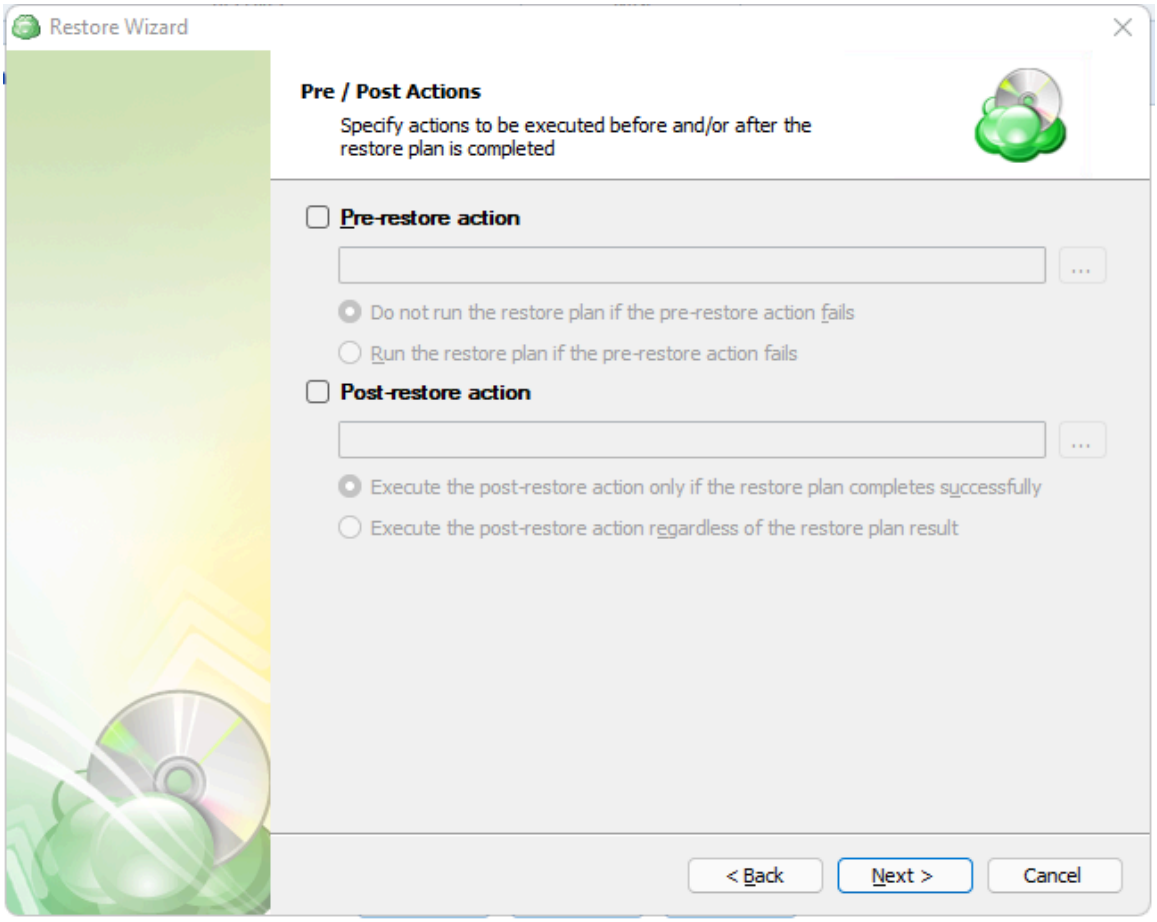


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.
- **Synchronize repository before restore**: Ensures the latest backup data is available before restoring.
- **Stop the plan if it runs for X time**: Automatically stops the restore if it exceeds the specified duration.
- **Run missed scheduled plan immediately when computer starts up**: If the restore was missed due to the system being off, it runs as soon as the computer starts..

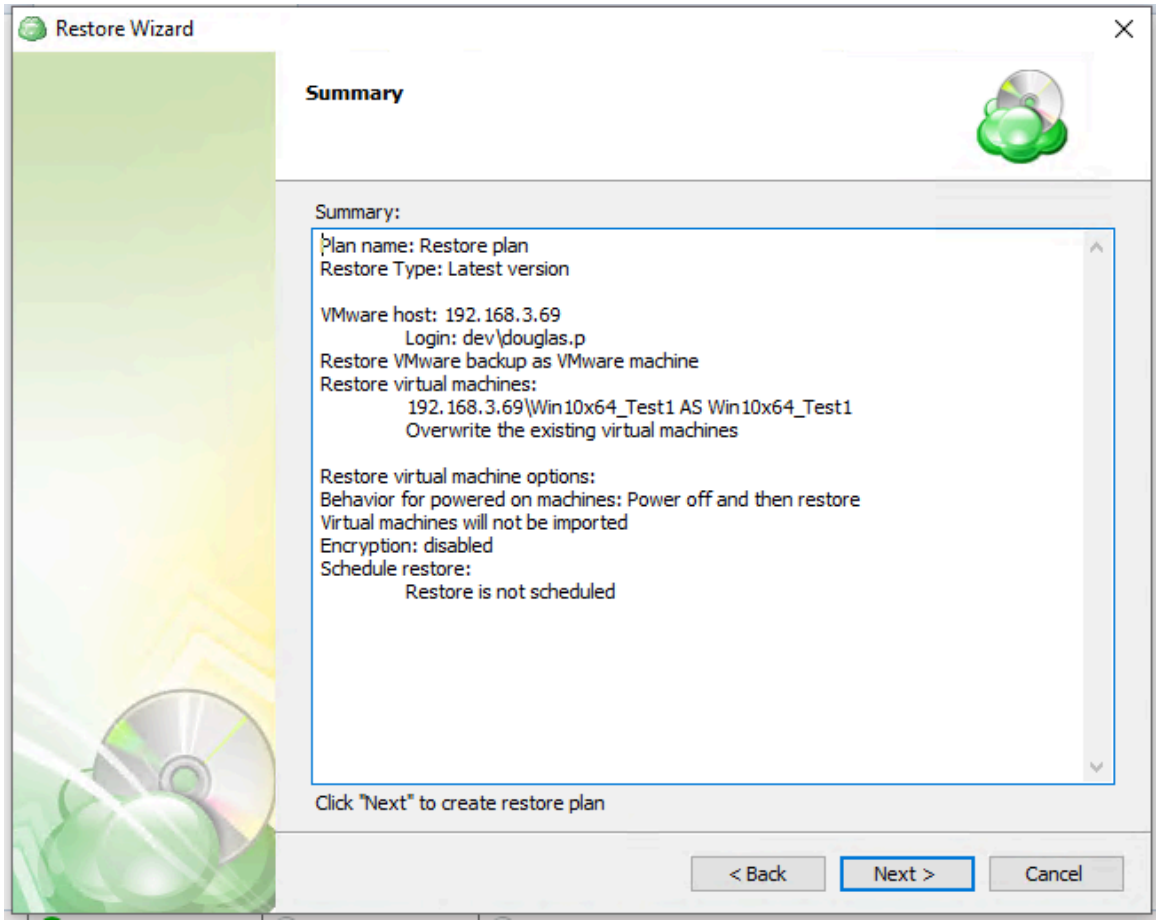
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 17. After setting the schedule, the next step allows pre and post actions to be defined.



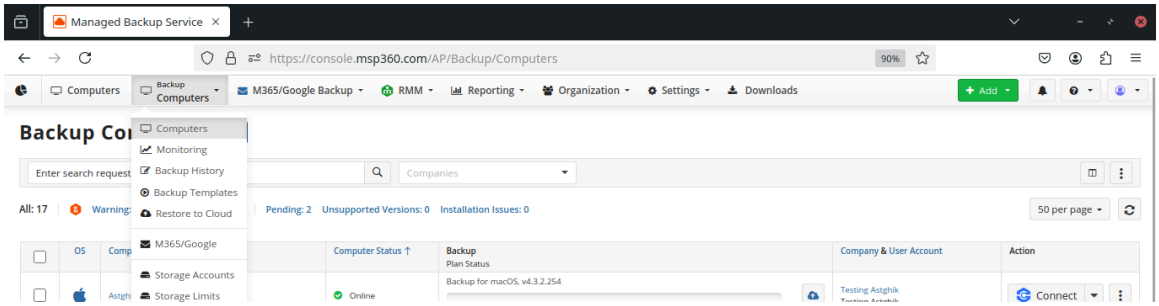
Step 18. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.



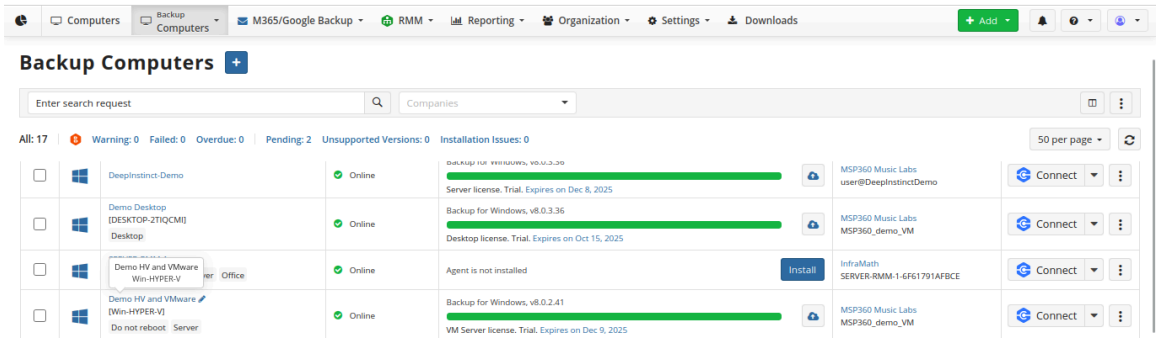
If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

Restore as a VM using MBS

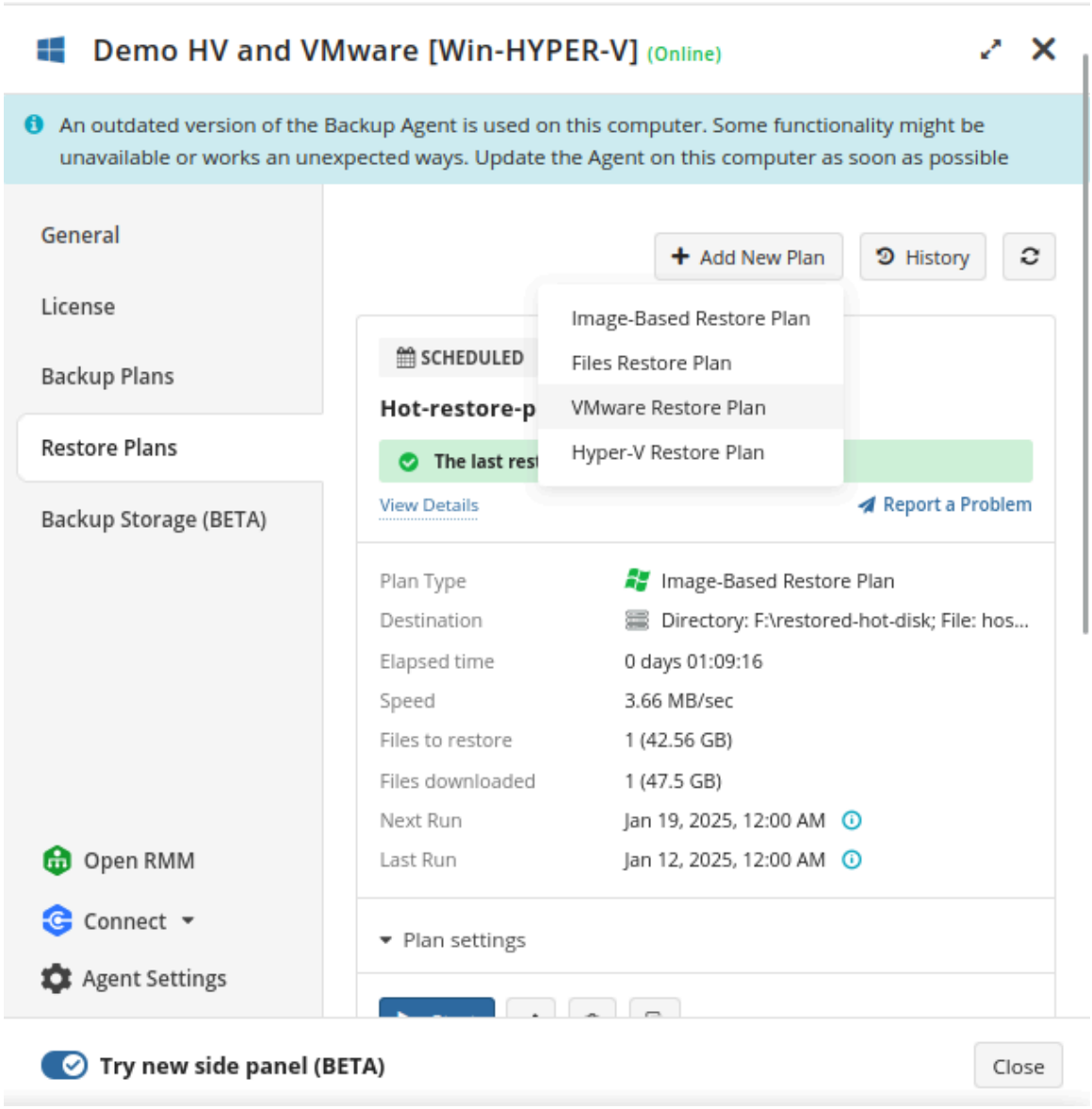
Step 1. From the MBS Portal, left-click Backup>Computers on the menu



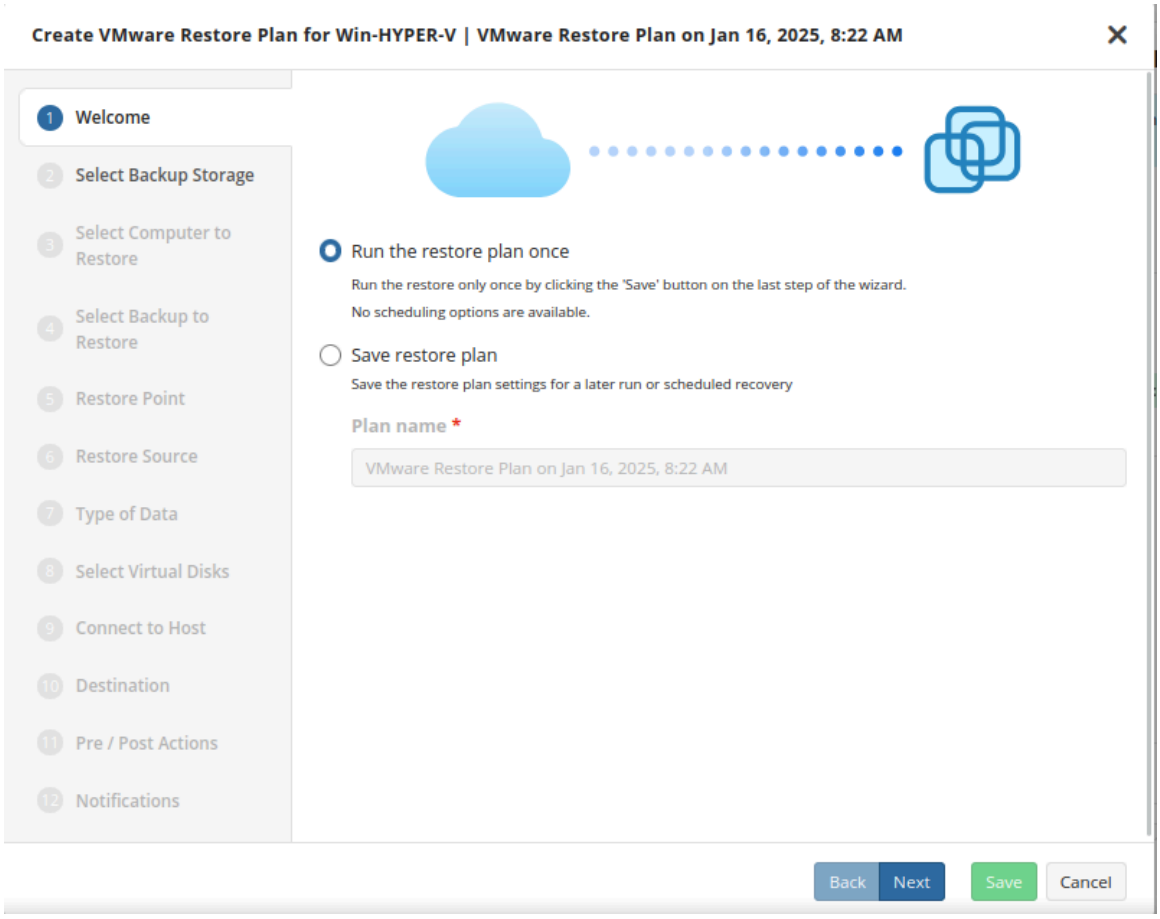
Step 2. Locate the computer you wish to restore from the list and open the current list of plans by either clicking on the name of the computer, or by selecting “Show Plans” from the gear menu.



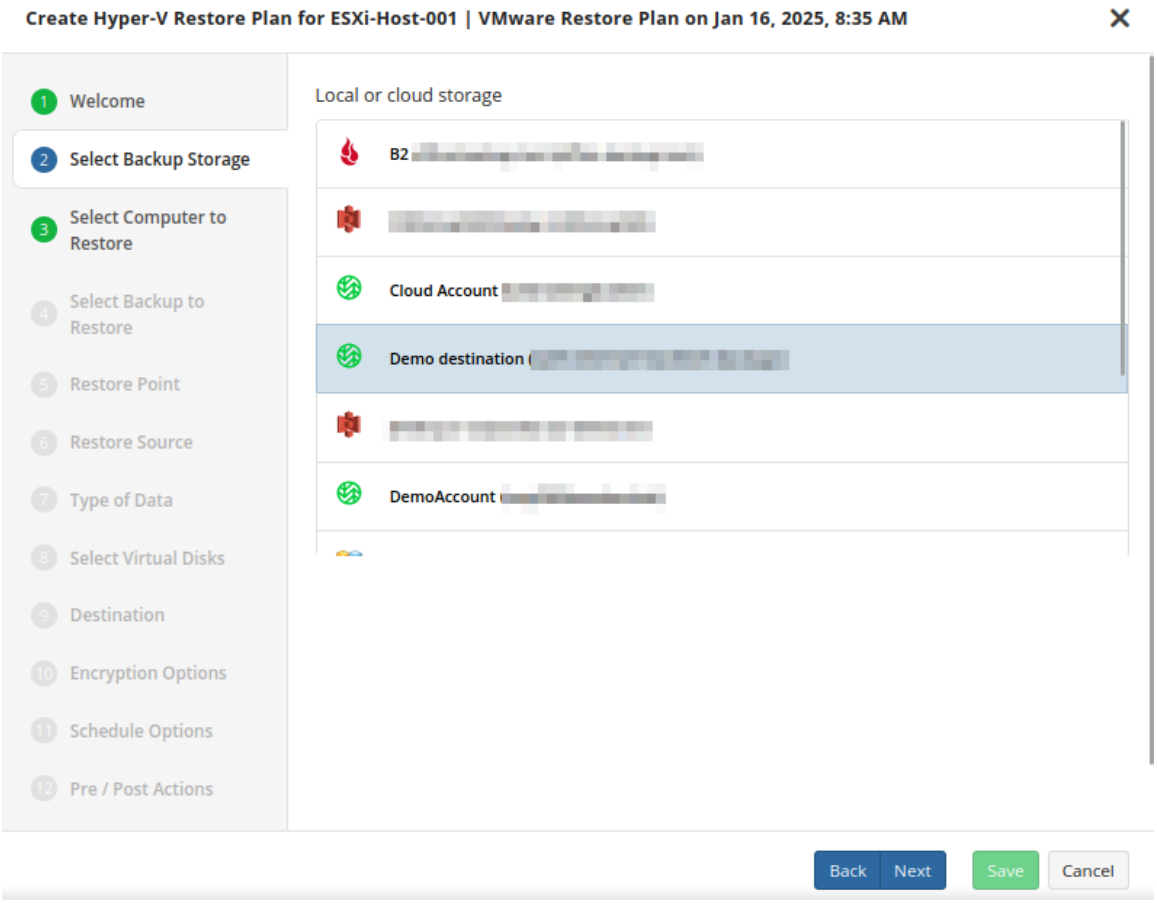
Step 3. Select ‘Restore Plans’ click on the “Add New Plan” icon and then select “VMware Restore Plan”



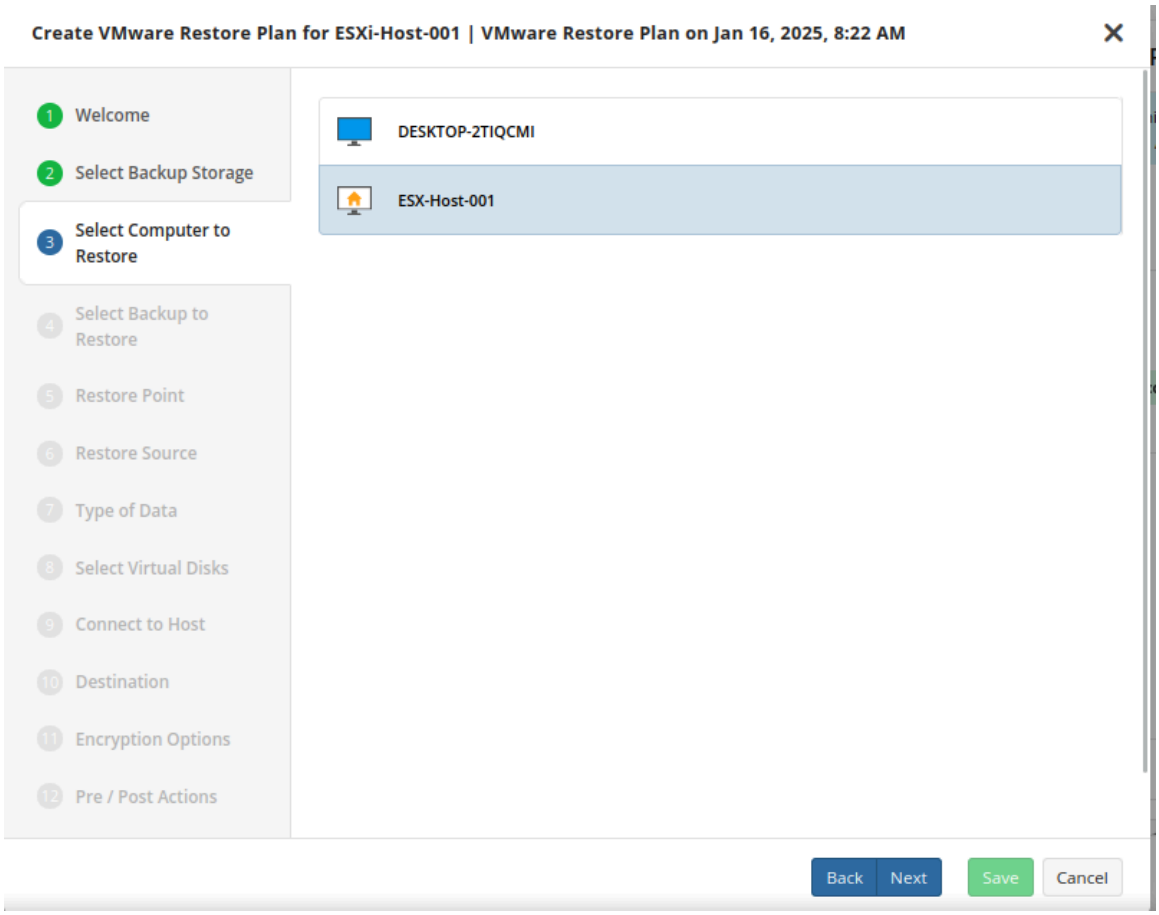
Step 4. The first step when making a Restore Plan is to select if it should run only once, or if it should be saved for future or scheduled use. The latter will allow you to name the plan.



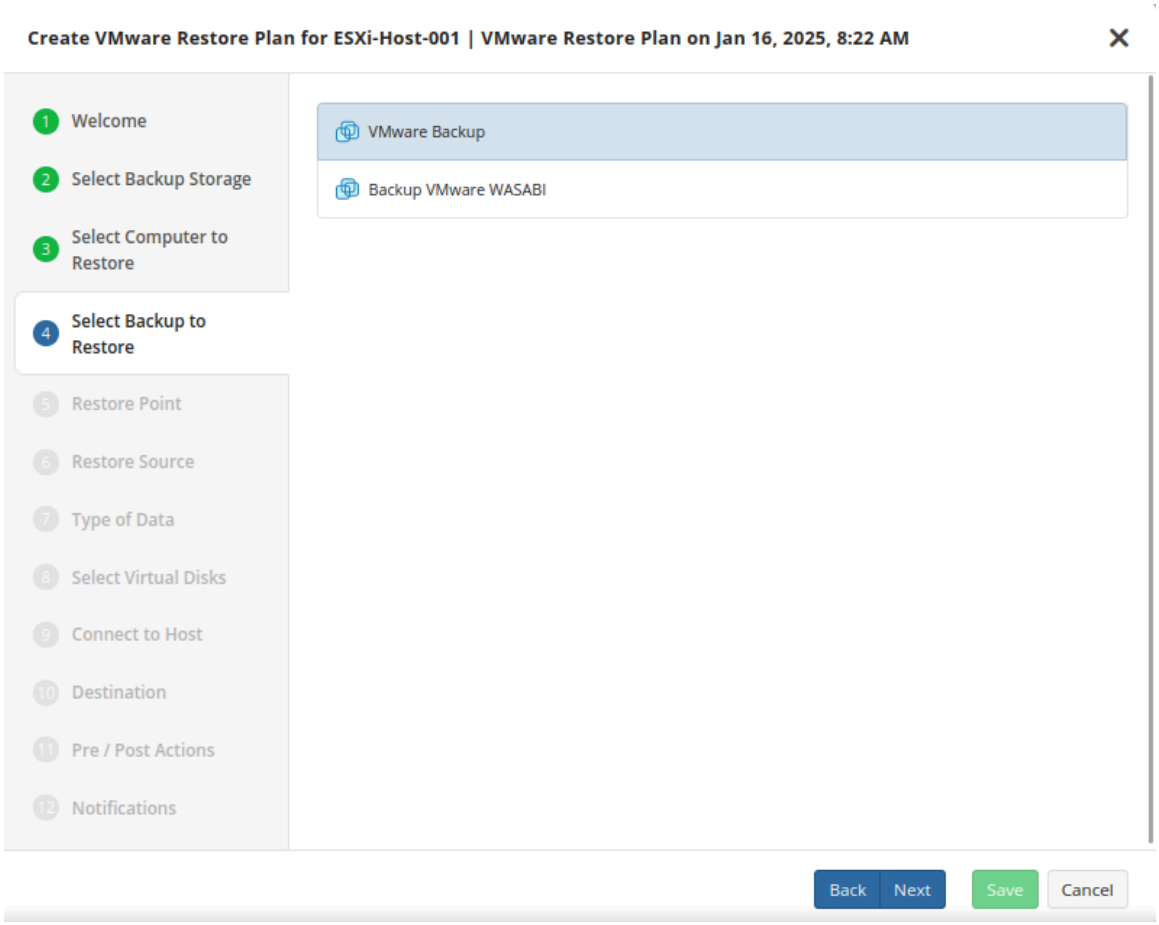
Step 5. Now we have to select the storage source to restore the backup.



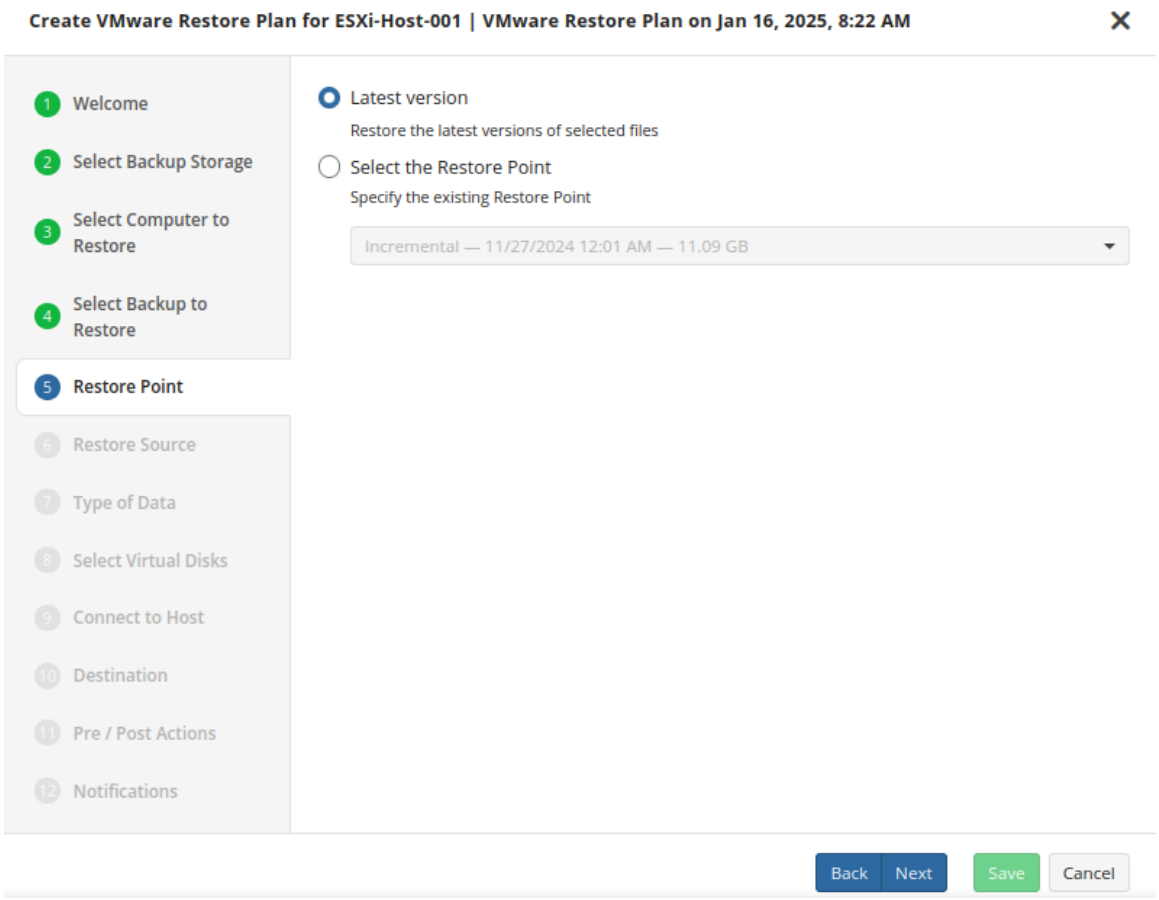
Step 6. Select the host you want to get the Vm backup from



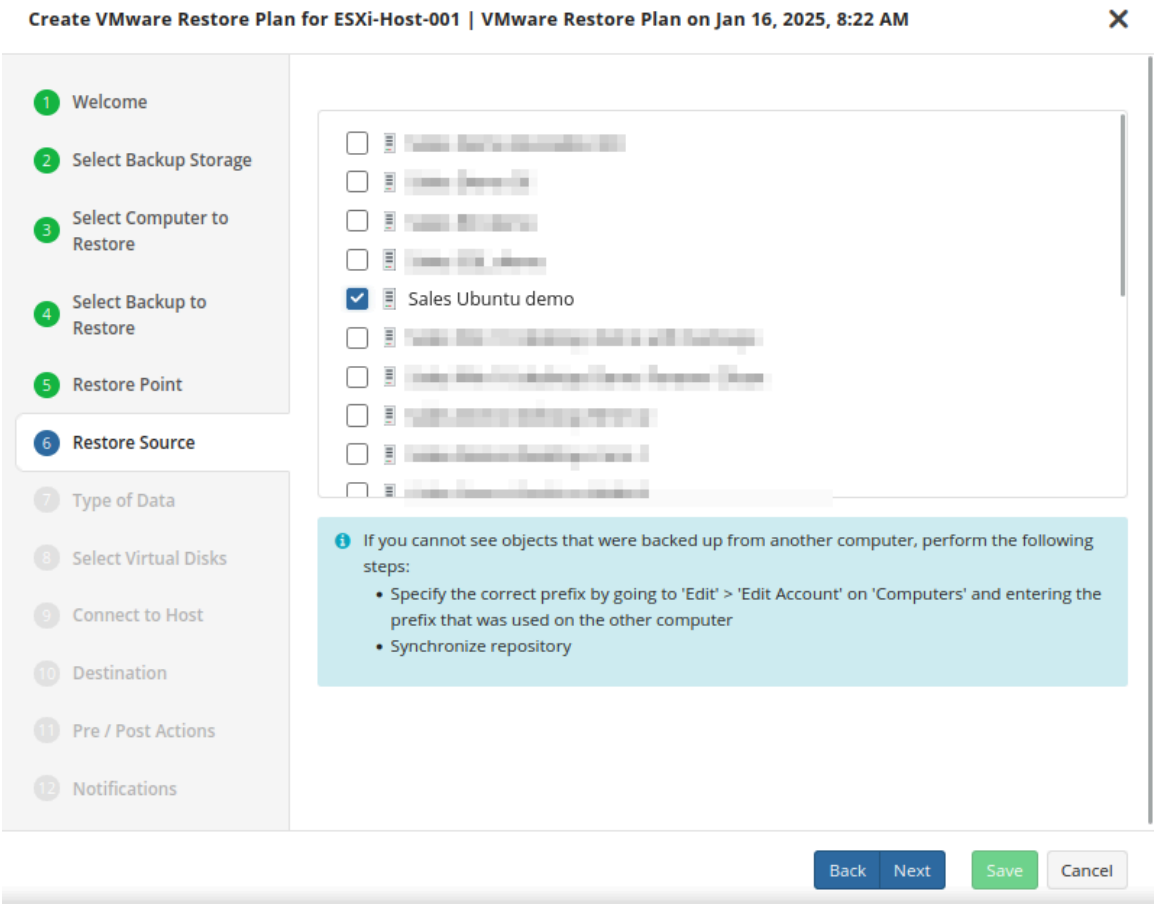
Step 7. Next, select the Backup Plan you want to restore



Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.

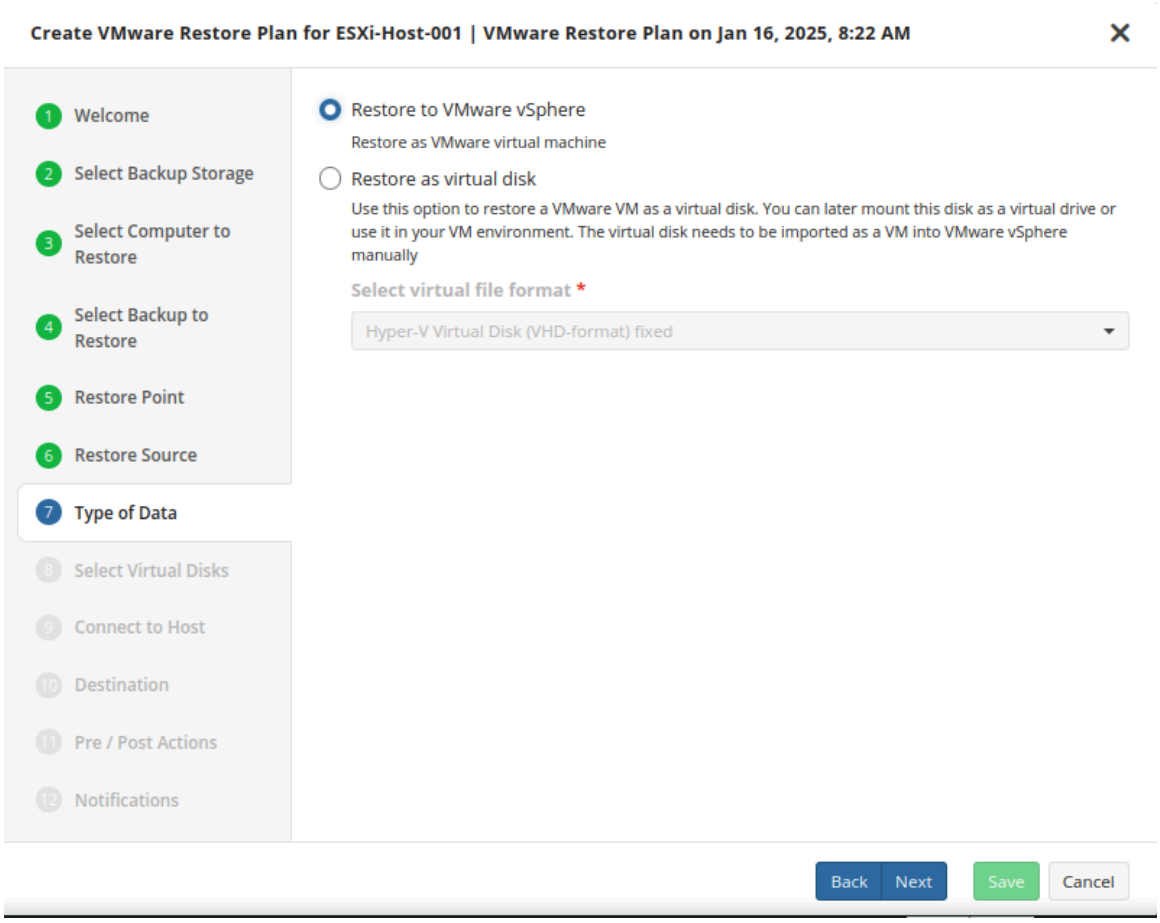


Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which VM to restore.



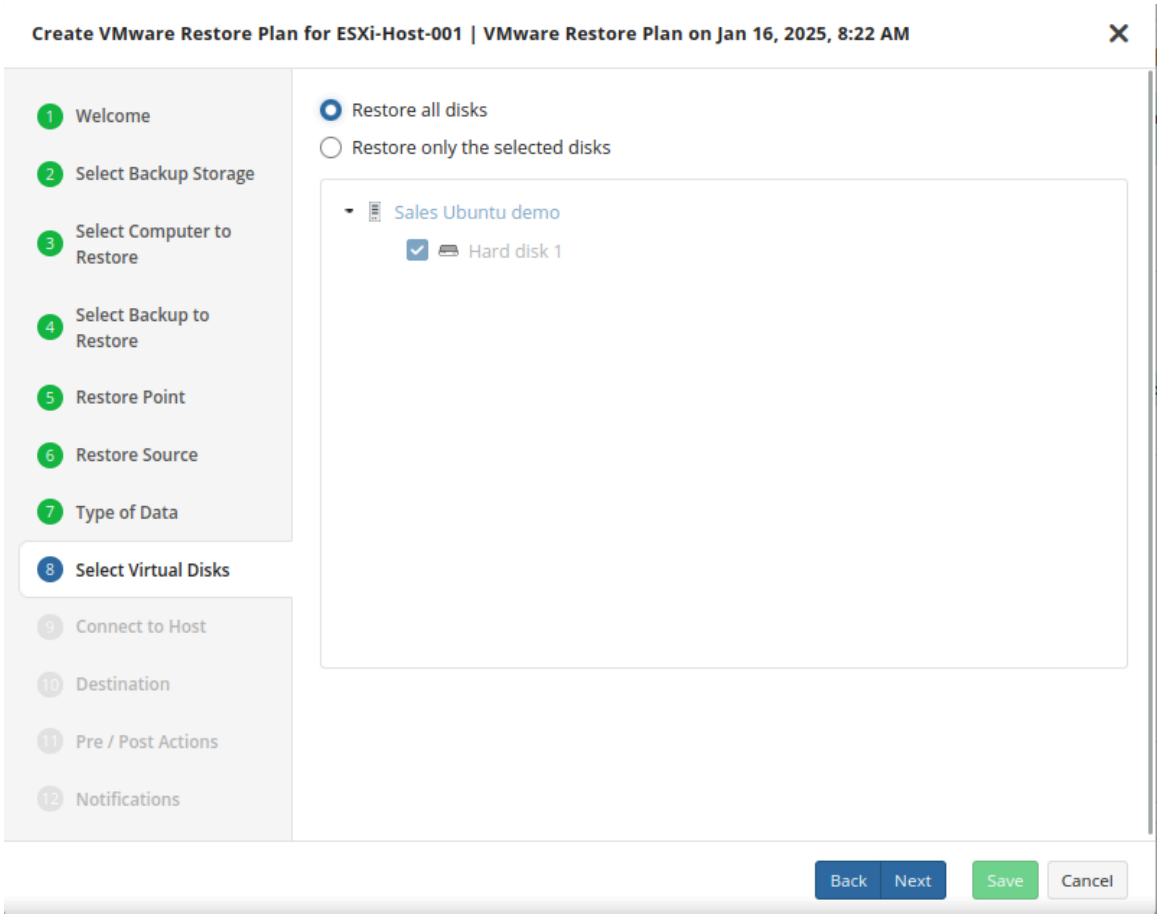
If backed-up objects are missing, ensure the correct **prefix** is specified (the same one used for backup) and verify that the **repository is synchronized** to update available backups.

Step 10: The next step of the wizard allows you to choose how the VM data should be restored.

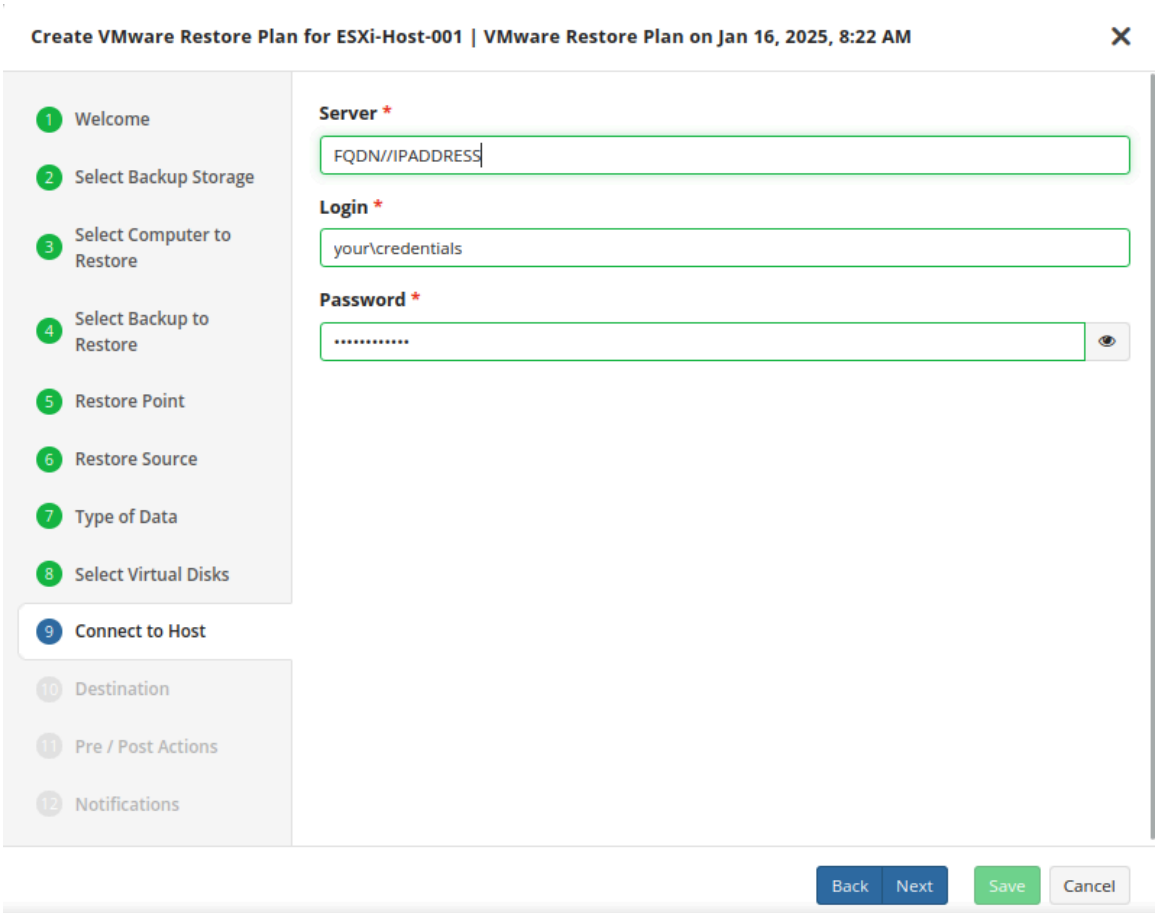


- **Restore to VMware VSphere:** Selecting this option restores the virtual machine configuration as well as the virtual disks to VSphere as a VM.
- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:

Step 11: The next step of the wizard allows you to choose the disks to be restored.

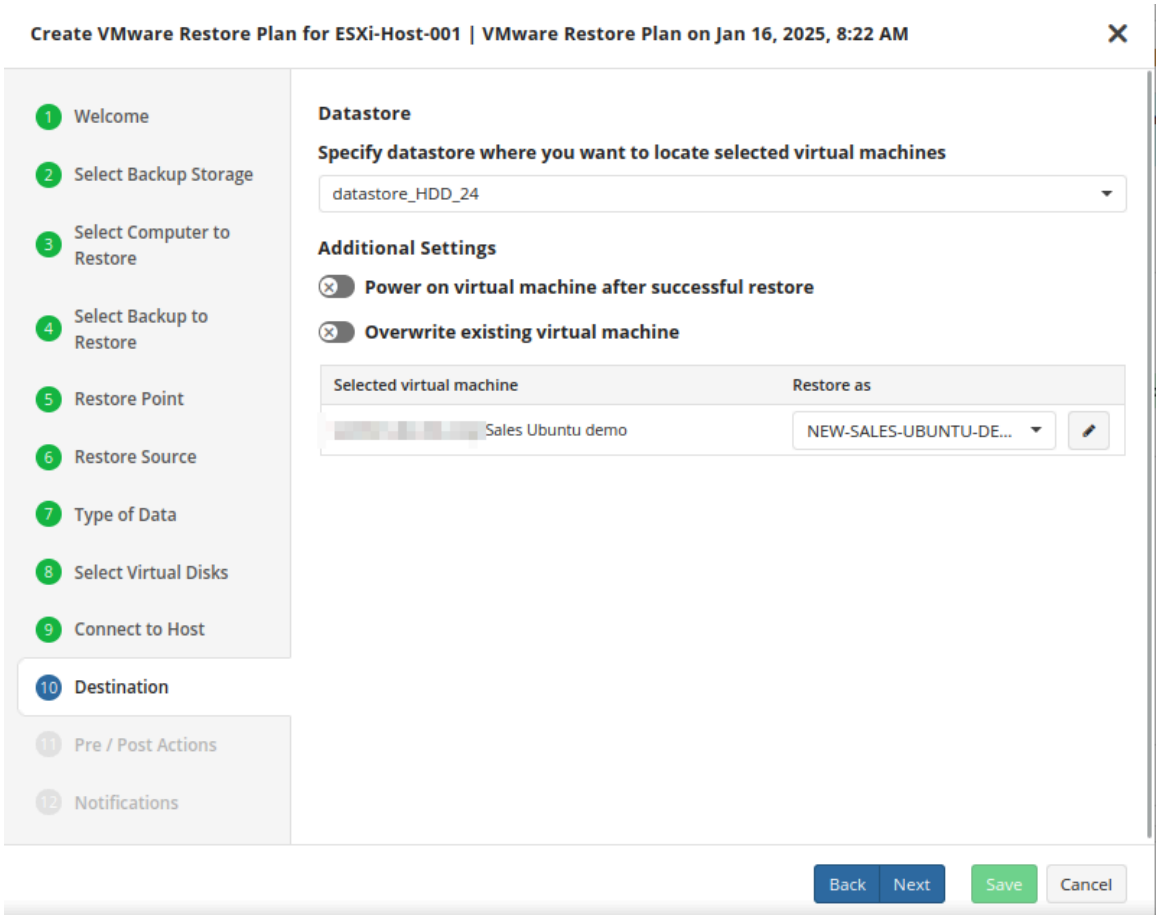


Step 12: Now you'll have to connect to the host by either using its IP address or FQDN.



It is important to determine whether FQDN or IP addresses will be used for all future plan configurations. The application will consider each to be unique hosts, even if the target machine is the same.

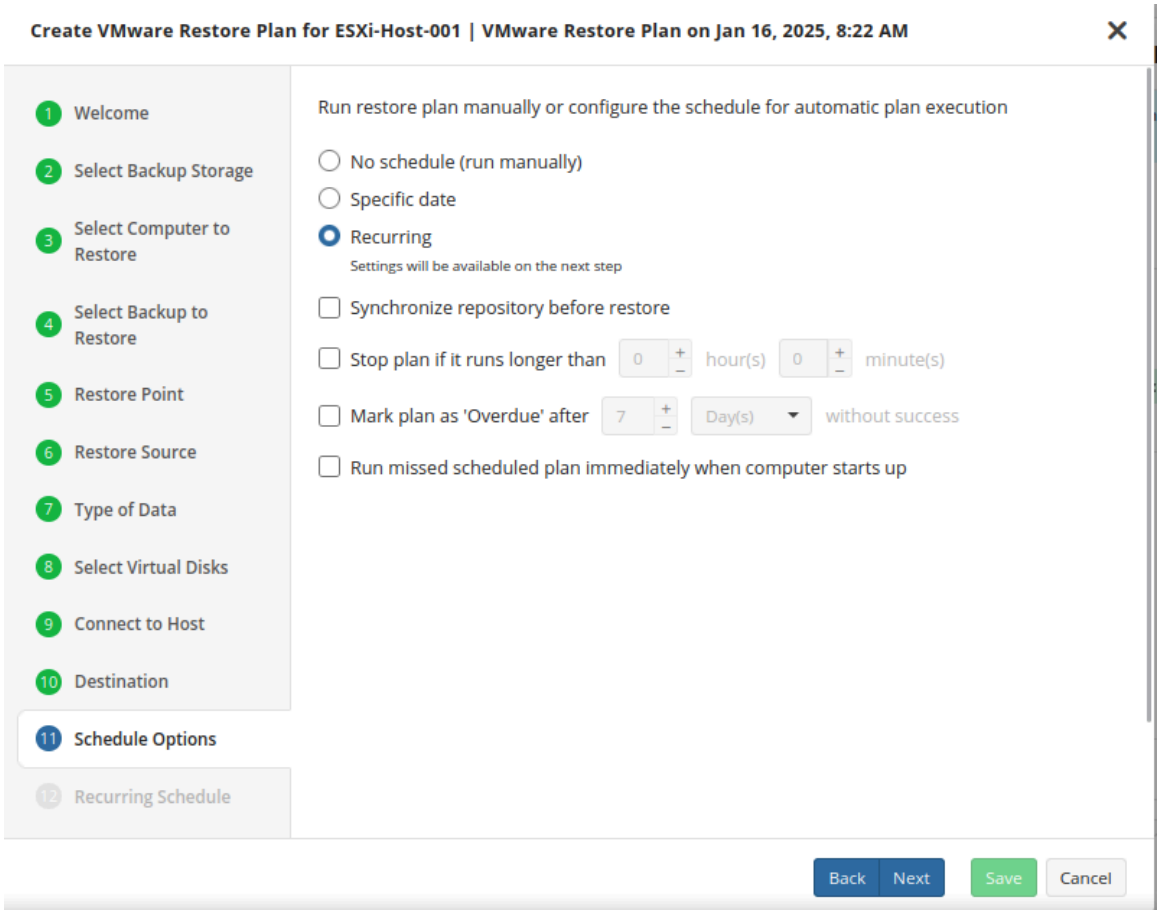
Step 13: In this step of the Restore Wizard, you configure where and how the virtual machine (VM) will be restored.



- **Specify datastore:** Select the destination disk on the VMware host where the VM should be restored to.
- **Additional Settings:** Choose the action to take if the target VM being overwritten is currently powered on. If you select “Skip” then any power on VMs will be ignored during the restore process.

> If you wish to restore it as a different name or target VM, select or type over the value in the “Restore as” list.

Step 14. If you choose to save the restore plan, the schedule is configured during steps 11 and 12 of the wizard.



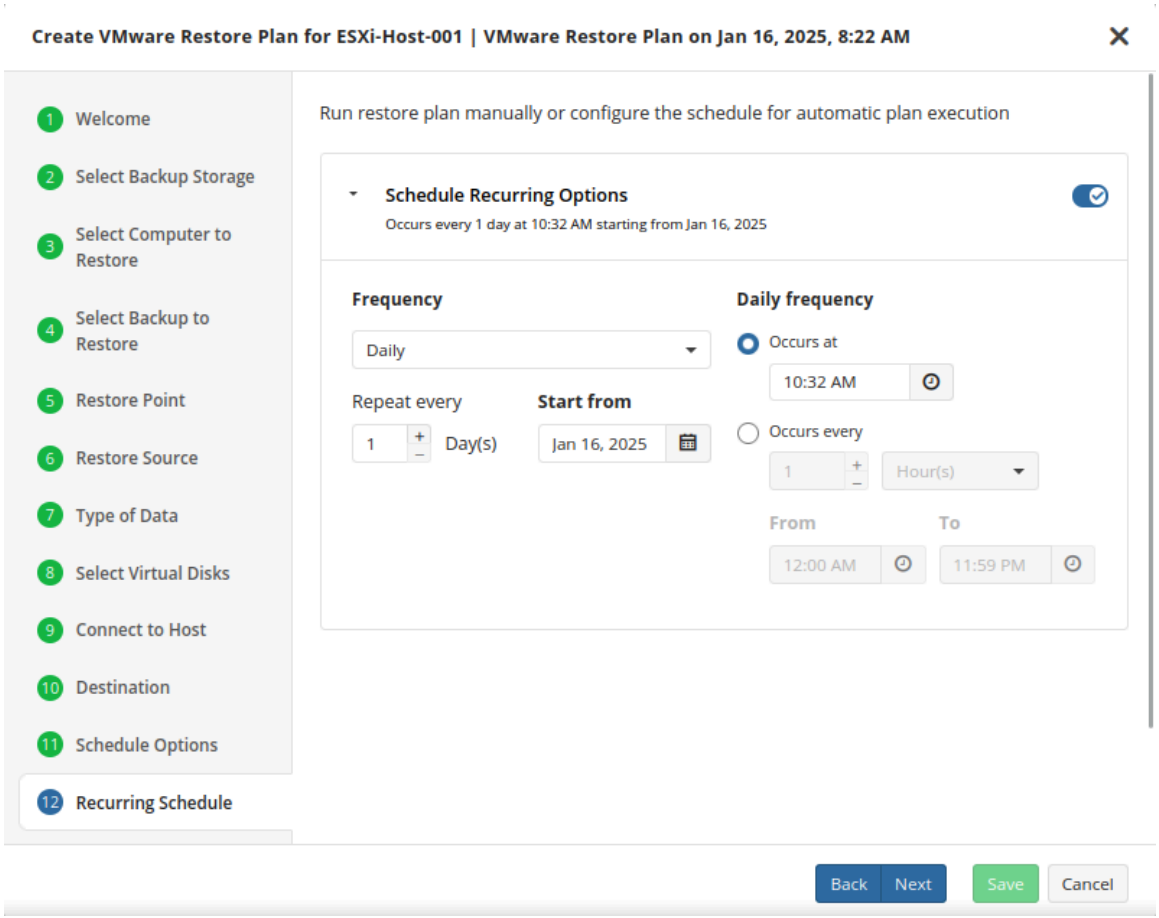
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

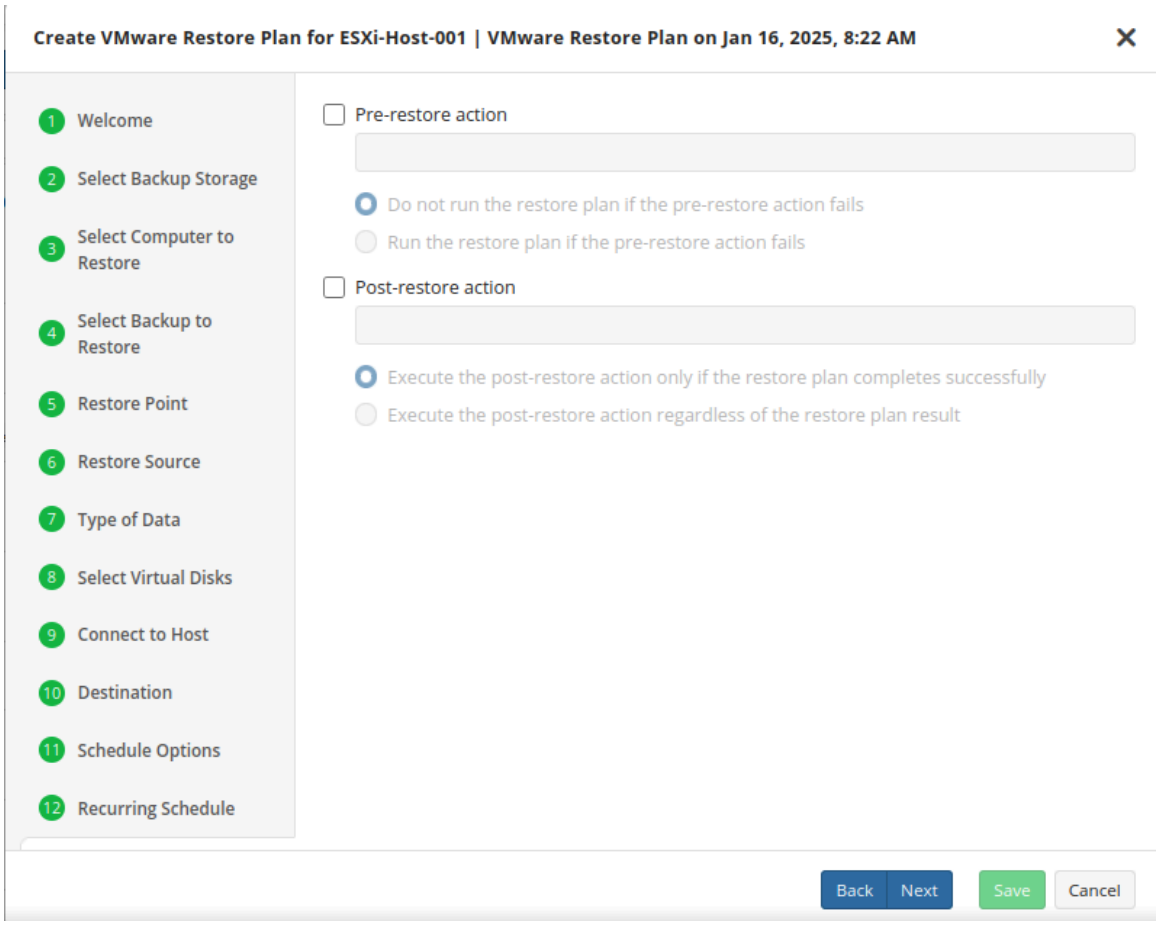
Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only

recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

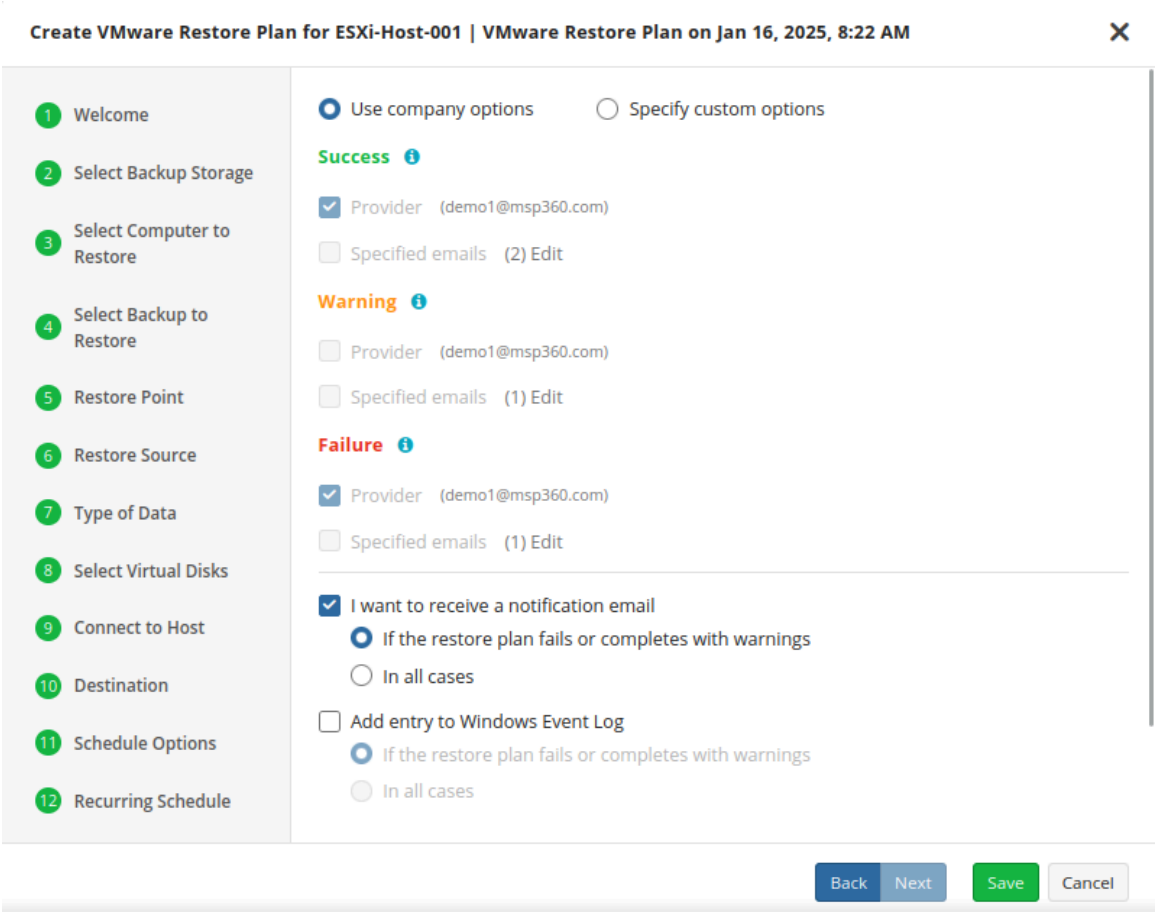
Step 15. If a recurring schedule was selected, now you can set up the frequency for the restore plan to be executed.



Step 16. Next, specify the pre/post actions if required.



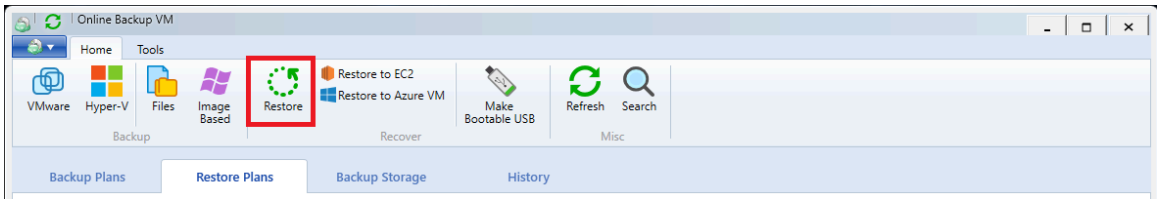
Step 17. After pre-post actions, you can configure the notifications for this restore plan.



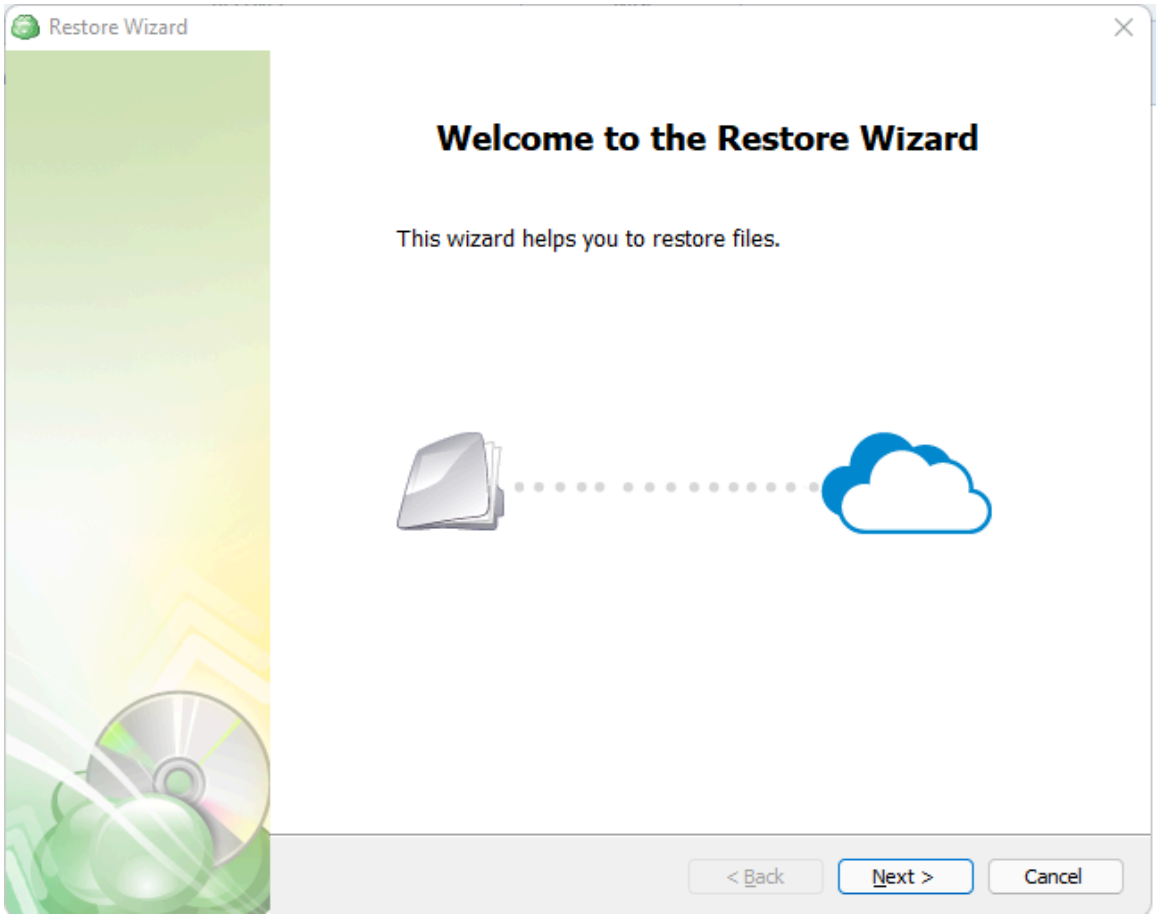
Step 18. Click on Save when you are happy with your selections. If the plan is set to run only a single time and has no set schedule, it will automatically start. Otherwise, if it is set to run only once and is scheduled, it will display in the list of plans until the scheduled time. If it is only set to run once, then when it completes successfully it will remove itself from the list of plans. Only Restore Plans which are saved will remain in the list for future use.

Restore as a Virtual Disk using the Agent

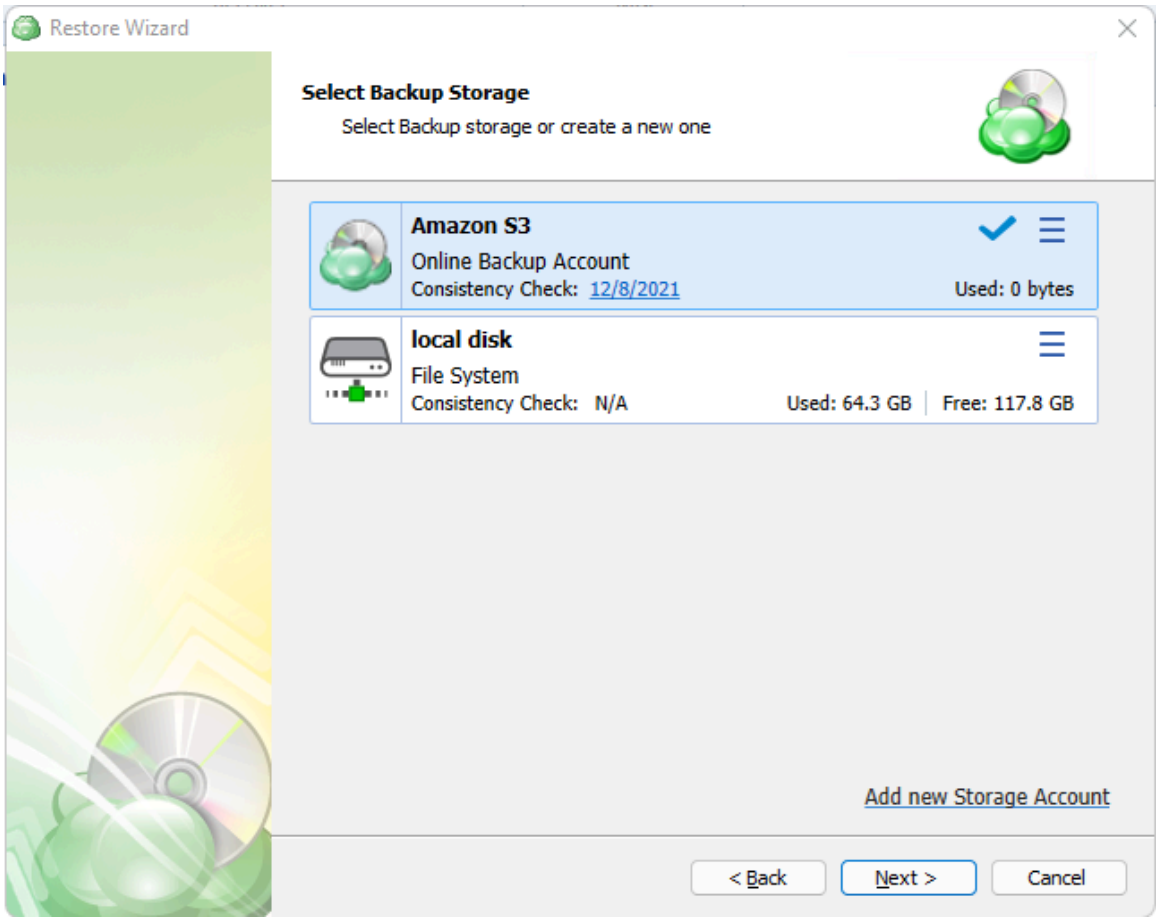
Step 1. Within the Online Backup Agent, click on “Restore”



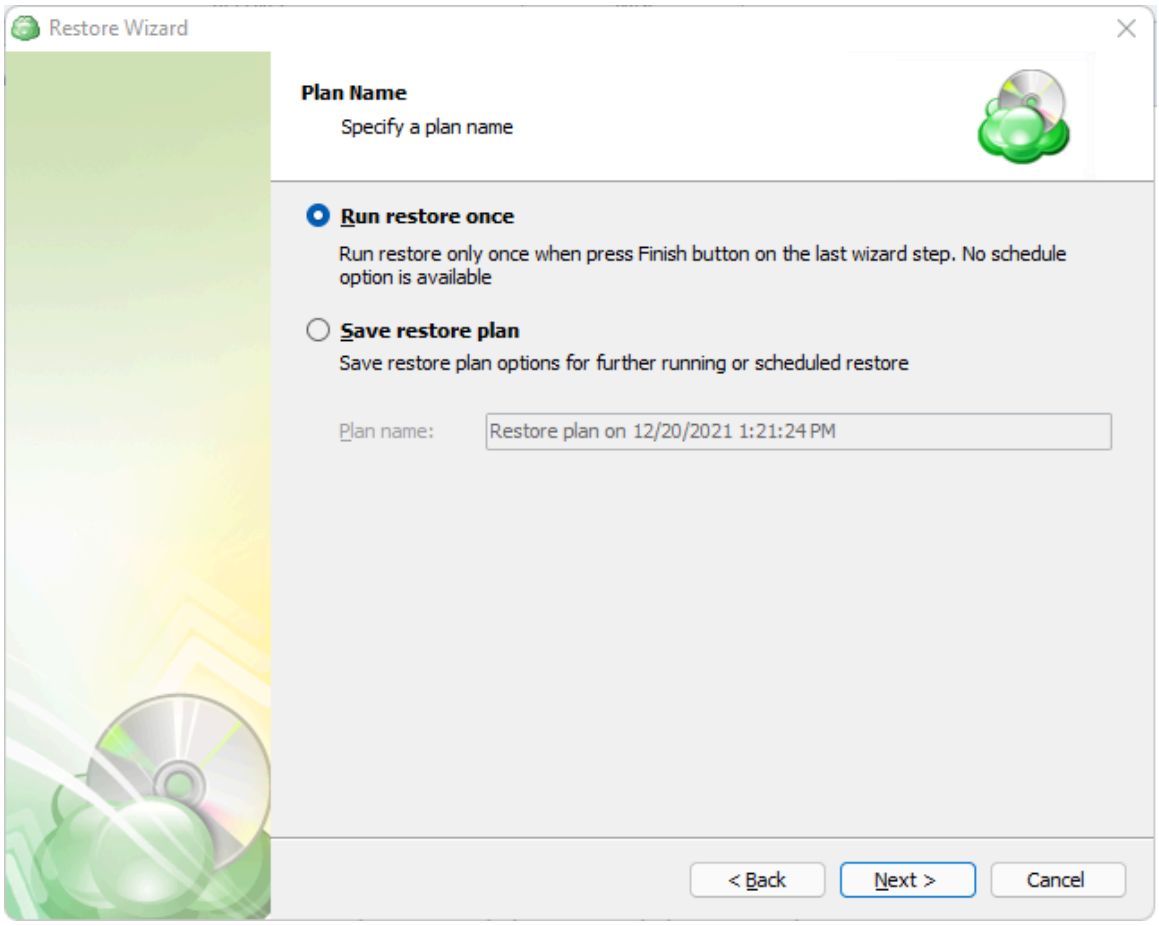
Step 2. Once the wizard starts, click on Next to advance to the next step.



Step 3. The next step will prompt you to select the source for the restore point.



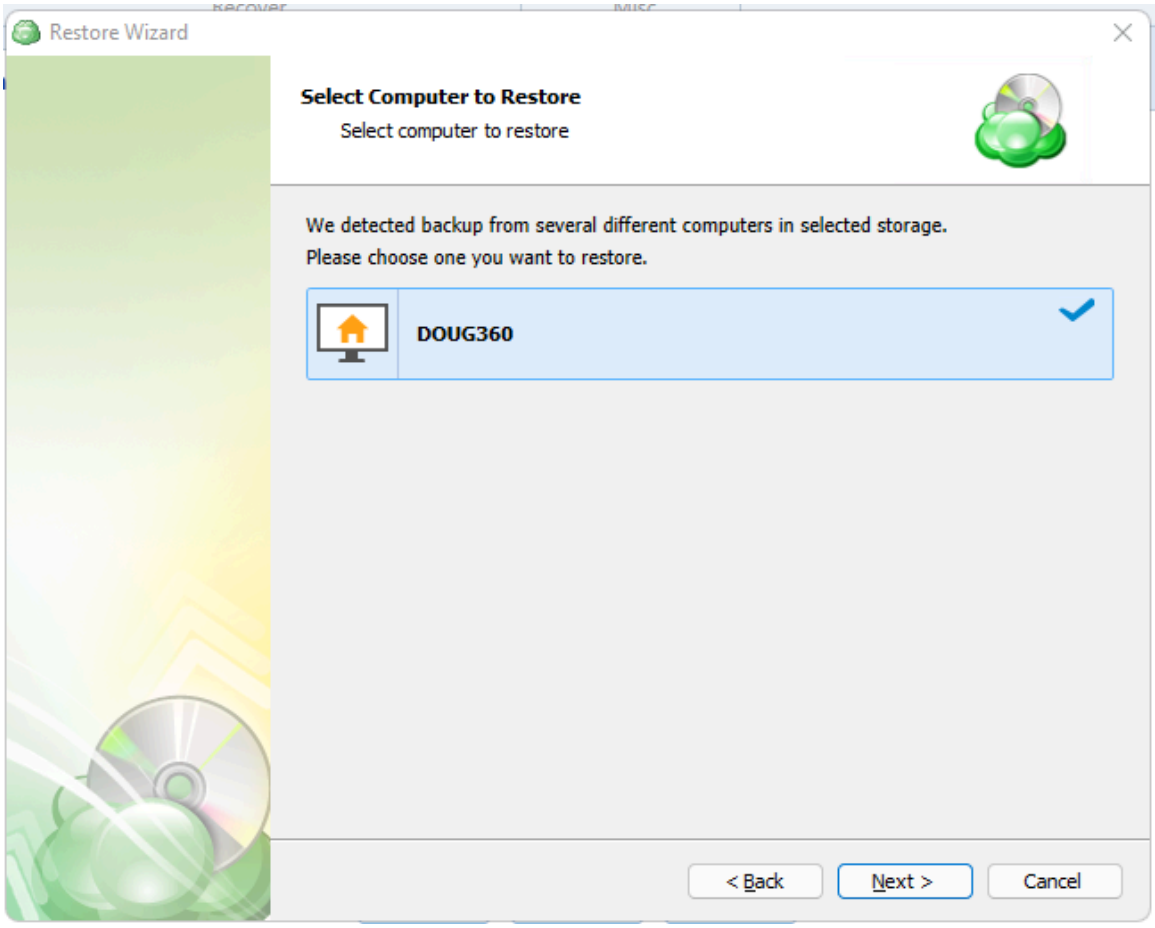
Step 4. Next, you will be given the option to either run the restore once or to save it to run later.



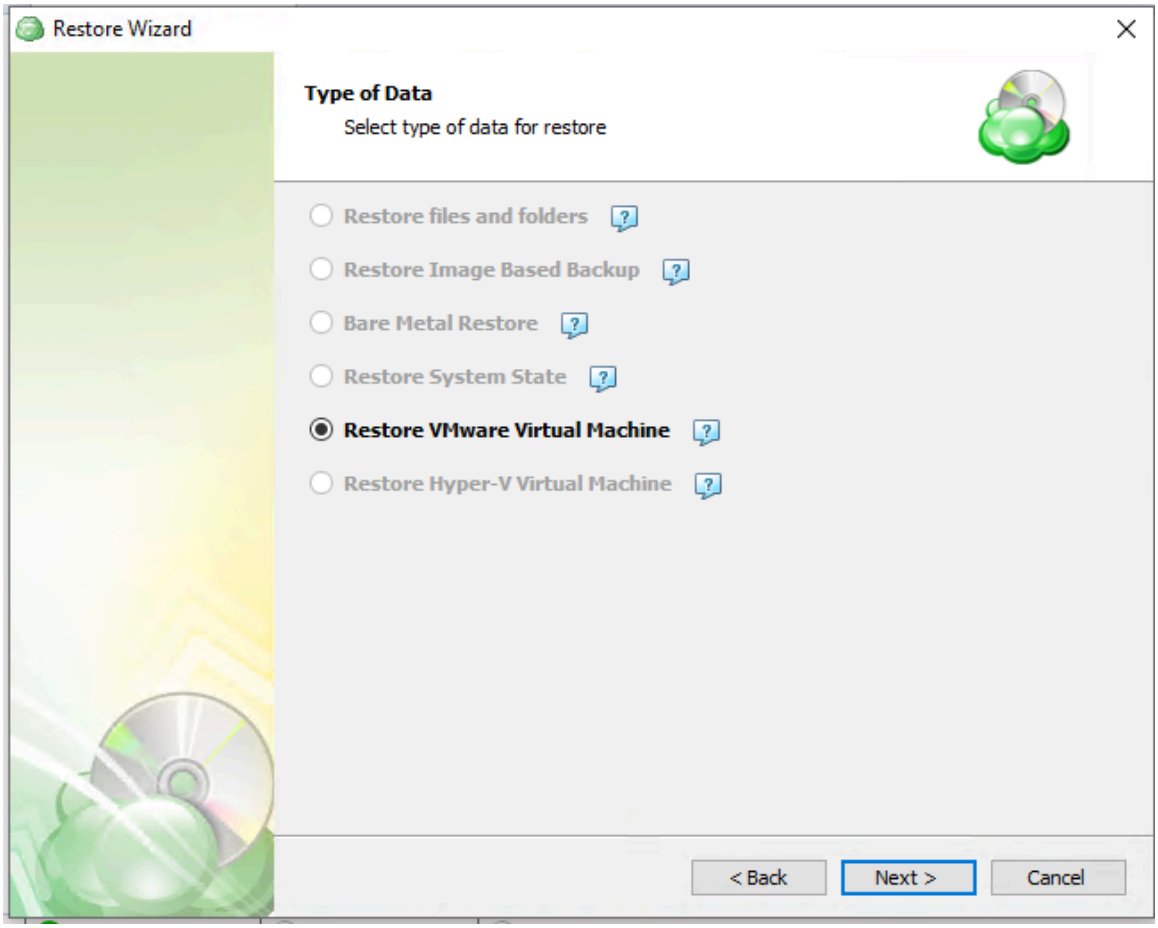
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

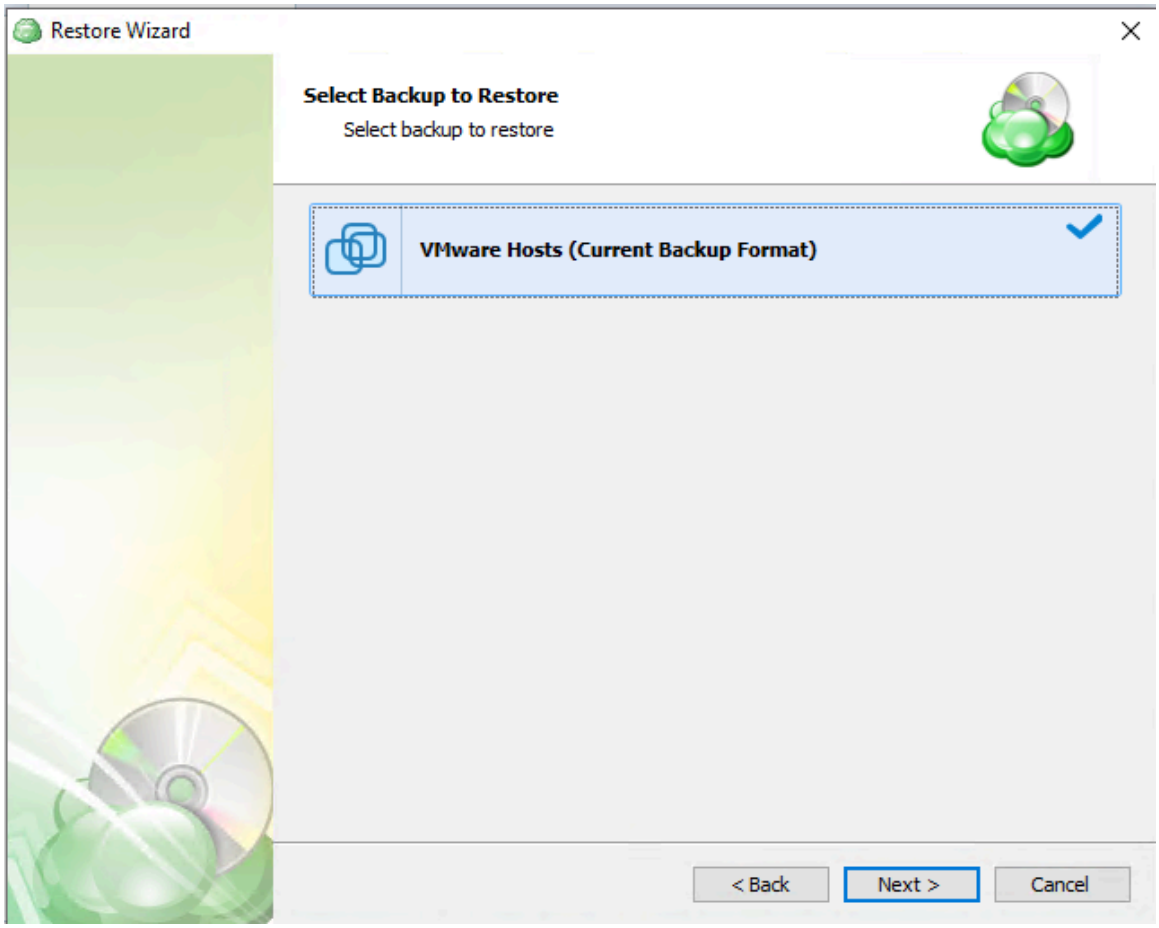
Step 5. With the type of restore selected, the next step is to select the correct Host server which the VM resides on.



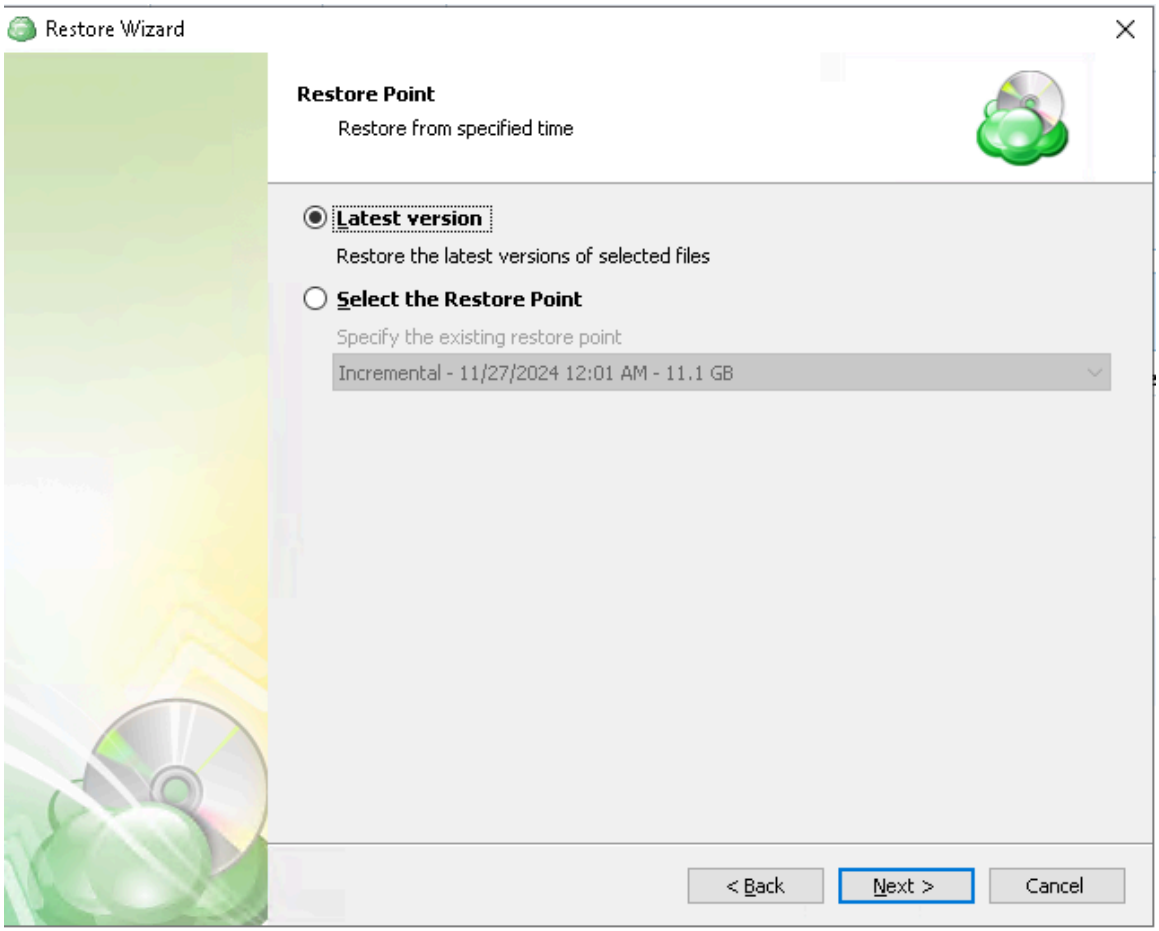
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore VMware Virtual Machine” option to continue.



Step 7. With the correct type of data selected, the application will generate a list of available VM backup plans.

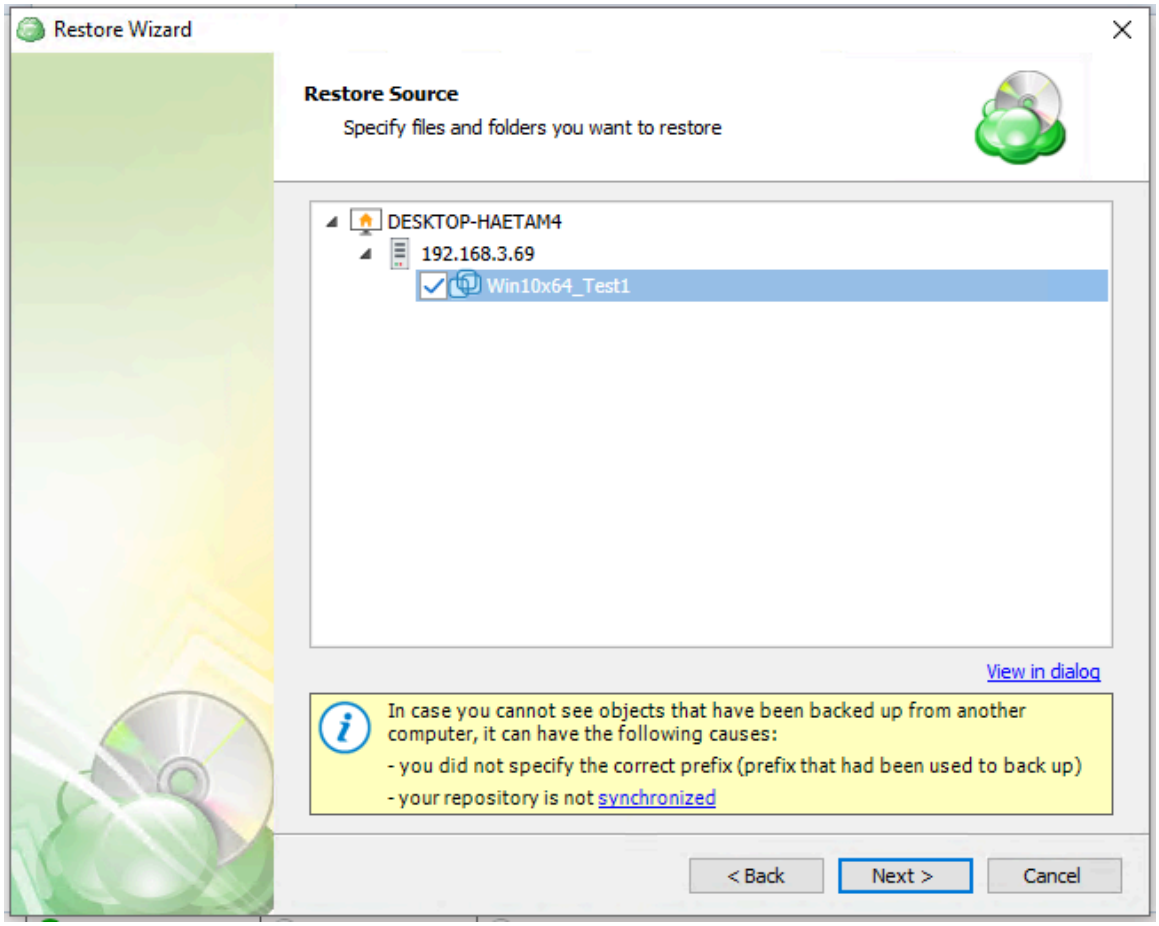


Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.

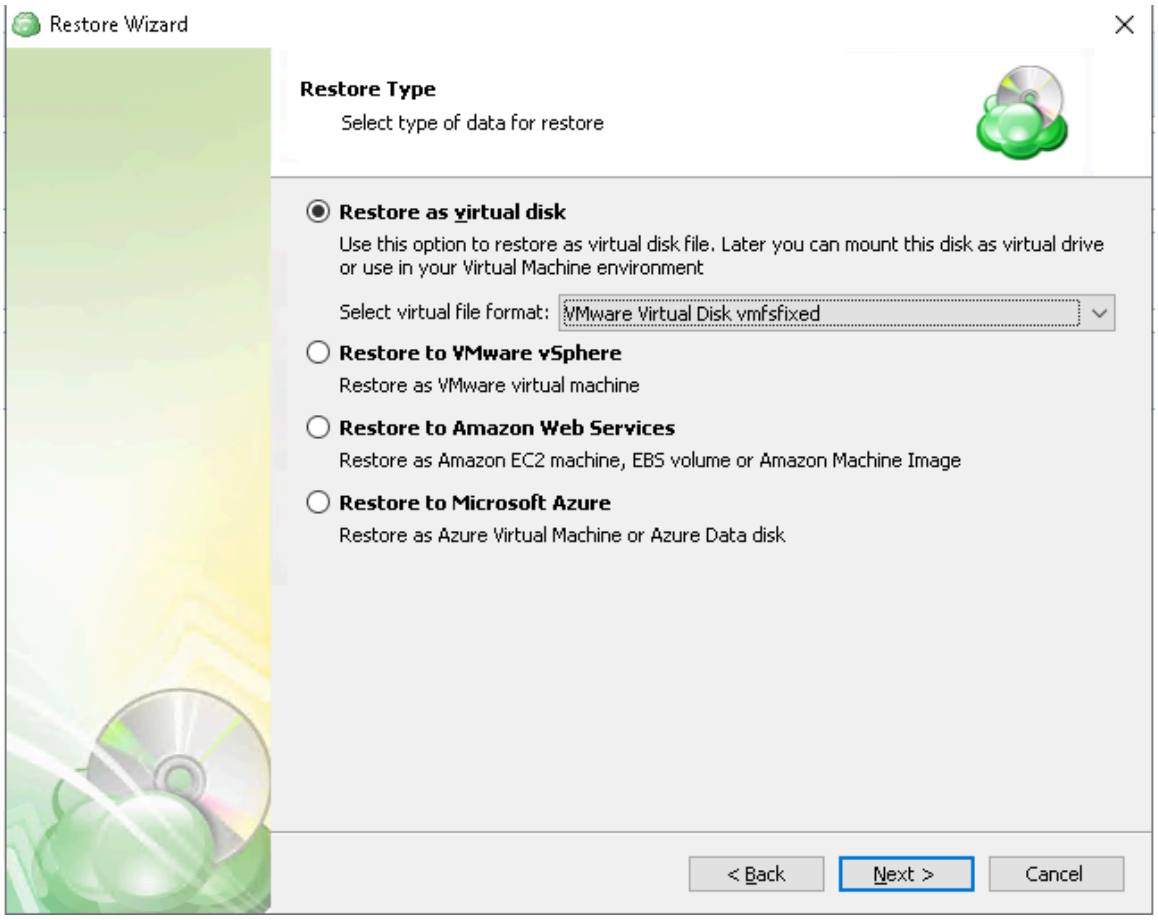


If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

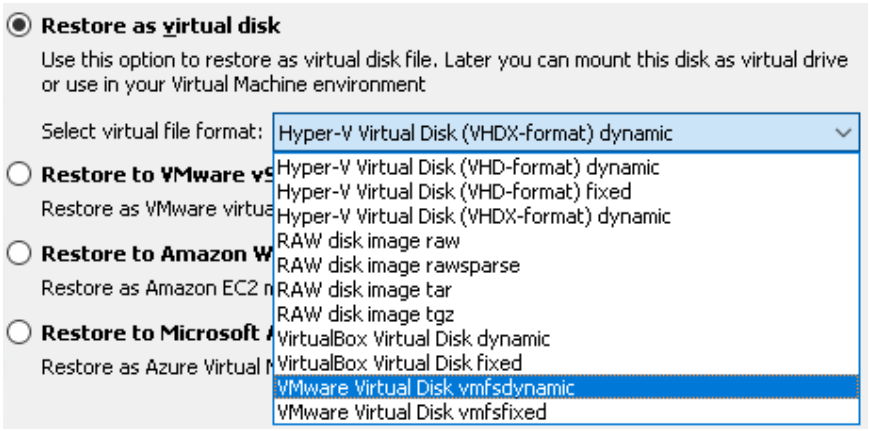
Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which to restore.



Step 10. The next step of the wizard allows you to choose how the VM data should be restored.

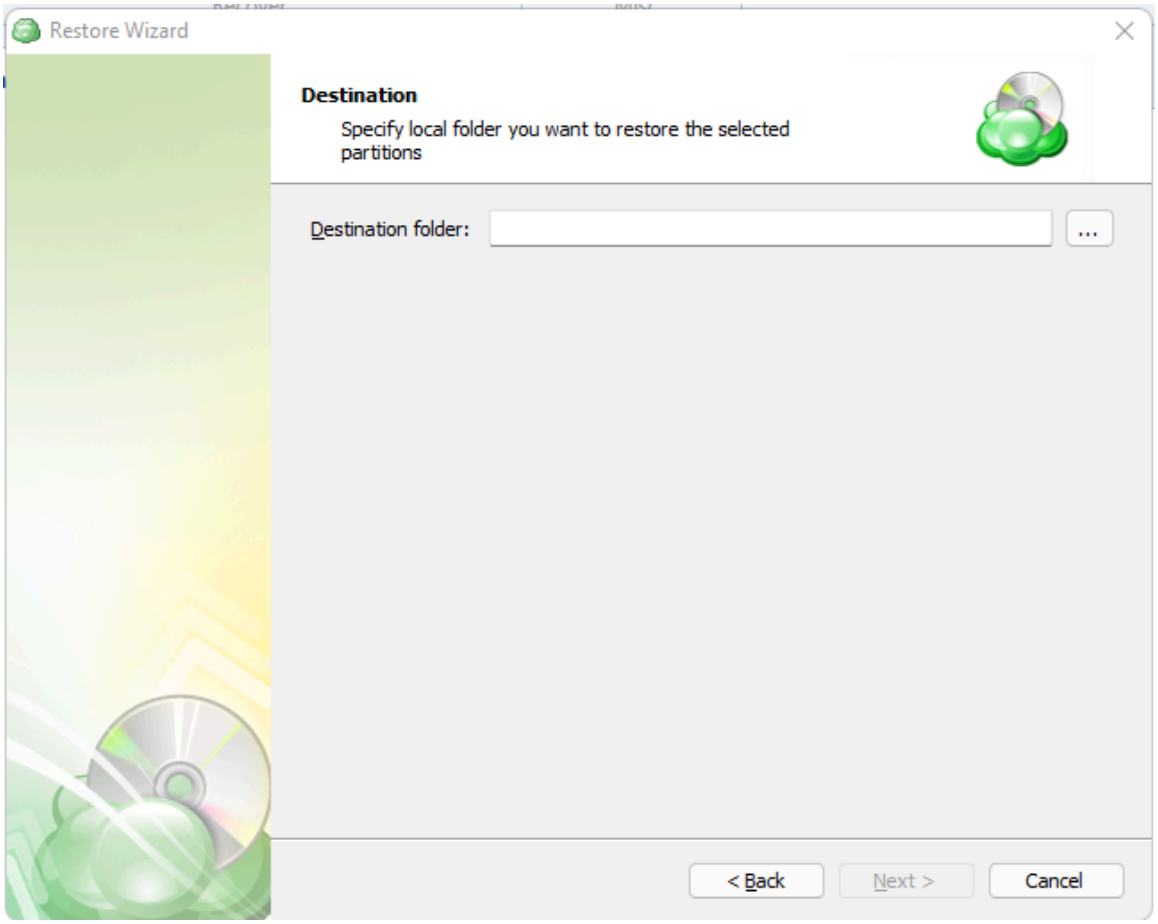


- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:

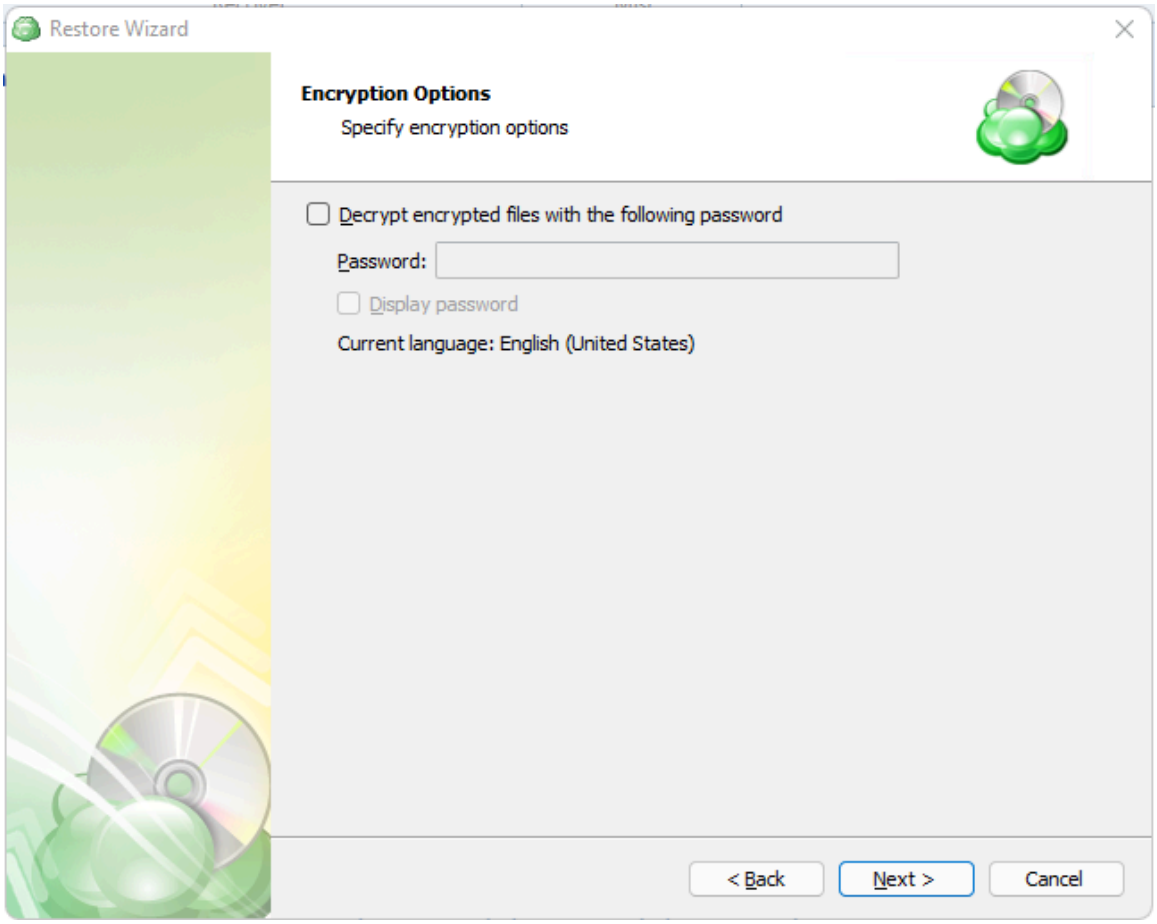


- **Restore to VMware VSphere:** Selecting this option restores the virtual machine configuration as well as the virtual disks to VSphere as a VM.
- **Restore to Amazon Web Services:** If enabled, this will restore the selected VM directly to AWS Cloud either as an EC2 instance, EBS volume, or AMI.
- **Restore to Microsoft Azure:** This will restore the VM directly to Azure as either an Azure Virtual Machine or Azure Data disk.

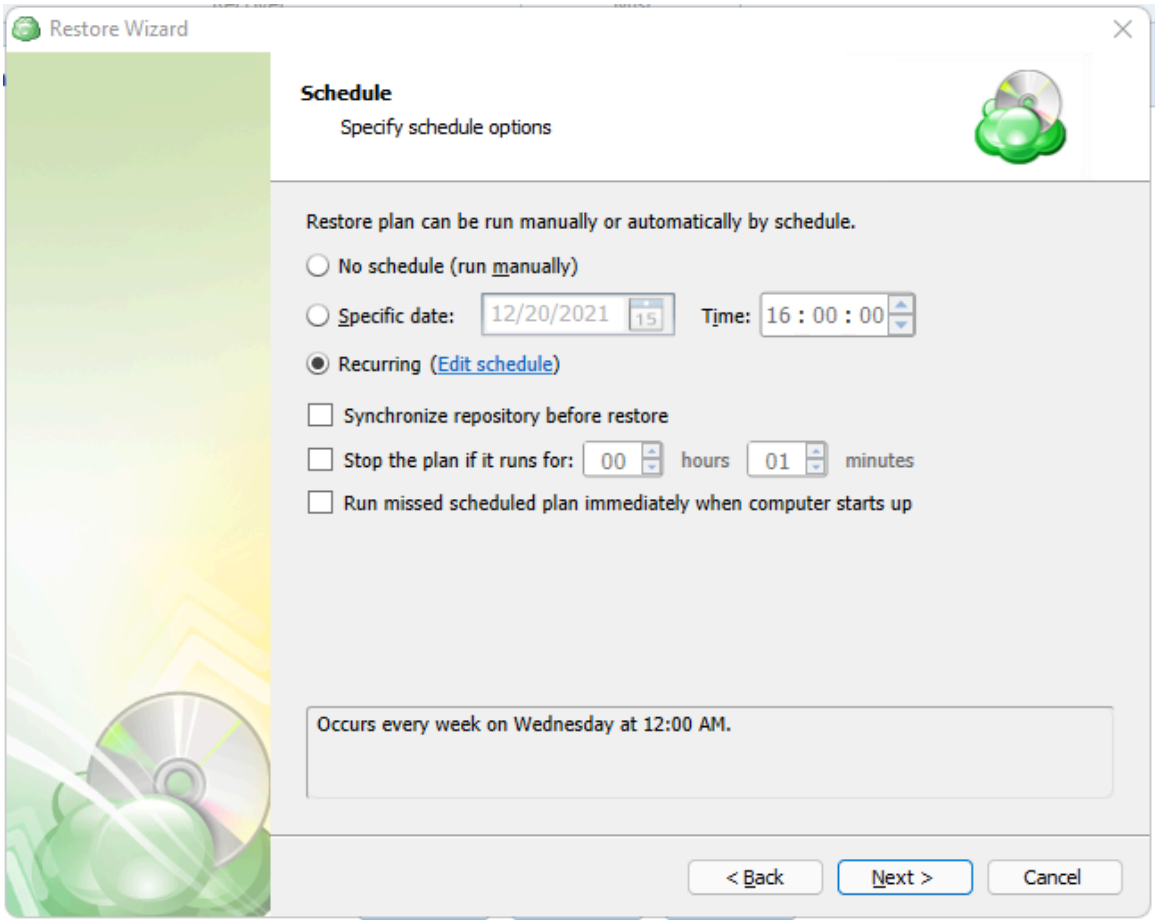
Step 11. With the checkpoint selected, you can now specify a destination folder for the virtual disk file.



Step 12. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the VM.



Step 13. With the decryption password entered, the next step is setting the schedule for the restore plan.

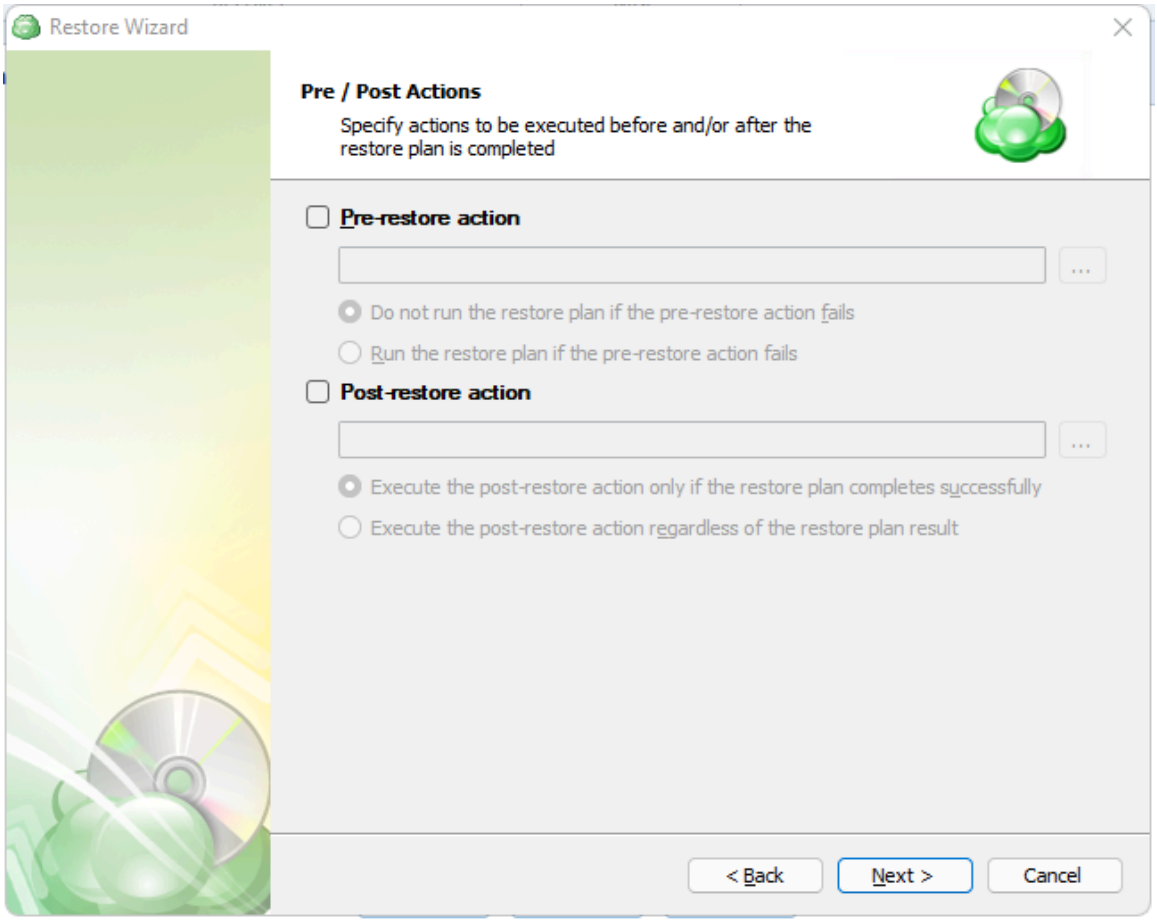


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.
- **Synchronize repository before restore**: Ensures the latest backup data is available before restoring.
- **Stop the plan if it runs for X time**: Automatically stops the restore if it exceeds the specified duration.
- **Run missed scheduled plan immediately when computer starts up**: If the restore was missed due to the system being off, it runs as soon as the computer starts.

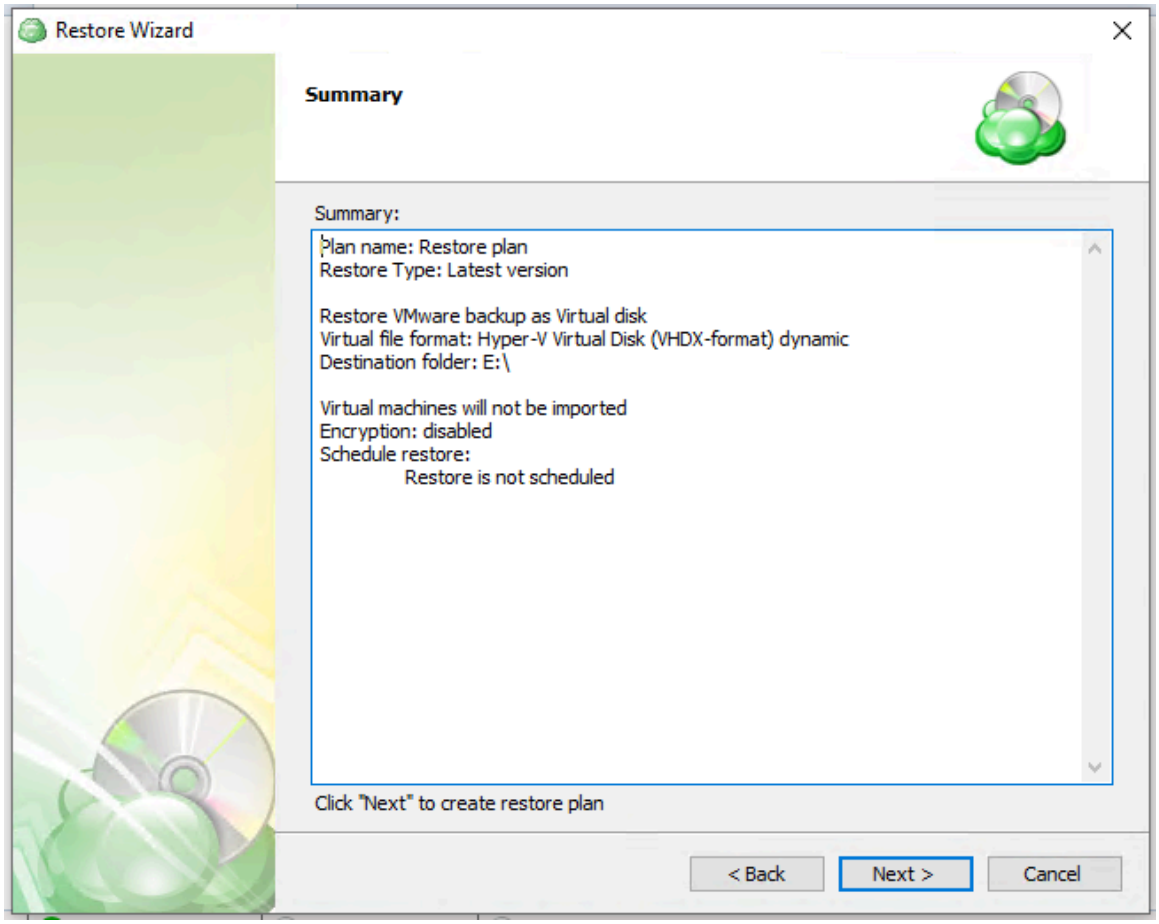
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 14. After setting the schedule, the next step allows pre and post actions to be defined.



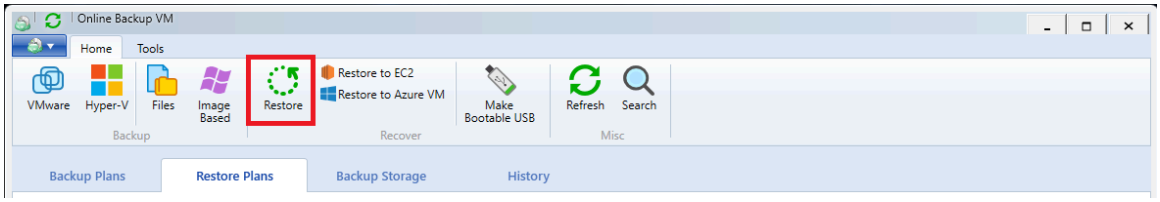
Step 15. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.



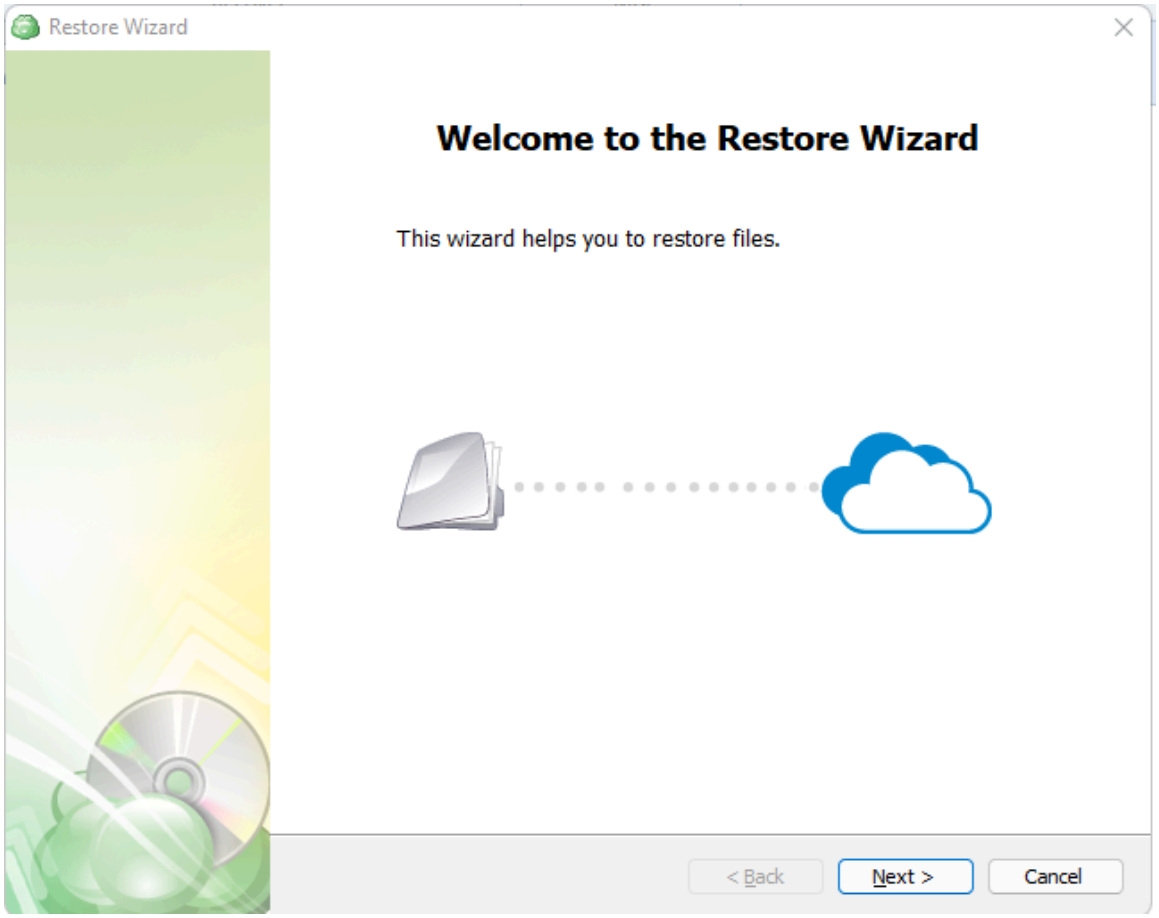
If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

Restore as an AWS EC2 Instance using the Agent

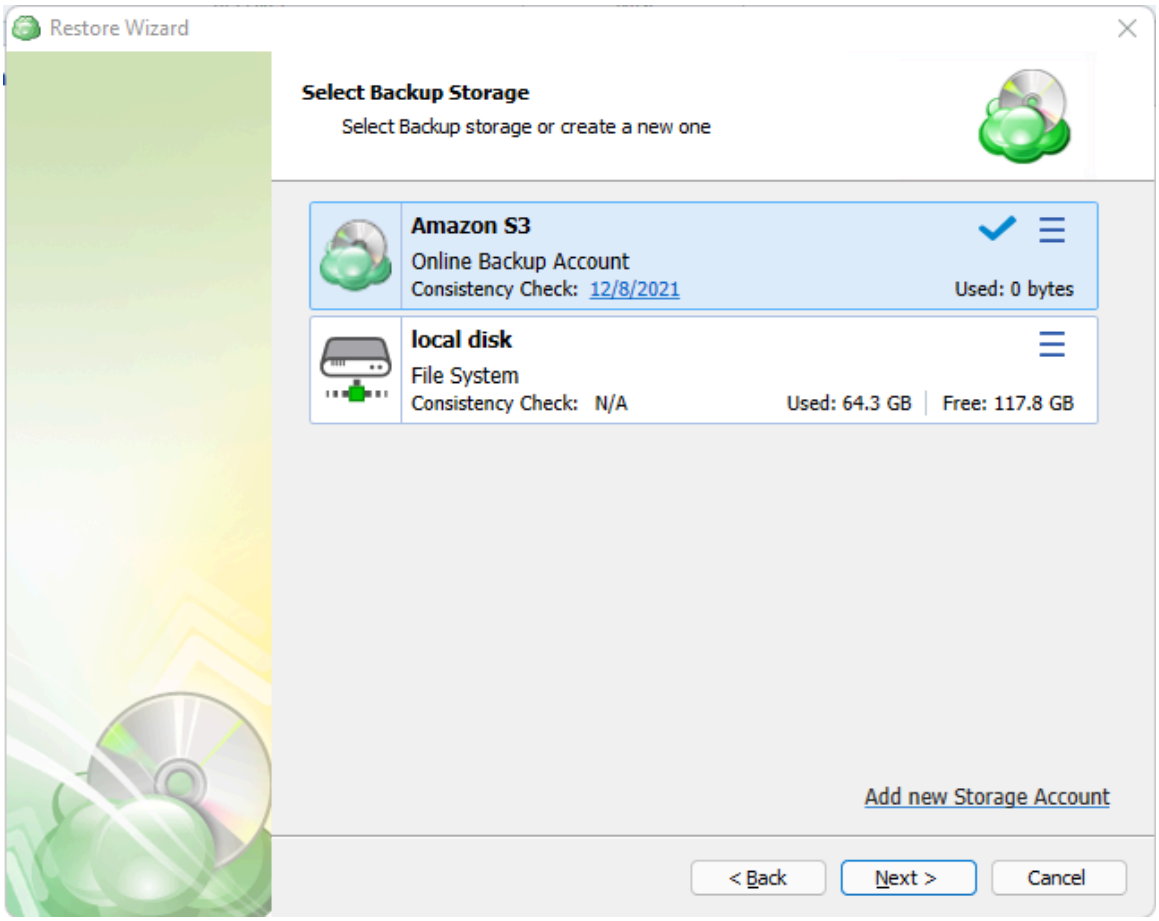
Step 1. Within the Online Backup Agent, click on “Restore”



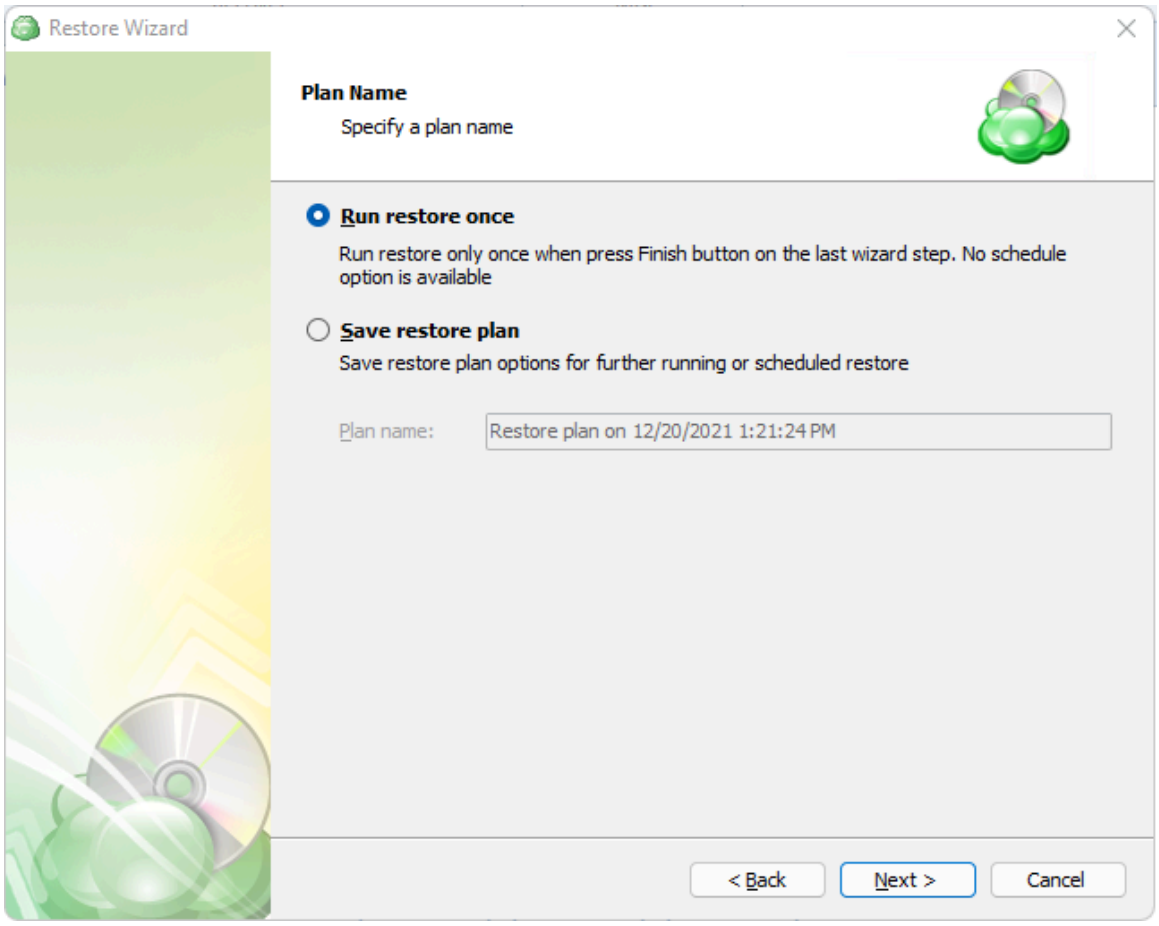
Step 2. Once the wizard starts, click on Next to advance to the next step.



Step 3. The next step will prompt you to select the source for the restore source.



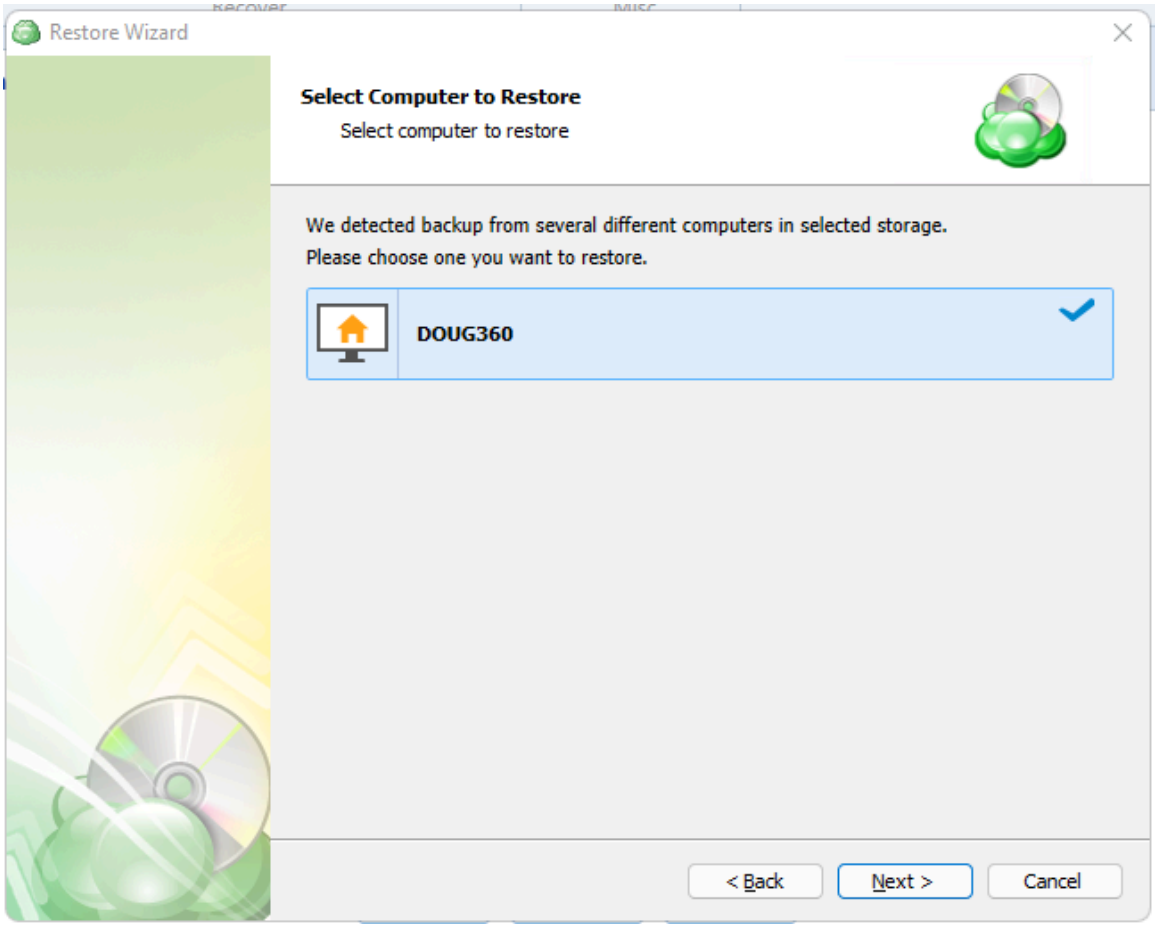
Step 4. Next, you will be given the option to either run the restore once or to save it to run later.



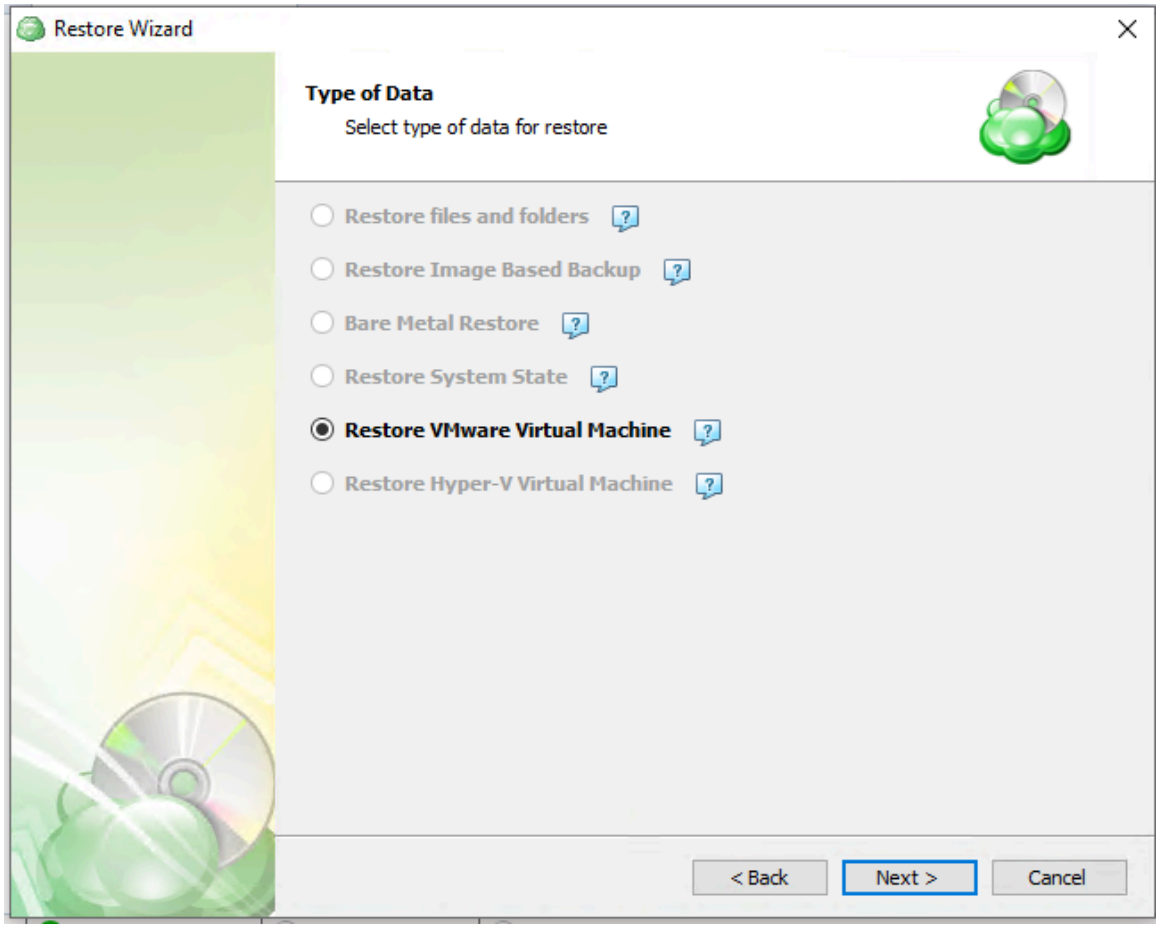
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

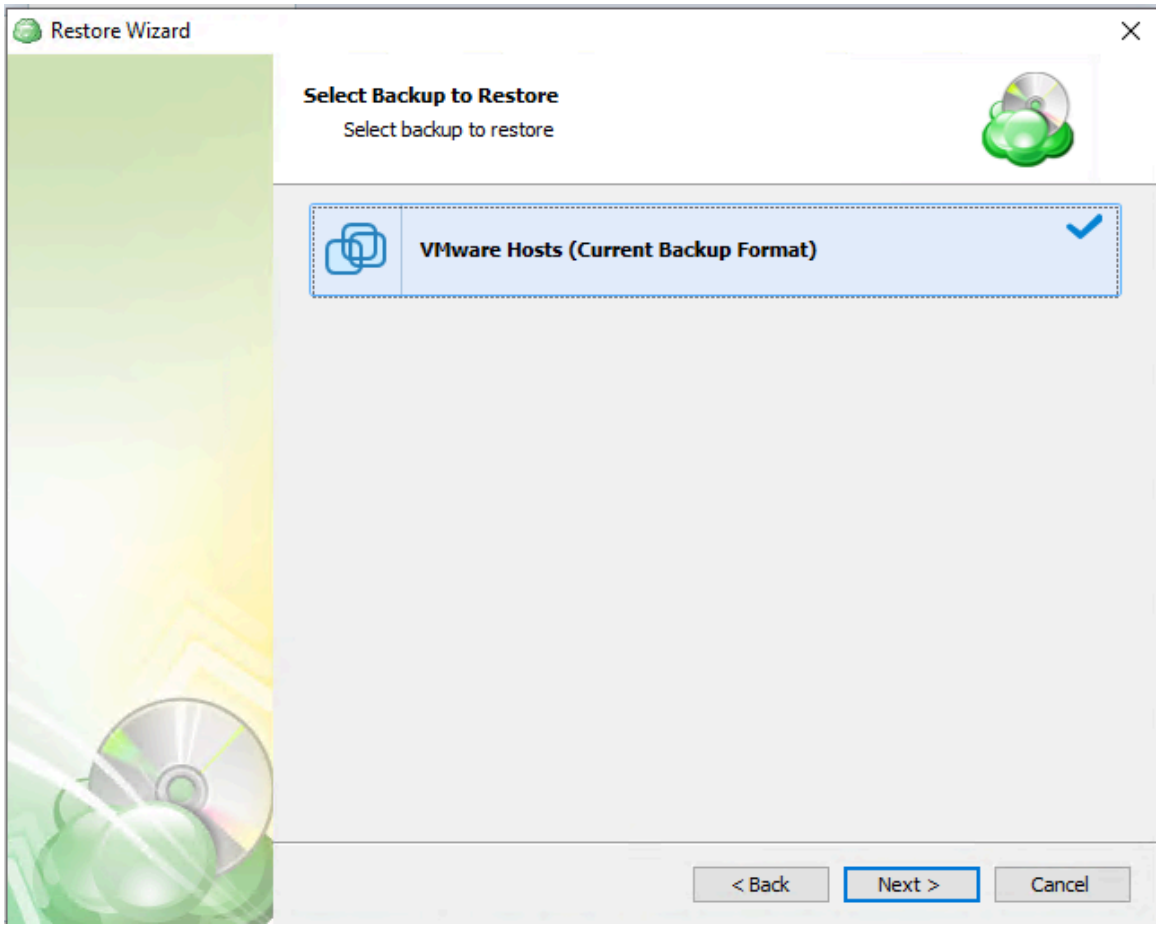
Step 5. With the type of restore selected, the next step is to select the correct Host server which the VM resides on.



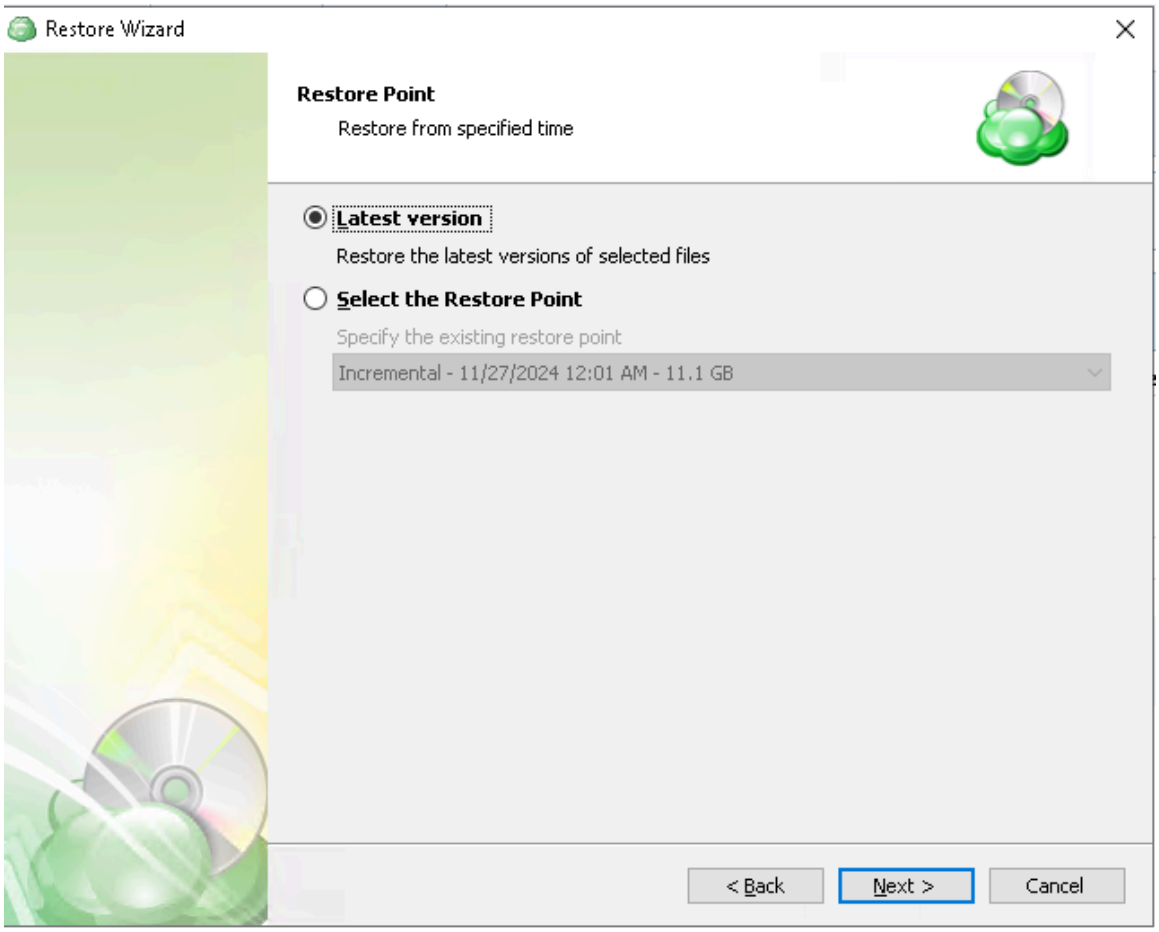
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore VMware Virtual Machine” option to continue.



Step 7. With the correct type of data selected, the application will generate a list of available VM backup plans.

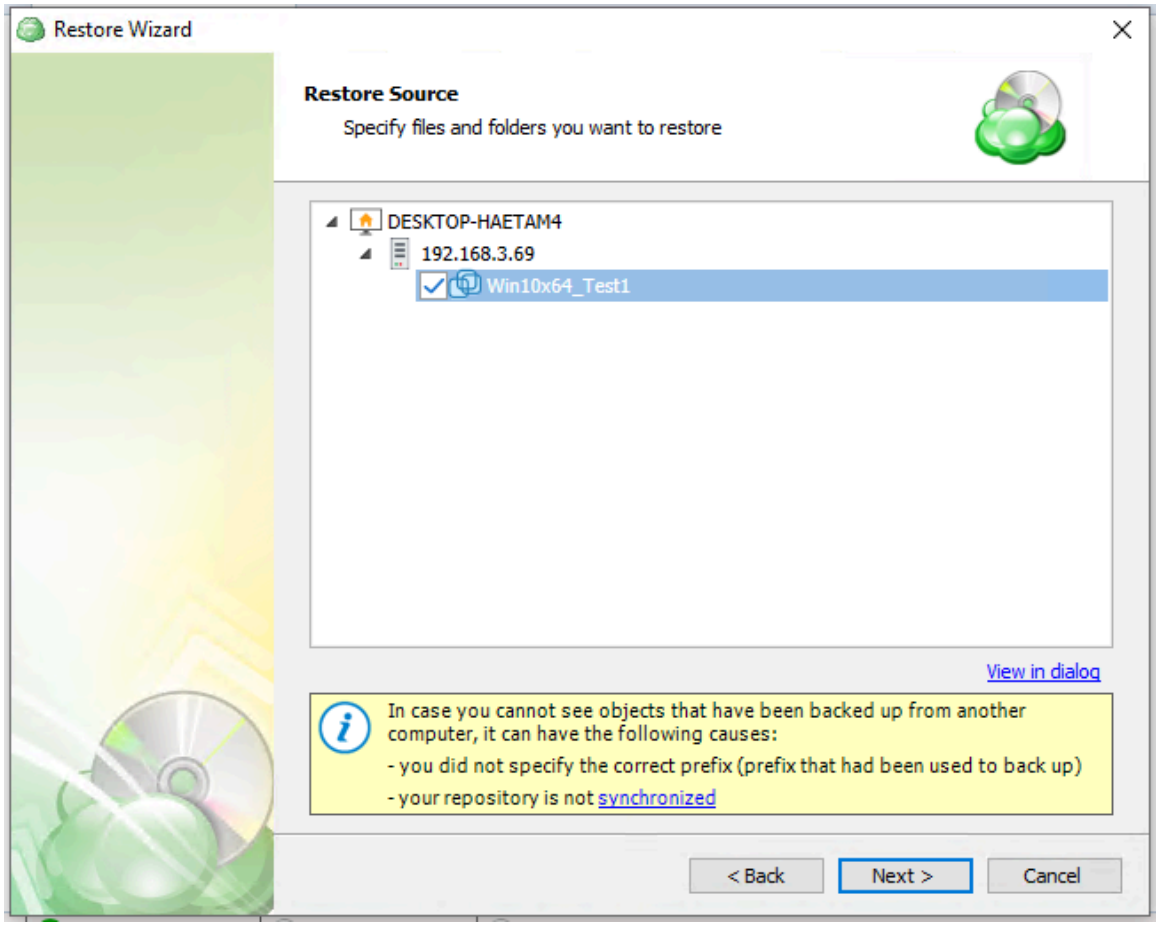


Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.



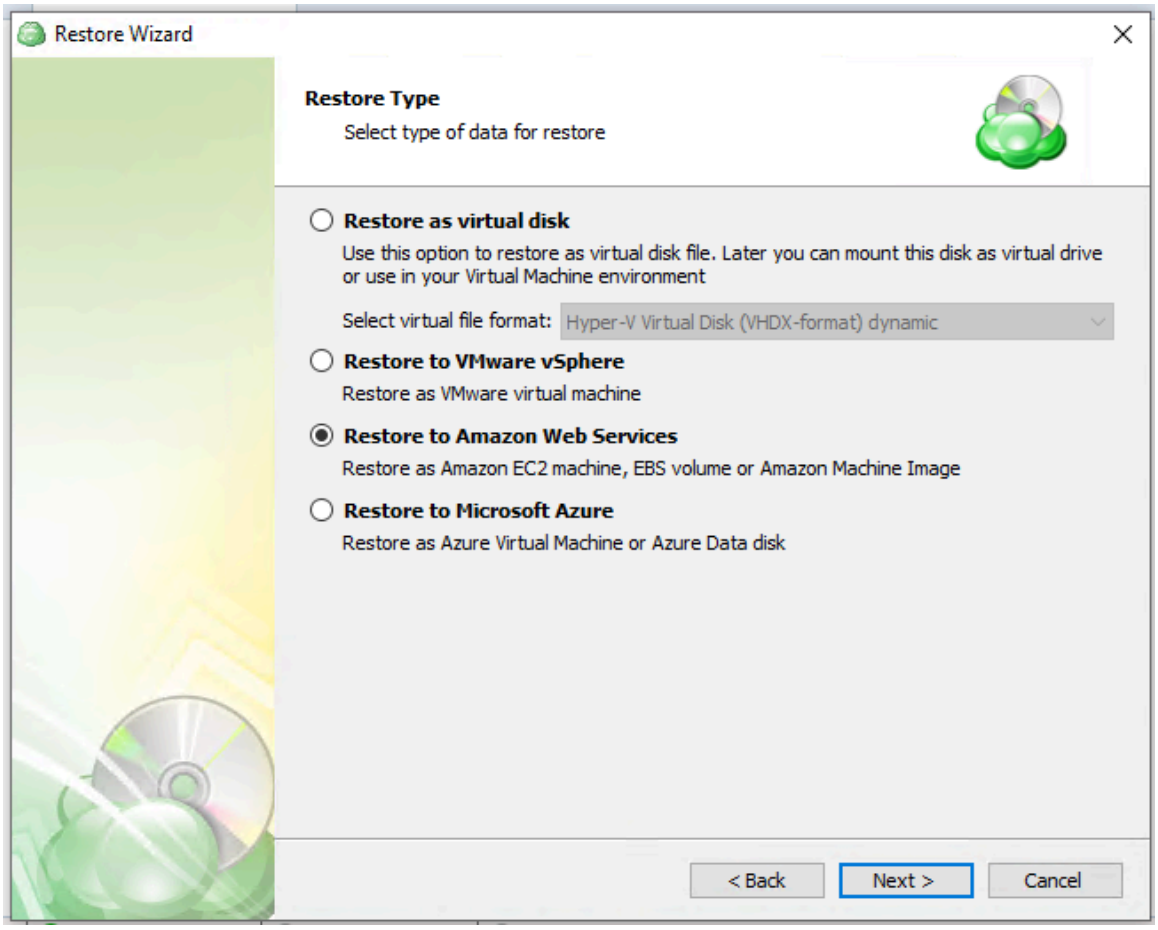
If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which to restore.

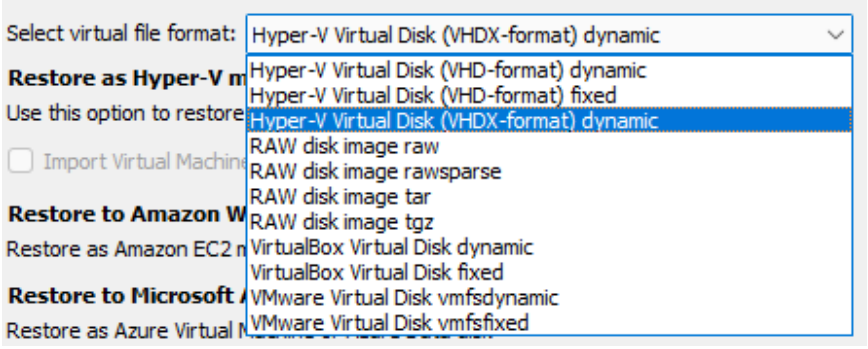


If backed-up objects are missing, ensure the correct **prefix** is specified (the same one used for backup) and verify that the **repository is synchronized** to update available backups.

Step 10. The next step of the wizard allows you to choose how the VM data should be restored.



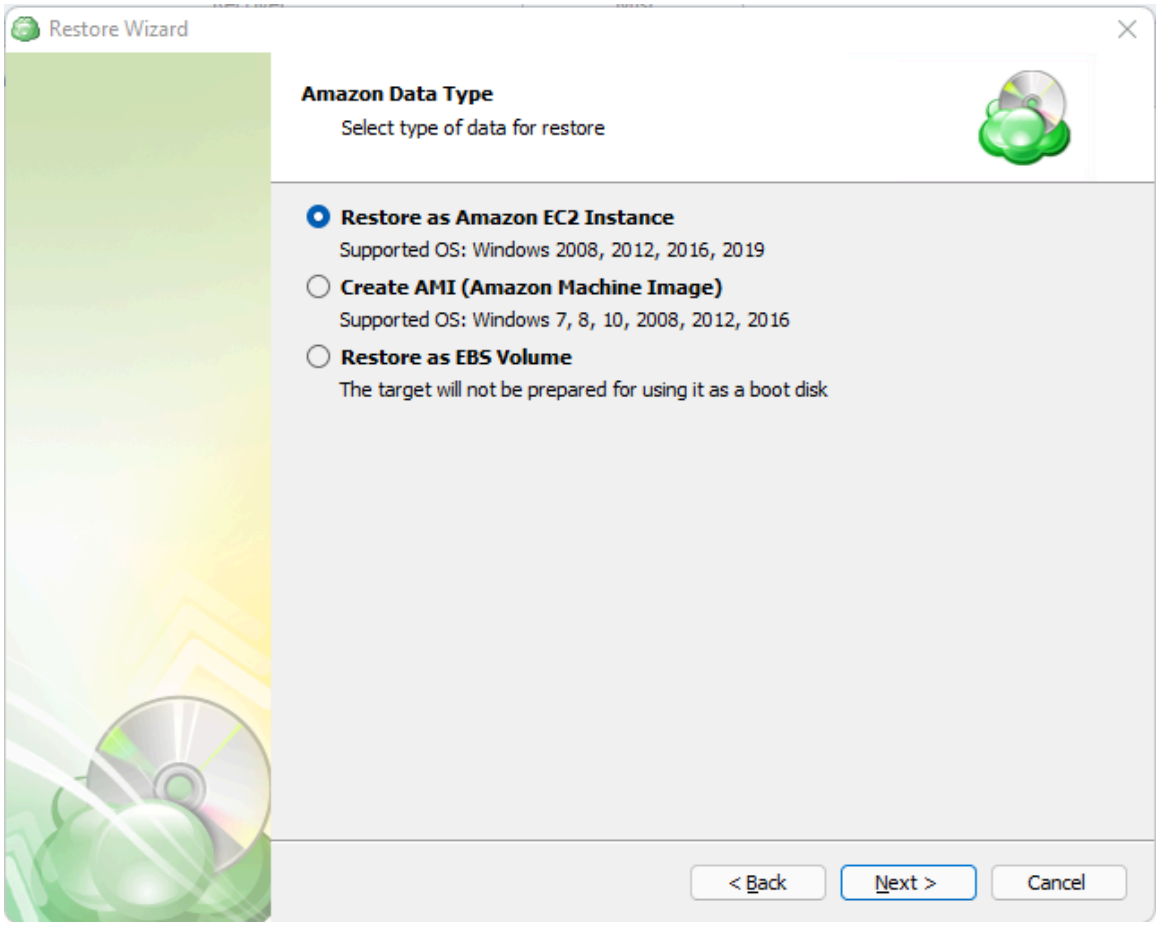
- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:



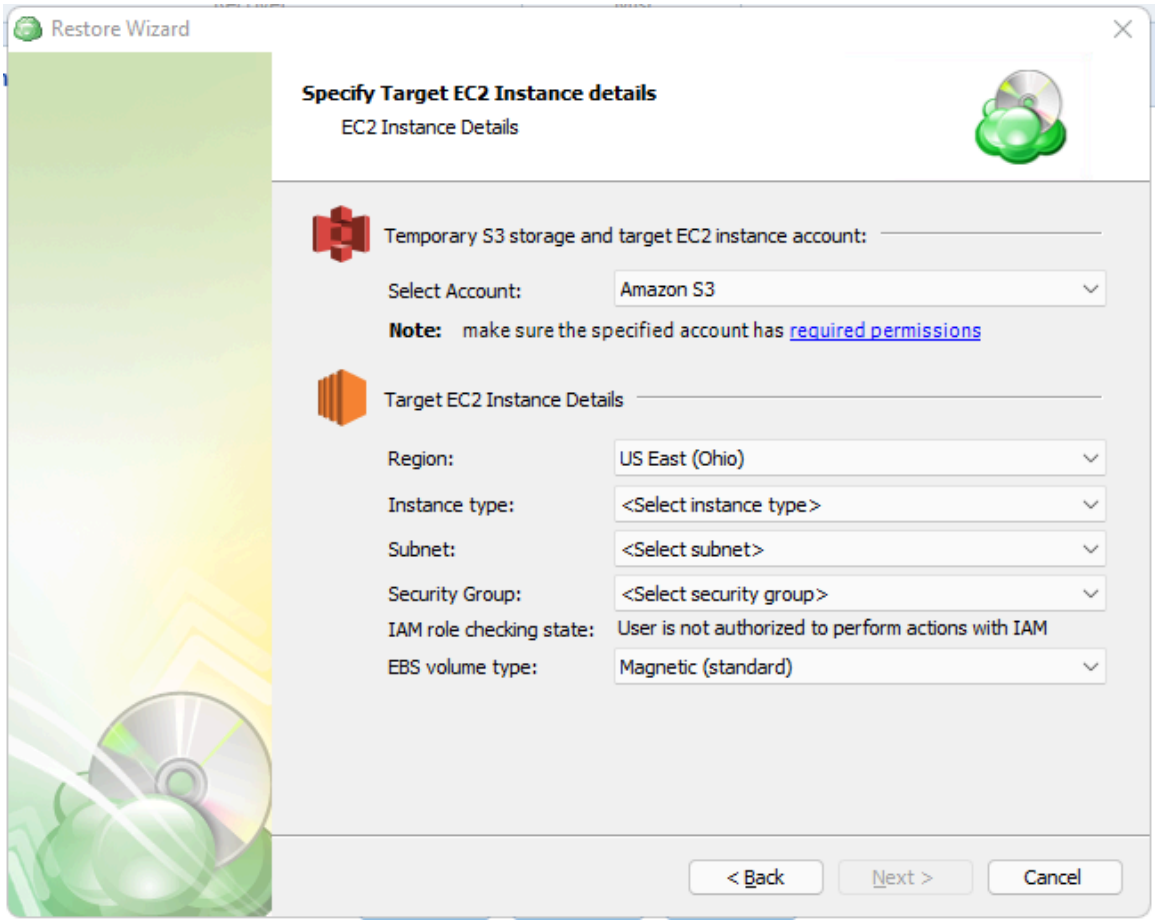
- **Restore to VMware VSphere:** Selecting this option restores the virtual machine configuration as well as the virtual disks to VSphere as a VM.

- **Restore to Amazon Web Services:** If enabled, this will restore the selected VM directly to AWS Cloud either as an EC2 instance, EBS volume, or AMI.
- **Restore to Microsoft Azure:** This will restore the VM directly to Azure as either an Azure Virtual Machine or Azure Data disk.

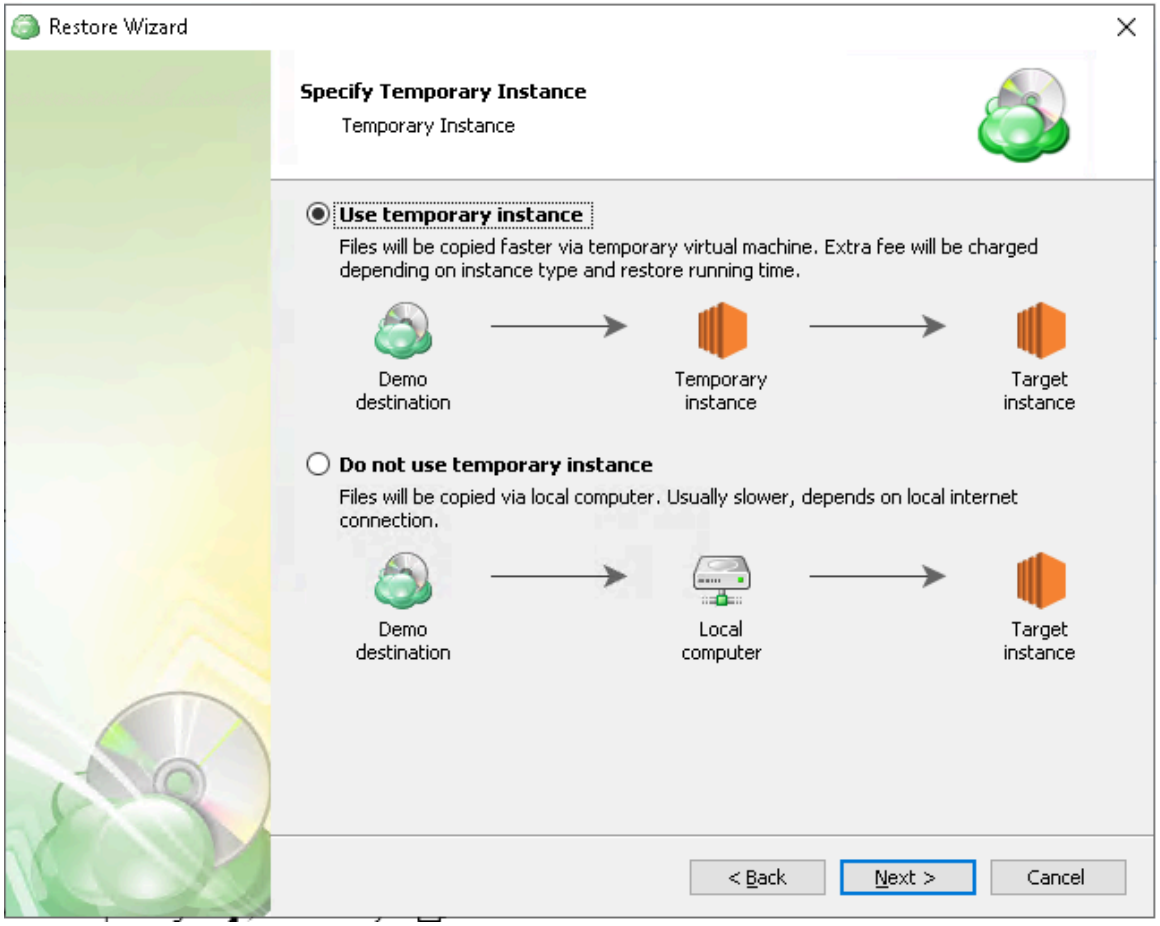
Step 11. With the target selected, you can now specify the type of instance you would like to create in AWS.



Step 12. The next step allows you to select the appropriate Amazon account from the upper dropdown box, and specify the EC2 Instance Details below. These options may vary depending on the type of instance selected in the previous step.

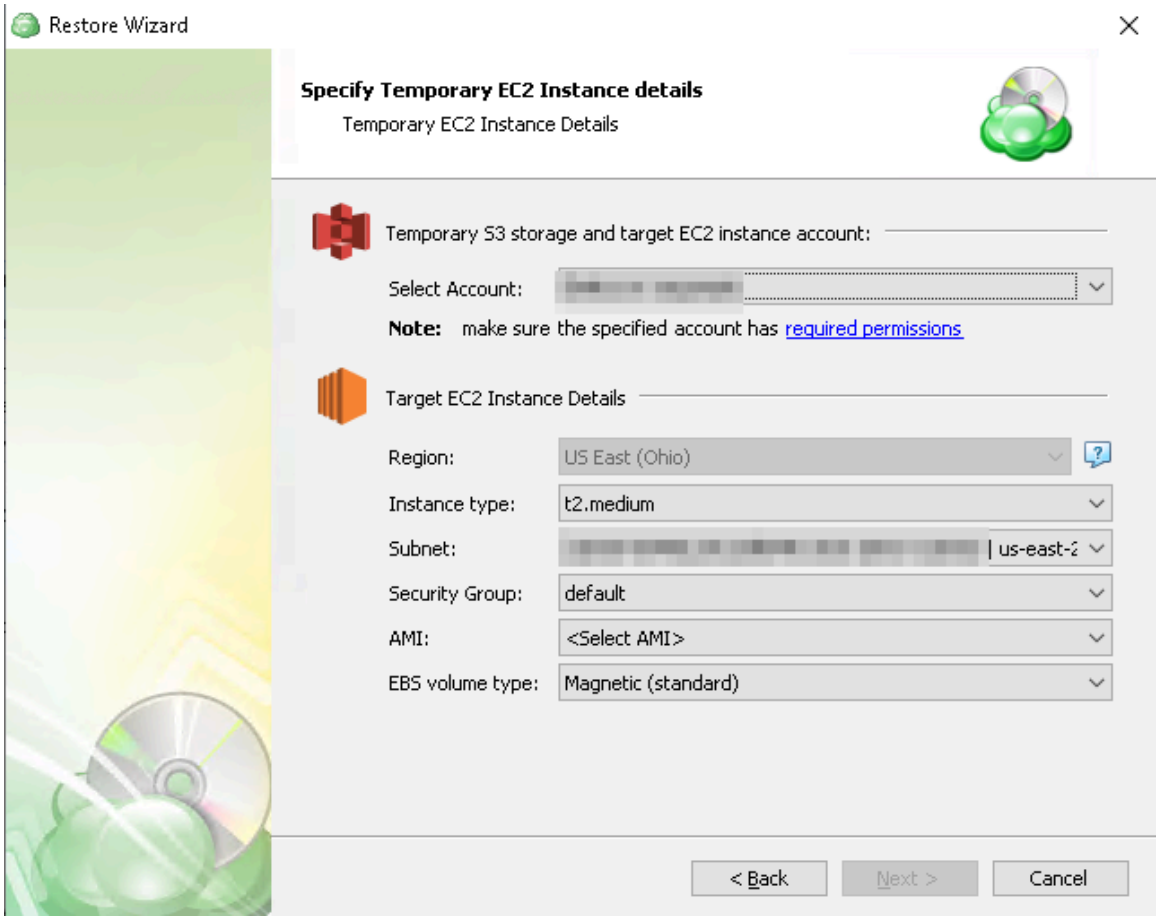


Step 13: After completing the AWS account/Instance details you'll have to choose if use a temporary instance or copy the files locally first.

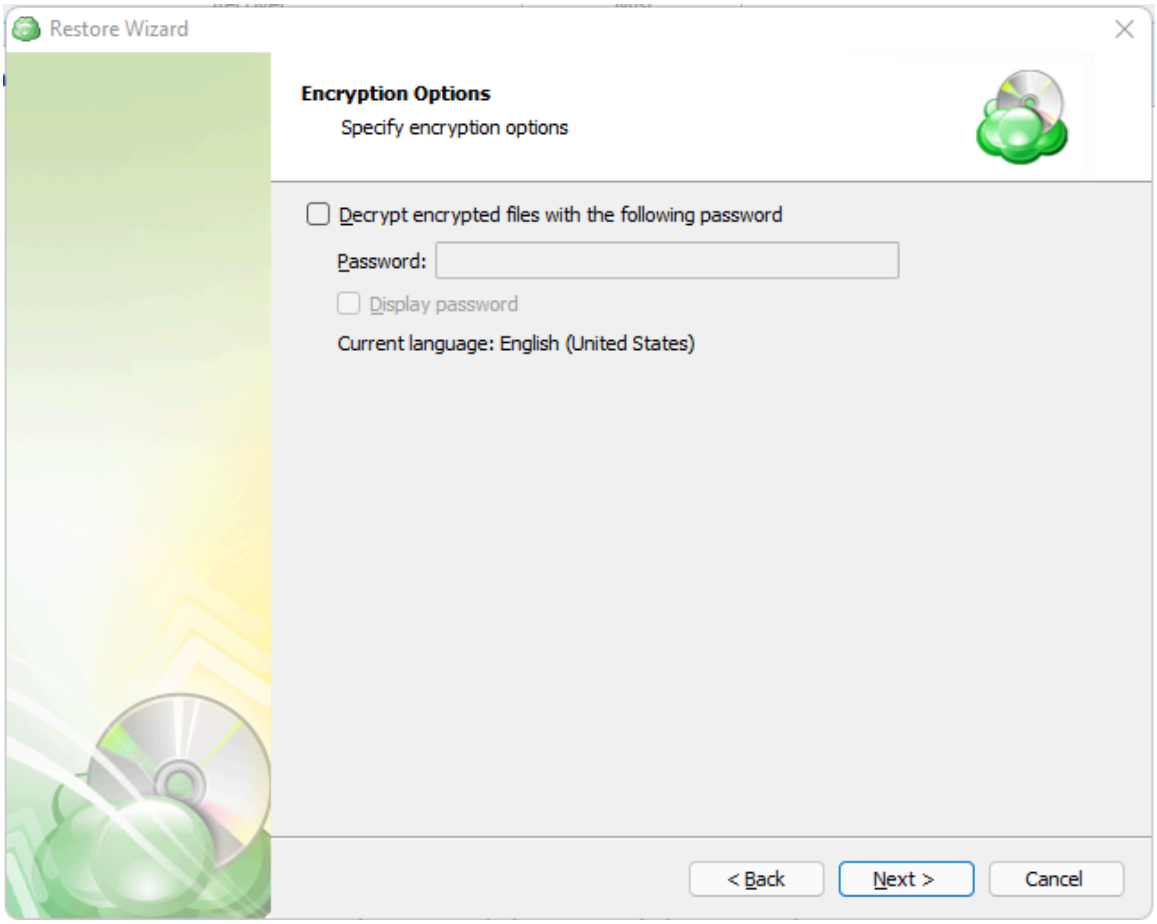


Use a temporary instance for faster cloud-to-cloud restores; avoid it to reduce cloud compute costs at the expense of speed.

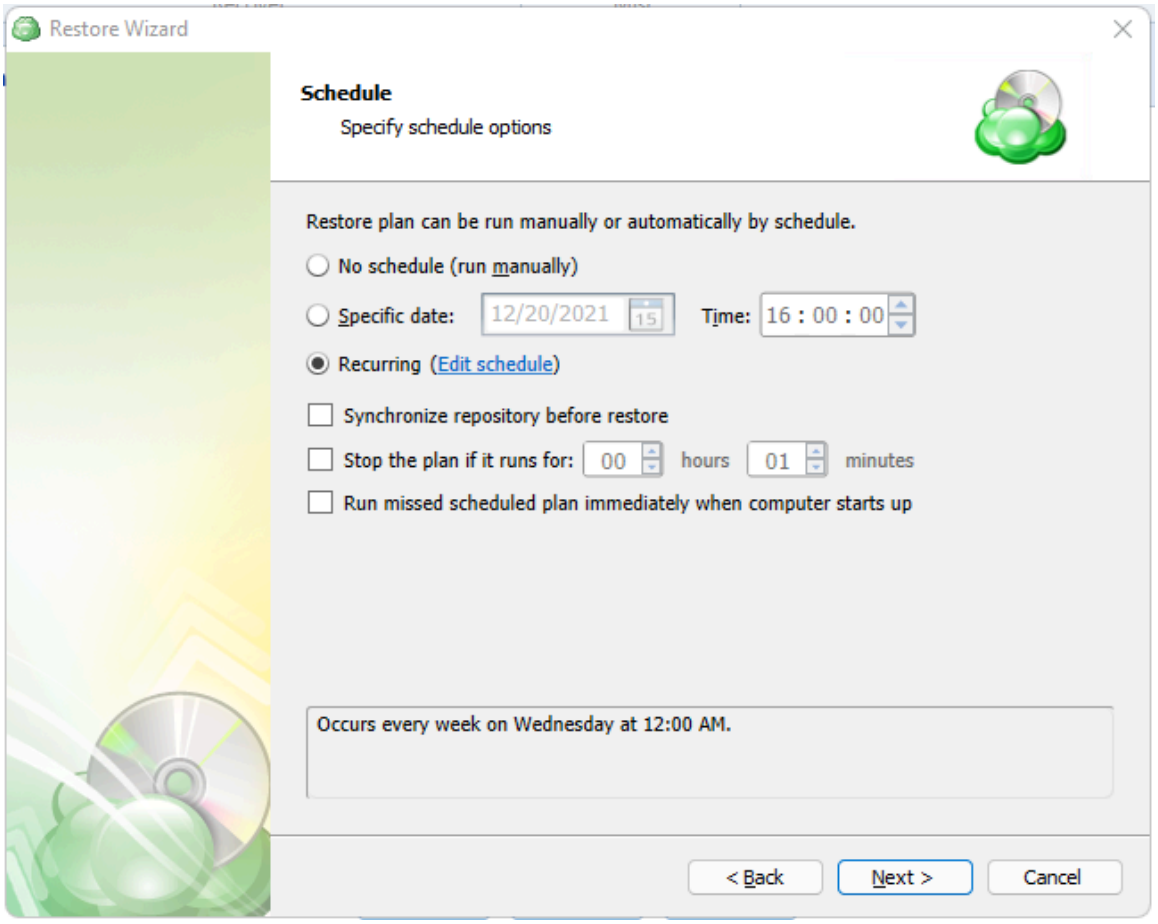
Step 14. If you opt to use a temporary instance, you'll need to specify the AWS Temporary EC2 Instance Details on the next step



Step 15. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the VM.



Step 16. With the decryption password entered, the next step is setting the schedule for the restore plan.

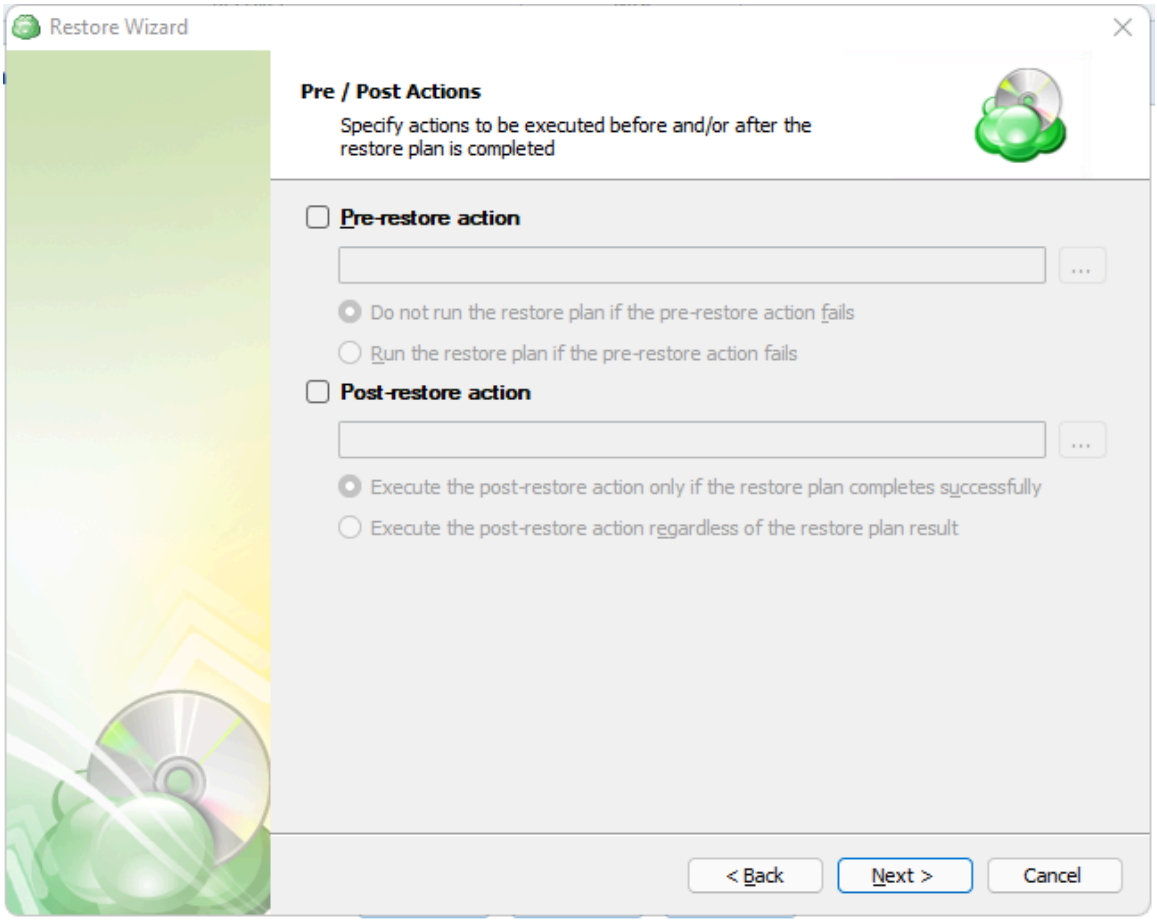


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.
- **Synchronize repository before restore**: Ensures the latest backup data is available before restoring.
- **Stop the plan if it runs for X time**: Automatically stops the restore if it exceeds the specified duration.
- **Run missed scheduled plan immediately when computer starts up**: If the restore was missed due to the system being off, it runs as soon as the computer starts.

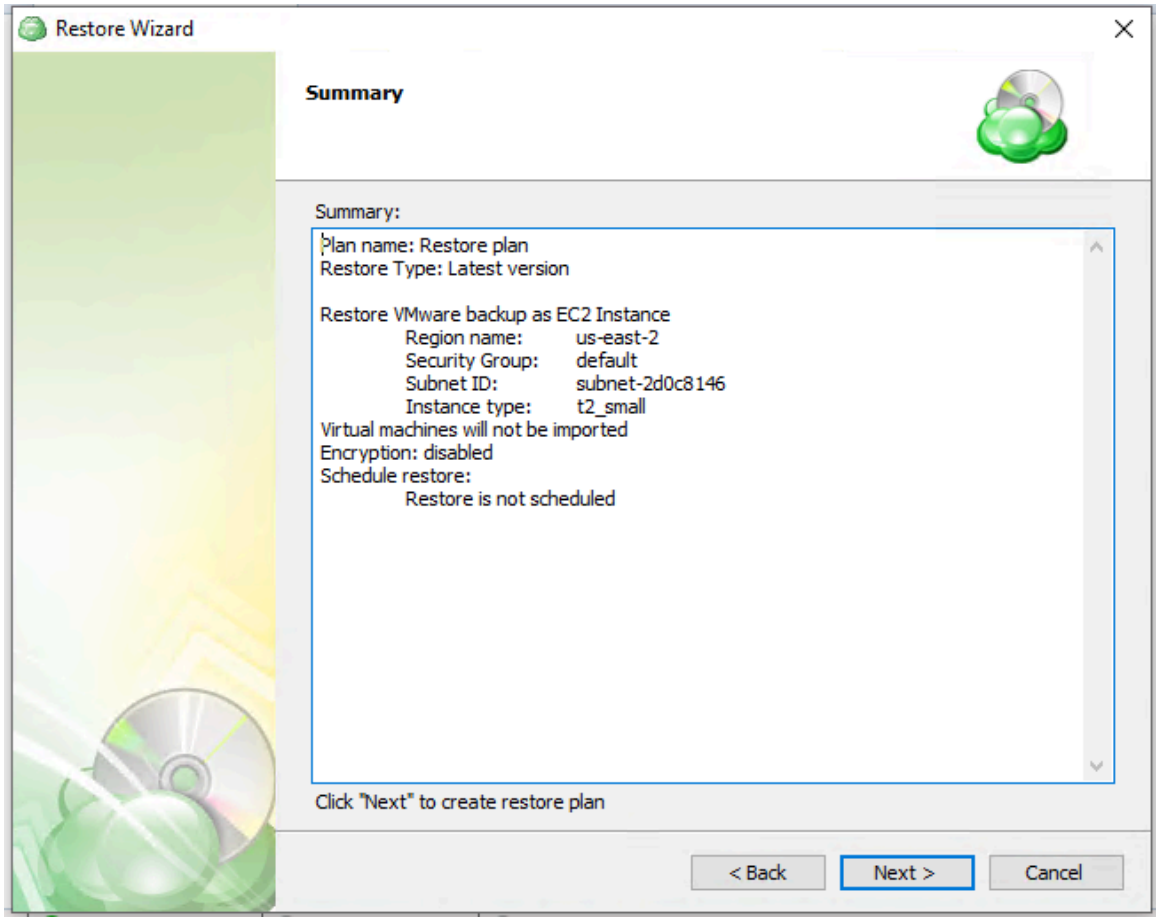
Do not use the “**Stop the plan if it runs for:**” option if you have a slow or unstable internet connection.

Enabling the “**Run missed scheduled restore immediately when computer starts up”** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 17. After setting the schedule, the next step allows pre and post actions to be defined.



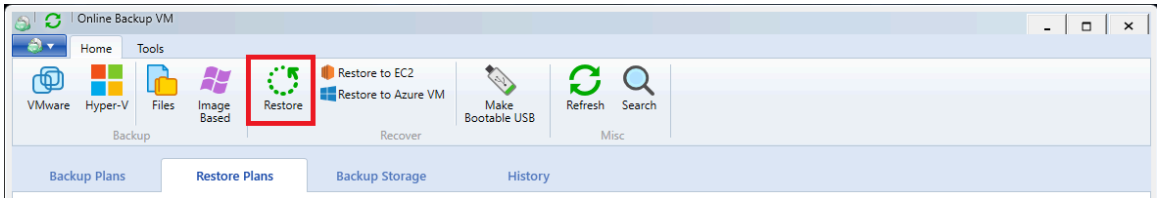
Step 18. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.



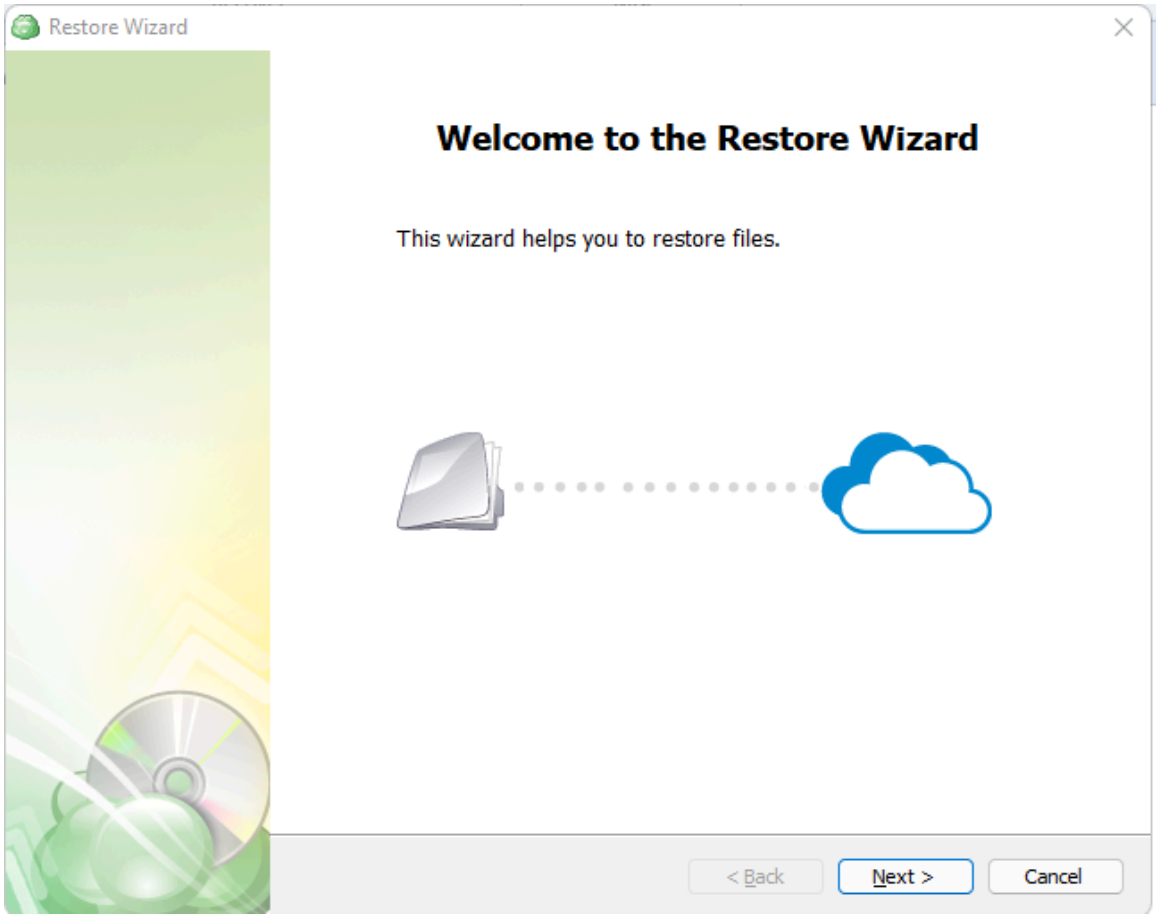
If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

Restore as an Azure VM using the Agent

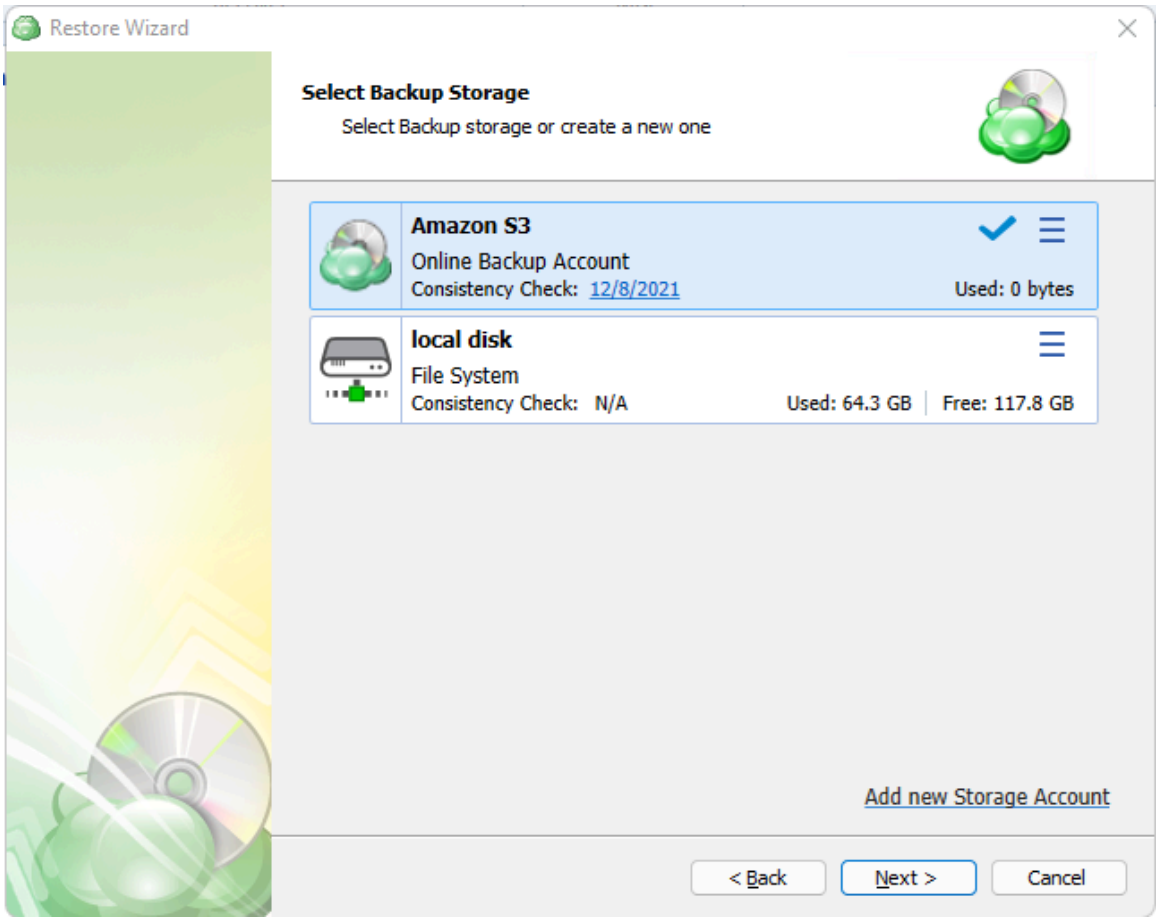
Step 1. Within the Online Backup Agent, click on “Restore”



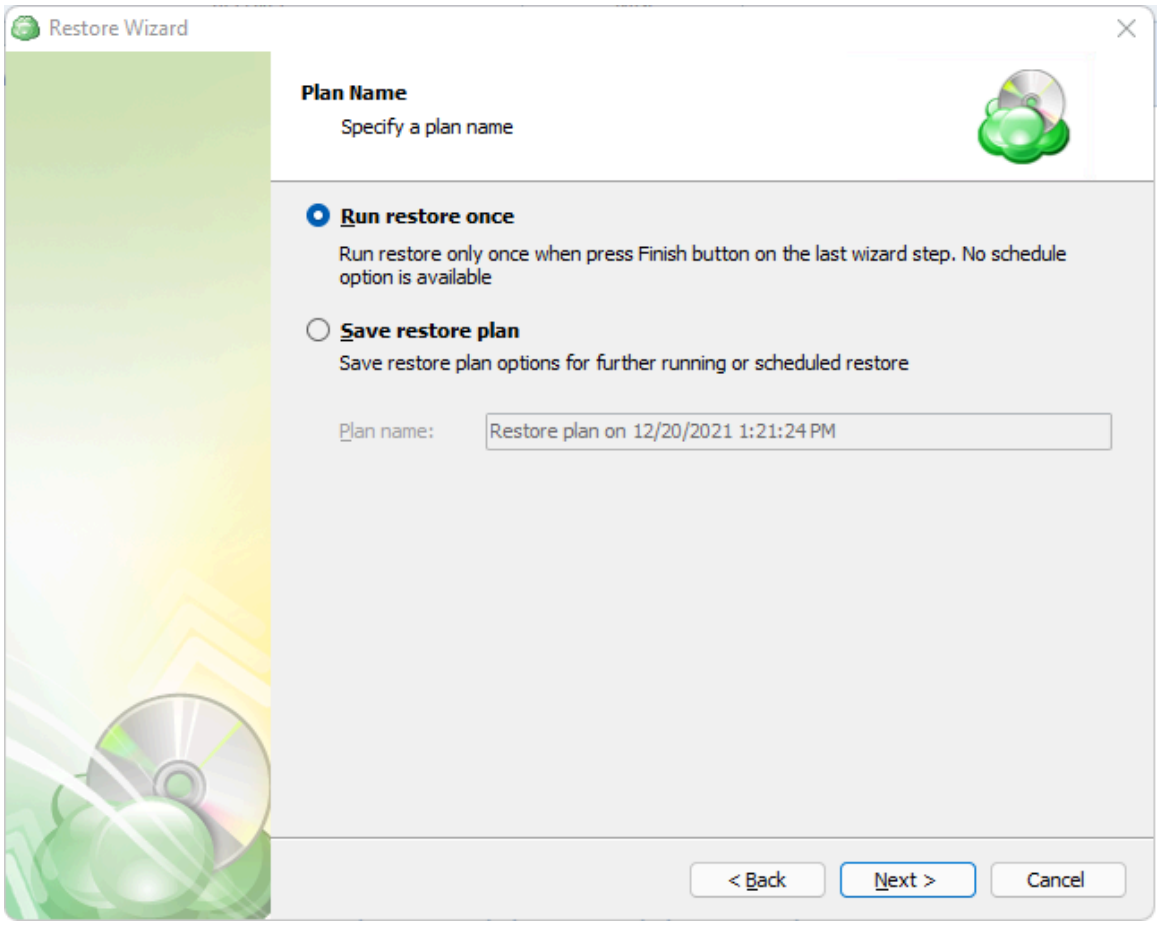
Step 2. Once the wizard starts, click on Next to advance to the next step.



Step 3. The next step will prompt you to select the source for the restore point.



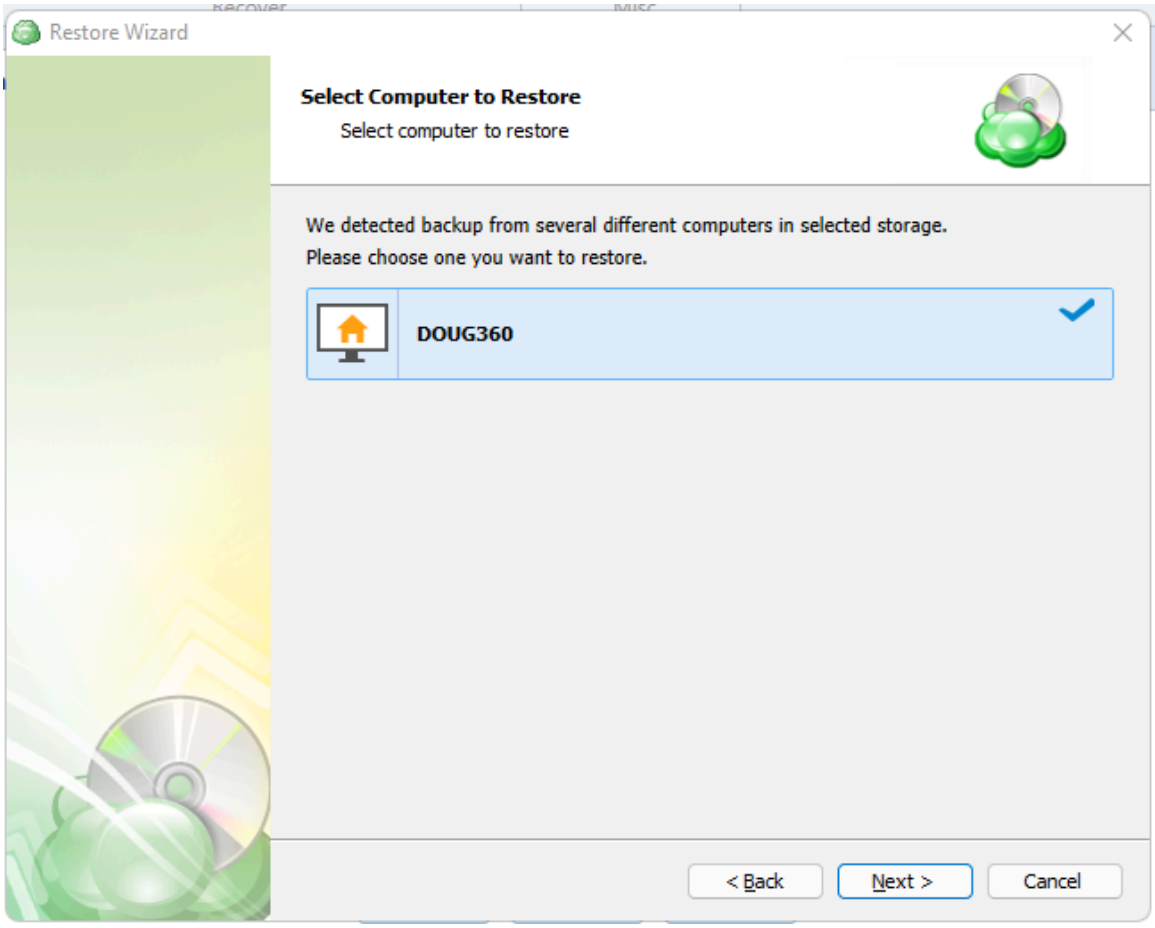
Step 4. Next, you will be given the option to either run the restore once or to save it to run later.



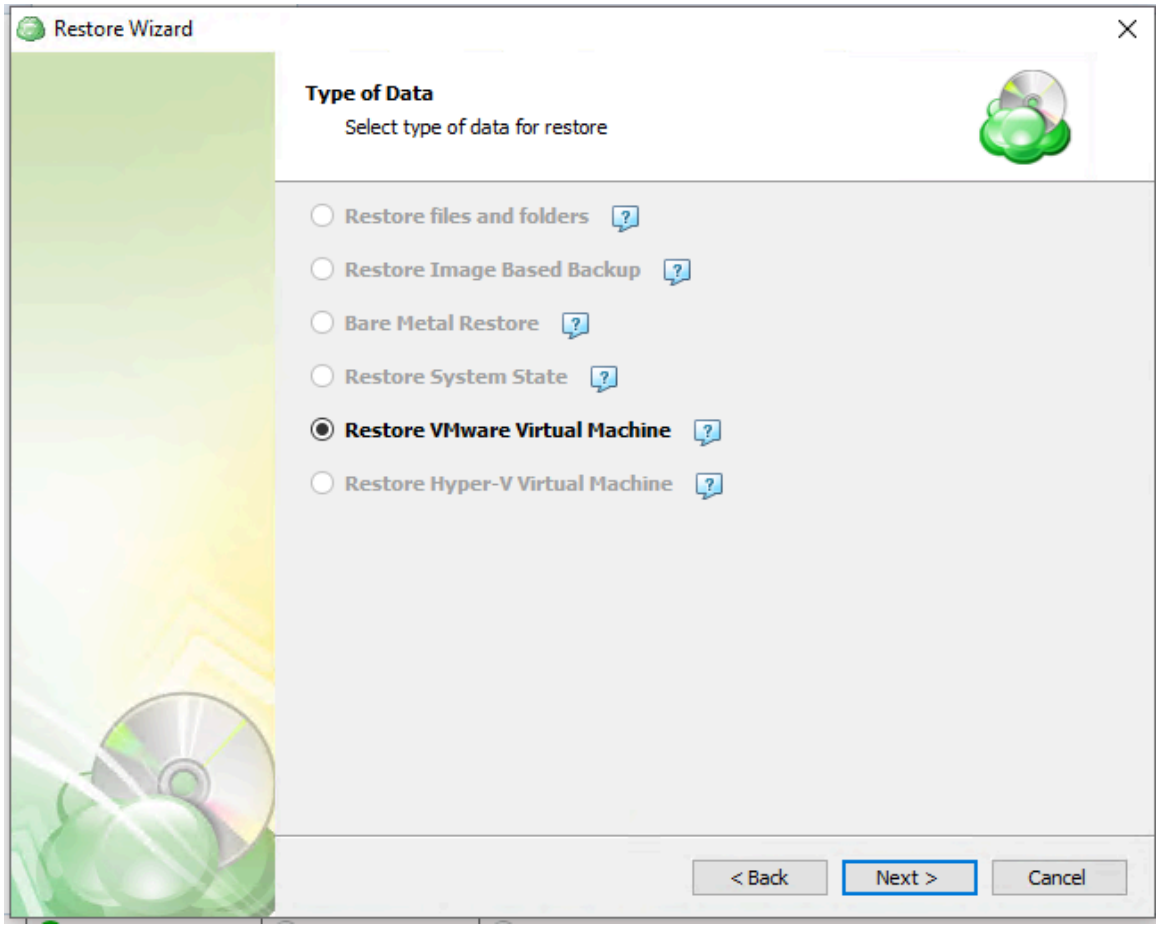
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

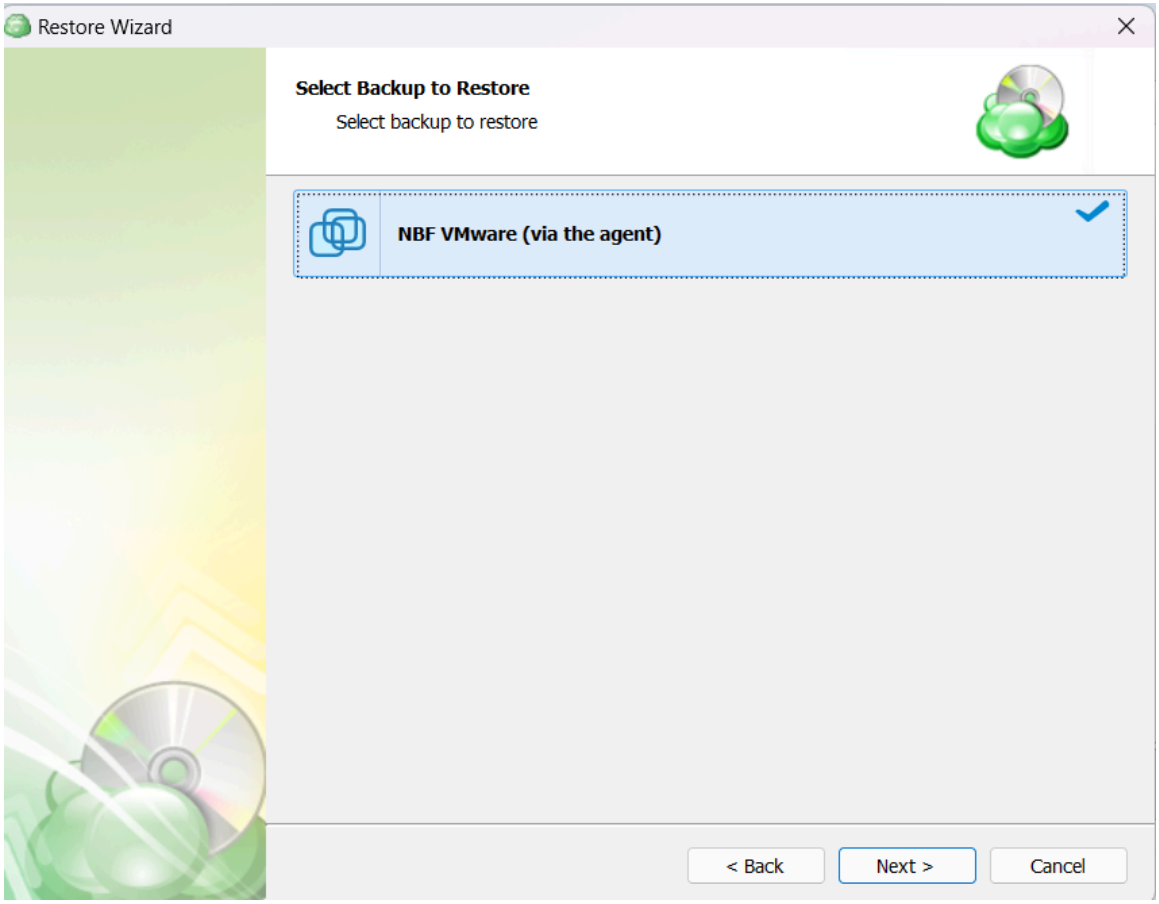
Step 5. With the type of restore selected, the next step is to select the correct Host server which the VM resides on.



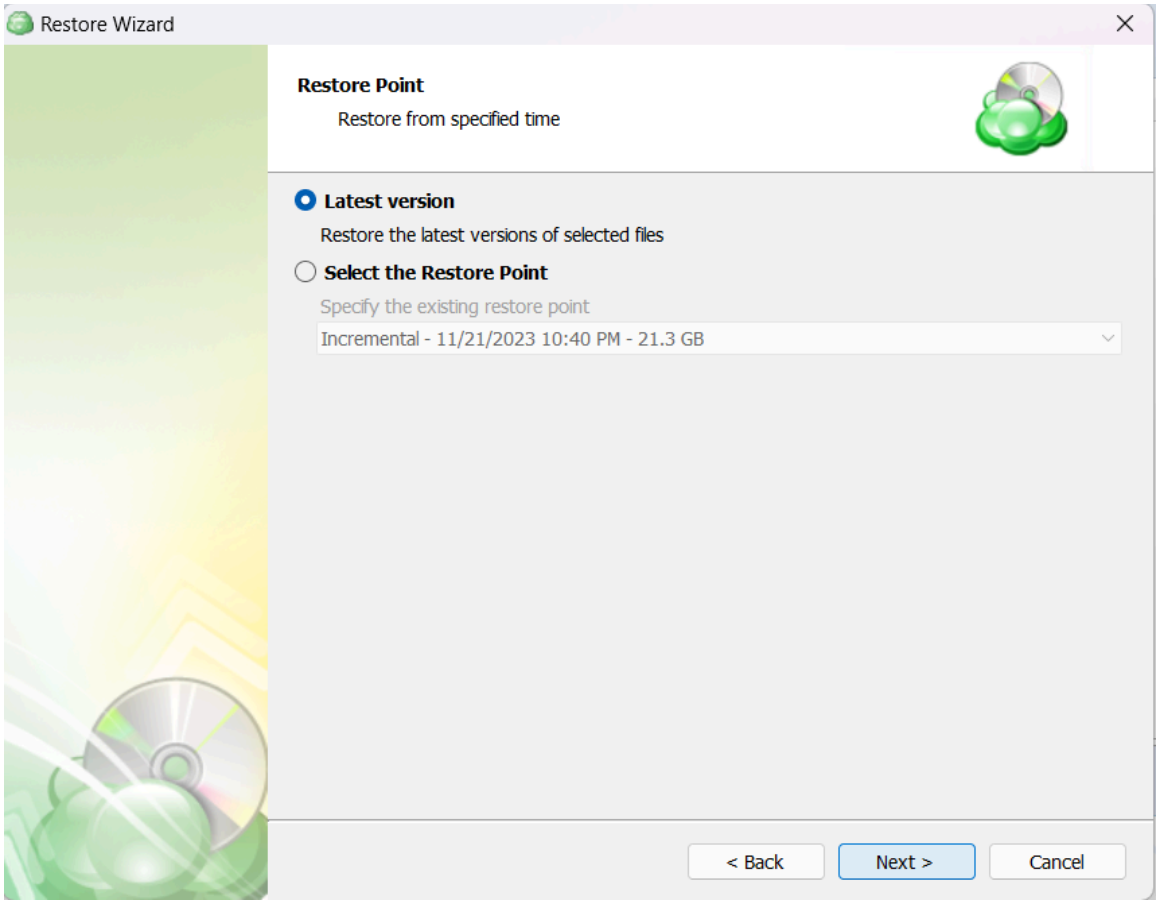
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore VMware Virtual Machine” option to continue.



Step 7. With the correct type of data selected, the application will generate a list of available VM backup plans.

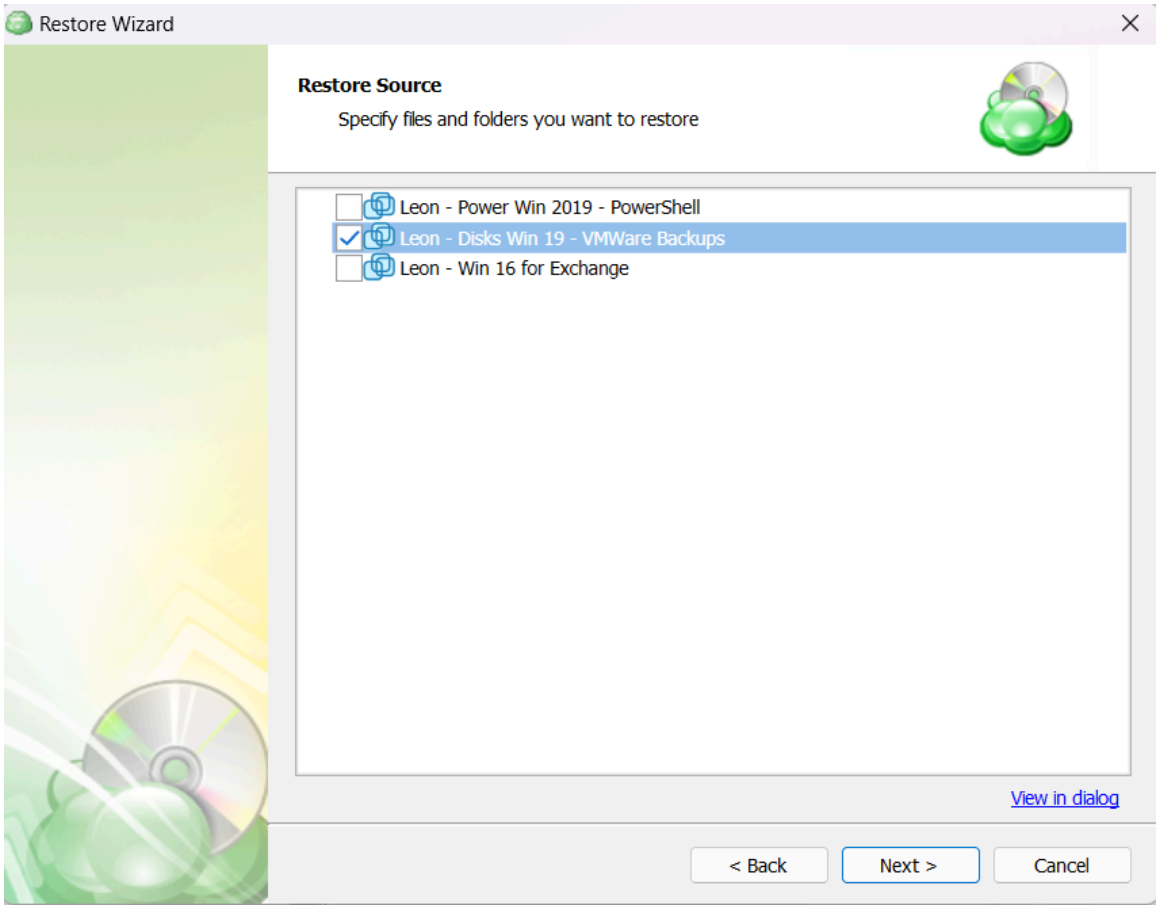


Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.

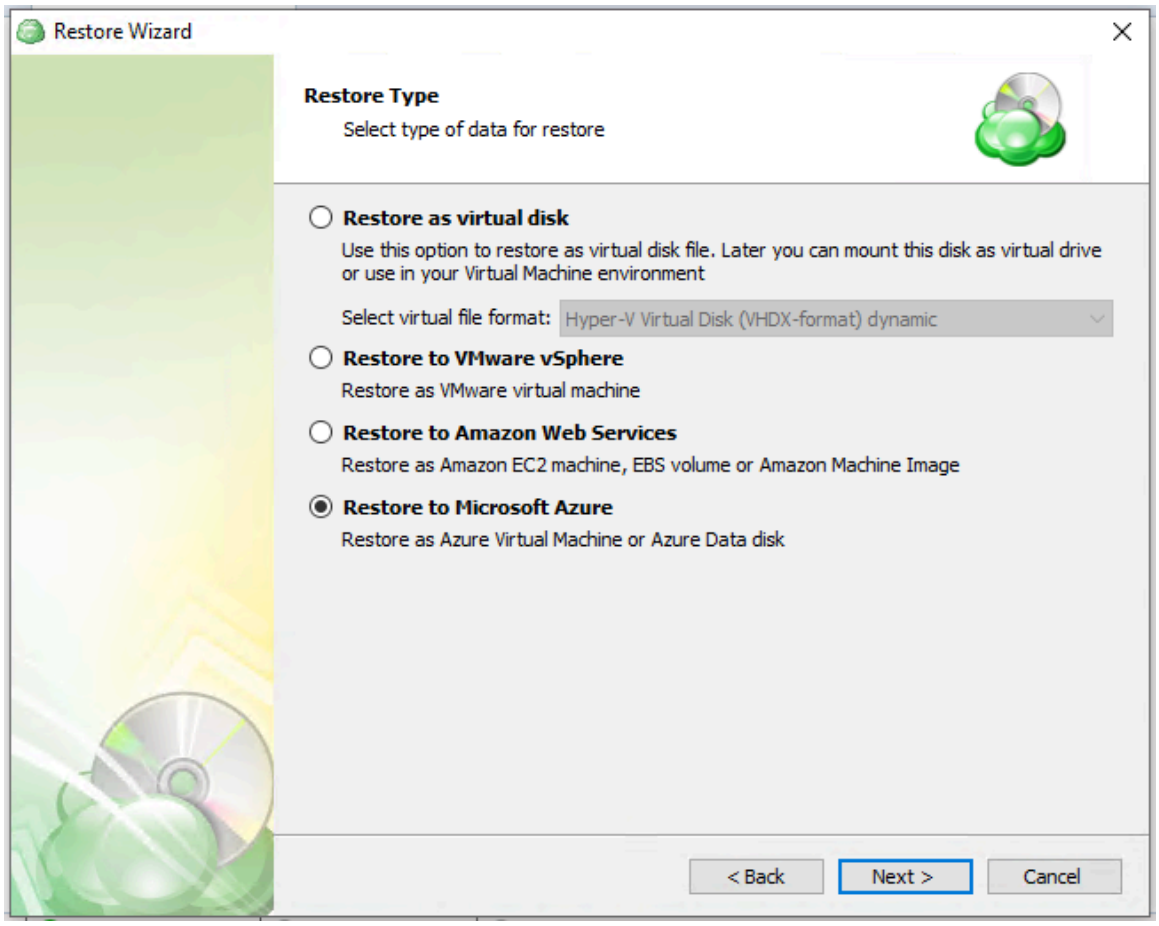


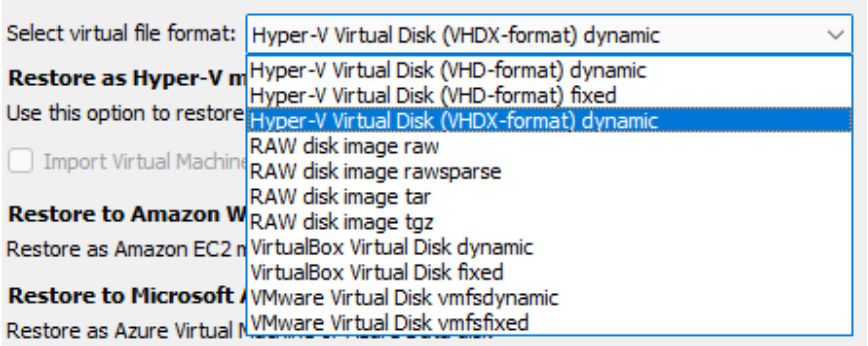
If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which to restore.



Step 10. The next step of the wizard allows you to choose how the VM data should be restored.

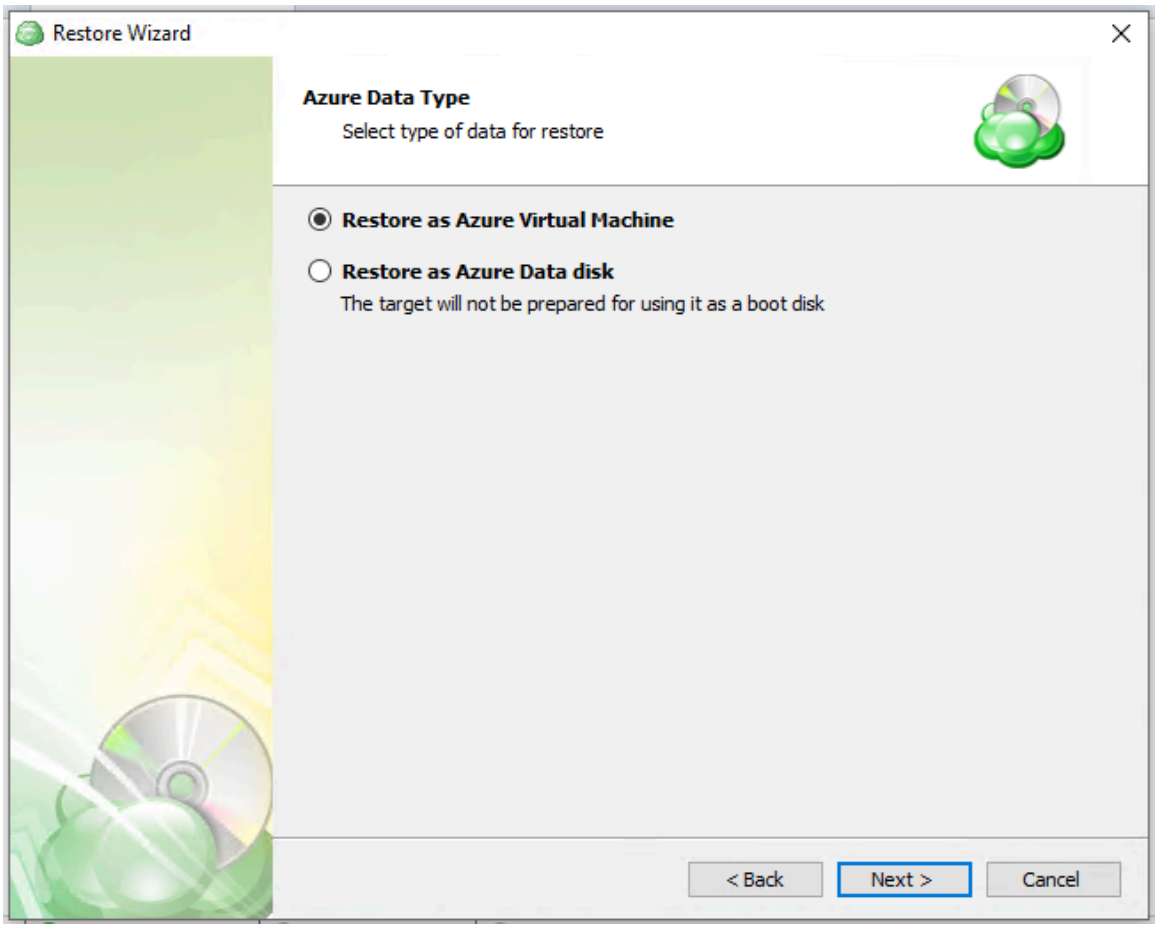


- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:
  - 

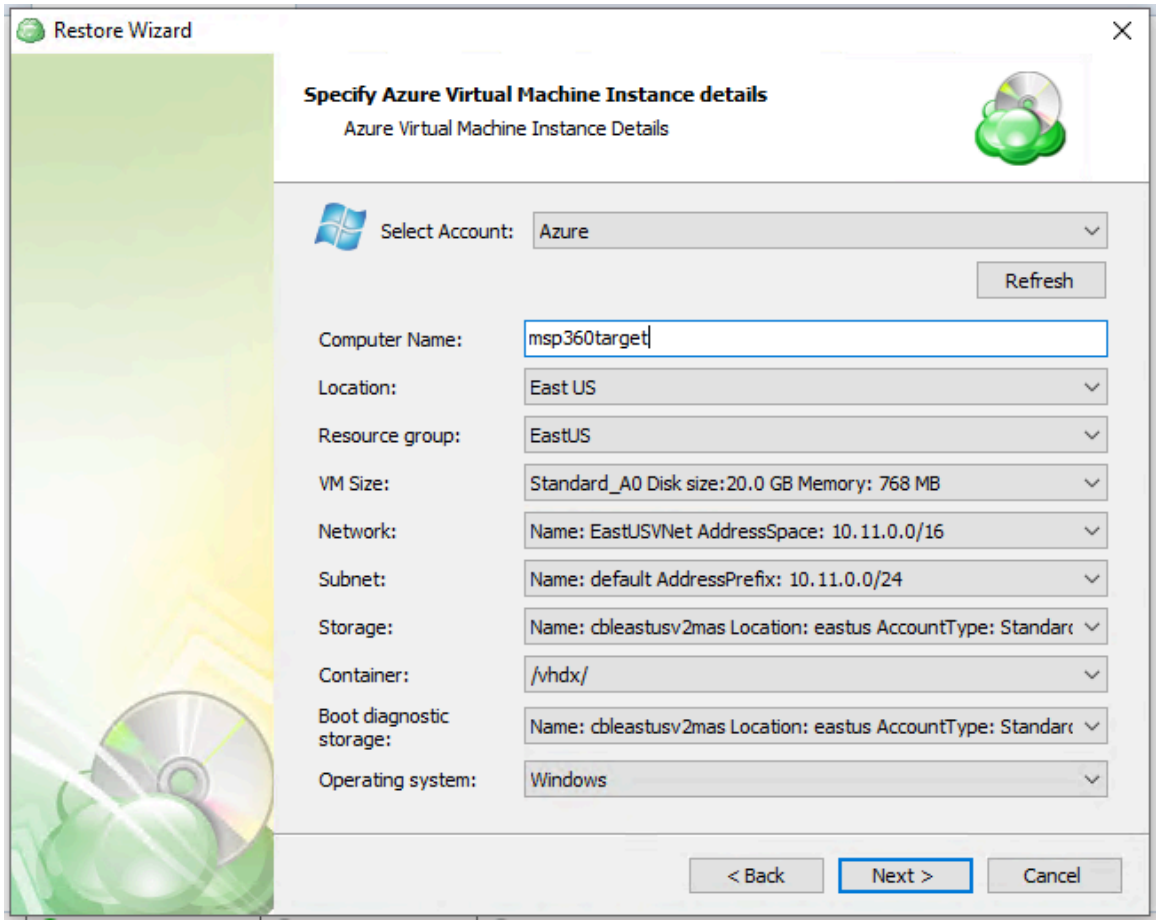
- **Restore to VMware VSphere:** Selecting this option restores the virtual machine configuration as well as the virtual disks to VSphere as a VM.

- **Restore to Amazon Web Services:** If enabled, this will restore the selected VM directly to AWS Cloud either as an EC2 instance, EBS volume, or AMI.
- **Restore to Microsoft Azure:** This will restore the VM directly to Azure as either an Azure Virtual Machine or Azure Data disk.

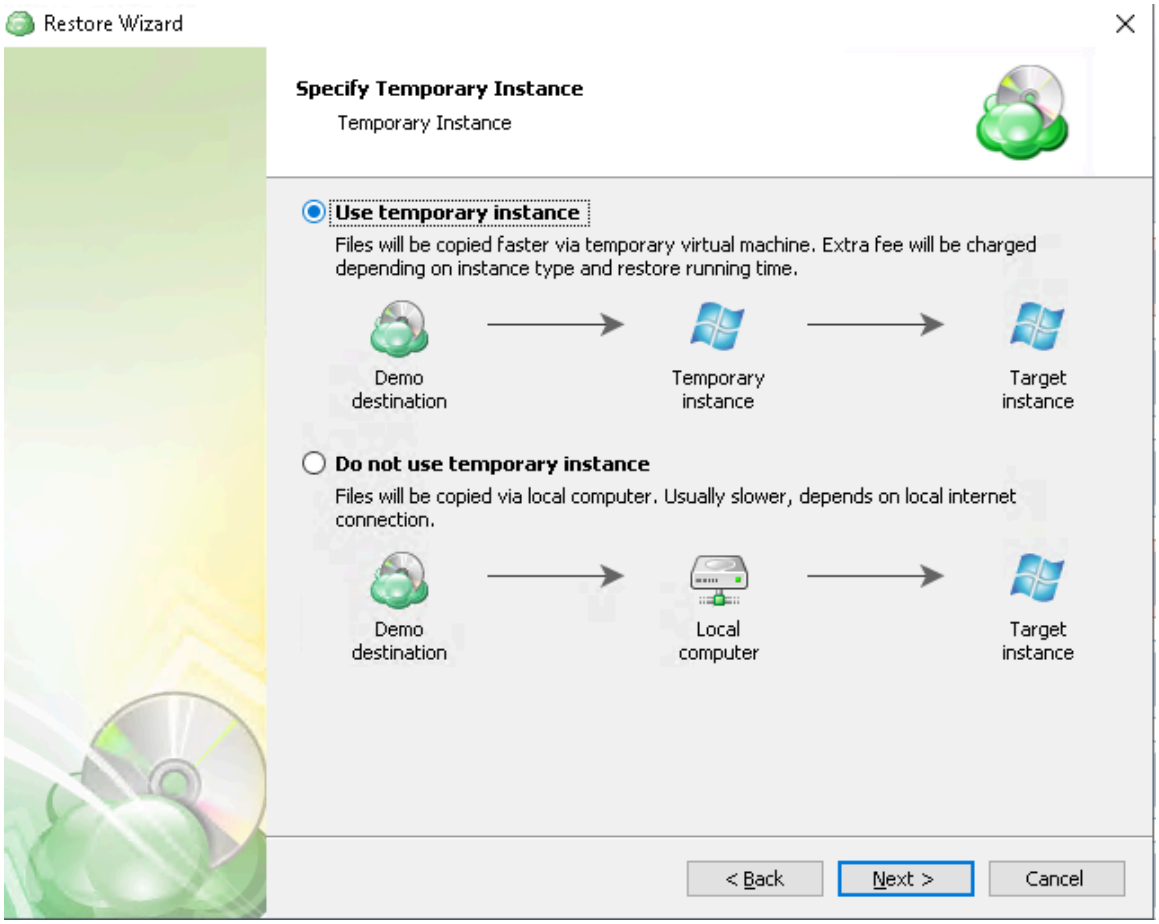
Step 11. With the target selected, you can now specify the type of instance you would like to create in Azure.



Step 12. The next step allows you to select the appropriate Azure account from the upper dropdown box, and specify the configuration below. These options may vary depending on the type of instance selected in the previous step.

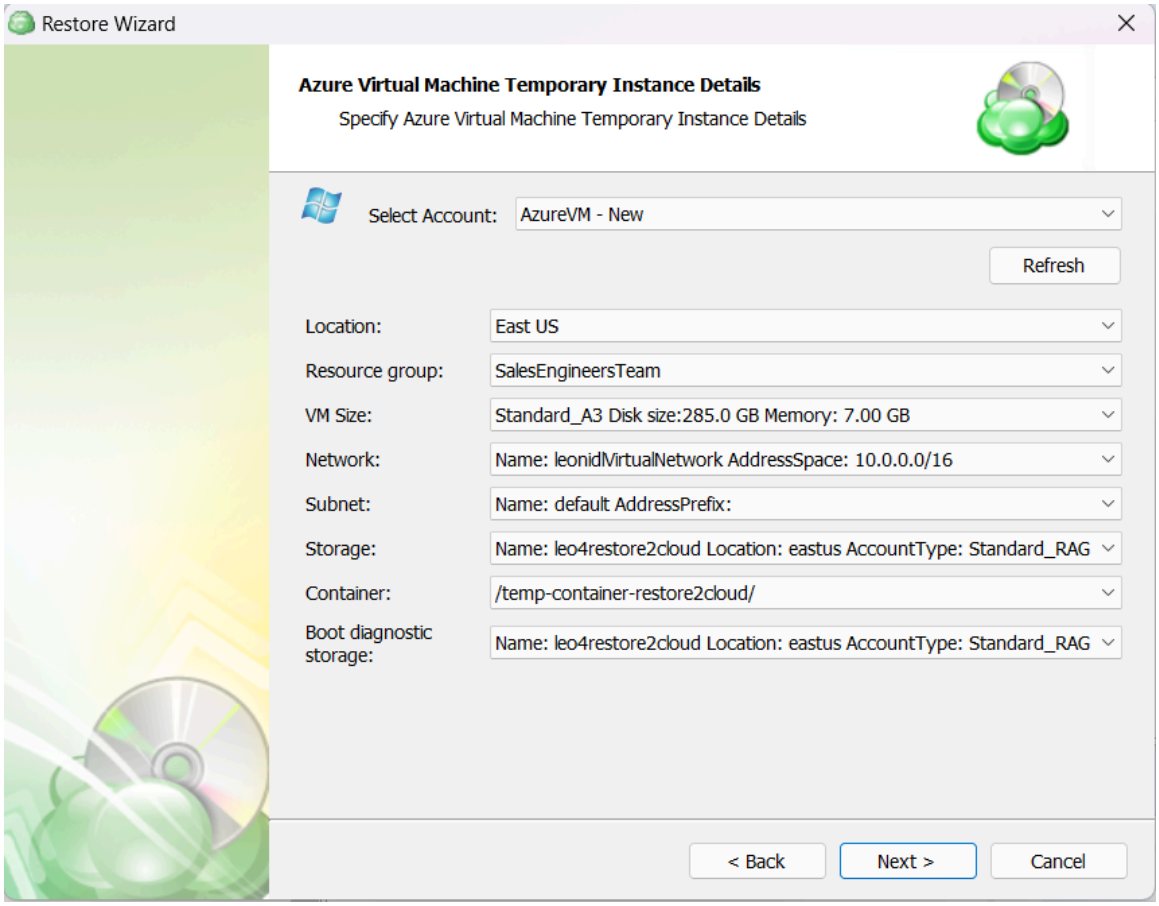


Step 13: After completing the Azure Virtual Machine or Azure Data Disk details, you'll have to choose to use a temporary instance or copy the files locally first.

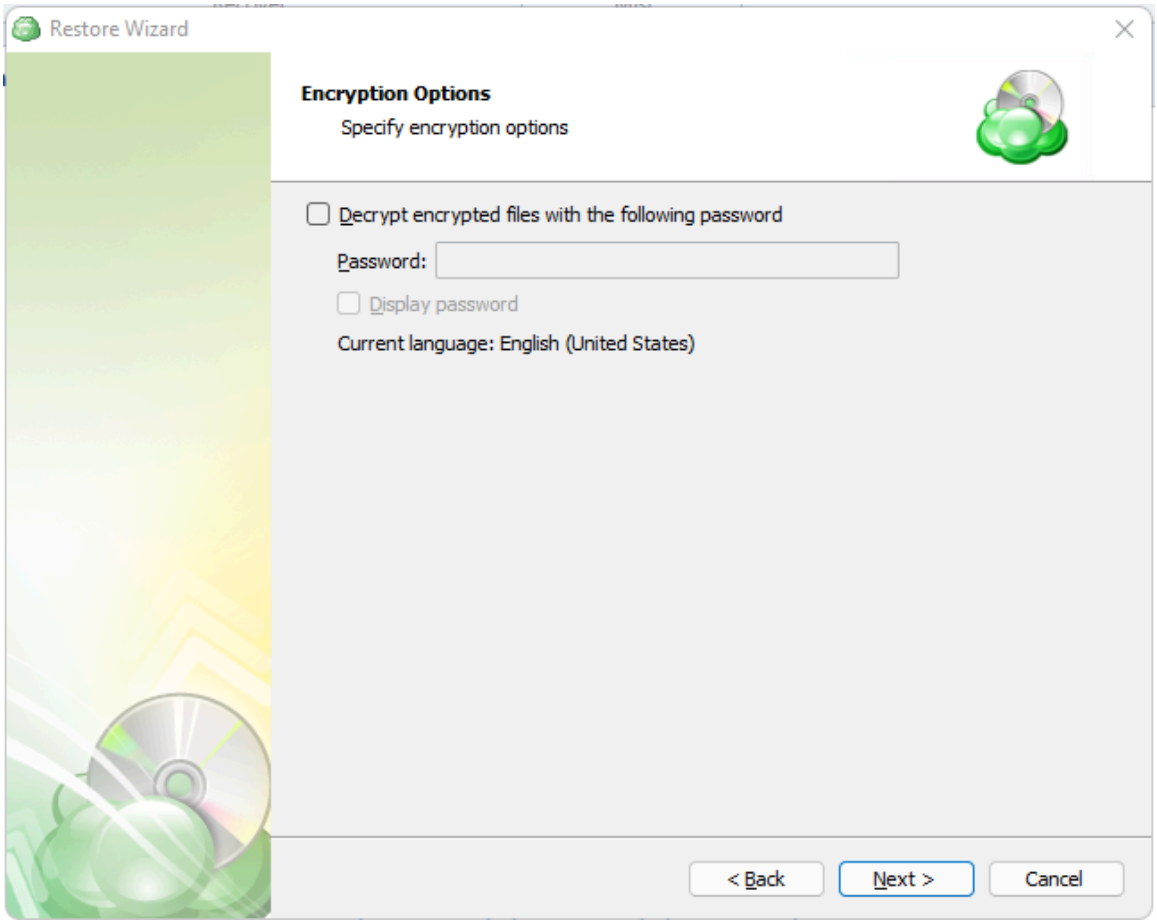


Use a temporary instance for faster cloud-to-cloud restores; avoid it to reduce cloud compute costs at the expense of speed.

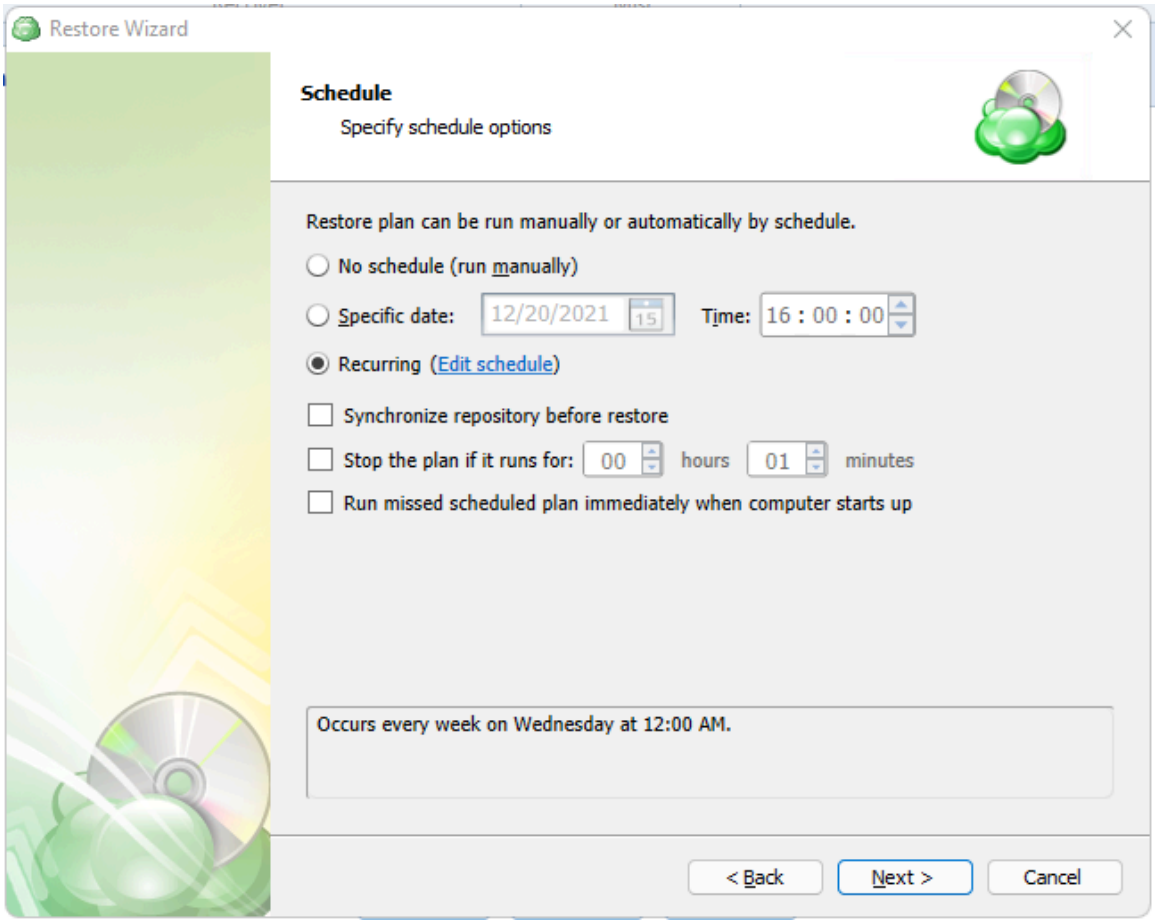
Step 14. Next you will need to specify the parameters of the temporary instance in the same way that the target instance is configured.



Step 15. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the VM.



Step 16. With the decryption password entered, the next step is setting the schedule for the restore plan.

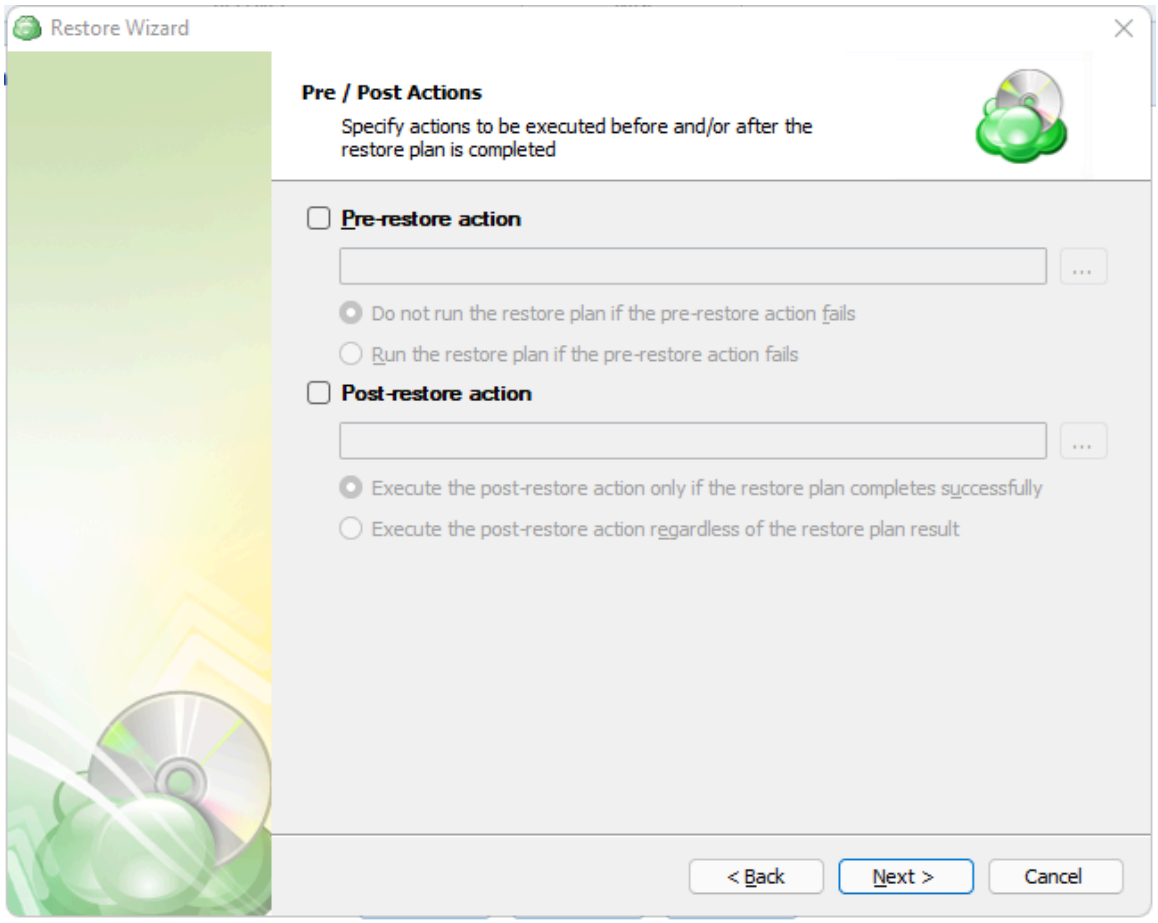


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

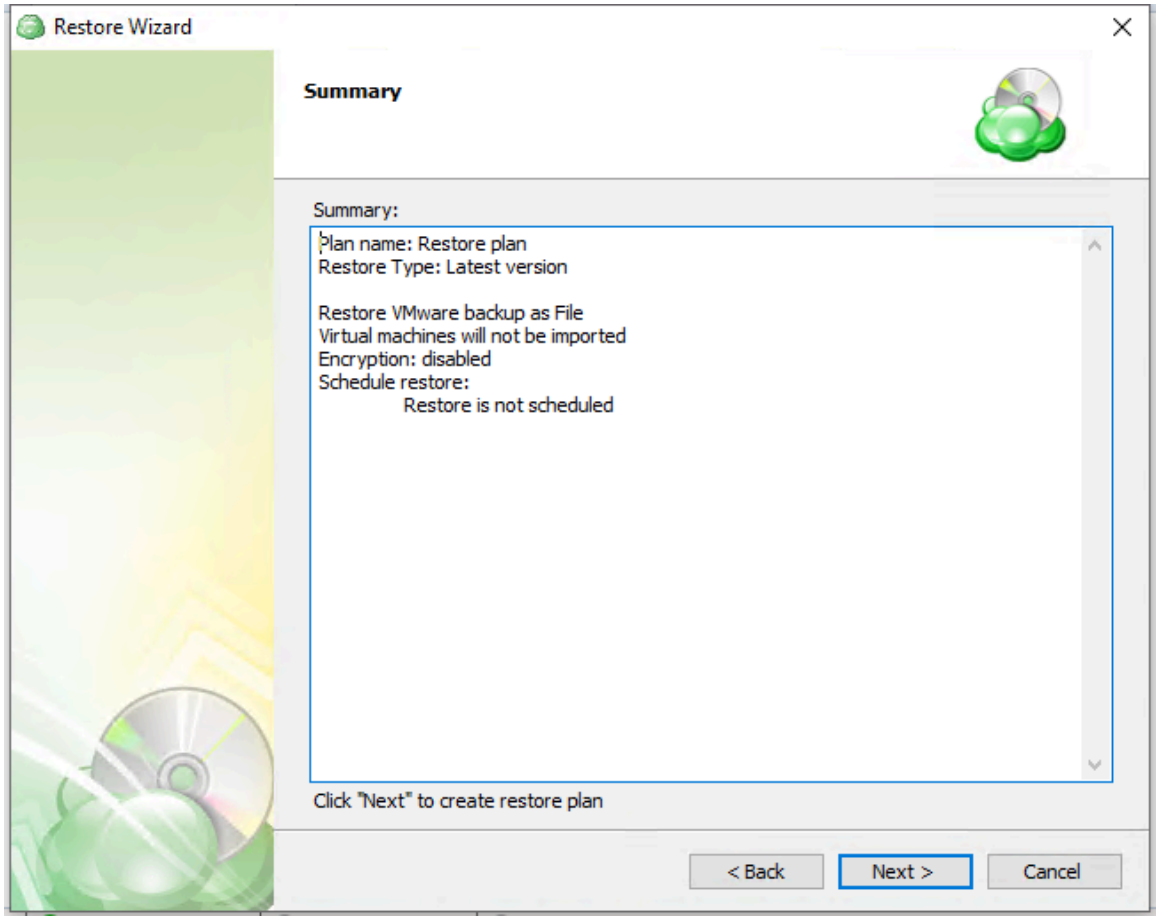
> Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 17. After setting the schedule, the next step allows pre and post actions to be defined.



Step 18. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.

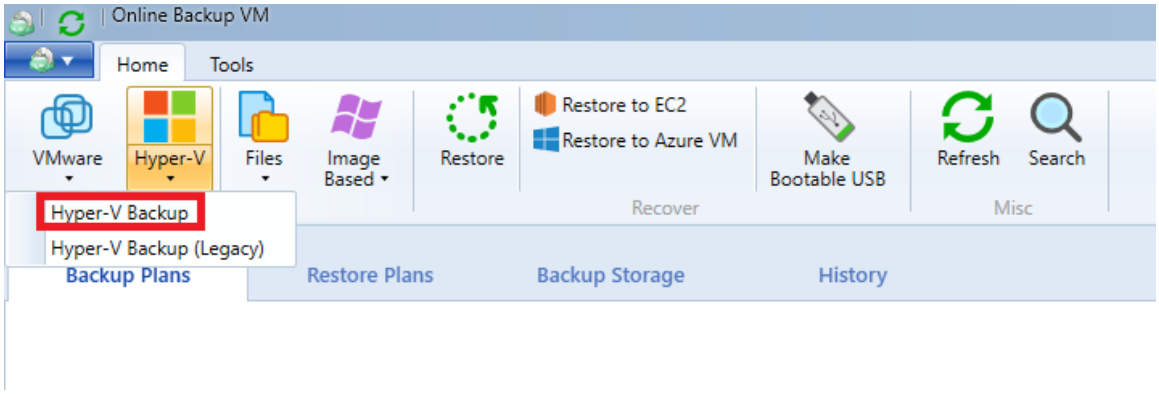


If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

Hyper-V Backup Plans

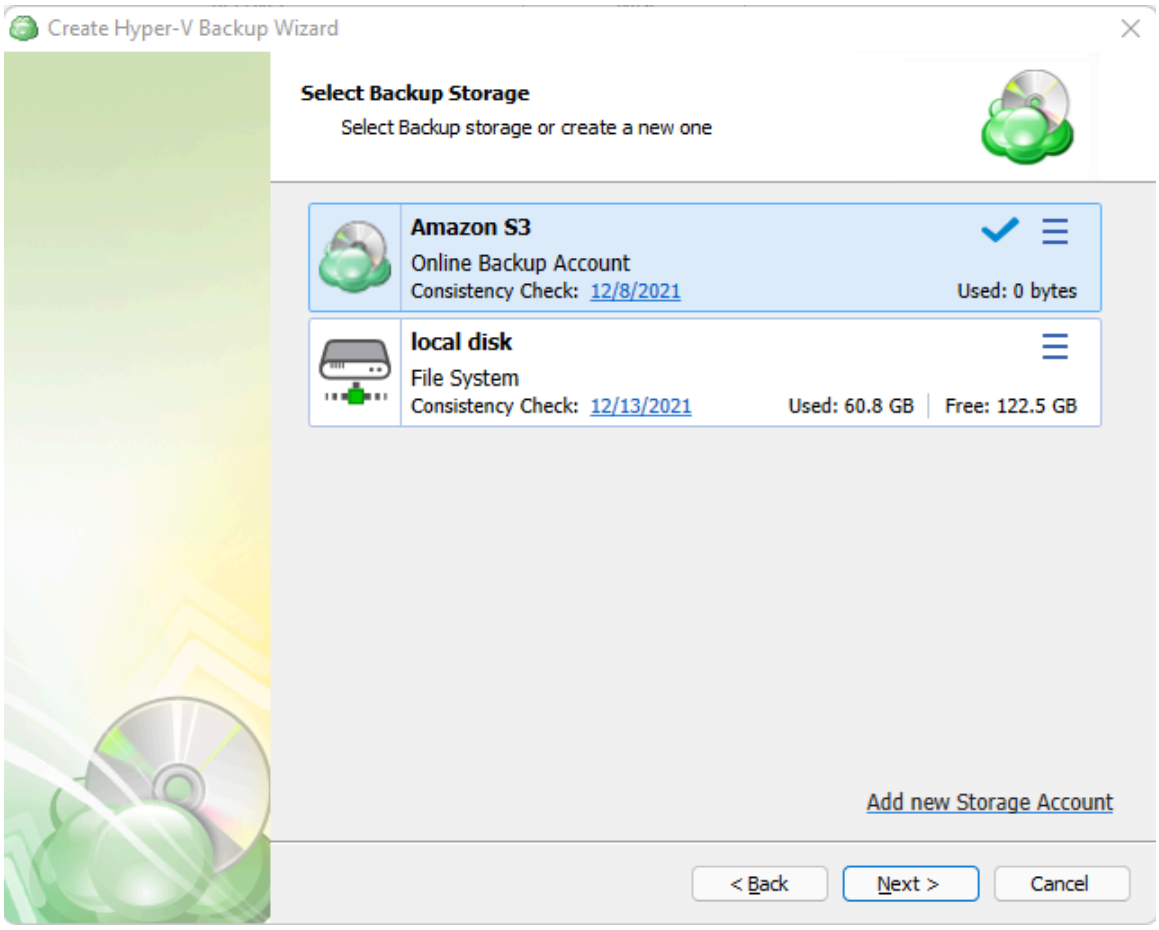
Backing up VMs using the Agent

Step 1. Within the Online Backup Agent, click on “Hyper-V”, then select “Hyper-V Backup”



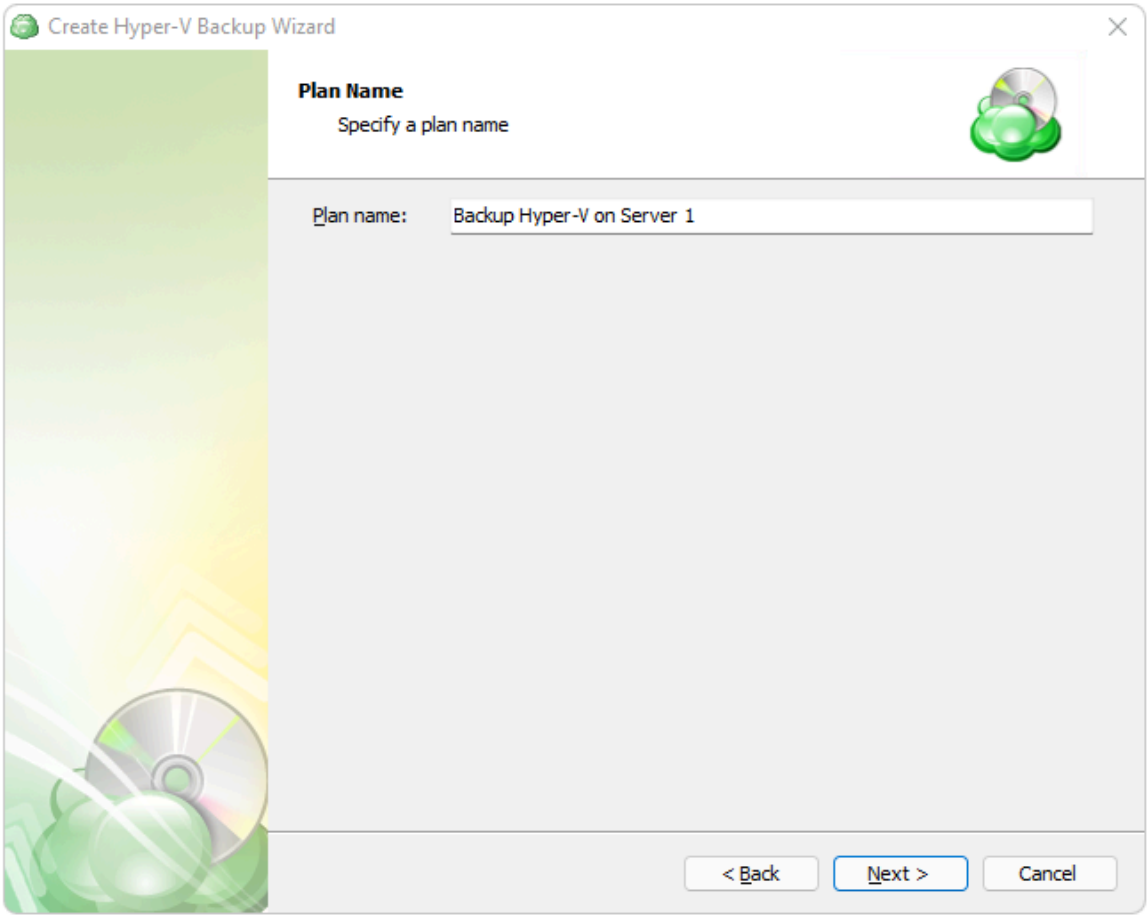
Step 2. You will then be prompted to start the backup wizard.

Step 3. The next step will prompt you to select the destination for the backup.



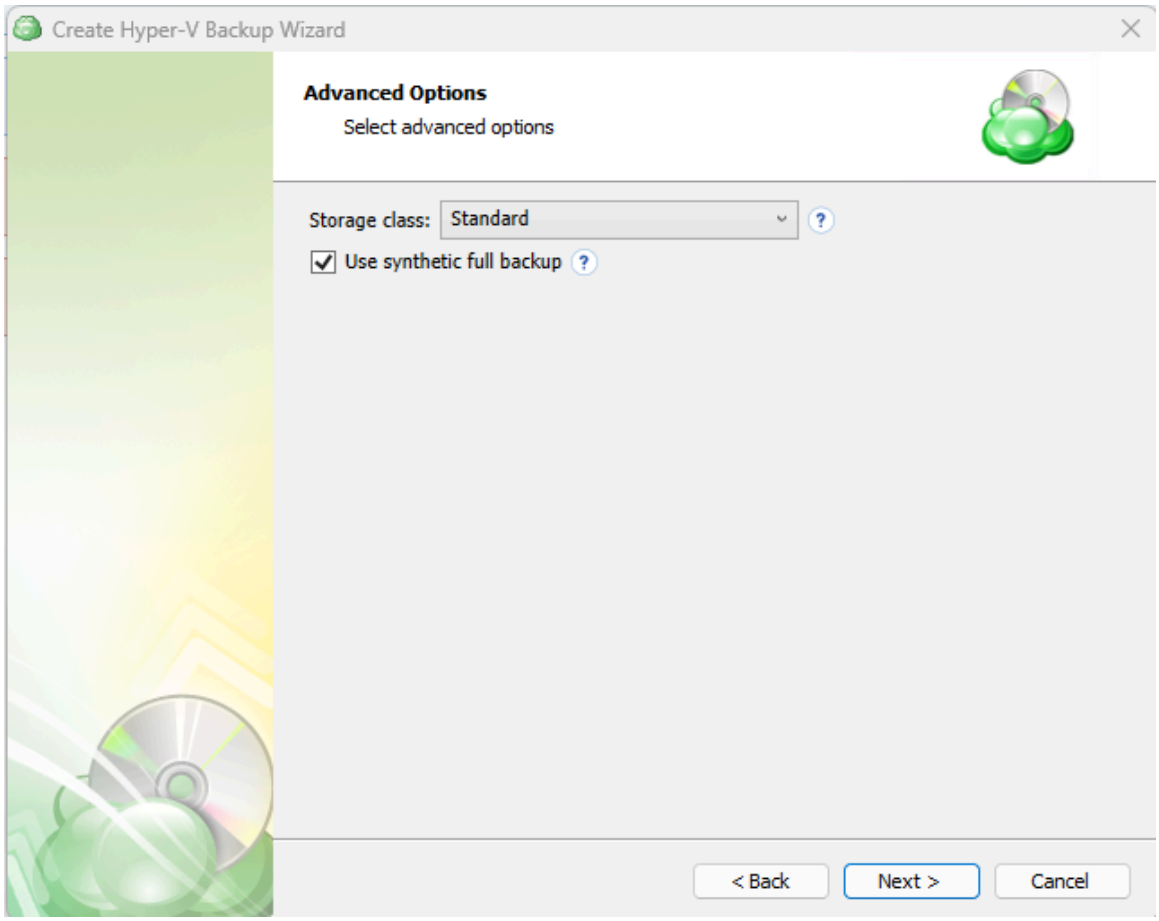
If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

Step 4. Next, you will be prompted to name the plan.



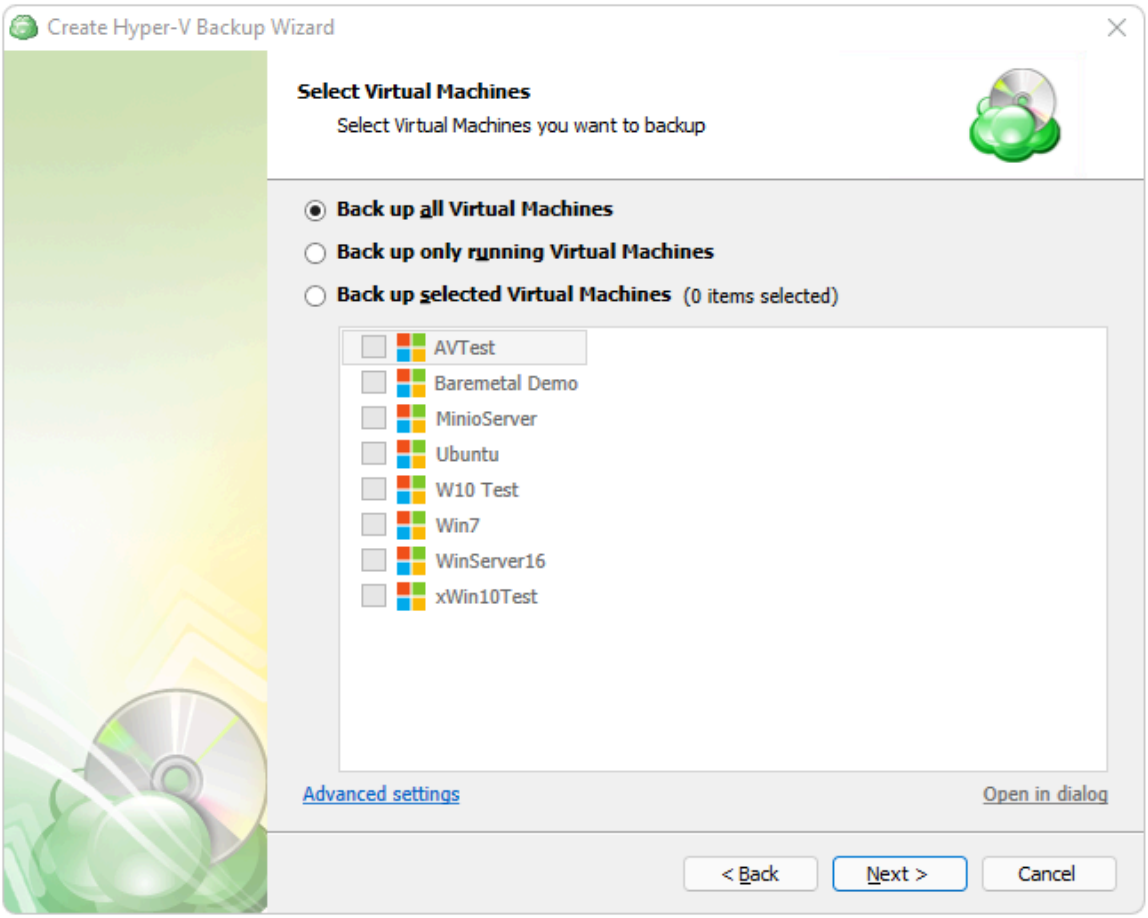
It is recommended to use a descriptive name which will distinguish the backup from others.

Step 5. Next, you are presented with the Advanced Options.



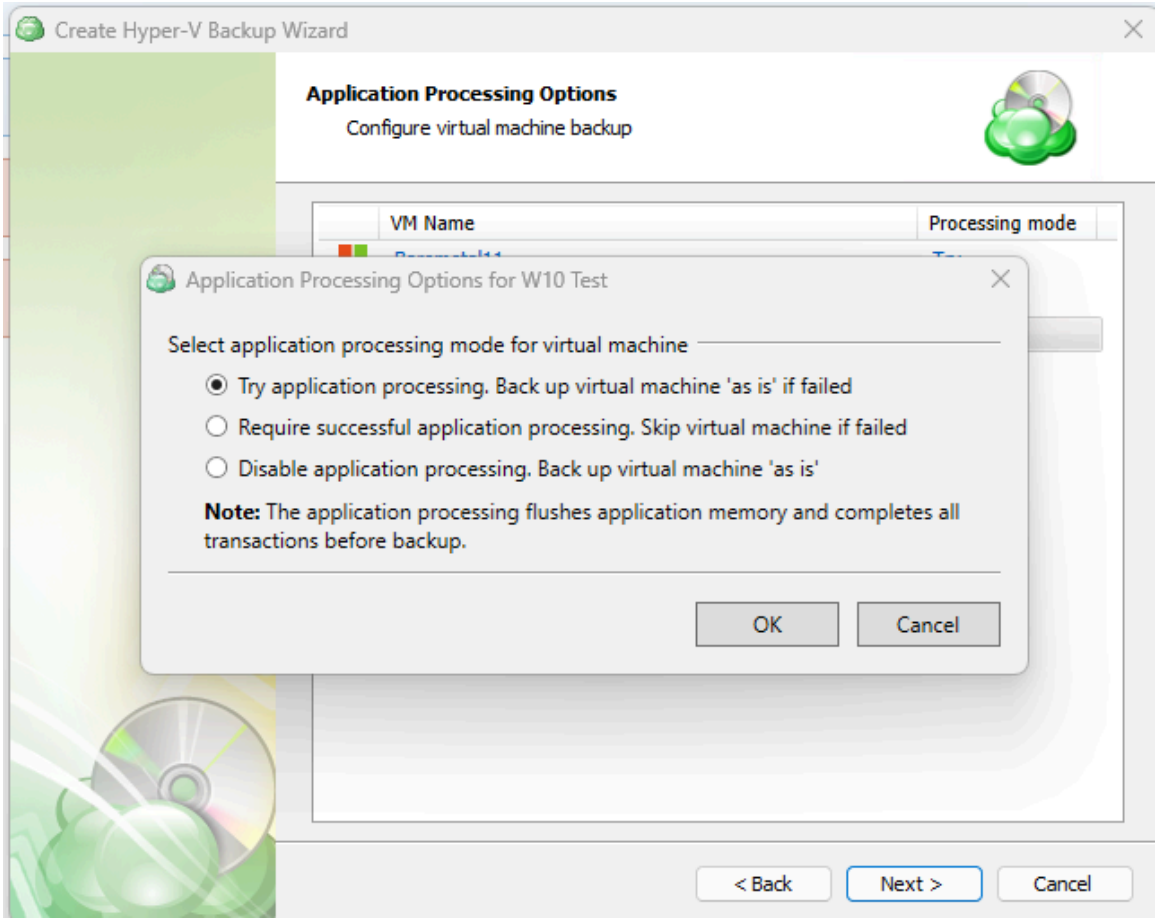
Synthetic Full Backups allow the system to merge a series of incremental backups together to form a new full backup, greatly reducing the time and bandwidth needed to perform full backups after the initial full. If the storage destination does not support Synthetic full, then a traditional full will be made instead.

Step 6. Next, select the Virtual Machines you wish to back up.



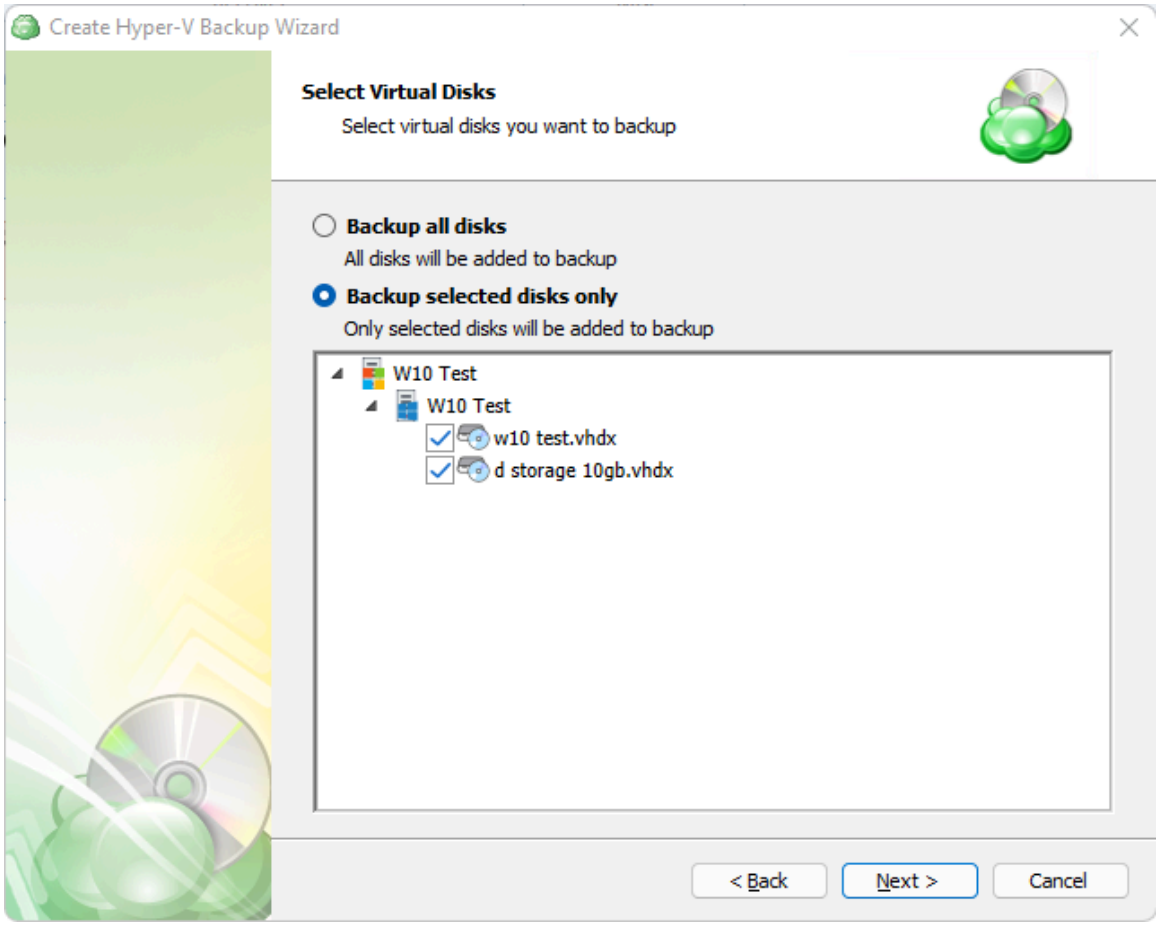
- **Back up all Virtual Machines:** will backup all VMs regardless of current state. This is recommended only for small environments.
- **Back up only running Virtual Machines**: Only backs up VMs currently in "Running" status and is recommended for clustered environments where backup servers planned for failover procedures are not required to be selected.
- **Backup up selected Virtual Machines:** Allows you to backup a group of VMs by selecting them from the list below. This allows for greater control of mixed status VMs and for larger environments where it is beneficial to split the backup into multiple plans.

Step 7. Now you'll need to select the application processing options

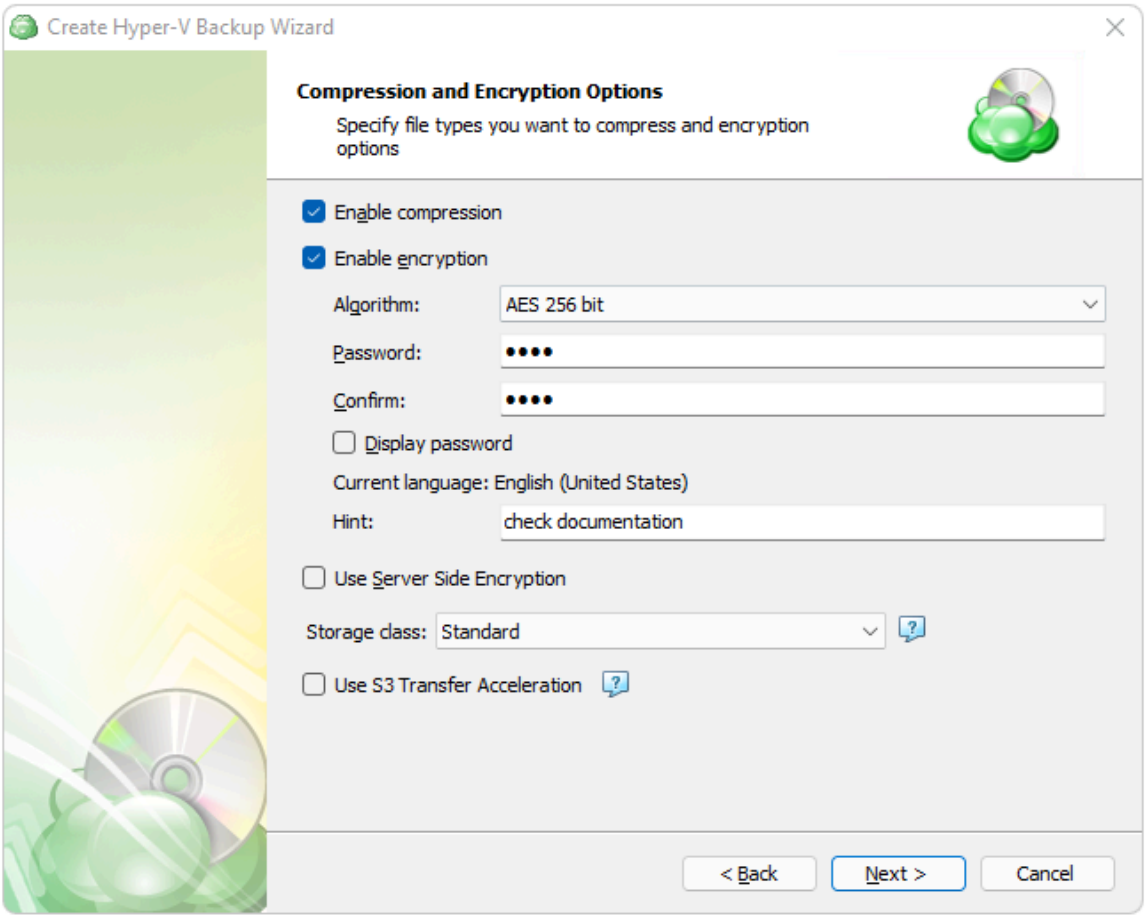


- **Try application processing**. Backup will perform whether or not the application-concistent process fails. If the processing fails, the backup will be done "as is", but data consistency is not guaranteed.
- **Require successful application processing**. Skip the virtual machine if processing fails. If processing is successful, it ensures that applications running in the VM, such as databases, are taken into consideration and the backup will ensure data consistency is maintained.
- **Disable application processing**. Backup virtual machine "as is" and does not perform any application processing. The VM is backed up in its current state, which may cause data inconsistencies.

Step 8. Once you have selected which VMs to backup, the application allows you to then choose whether to backup all virtual disks on the selected VMs or to only backup selected virtual disks.



Step 9. After you have selected which VMs and disks to backup, the next step is to set the compression or encryption options.



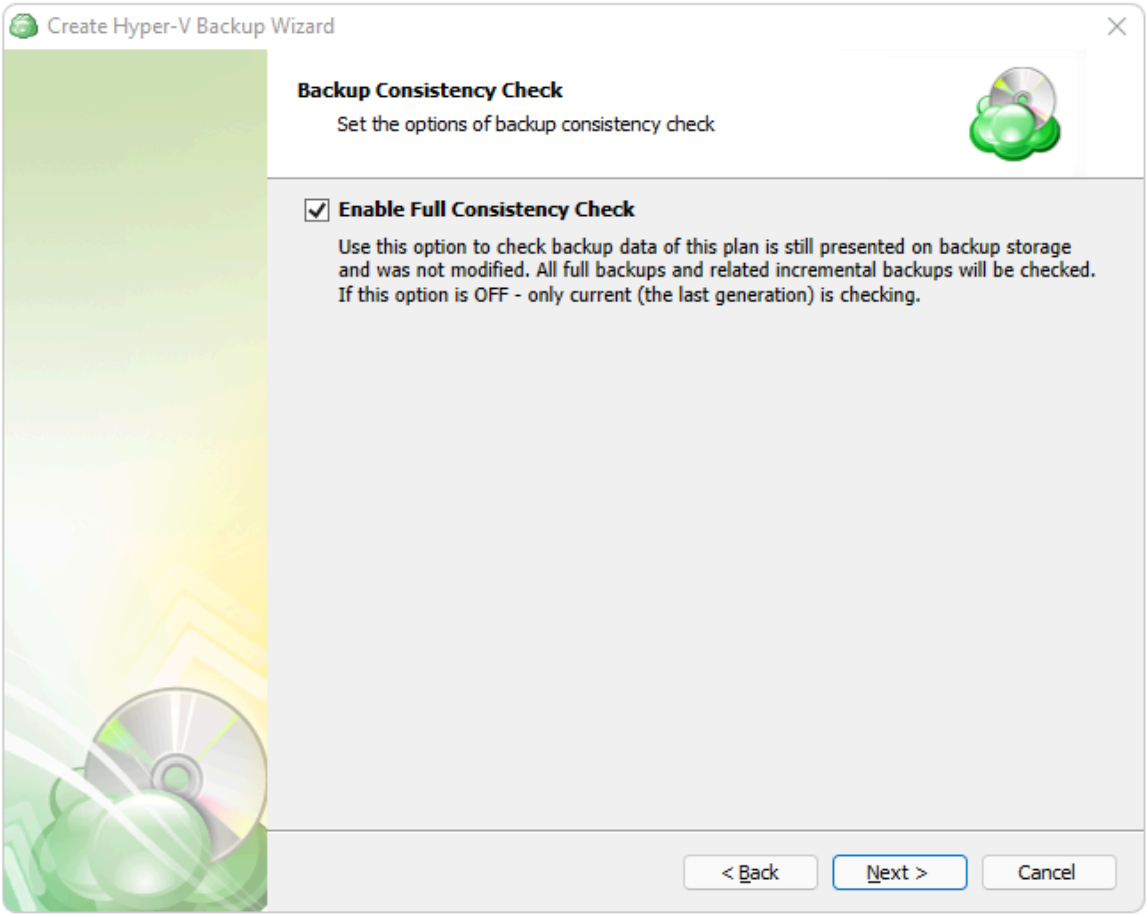
Other features may appear here which are specific to the selected backup destination. Some of these options may incur additional costs with the storage provider.

Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

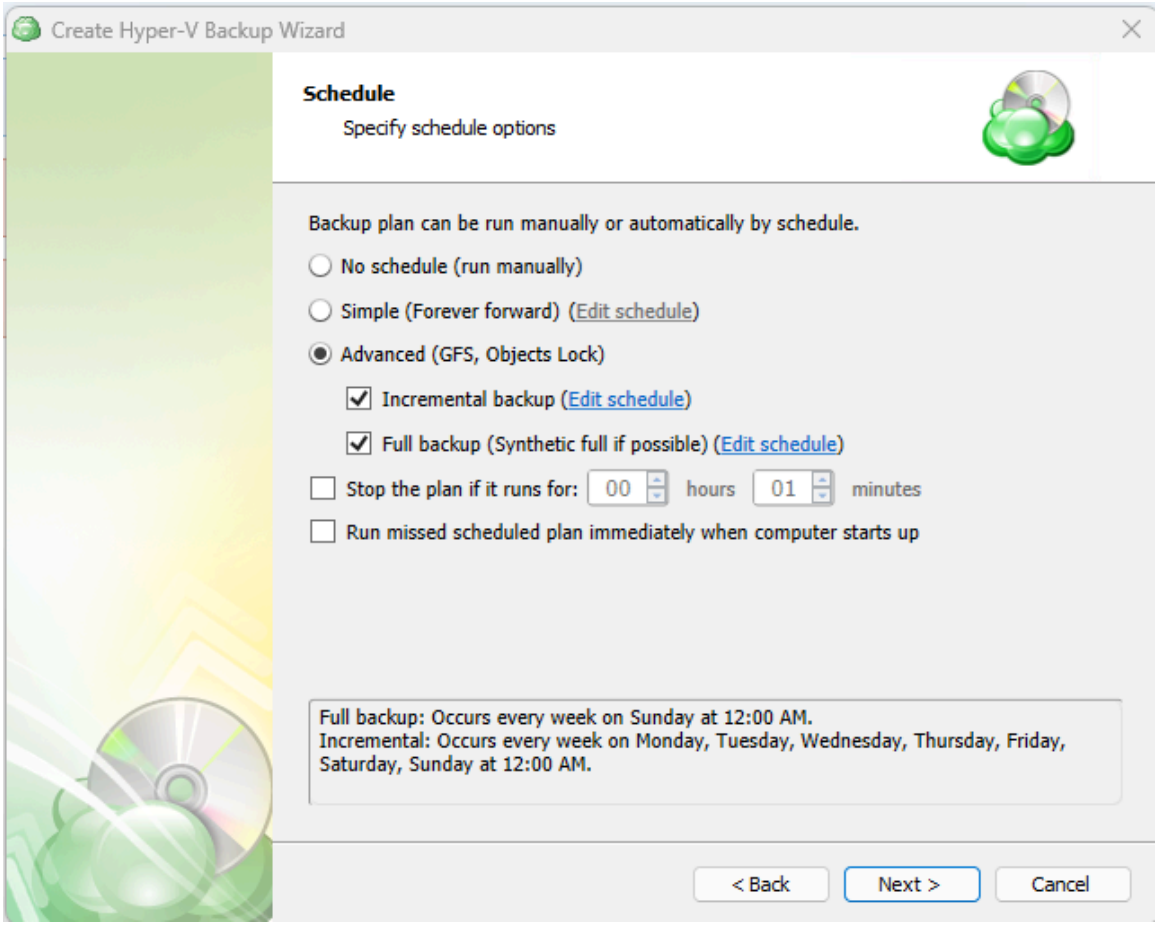
It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place and enable the Password Recovery Service.

Step 10. Next you are presented with an option for the type of Backup Consistency Check to use with the plan. It is recommended that you leave “Enable Full Consistency Check” enabled.



It is recommended to leave the Consistency Check enabled to ensure the integrity of your backed up data.

Step 11. Next you are prompted to set the schedule for your backup plan and the additional settings



- **No schedule**: The backup runs only when manually started.
- **Simple (Forever Forward Incremental - FFI)**: Runs incrementally, keeping a single full backup and merging old incrementals.
- **Advanced (GFS, Object Lock)**: Allows scheduling full backups separately, enabling features like GFS retention and Object Lock.

> Synthetic Full Backups allow the system to merge a series of incremental backups together to form a new full backup, greatly reducing the time and bandwidth needed to perform full backups after the initial full. If the storage destination does not support Synthetic full, then a traditional full will be made instead.

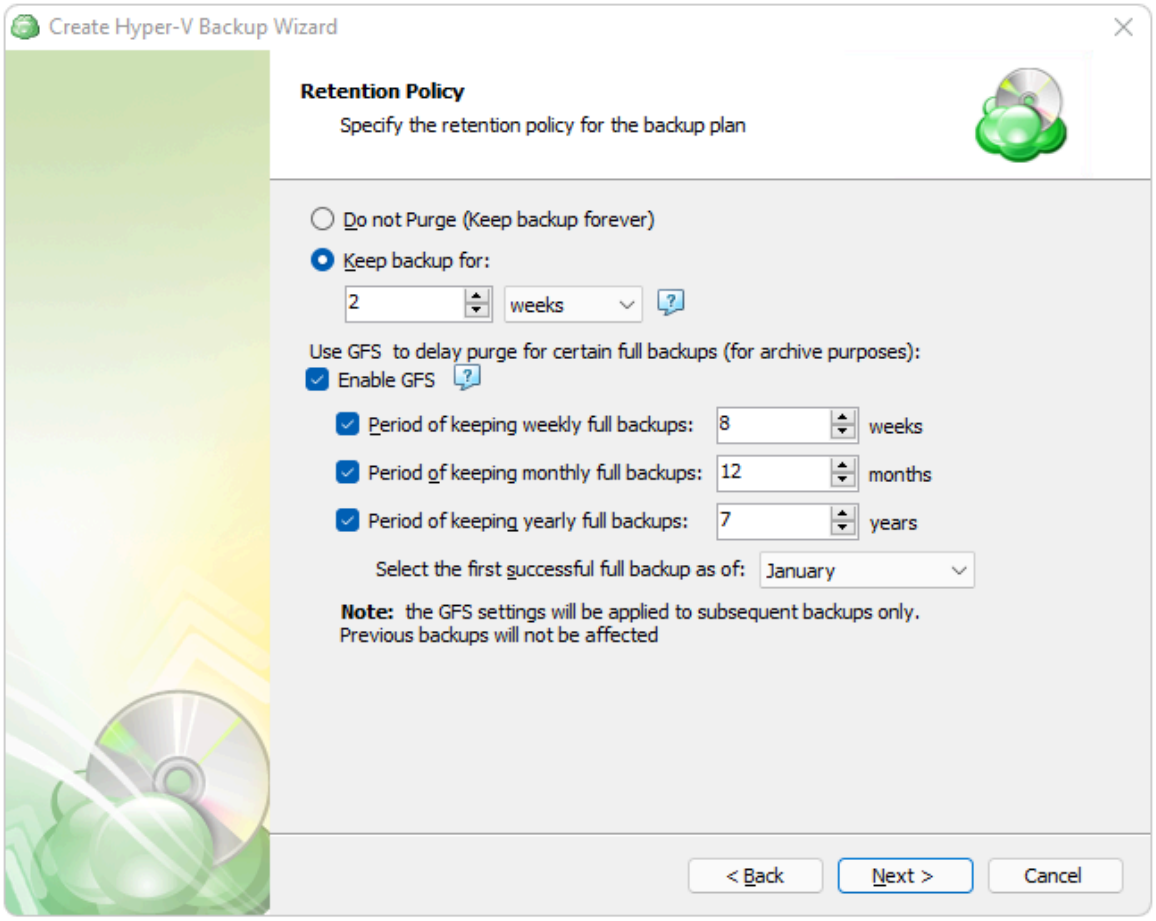
The Advanced retention policy will only perform properly with regular scheduled full backups.

Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

A common backup schedule which fits most scenarios includes a weekly Full backup and daily Incremental backups.

Step 12. On the “Retention Policy" step, you can set the policies the application will use to determine which data to purge at regular intervals and define the multigenerational Grandfather-Father-Son (GFS) parameters if required.



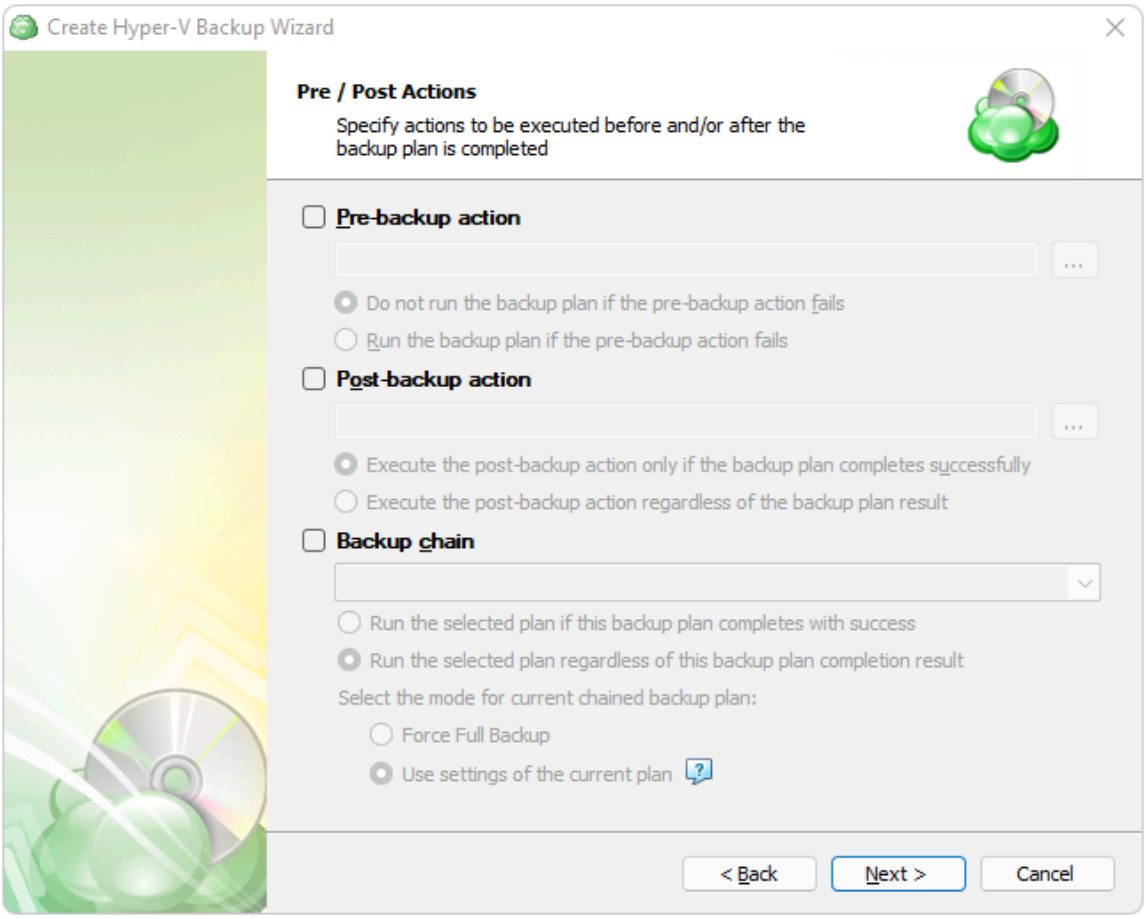
- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.
- **Enable GFS**: Select this option if you want to keep Full Backups for archival purposes at the selected intervals.
- **Period of keeping weekly full backups**: Set the number of Weekly Full Backups to retain. This is determined separately from the “Keep backup for” value and relies on Full Backups to be scheduled on at least a weekly basis in the previous step.
- **Period of keeping monthly full backups:** Number of Monthly Full Backups to retain. A Full Backup can be flagged as both a Weekly and Monthly backup, but once the number of Weekly Full Backups has exceeded their retention setting, only those also flagged as a Monthly will be retained.

- **Period of keeping yearly full backups:** Set the number of Yearly Full Backups to retain. A Full Backup can be flagged as a Weekly, Monthly, and Yearly Backup. Once the number of Monthly Full Backups has exceeded their retention setting, only those also flagged as a Yearly will be retained.
    - **Select the first successful full backup as of**: Select the first Monthly Full Backup you would like to flag and retain as the first Yearly Full Backup.

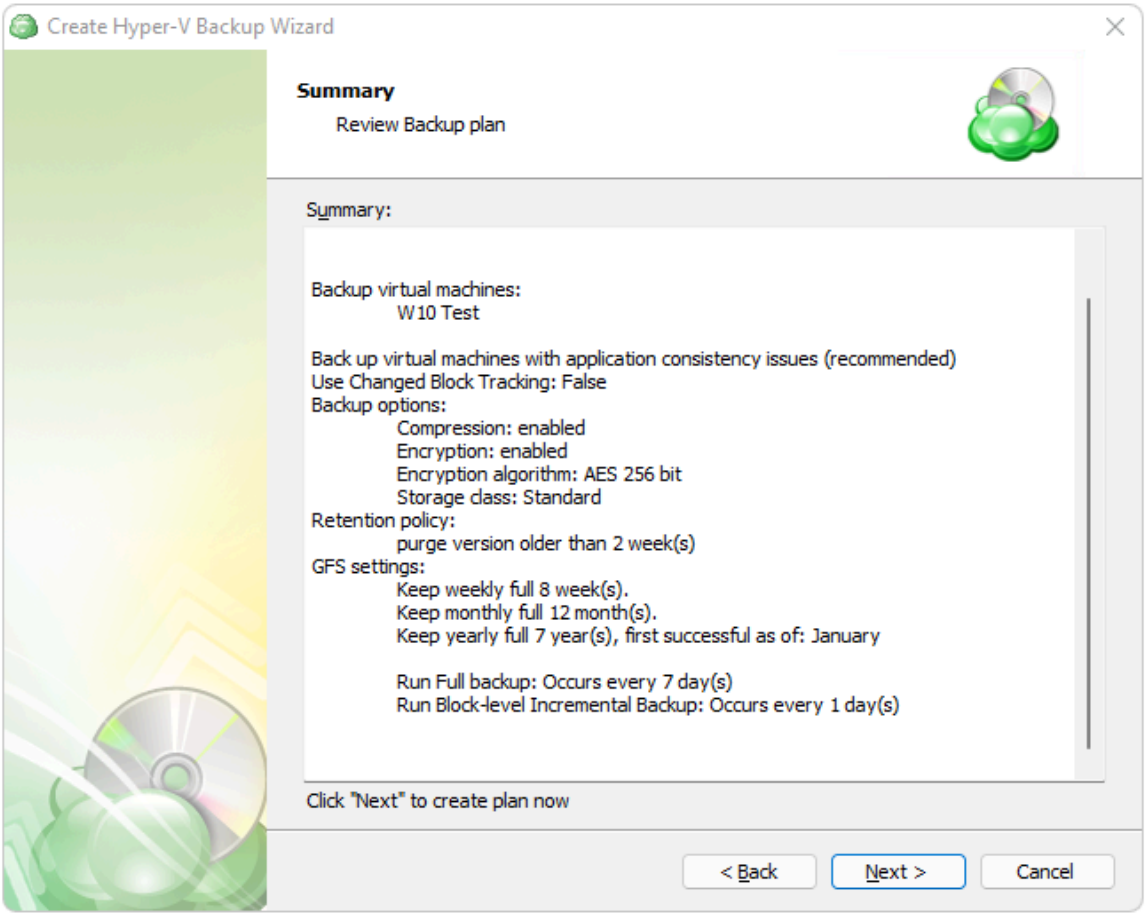
Restore Points will not be deleted until the youngest point in the chain has met the retention criteria.

GFS Retention provides an excellent way to efficiently archive data for compliance. Additional information can be found in GFS Policy topics in the MBS Documentation

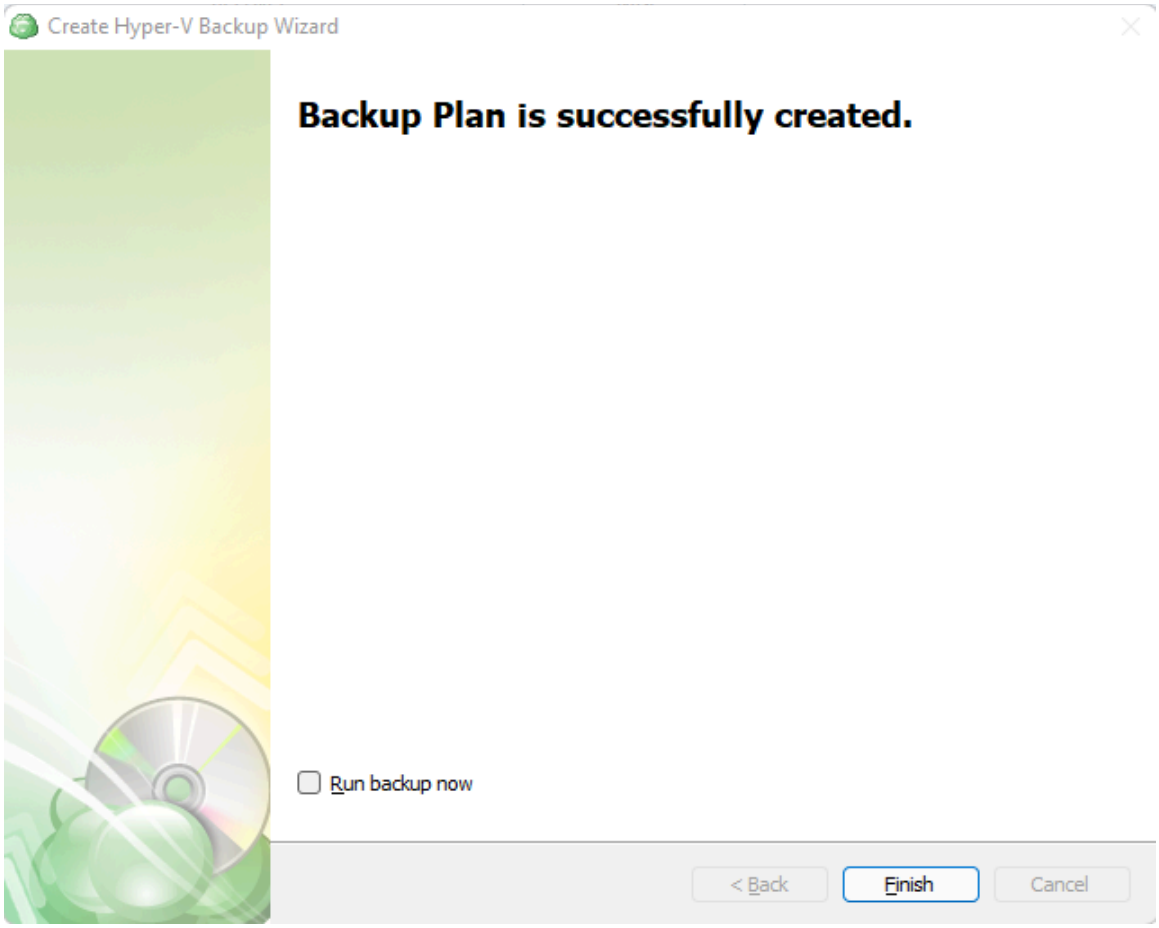
Step 13. After the schedule is set, the next section is used to set the “Pre” and “Post” Actions



Step 14. After the pre and post actions are set, you will be shown a summary of the selected options.

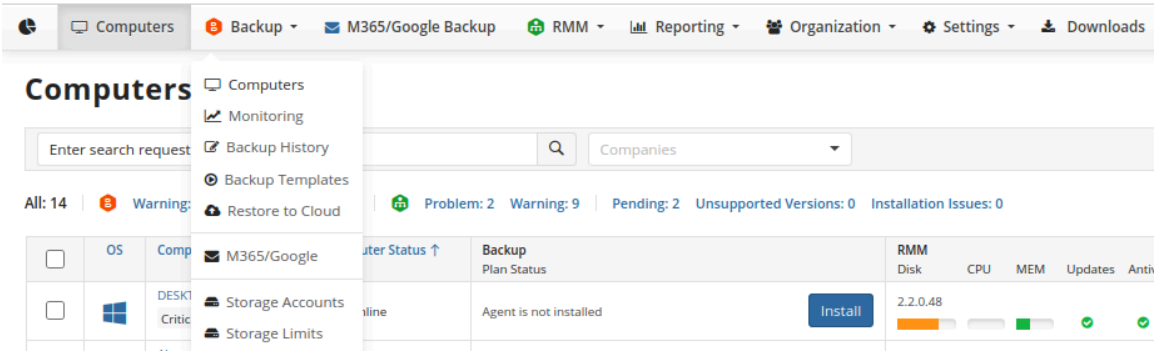


Step 15. The final step of the wizard will confirm that the Backup Plan was successfully created. If you select the “Run backup now” box, the application will initiate it immediately upon exiting the wizard, otherwise it will run at the next scheduled time.

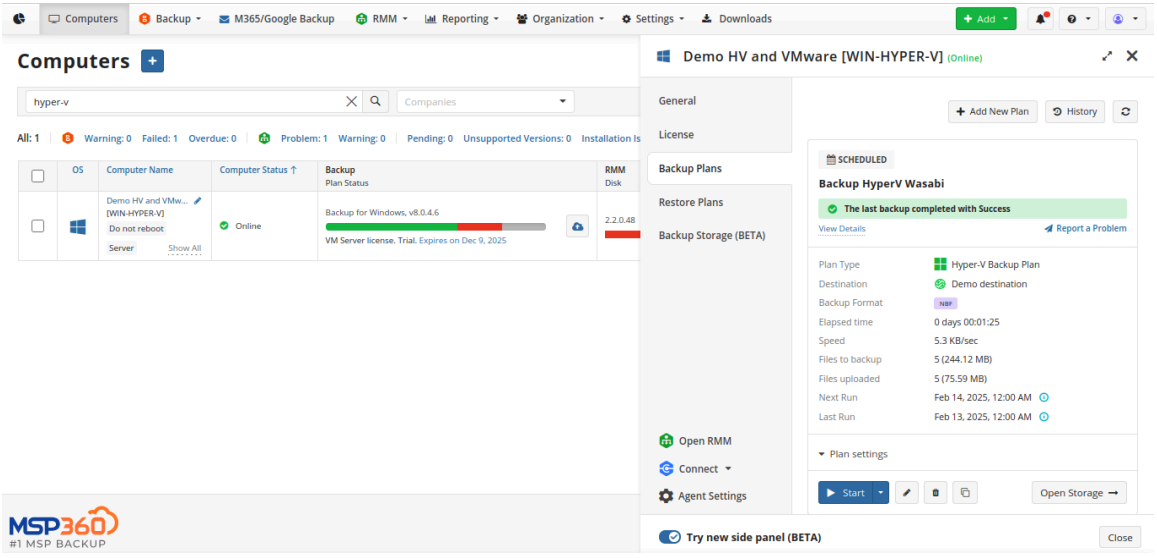


Backing up the VMs using MBS

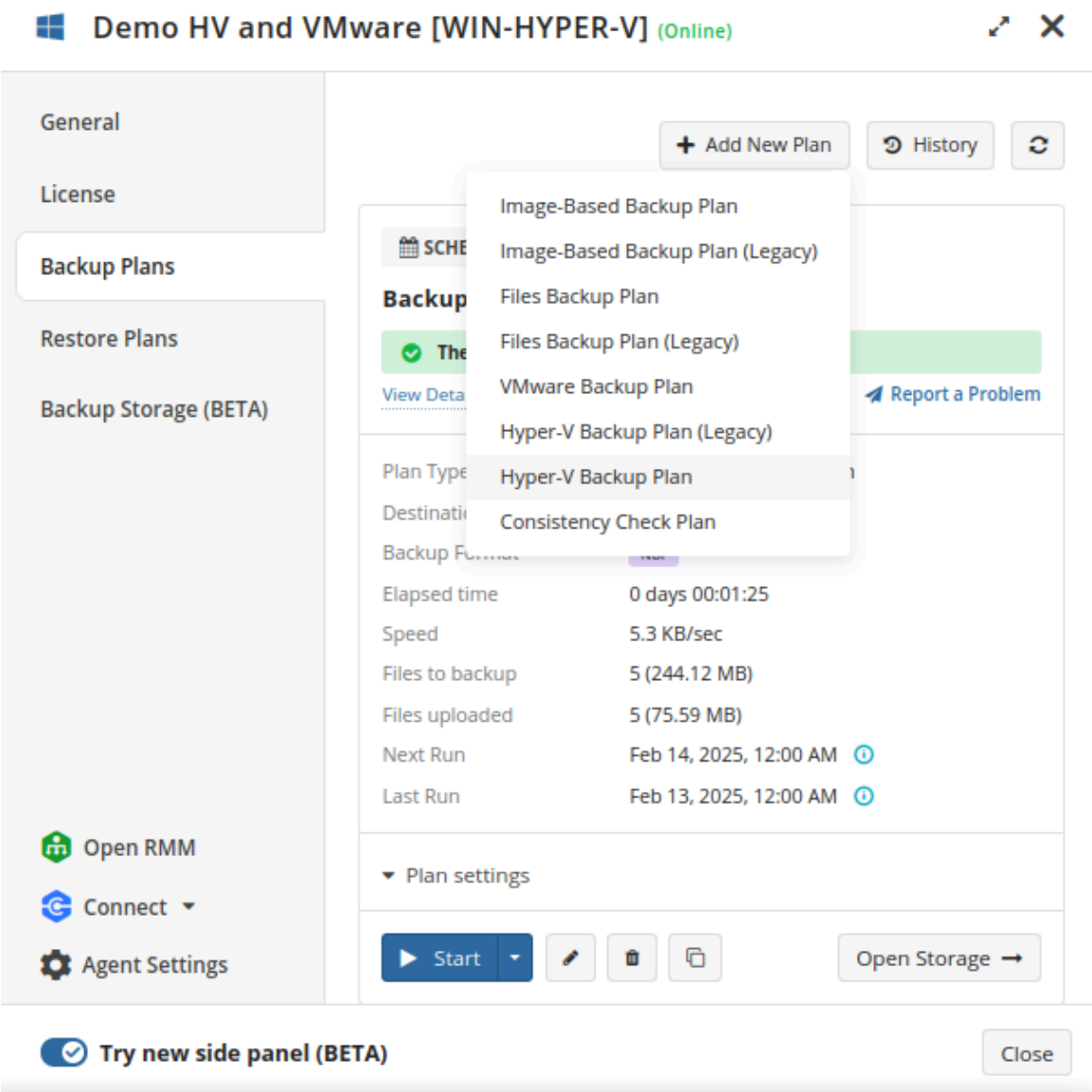
Step 1. From the MBS Portal, left-click Backups on the menu, then select “Computers”



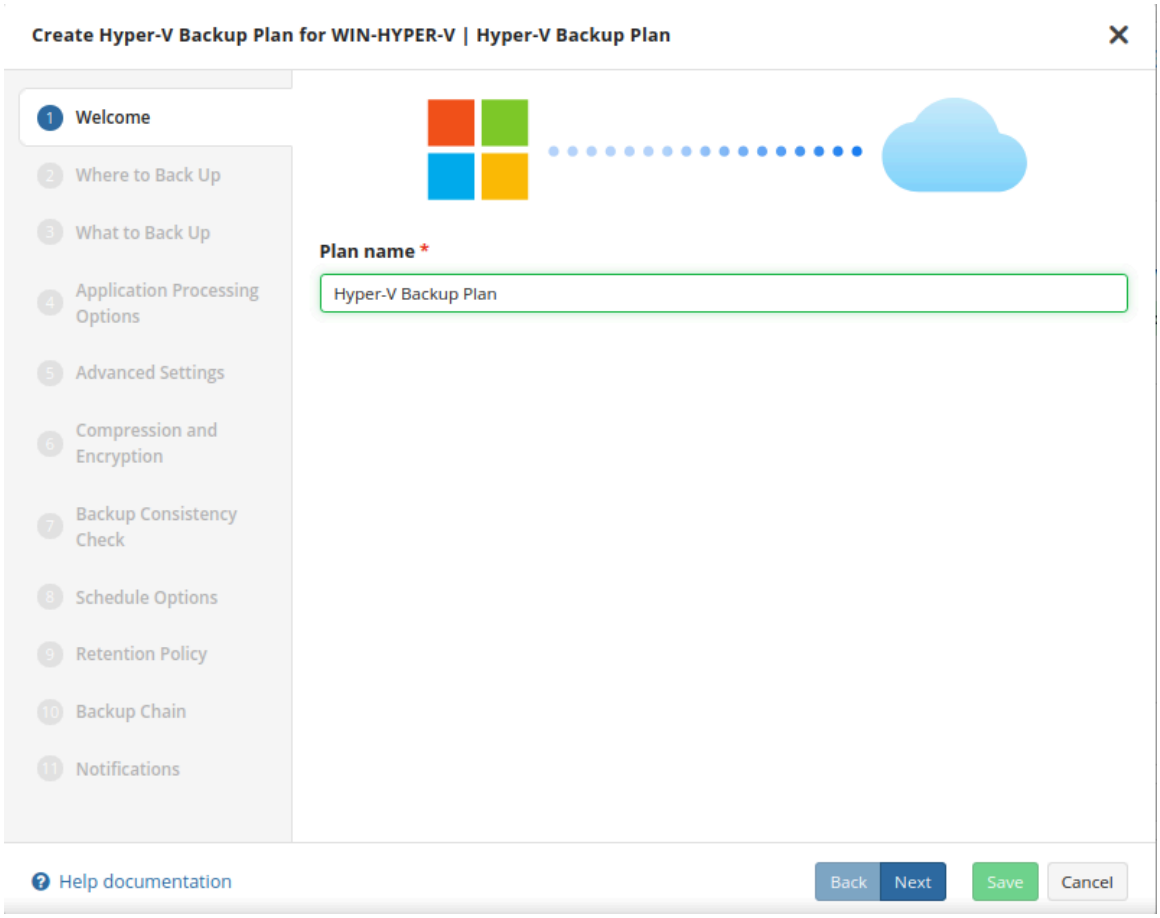
Step 2. Locate the computer you wish to backup from the list and open the current list of plans by either clicking on the name of the computer, or by selecting “Show Plans” from the gear menu.



Step 3. If it is a newly deployed computer, you will be prompted with a list of options to create new plans, otherwise, click on the “Add New Plan” Button and then under “Backup” header click “Hyper-V Backup Plan”.

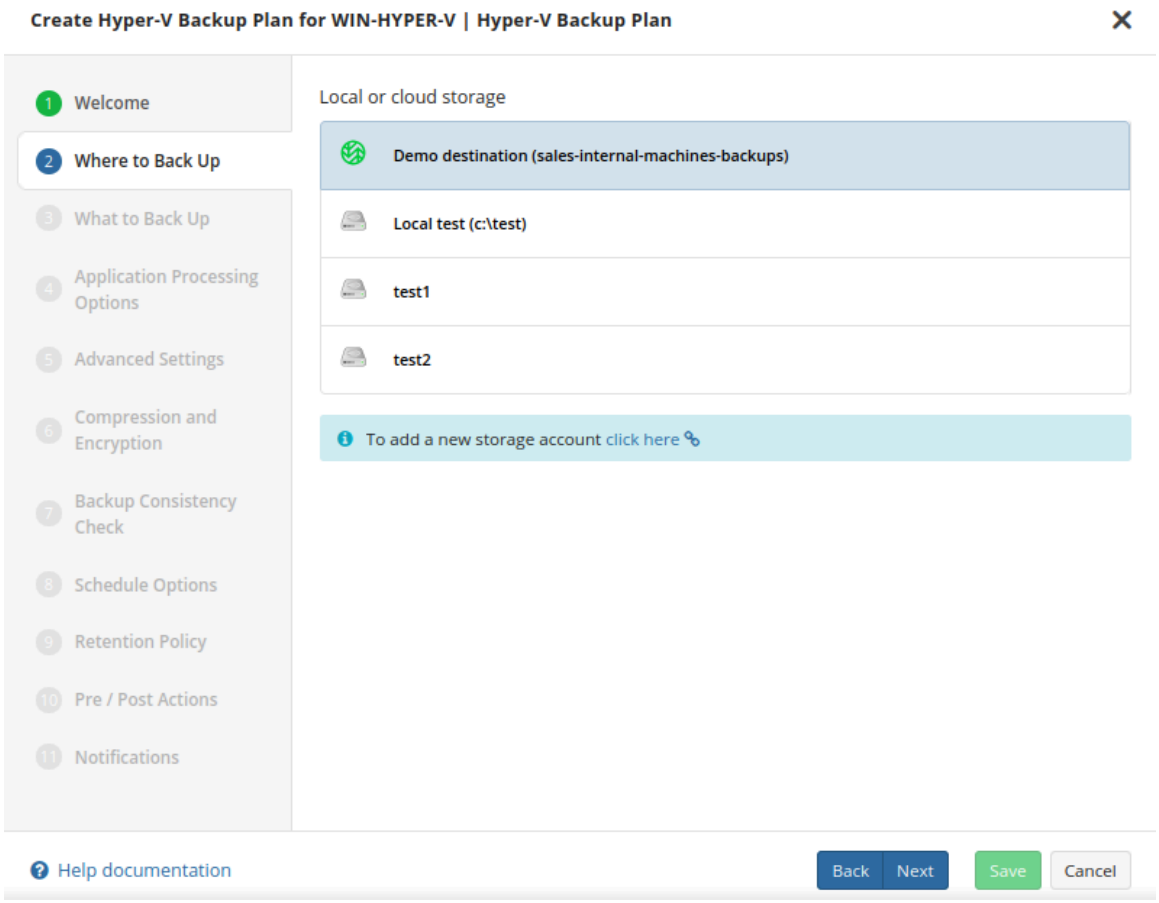


Step 4. The first step when creating a new Hyper-V backup plan is to give the plan a name.

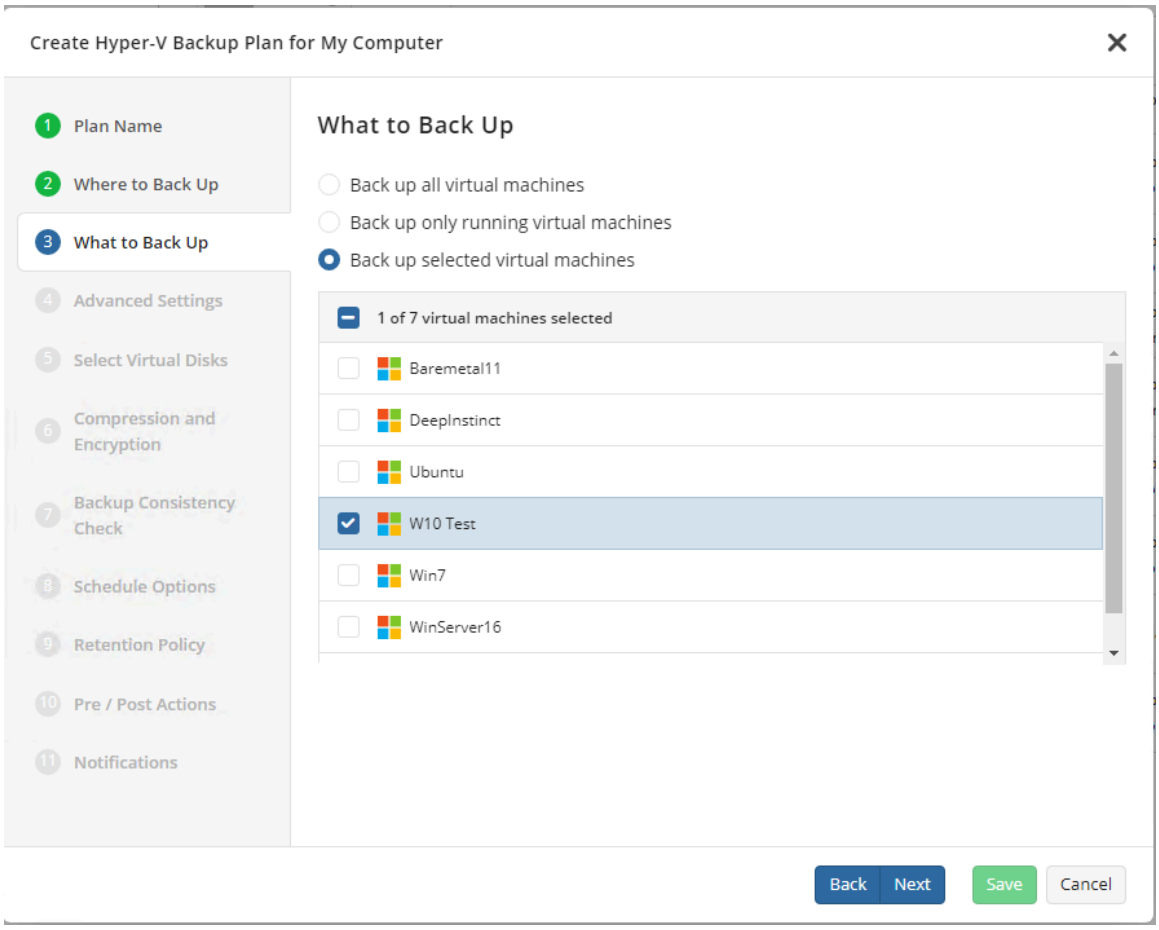


It is recommended to use a descriptive name which will distinguish the backup from others.

Step 5. In the next section, you are prompted to select the destination.

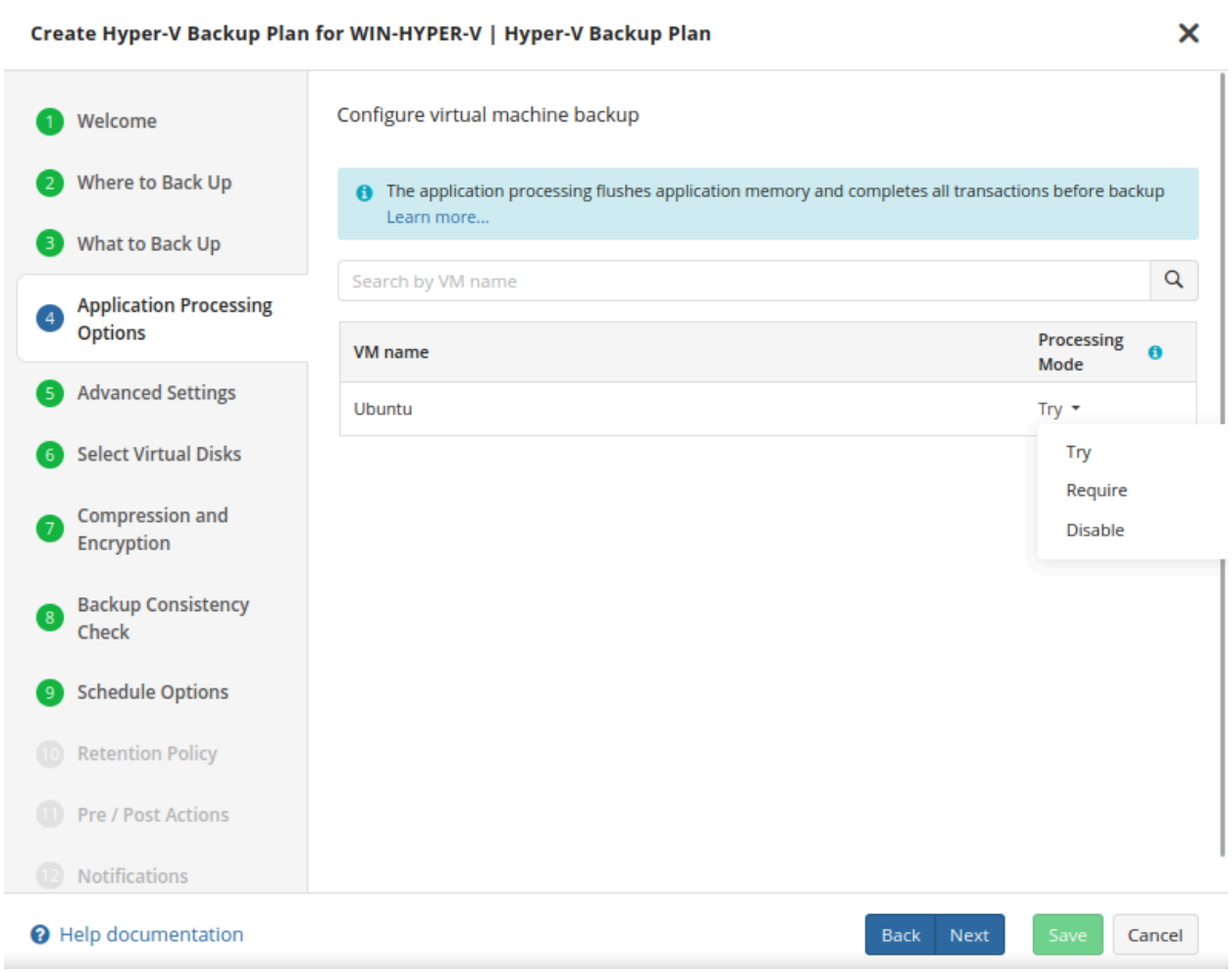


Step 6. Next, select the Virtual Machines you wish to back up.



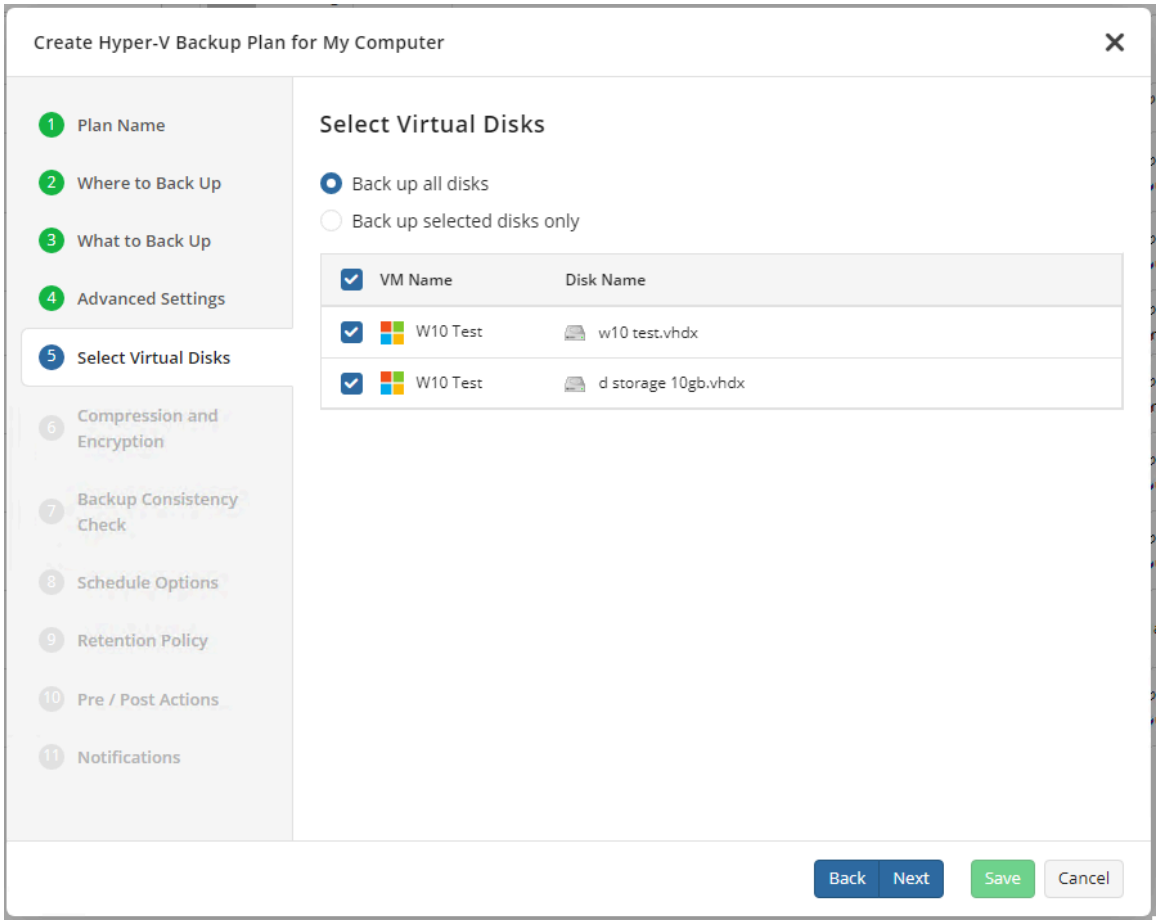
- **Back up all Virtual Machines:** will backup all VMs regardless of current state. This is recommended only for small environments.
- **Back up only running Virtual Machines**: Only backs up VMs currently in "Running" status and is recommended for clustered environments where backup servers planned for failover procedures are not required to be selected.
- **Backup up selected Virtual Machines:** Allows you to backup a select group of VMs by entering a list of VMs by name in the box below. This allows for greater control of mixed status VMs and for larger environments where it is beneficial to split the backup into multiple plans.

Step 7. Now you'll need to select the application processing options

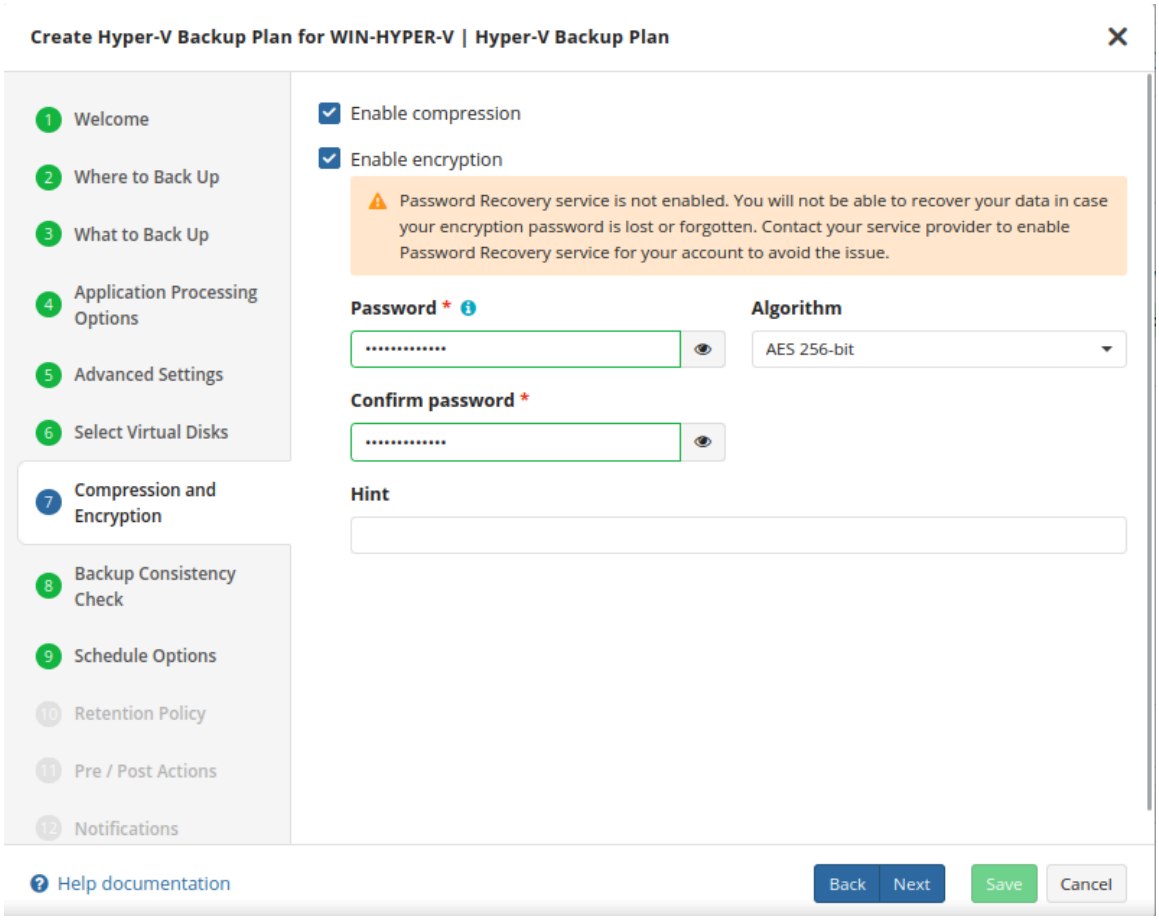


- **Try application processing**. Backup will perform whether or not the application-concistent process fails. If the processing fails, the backup will be done "as is", but data consistency is not guaranteed.
- **Require successful application processing**. Skip the virtual machine if processing fails. If processing is successful, it ensures that applications running in the VM, such as databases, are taken into consideration and the backup will ensure data consistency is maintained.
- **Disable application processing**. Backup virtual machine "as is" and does not perform any application processing. The VM is backed up in its current state, which may cause data inconsistencies.

Step 8. With the VMs selected, you are then presented with a choice to backup all disks for each VM or to specify only select disks.



Step 9. Once the desired Virtual Machines are selected, the next step allows you to choose whether or not to compress the backed up data or enable encryption.



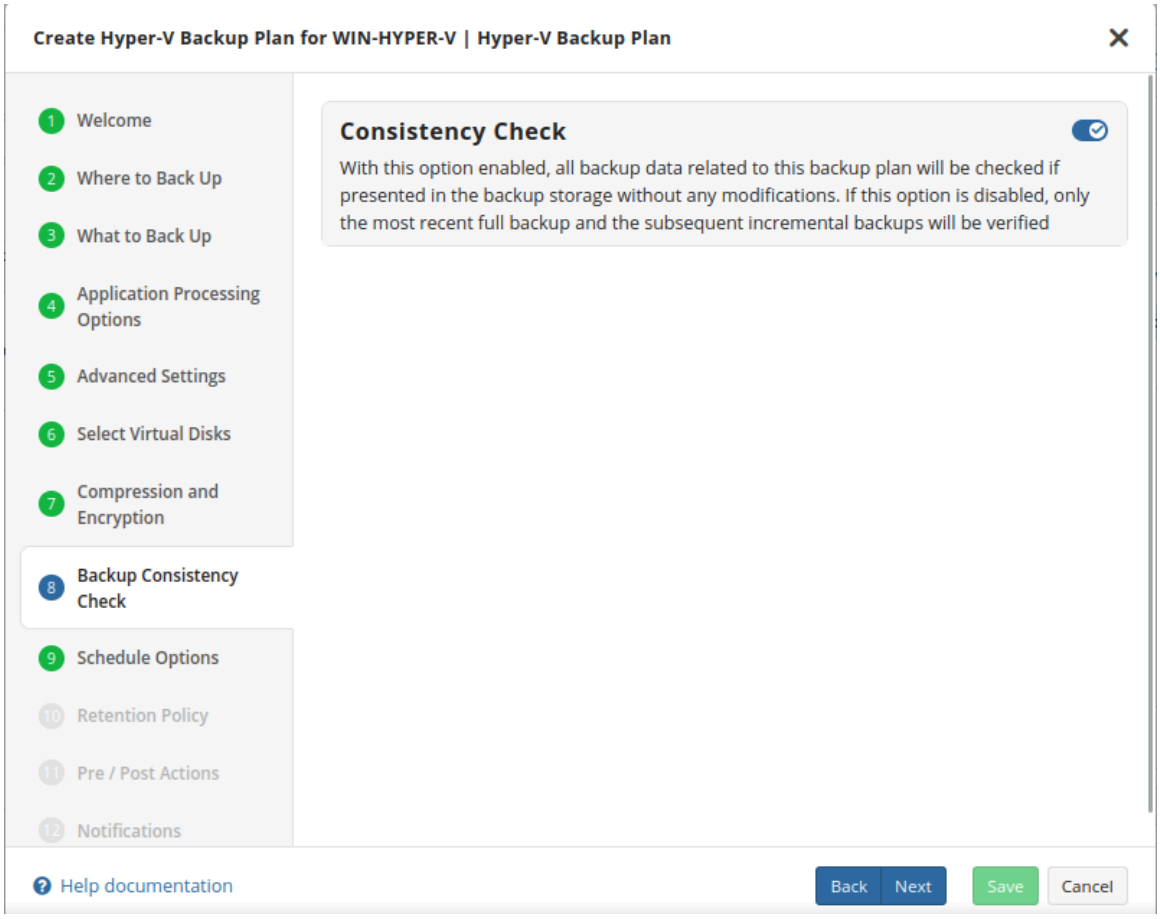
Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a

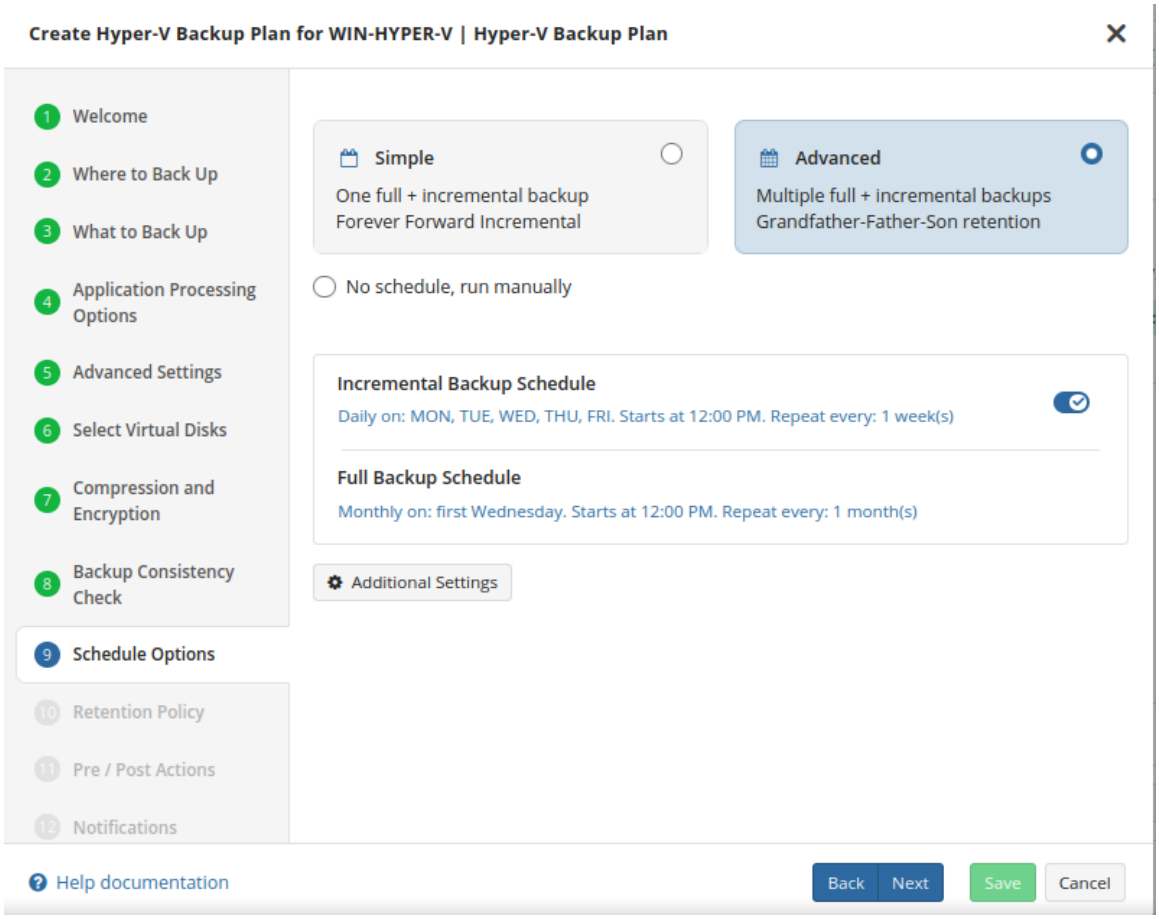
secure place and enable the Password Recovery Service.

Step 10. Next you are presented with an option for the type of Backup Consistency Check to use with the plan. It is recommended that you leave “Enable Full Consistency Check” enabled.



It is recommended to leave the Consistency Check enabled to ensure the integrity of your backed up data.

Step 11. Next you are prompted to set the schedule for your backup plan



- **No schedule**: The backup runs only when manually started.
- **Simple (Forever Forward Incremental - FFI)**: Runs incrementally, keeping a single full backup and merging old incrementals.
- **Advanced (GFS, Object Lock)**: Allows scheduling full backups separately, enabling features like GFS retention and Object Lock.

> Synthetic Full Backups allow the system to merge a series of incremental backups together to form a new full backup, greatly reducing the time and bandwidth needed to perform full backups after the initial full. If the storage destination does not support Synthetic full, then a traditional full will be made instead.

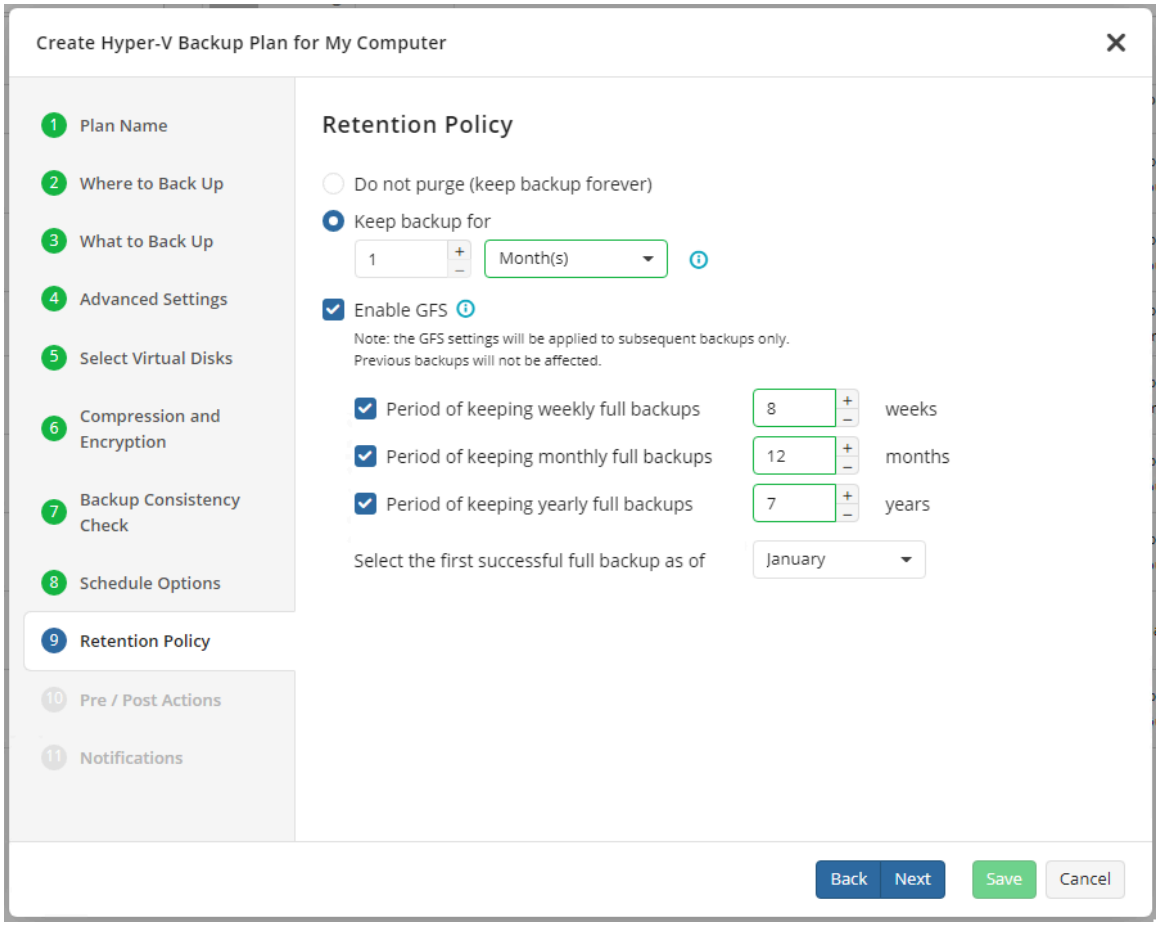
The retention policy will only perform properly with regular scheduled full backups.

Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

A common backup schedule which fits most scenarios includes a weekly Full backup and daily Incremental backups.

Step 12. On the “Retention Policy" step, you can set the policies the application will use to determine which data to purge at regular intervals and define the multigenerational Grandfather-Father-Son (GFS) parameters if required.



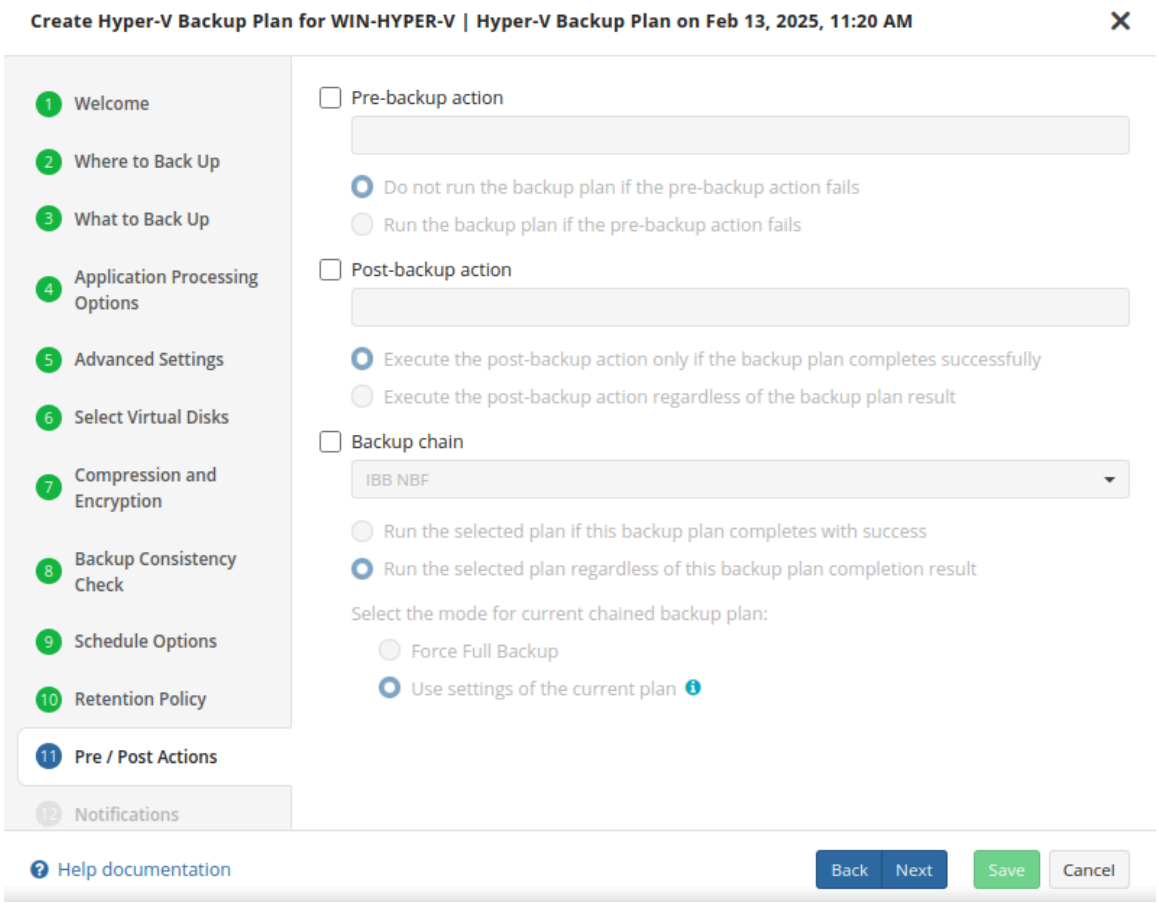
- **Keep backup for:** Determines the minimum age a restore point will be before deletion. Full Backups cannot be purged until the youngest dependent Incremental Backup has reached this age.
- **Enable GFS**: Select this option if you want to keep Full Backups for archival purposes at the selected intervals.
- **Period of keeping weekly full backups**: Set the number of Weekly Full Backups to retain. This is determined separately from the “Keep backup for” value and relies on Full Backups to be scheduled on at least a weekly basis in the previous step.
- **Period of keeping monthly full backups:** Number of Monthly Full Backups to retain. A Full Backup can be flagged as both a Weekly and Monthly backup, but once the number of Weekly Full Backups has exceeded their retention setting, only those also flagged as a Monthly will be retained.

- **Period of keeping yearly full backups:** Set the number of Yearly Full Backups to retain. A Full Backup can be flagged as a Weekly, Monthly, and Yearly Backup. Once the number of Monthly Full Backups has exceeded their retention setting, only those also flagged as a Yearly will be retained.
    - **Select the first successful full backup as of**: Select the first Monthly Full Backup you would like to flag and retain as the first Yearly Full Backup.

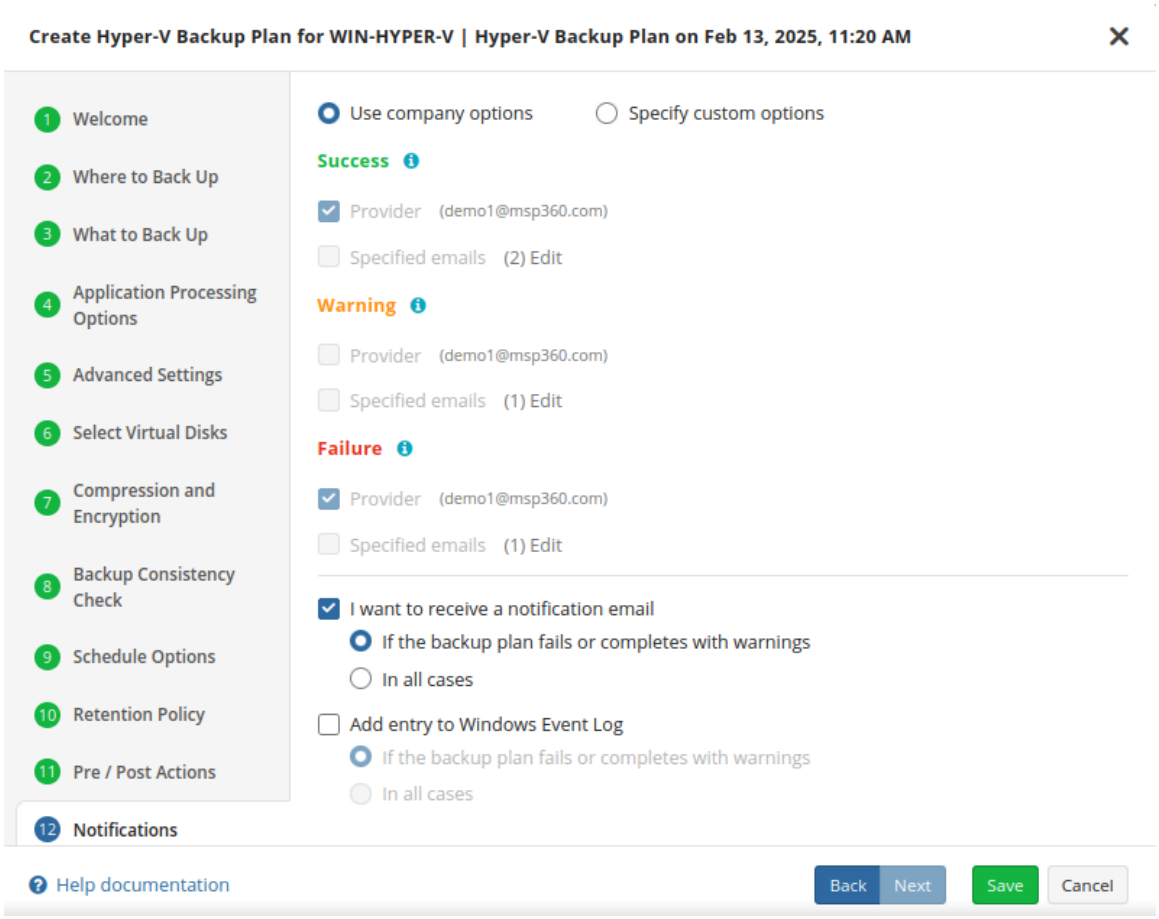
Restore Points will not be deleted until the youngest point in the chain has met the retention criteria.

GFS Retention provides an excellent way to efficiently archive data for compliance. Additional information can be found in GFS Policy topics in the MBS Documentation

Step 13. After the schedule is set, the next section is used to set the “Pre” and “Post” Actions



Step 14. The final step is to review the Notifications and Logging. The default settings applied at the Company level are selected by default, however you are also able to specify custom options per plan.

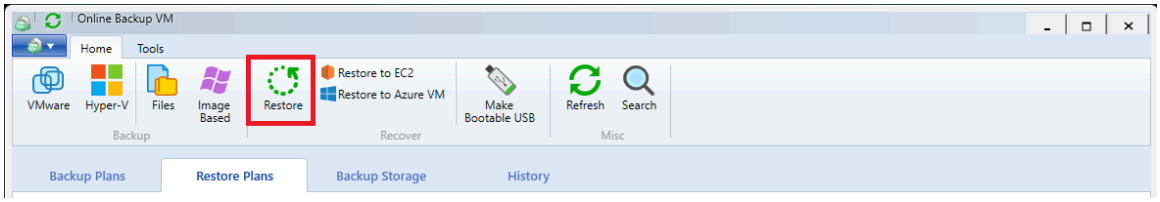


Once you are satisfied with the selected notifications and logging, clicking “Save” will create the new plan and close the wizard.

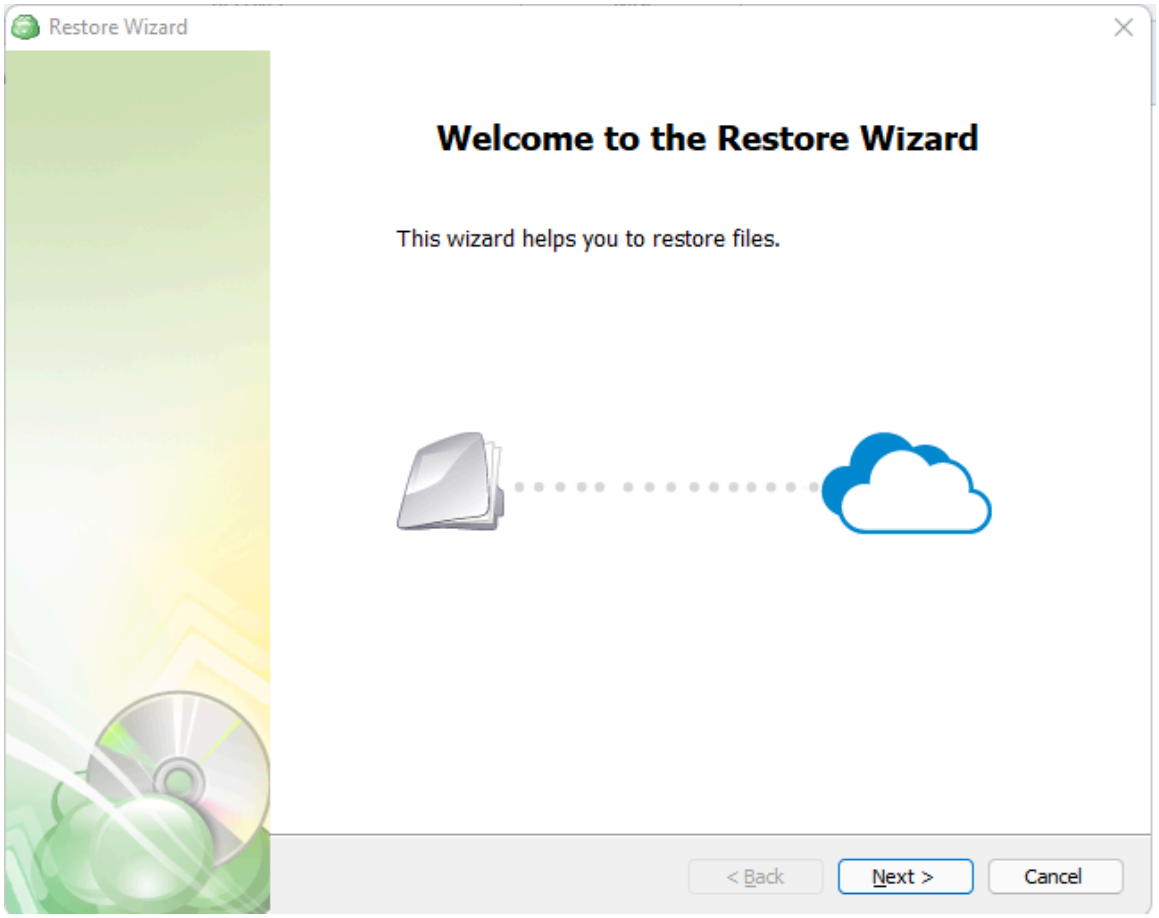
Hyper-V Restore Plans

Restore as a VM using the Agent

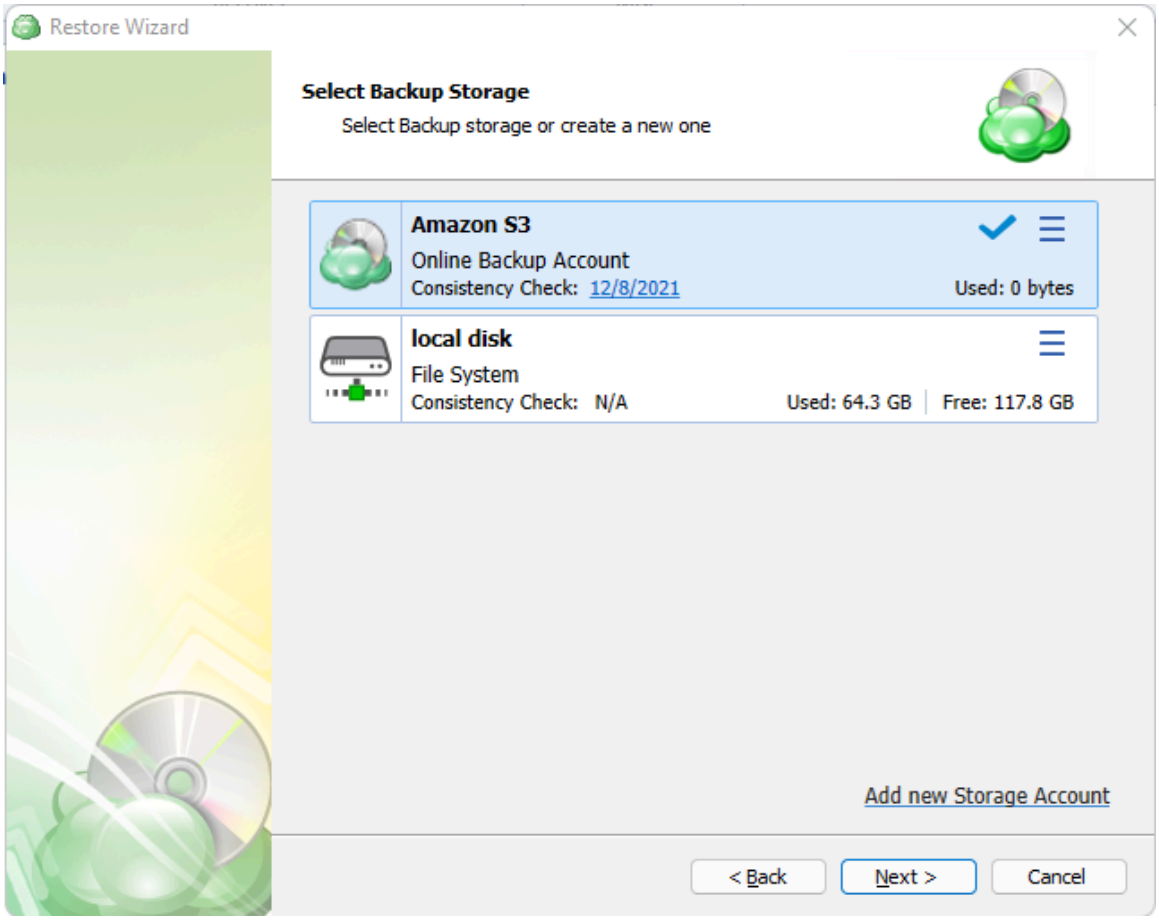
Step 1. Within the Online Backup Agent, click on “Restore”



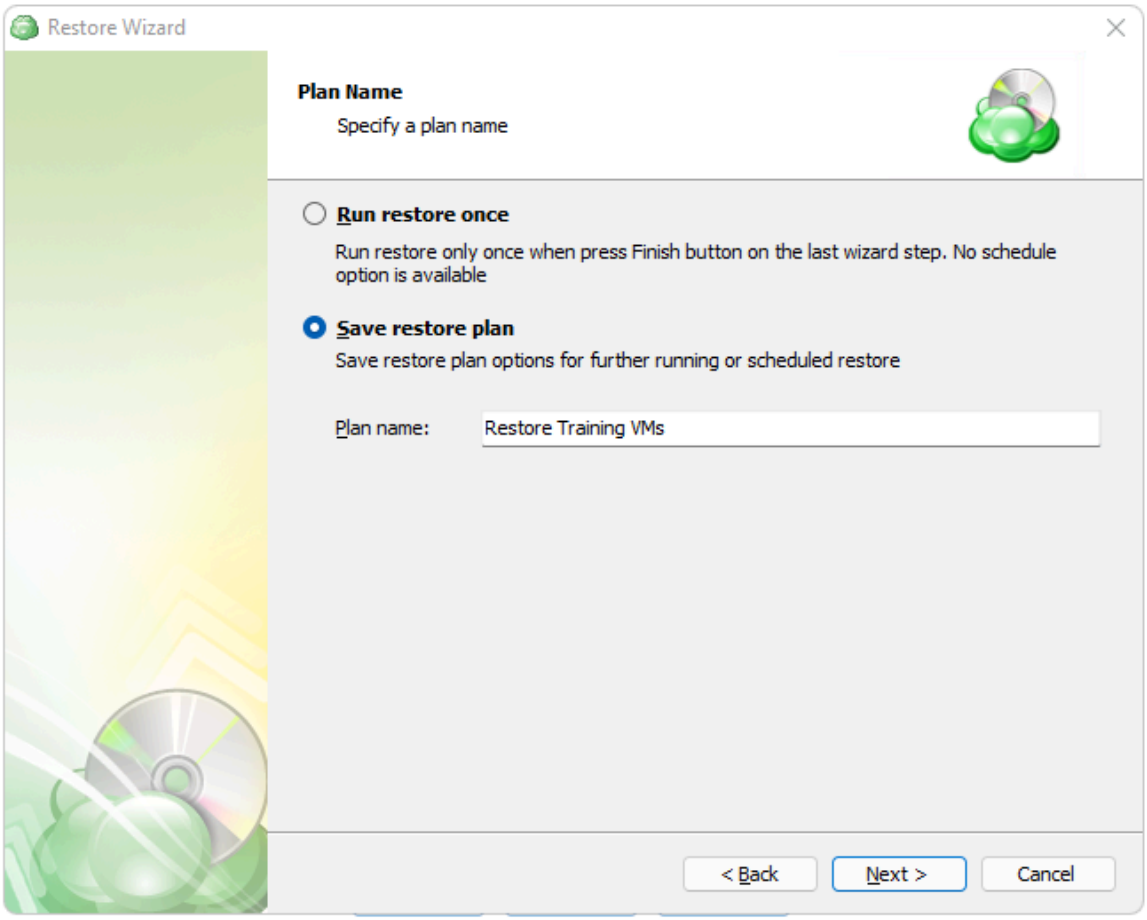
Step 2. Once the wizard starts, click on Next to advance to the next step.



Step 3. The next step will prompt you to select the source for the restore point.



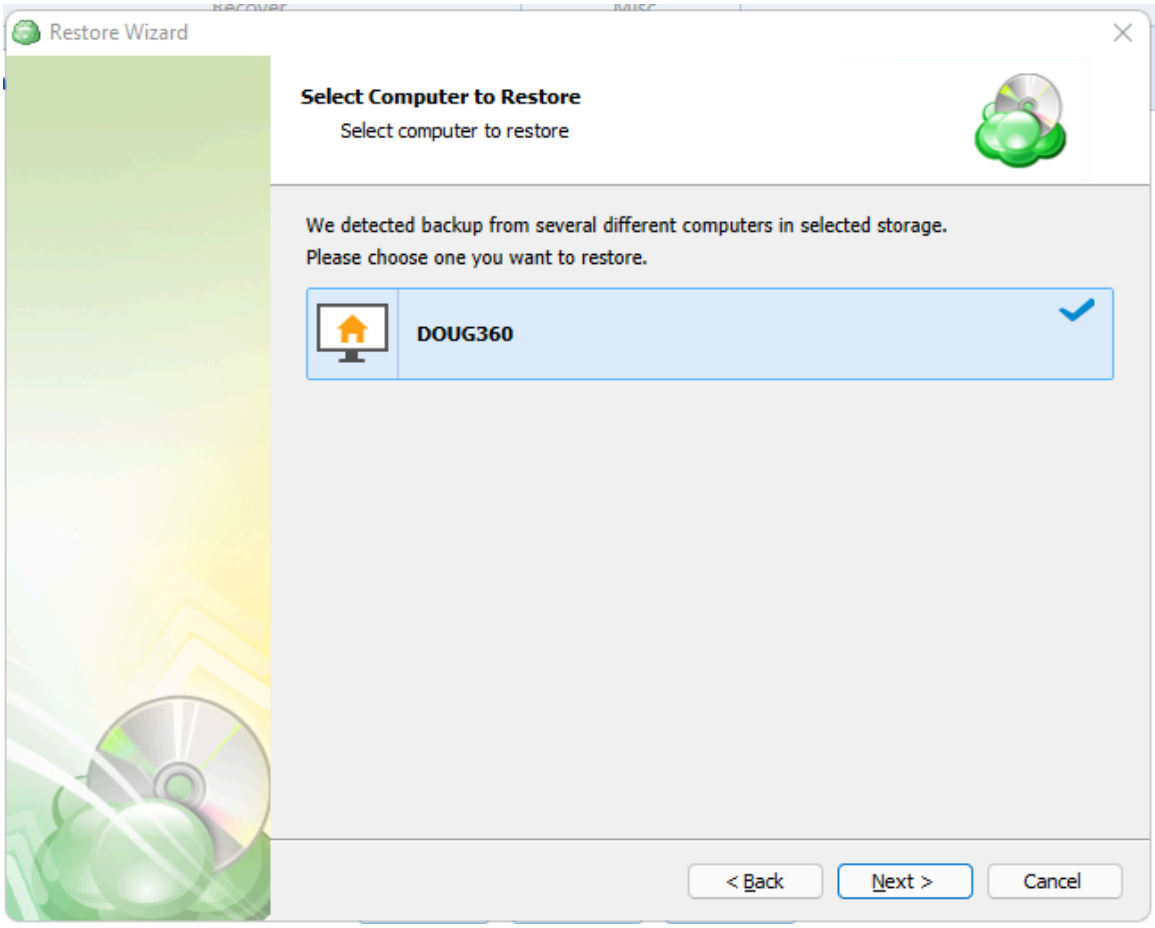
Step 4. Next, you will be given the option to either run the restore once or to save it to run later.



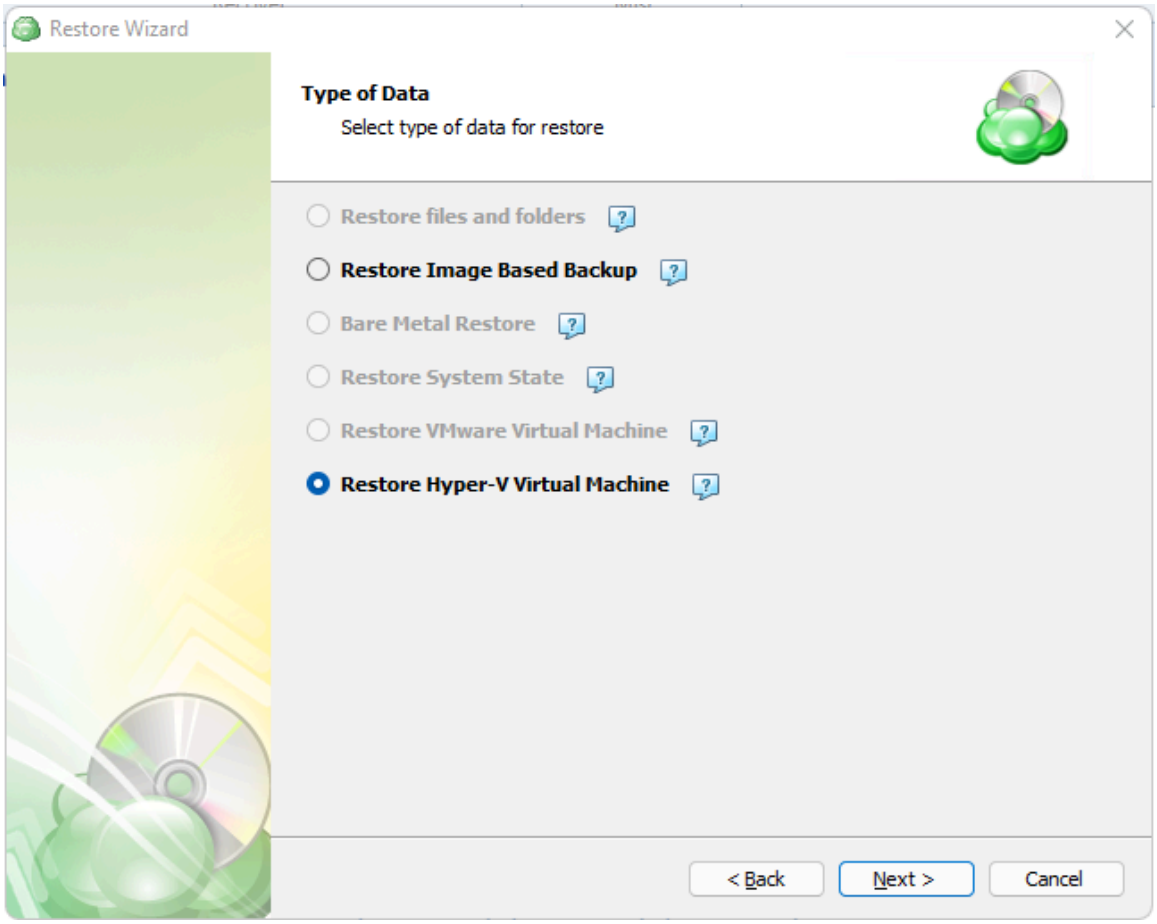
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

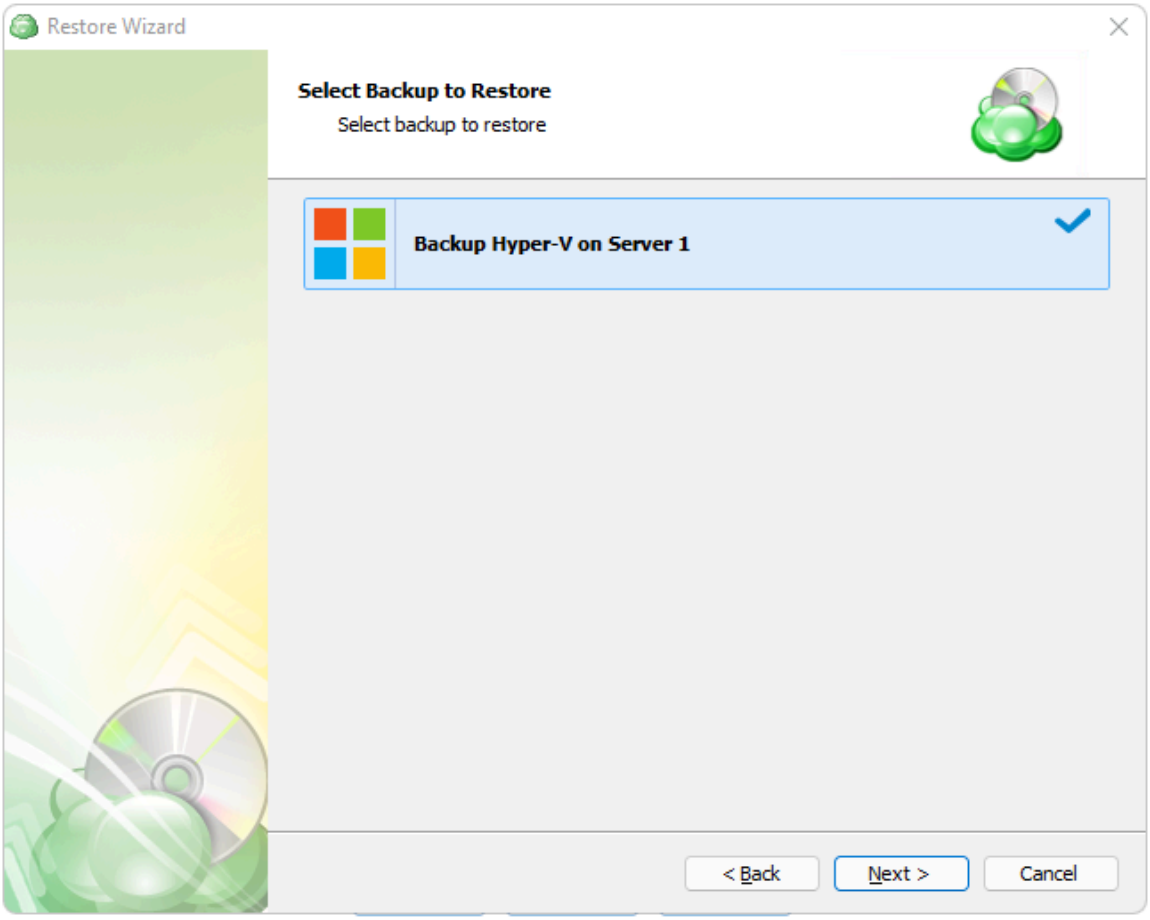
Step 5. With the type of restore selected, the next step is to select the correct Host server which the VM resides on.



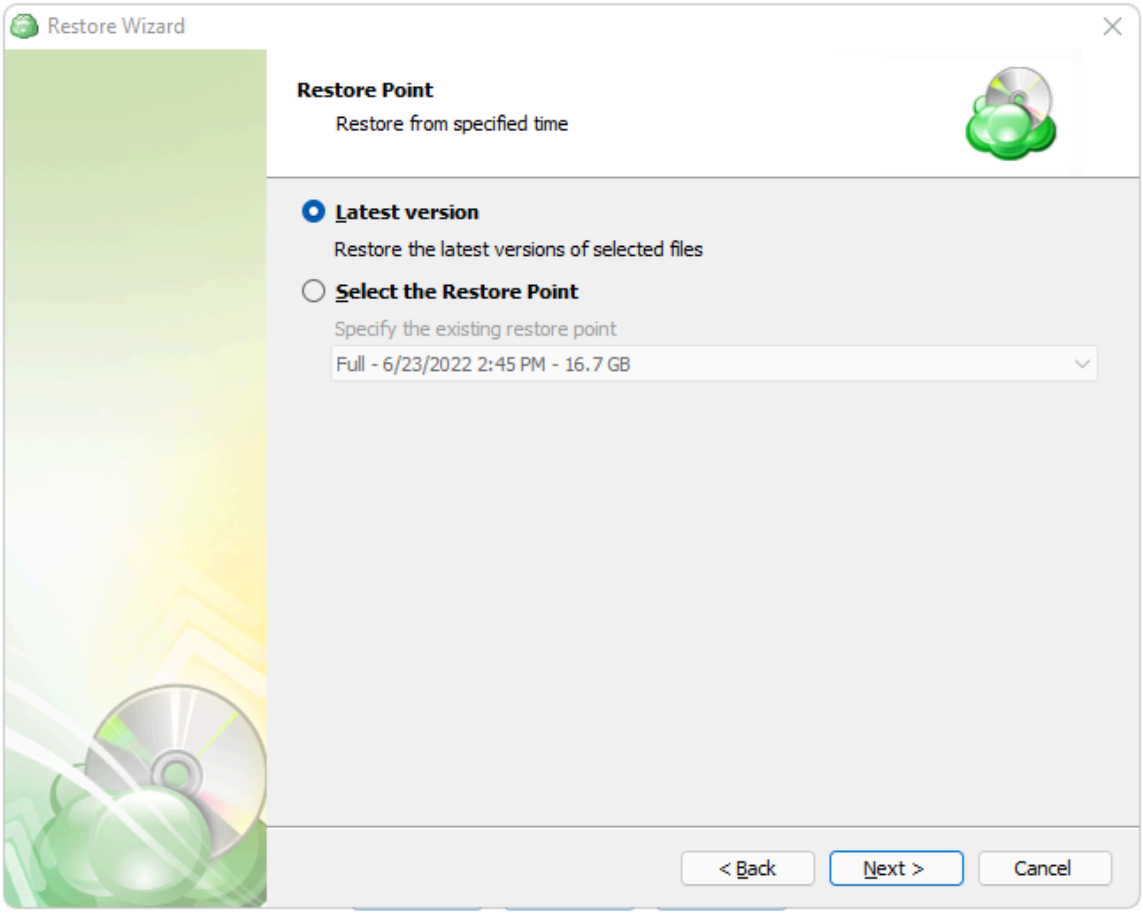
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore Hyper-V Virtual Machine” option to continue.



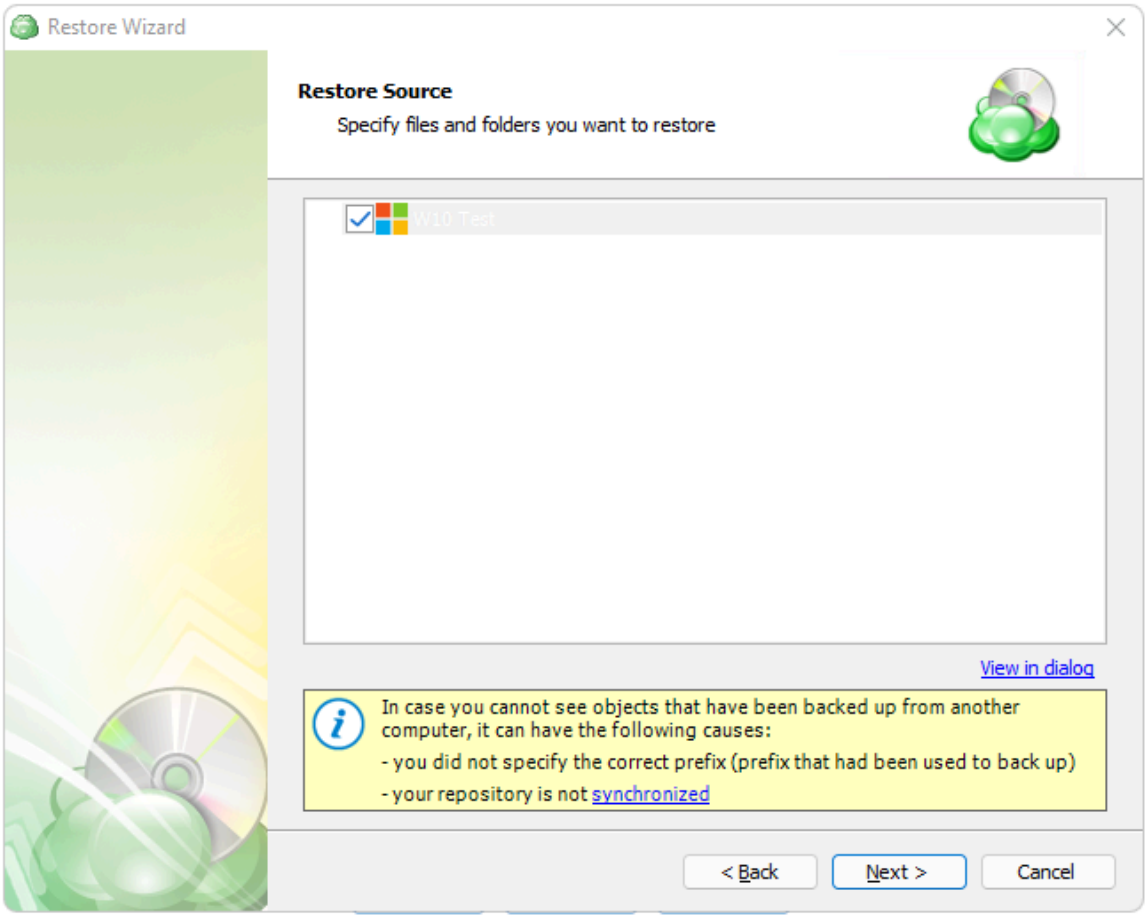
Step 7. With the correct type of data selected, the application will generate a list of available VM backup plans.



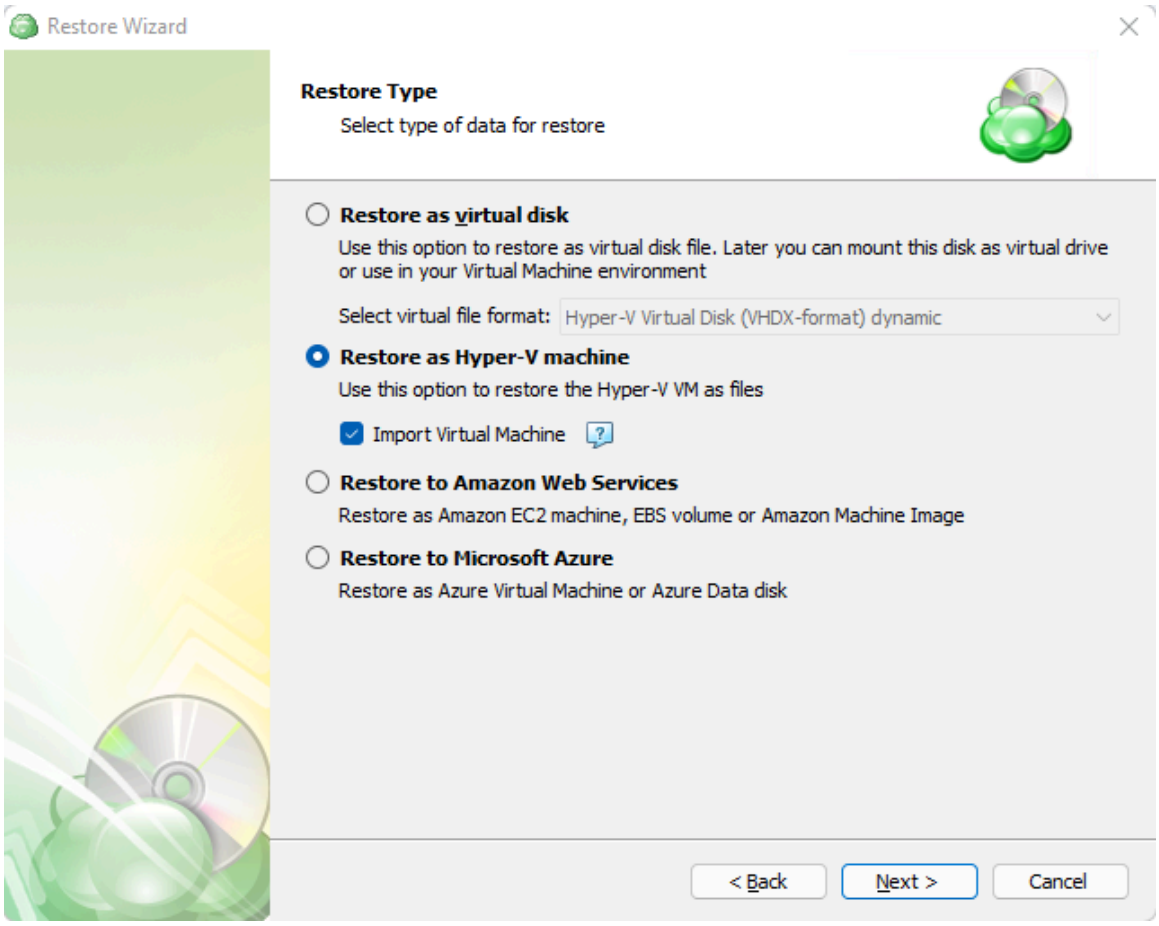
Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.



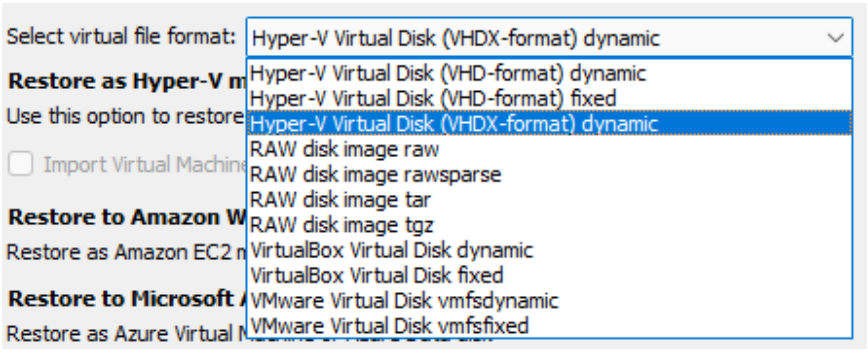
Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which to restore.



Step 10. The next step of the wizard allows you to choose how the VM data should be restored.

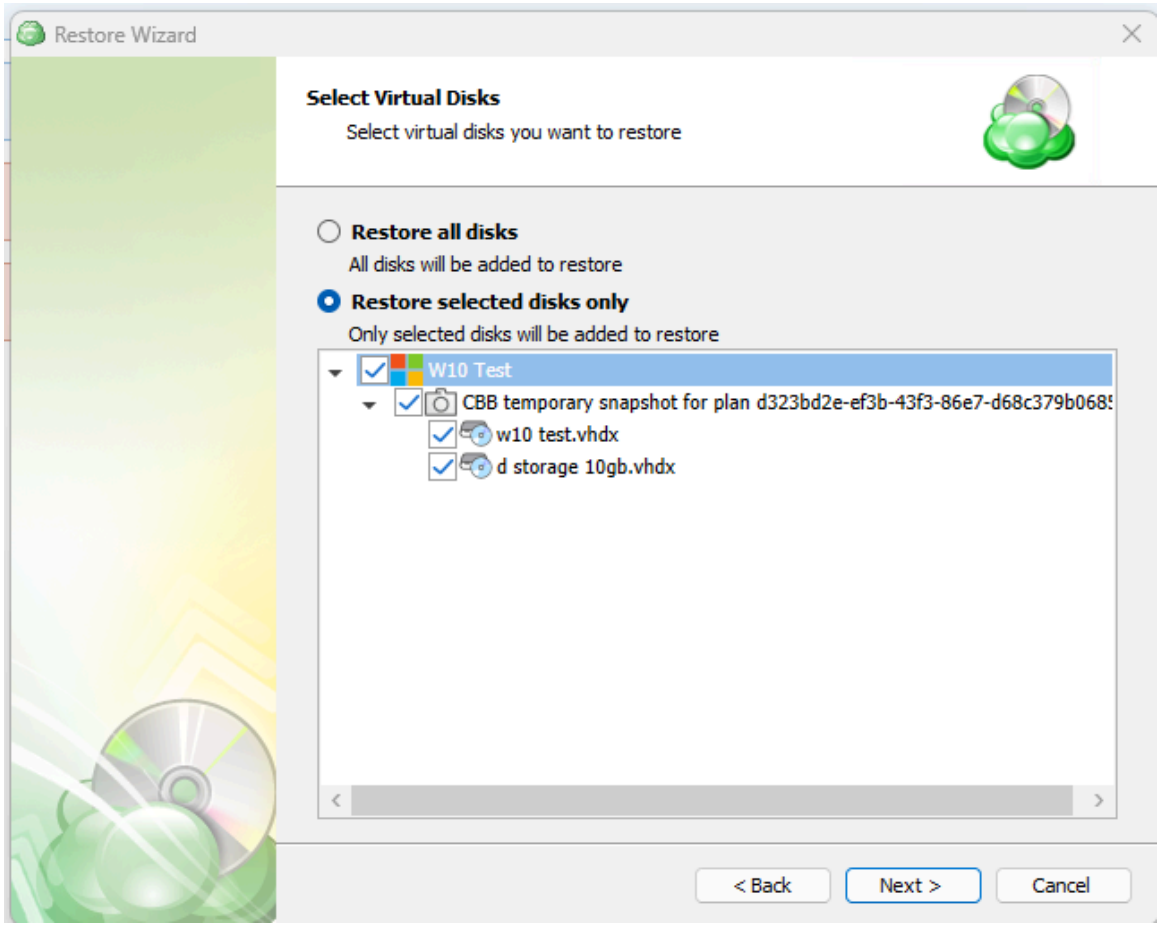


- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:



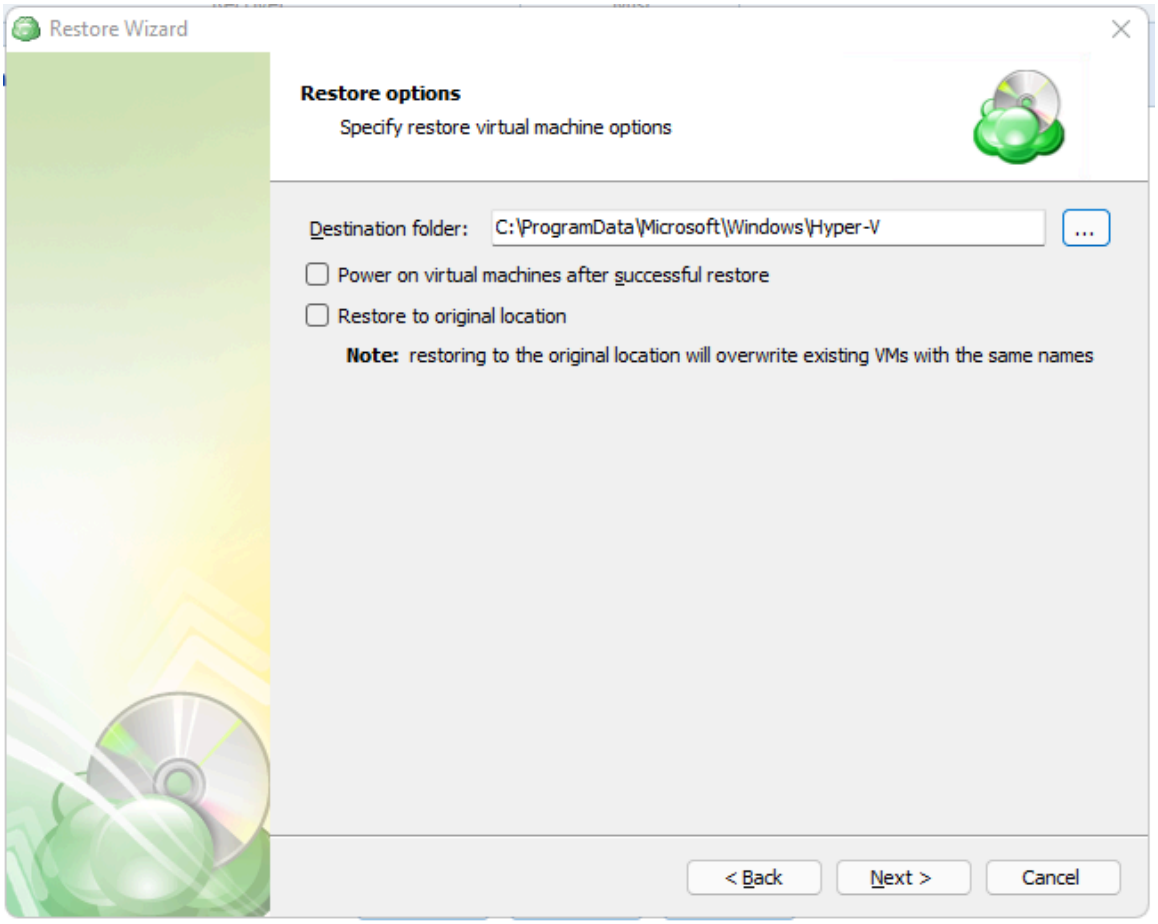
- **Restore as a Hyper-V machine:** Selecting this option restores the virtual machine configuration as well as the virtual disks as files, but does not import the VM into the hypervisor by default.
    - **Import Virtual Machine:** Use this option to have the VM automatically imported to the hypervisor.
- **Restore to Amazon Web Services:** If enabled, this will restore the selected VM directly to AWS Cloud either as an EC2 instance, EBS volume, or AMI.
- **Restore to Microsoft Azure:** This will restore the VM directly to Azure as either an Azure Virtual Machine or Azure Data disk.

Step 11. The next step is to choose the disks to be restored.

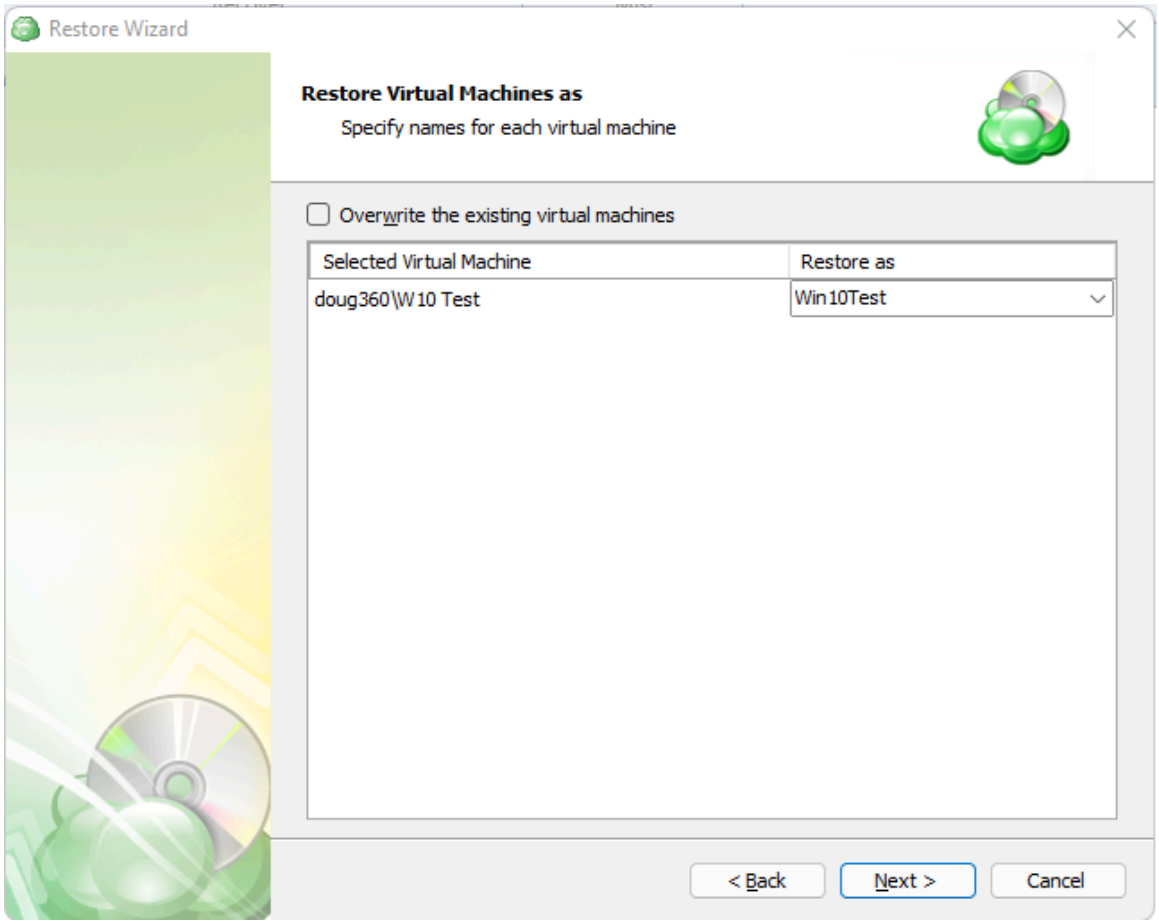


Here you can choose whether to restore all virtual disks associated with each selected VM or only restore selected disks.

Step 12. The next step is to choose a destination for the restored VM or virtual disk.

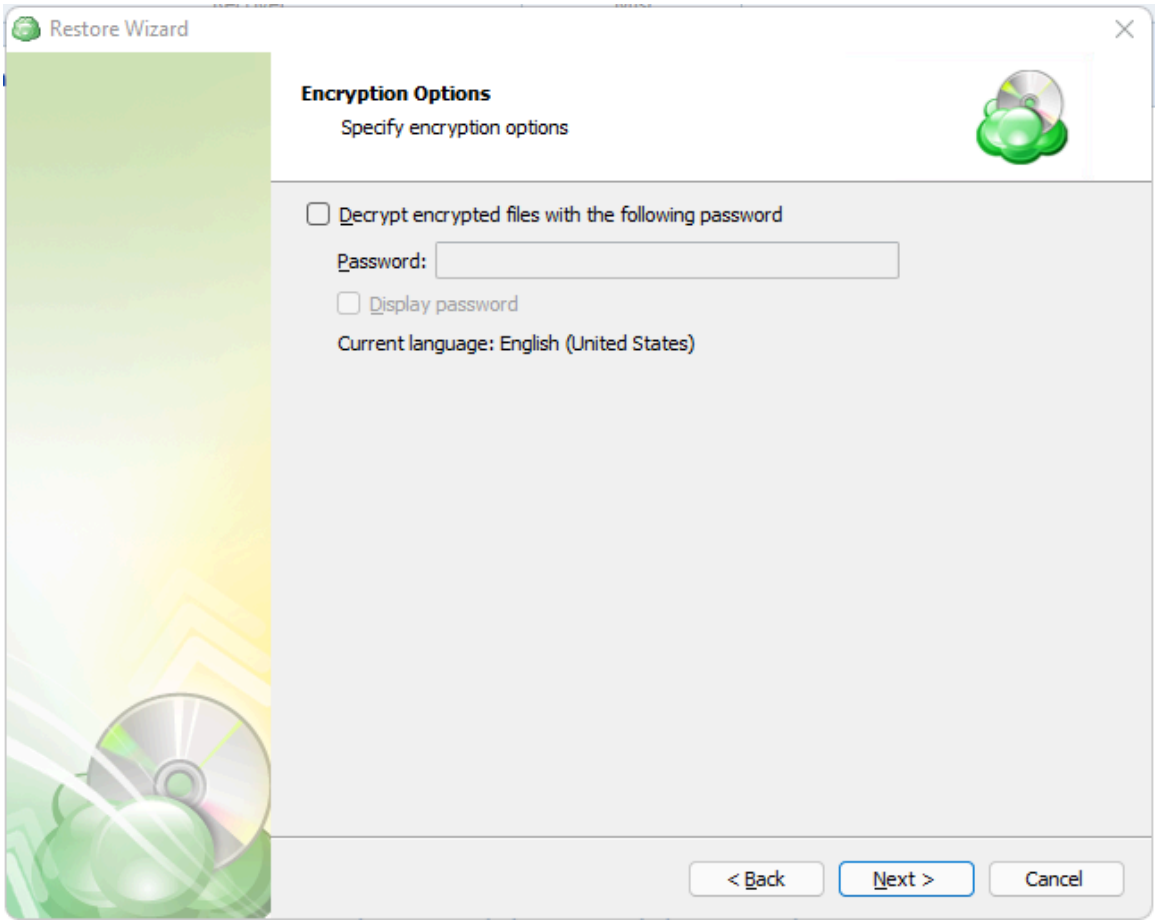


Step 13. Once the destination is selected, you are presented with additional options for importing the restored VM.

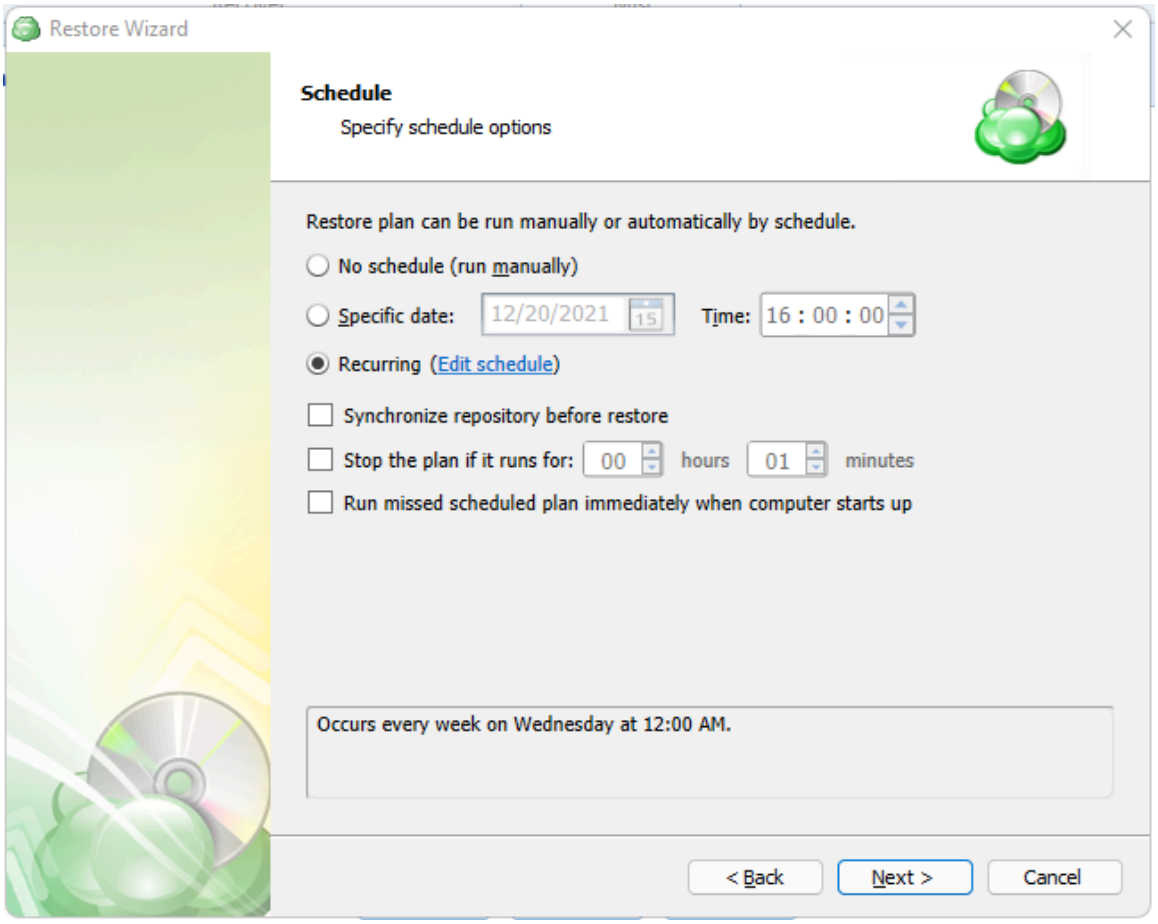


> Selecting a VM from the dropdown will require you to click on “Overwrite the existing virtual machines” in order to continue. To specify that it should be restored as a new VM, click into the text of the dropdown and type in the new name.

Step 14. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the VM.



Step 15. With the decryption password entered, the next step is setting the schedule for the restore plan.

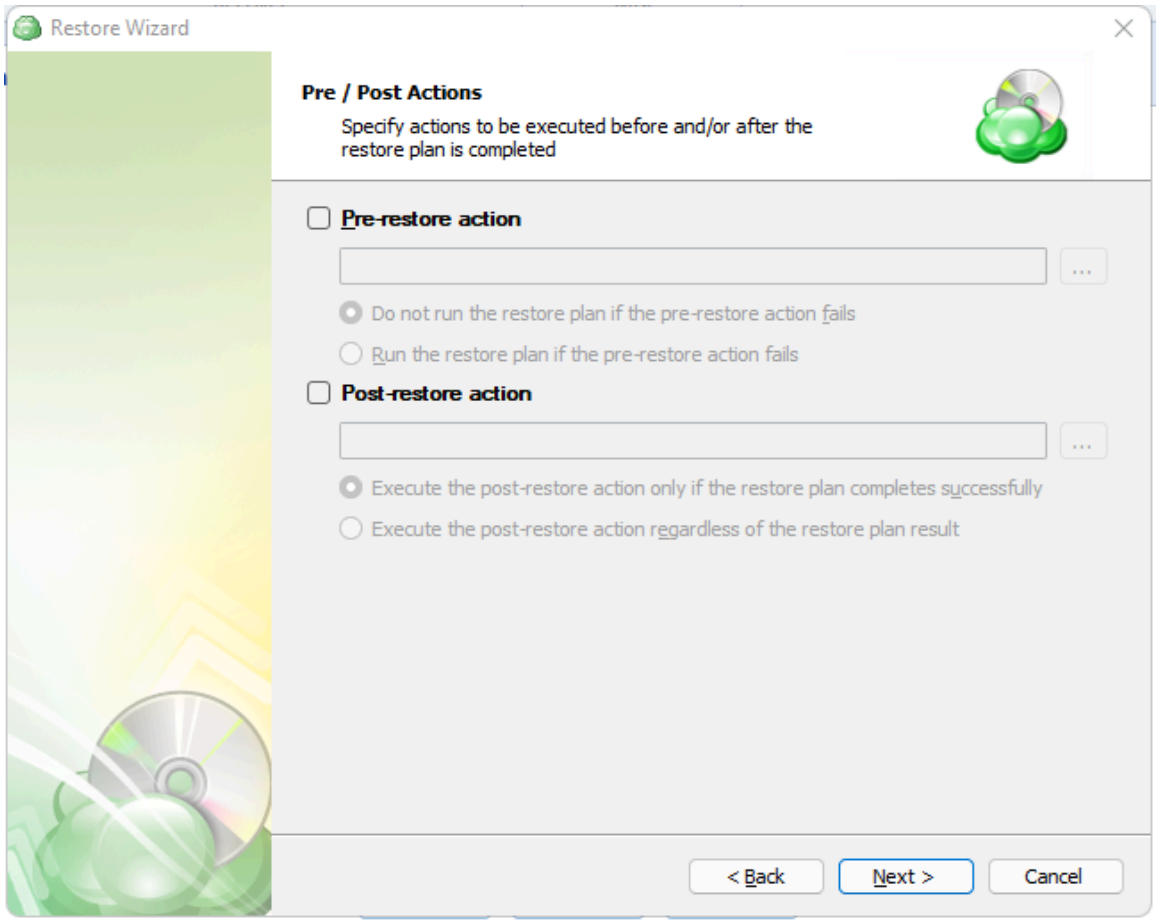


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

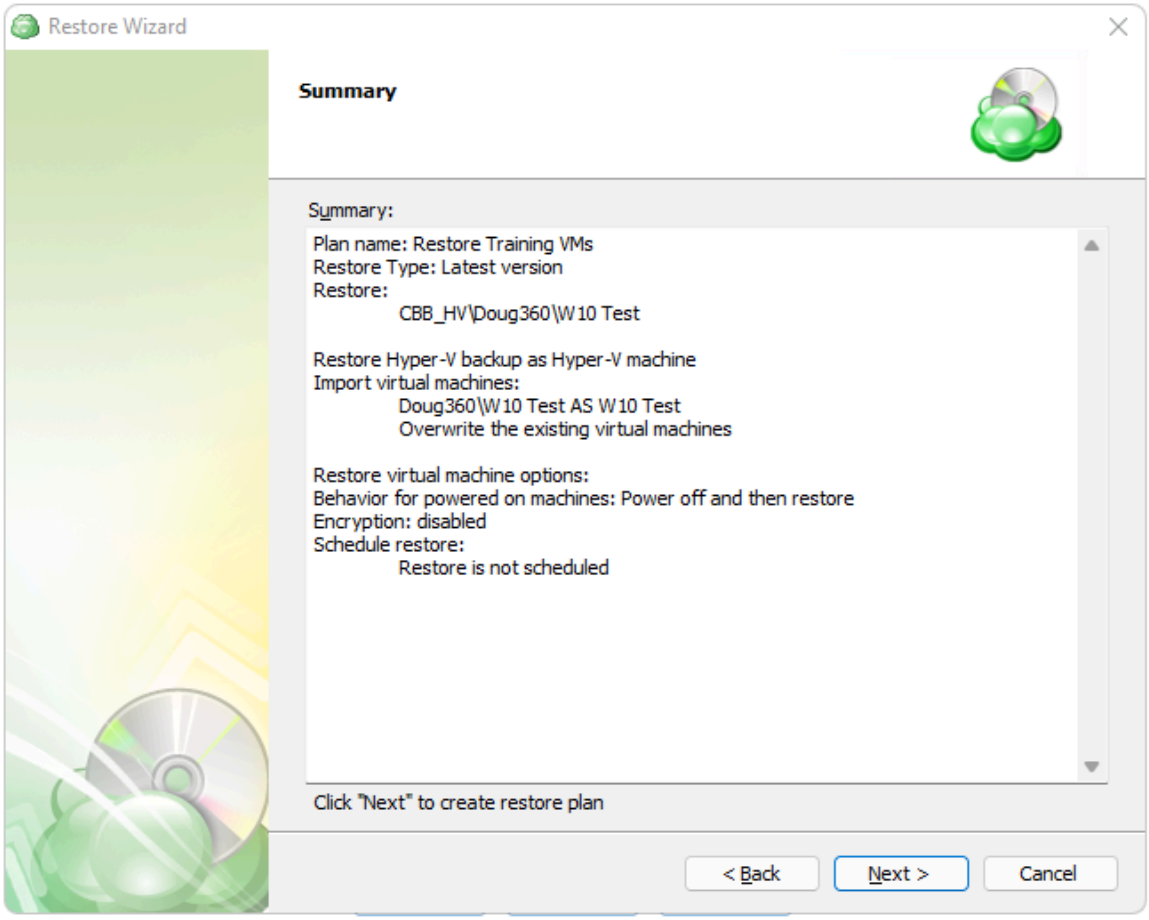
> Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 16. After setting the schedule, the next step allows pre and post actions to be defined.



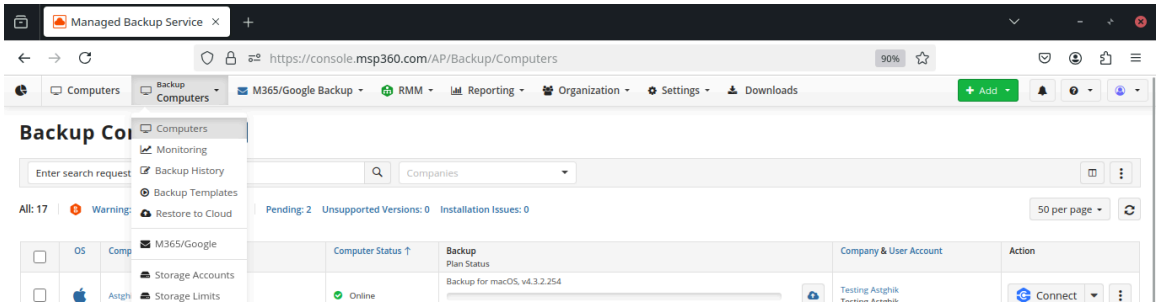
Step 17. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.



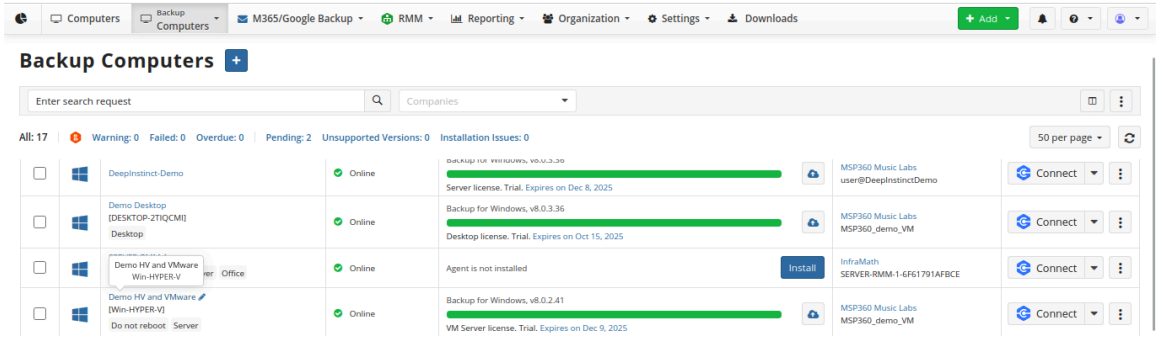
If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

Restore as a VM using MBS

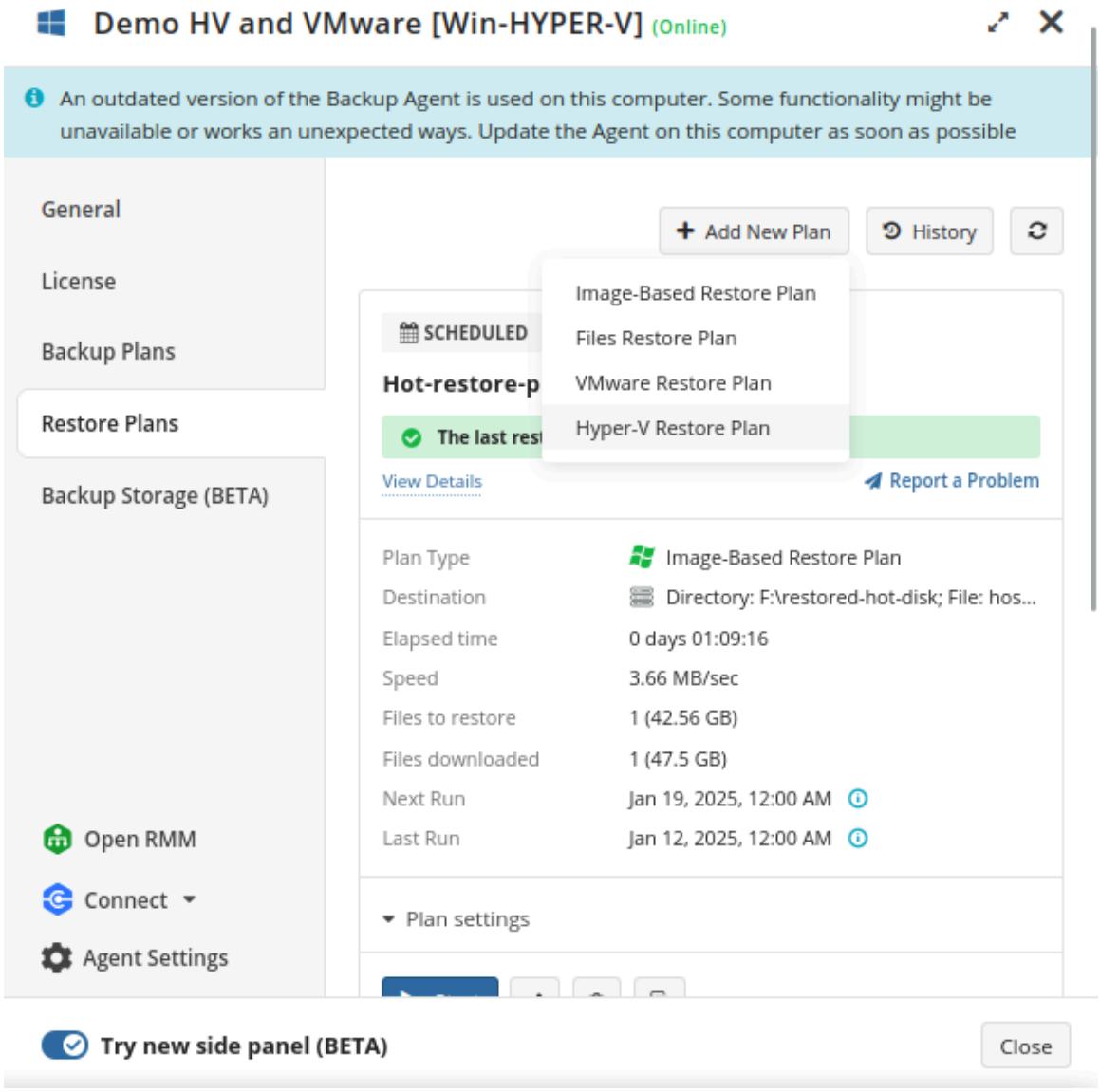
Step 1. From the MBS Portal, left-click Backup > Computers



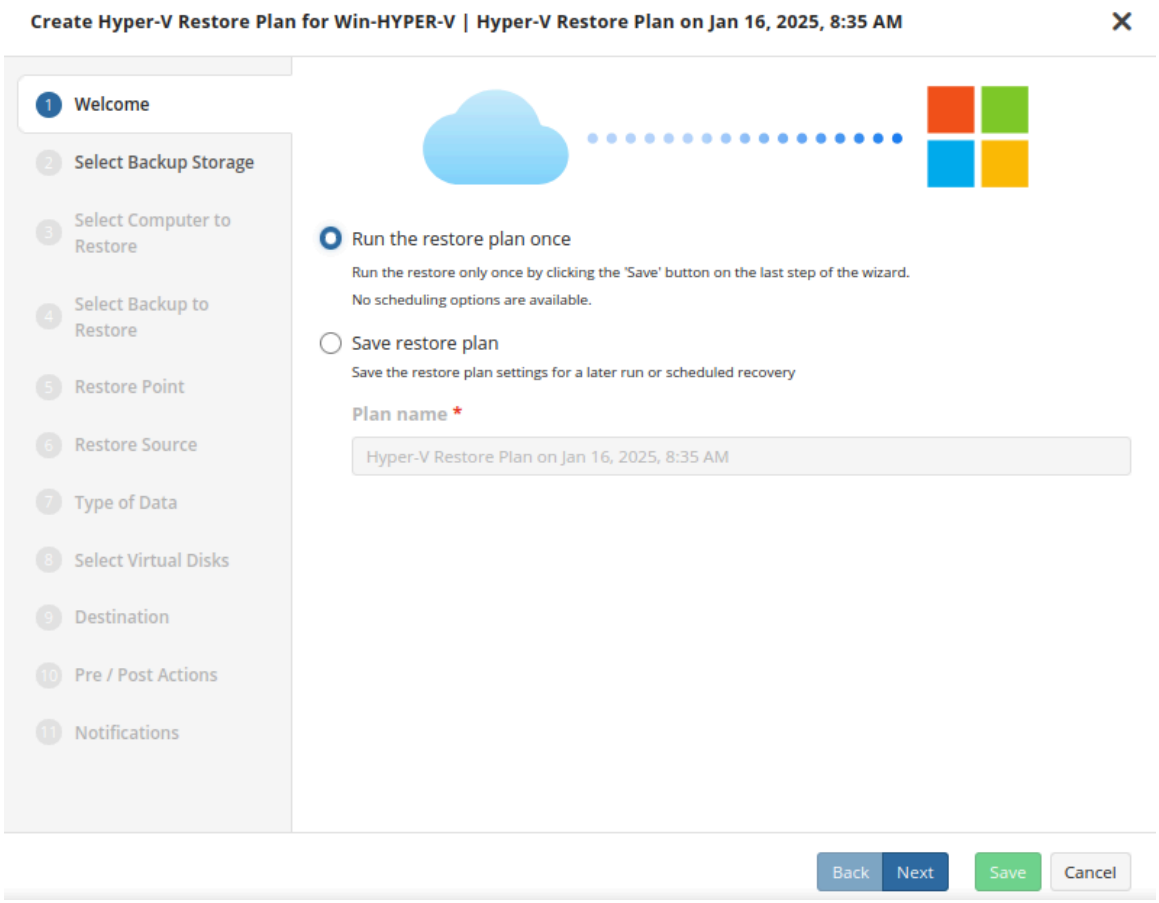
Step 2. Locate the computer you wish to backup from the list and open the current list of plans by either clicking on the name of the computer, or by selecting “Show Plans” from the gear menu.



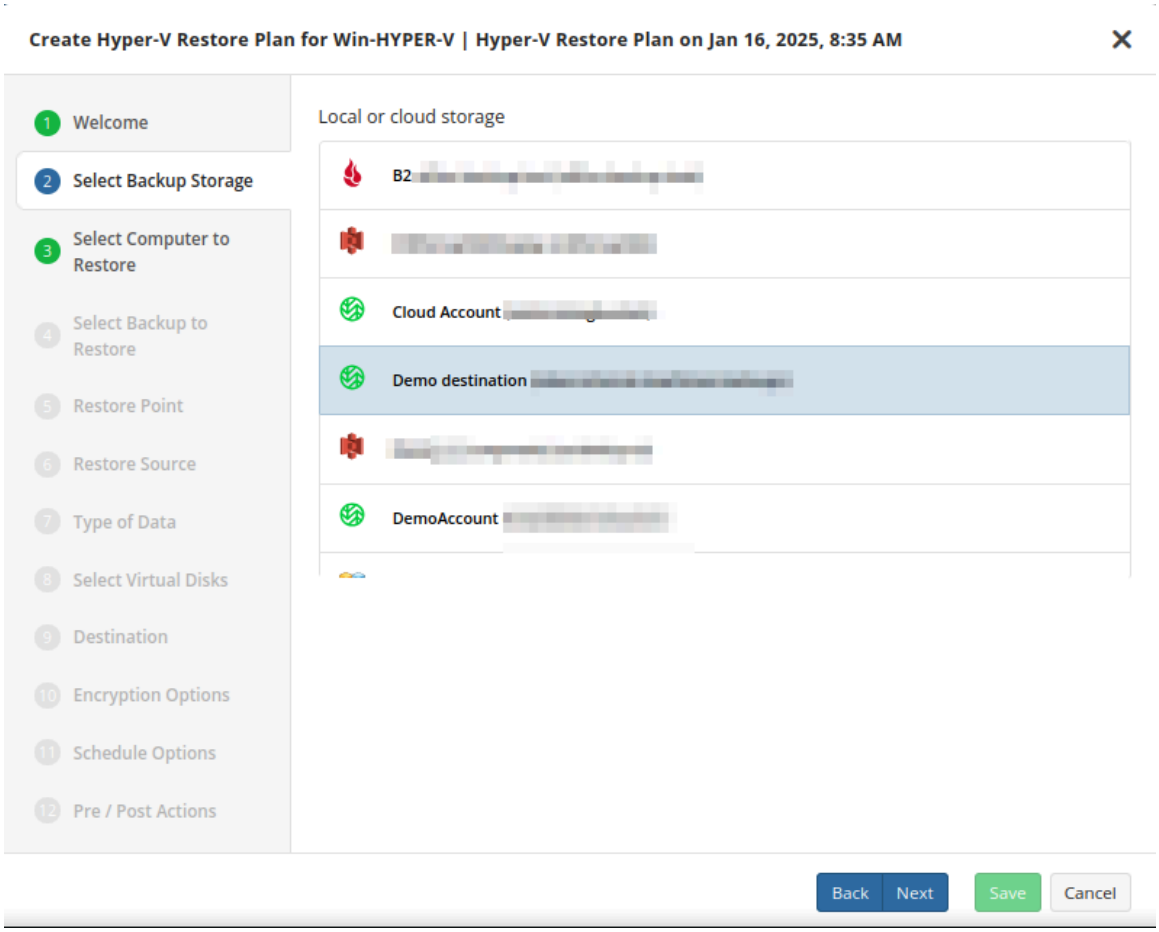
Step 3. Click ‘Restore Plans’ then ‘Add New Plan’ button and select ‘Hyper-V Restore Plan’



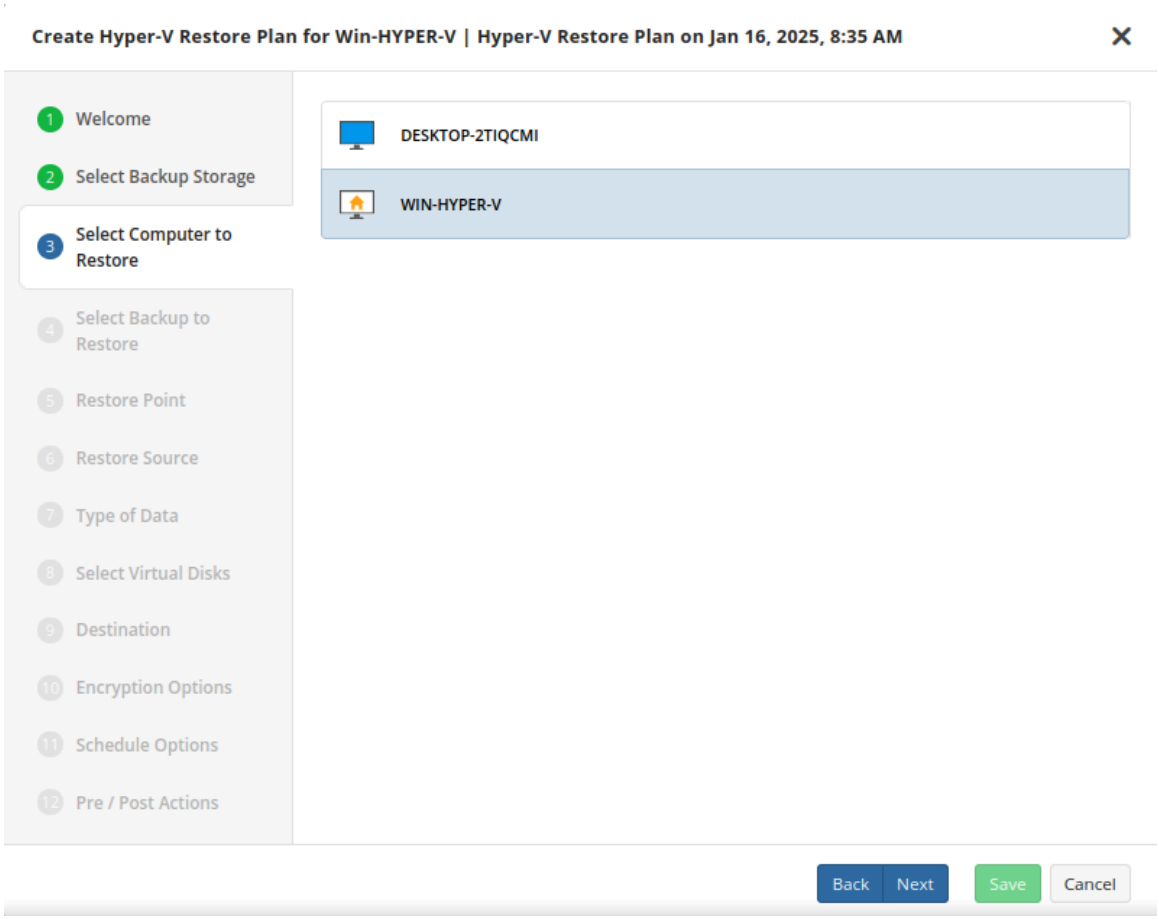
Step 4. The first step when making a Restore Plan is to select if it should run only once, or if it should be saved for future or scheduled use. The latter will allow you to name the plan.



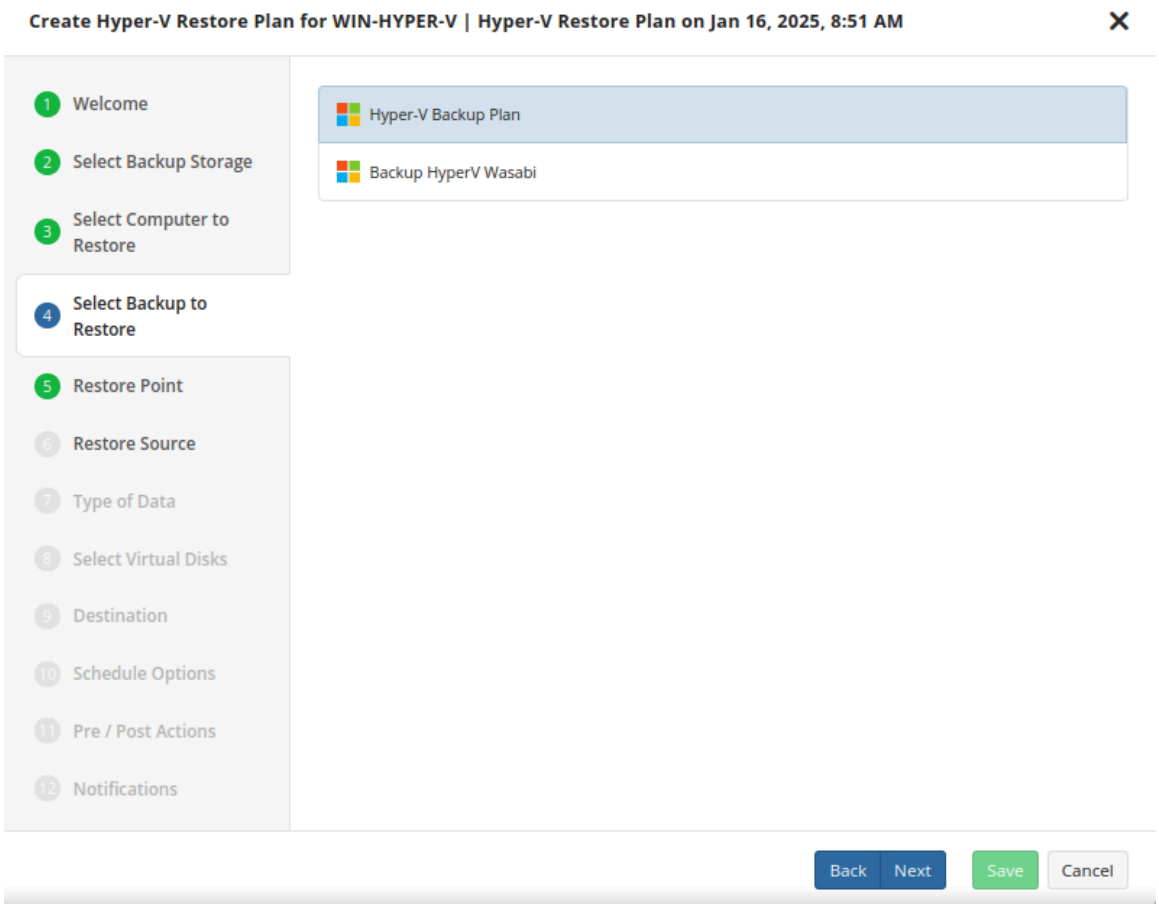
Step 5. Next, select the storage which contains the desired data.



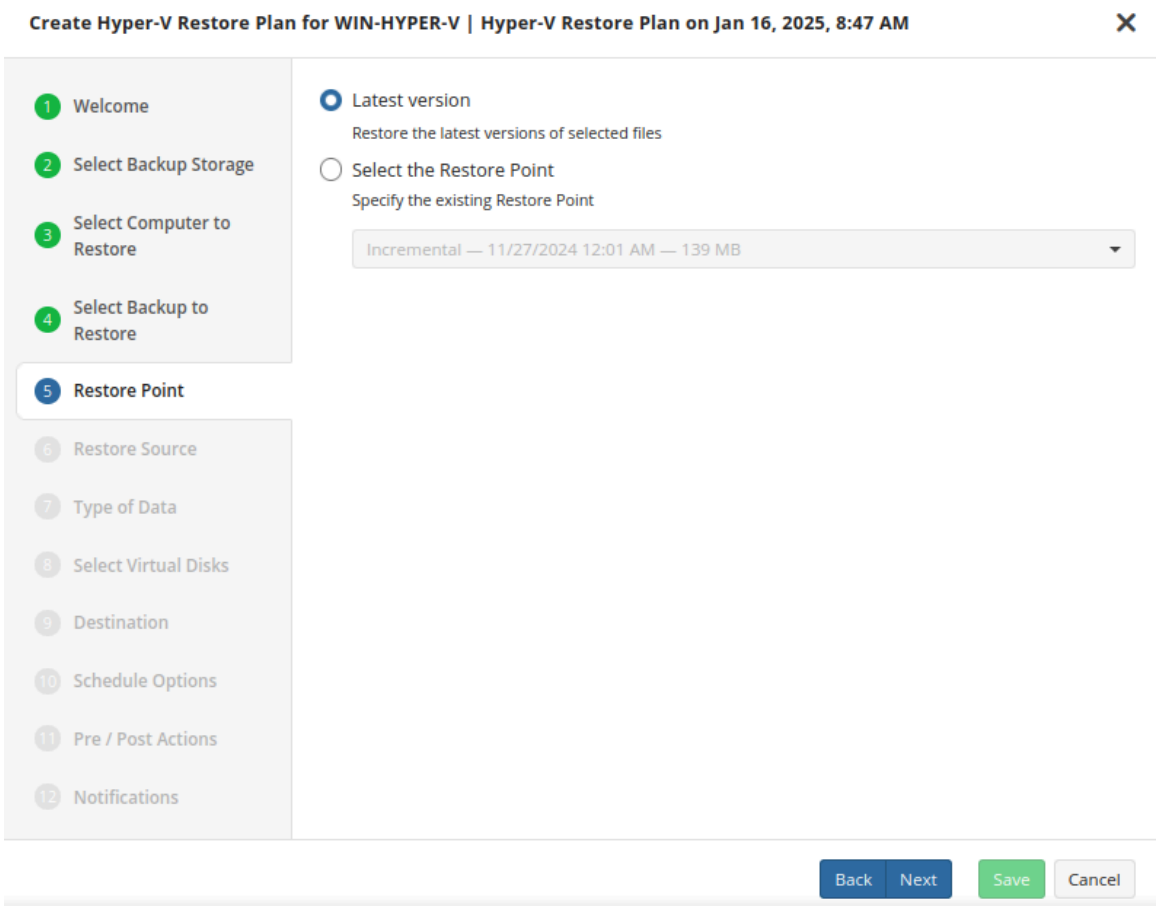
Step 6. Next, select the Host that the VM was backed up from.



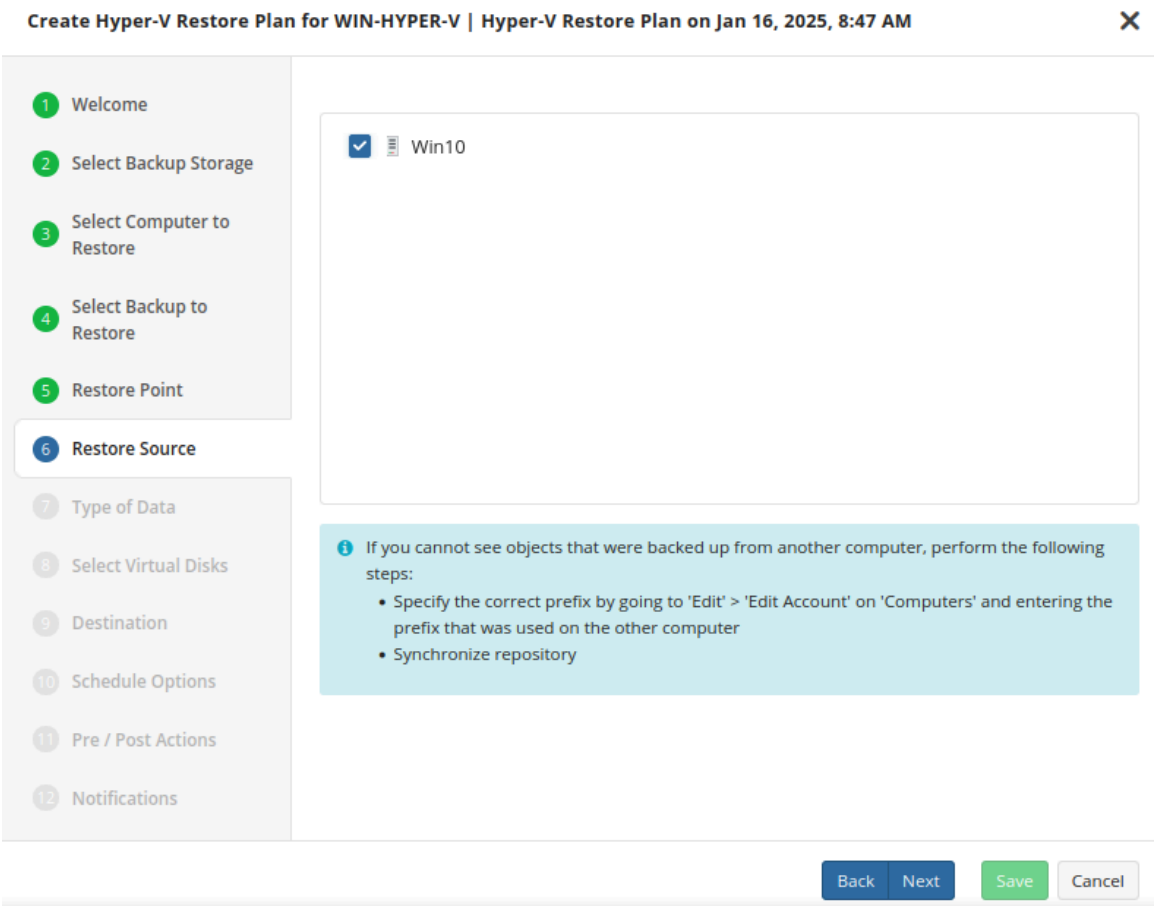
Step 7: Select the backup plan you want to restore from.



Step 8: Select the restore point you want to restore

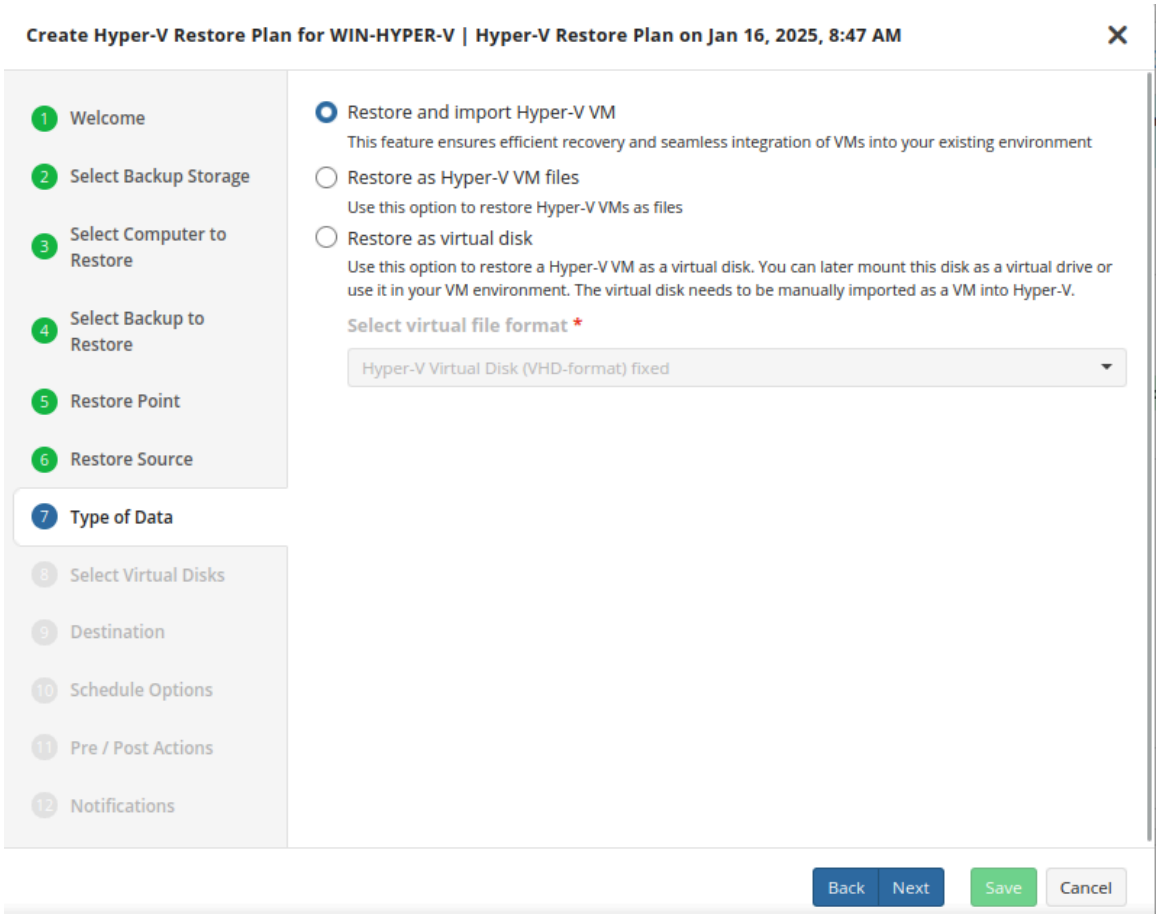


Step 9: Next, you will be able to expand the list of VM backups on the selected host and choose which VM to restore.



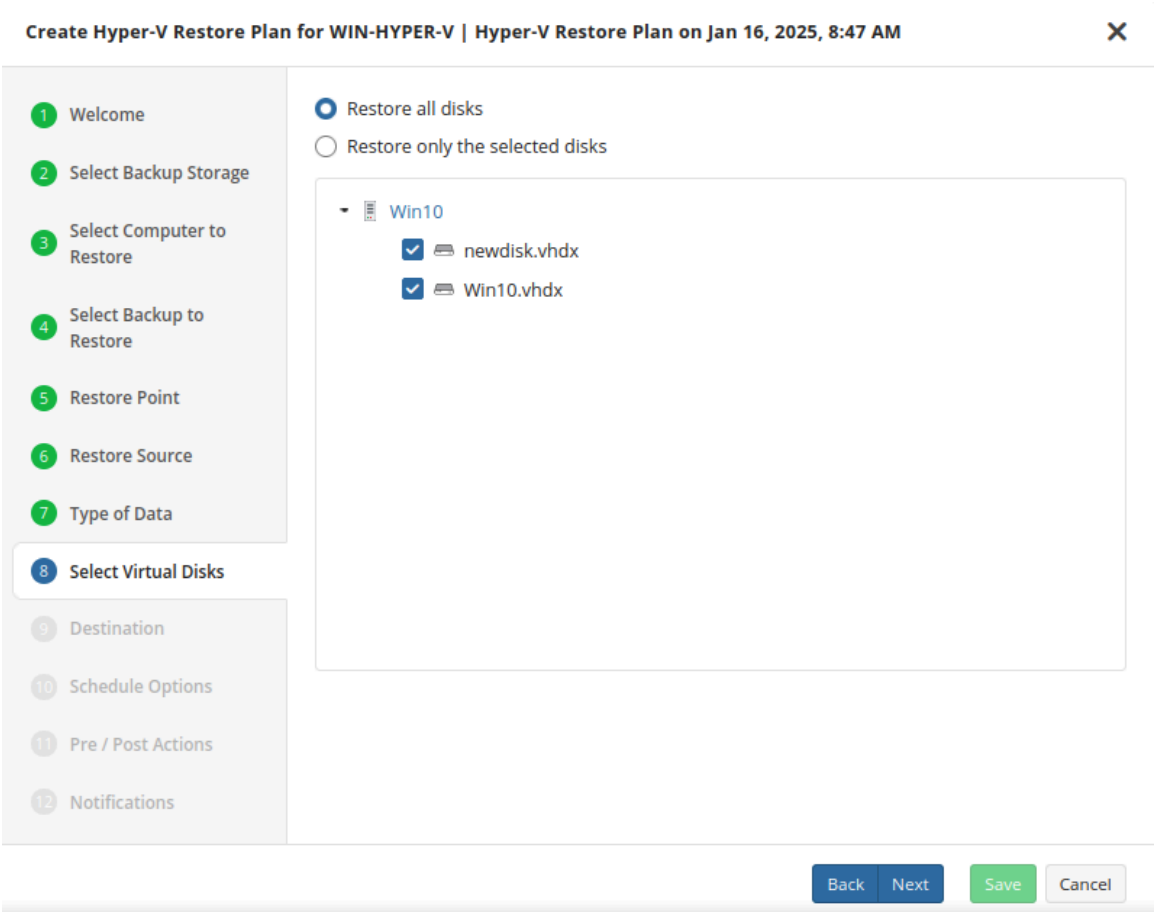
If backed-up objects are missing, ensure the correct **prefix** is specified (the same one used for backup) and verify that the **repository is synchronized** to update available backups.

Step 10: The next step of the wizard allows you to choose how the VM data should be restored. To restore as a Hyper-V VM and automatically import it to the hypervisor, select “Restore and Import Hyper-V VM”.

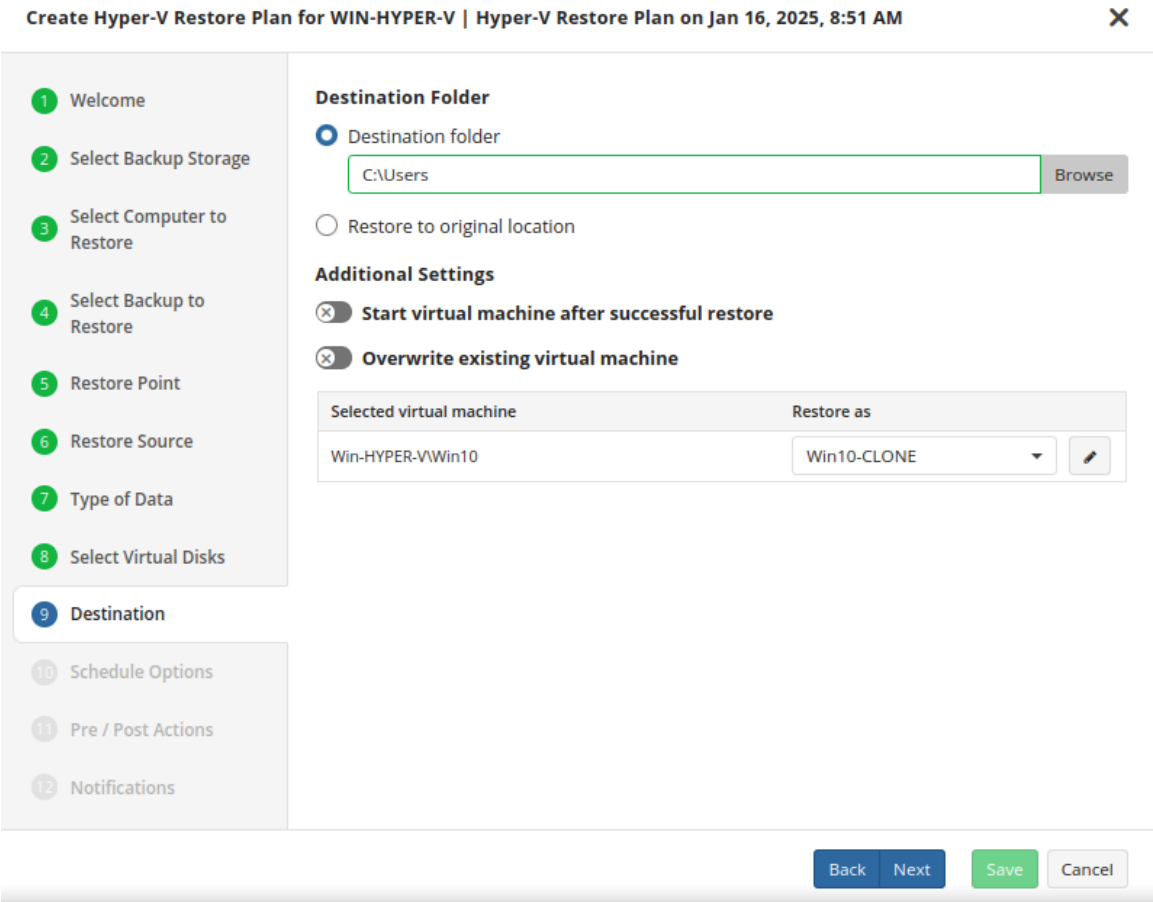


- **Restore and Import Hyper-V VM:** Selecting this option restores the virtual machine configuration as well as the virtual disks to your Hyper-V existing environment
- **Restore as Hyper-V VM Files:** It lets you restore your Virtual machines as files (vhdx extension)
- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:

Step 11: The next step of the wizard allows you to choose the disks to be restored.



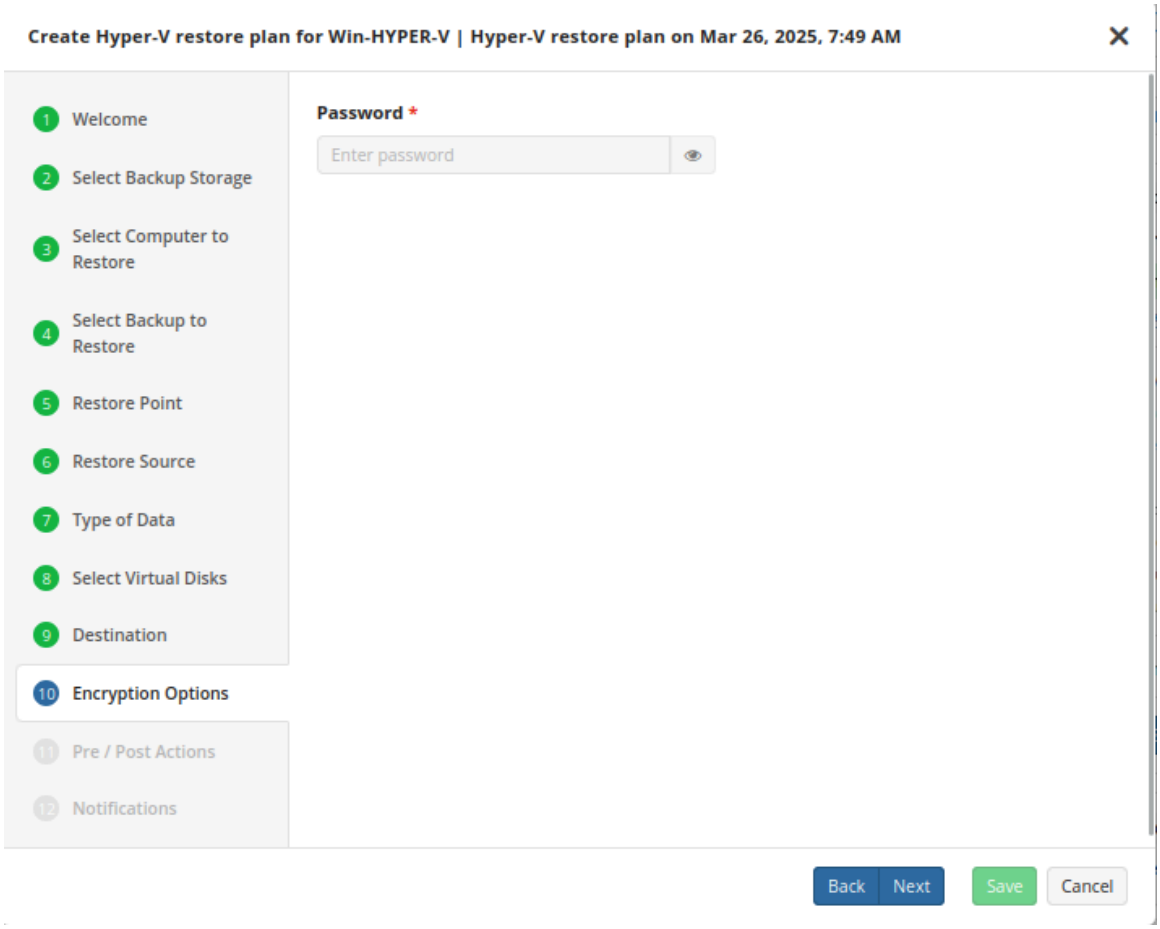
Step 12: In this step of the Restore Wizard, you configure where and how the virtual machine (VM) will be restored.



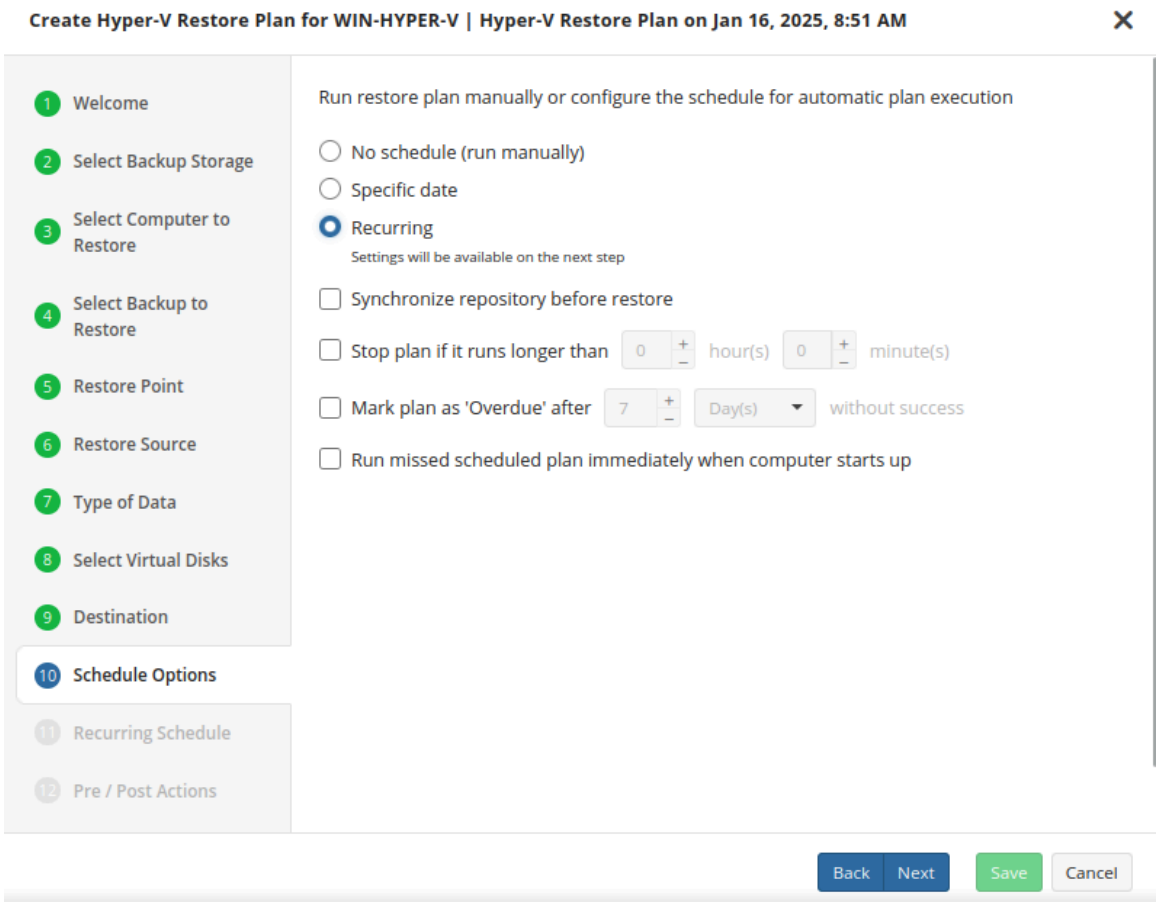
- **Destination Folder:** Select the destination disk on the VMware host where the VM should be restored to.
- **Restore to original location:** Restores the virtual disks to the original path specified in the VM configuration.
- **Start virtual machine after successful restore:** Enabling will start the VM automatically after a successful restore.
- **Overwrite existing virtual machine:** Enabling this will allow the restore to replace any existing VM files.

> If you wish to restore it as a different name or target VM, select or type over the value in the “Restore as” list.

Step 13. If your backups were encrypted within the backup plan, enter the password to decrypt them.



Step 14: If you choose to save the restore plan, the schedule is configured during steps 10 and 11 of the wizard.



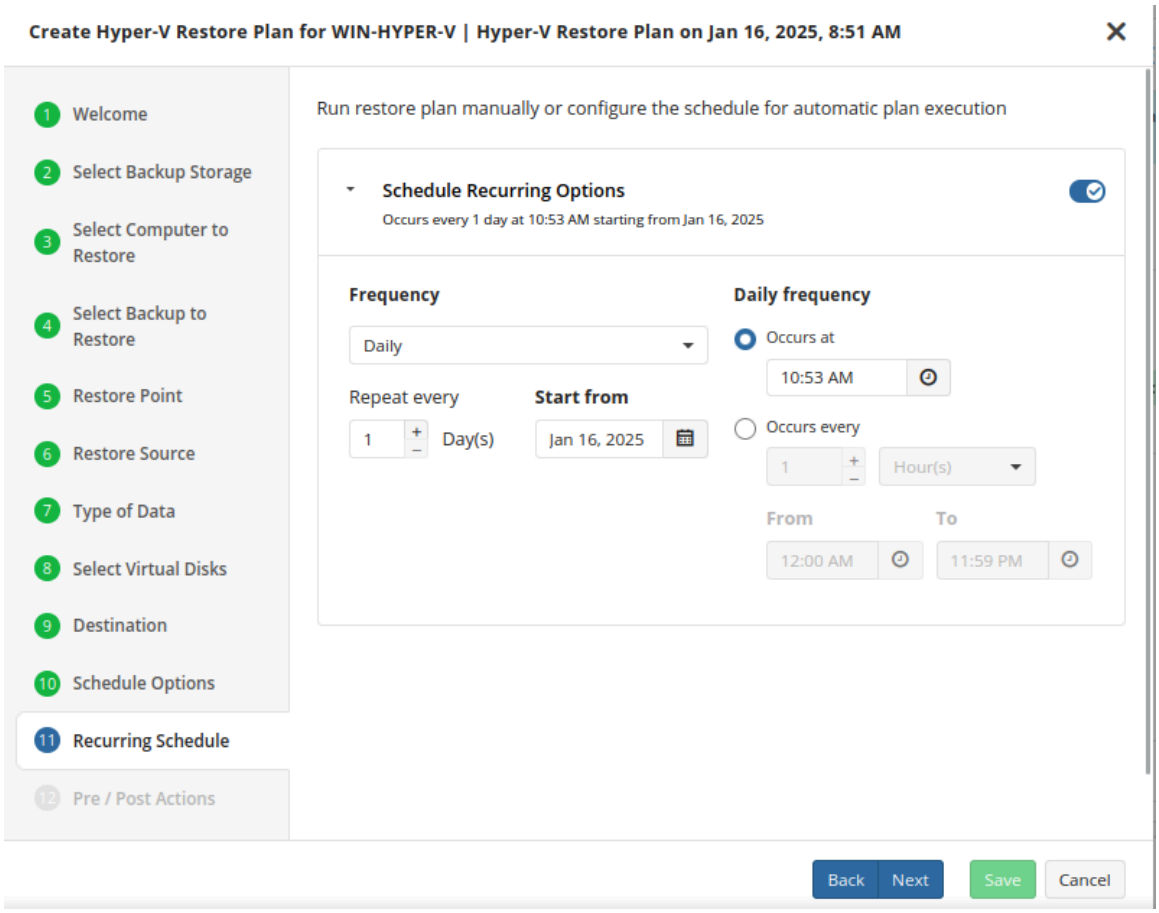
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

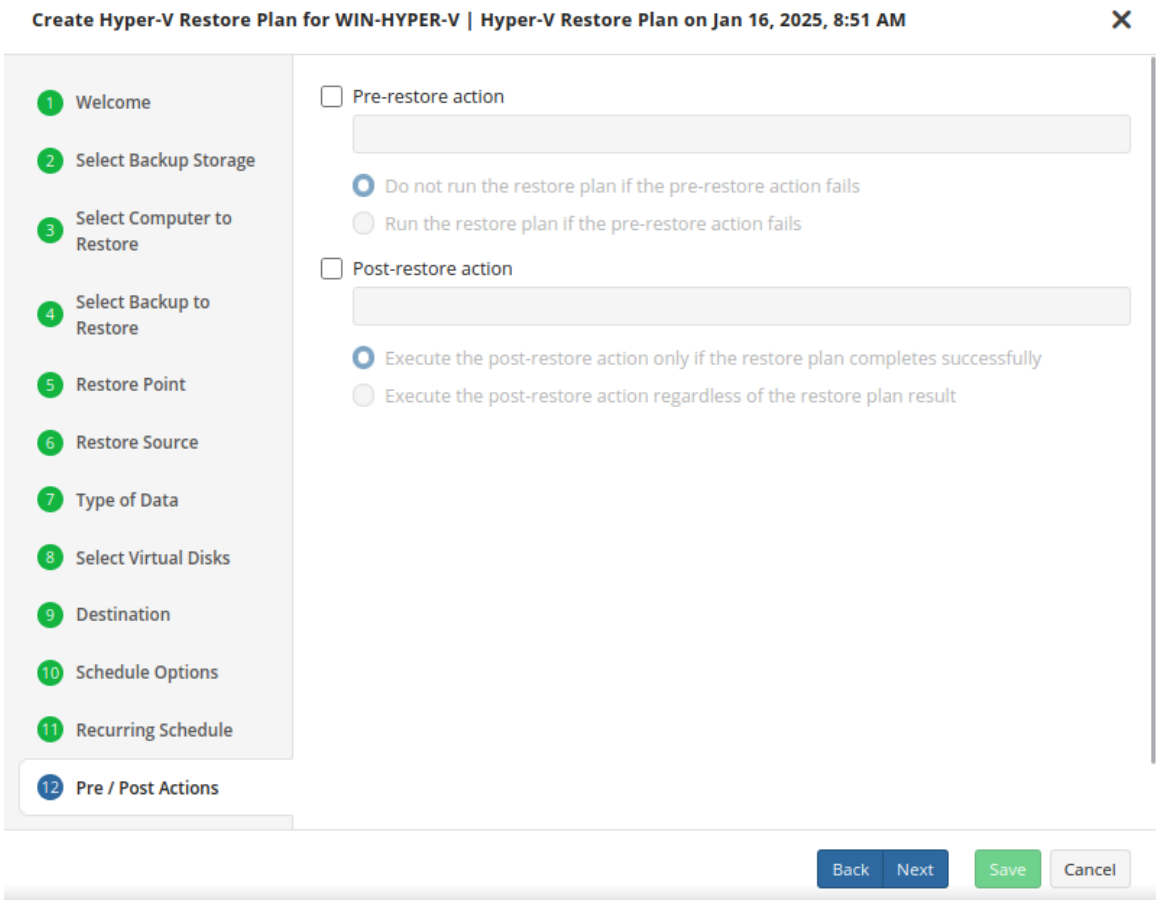
Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after

> the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

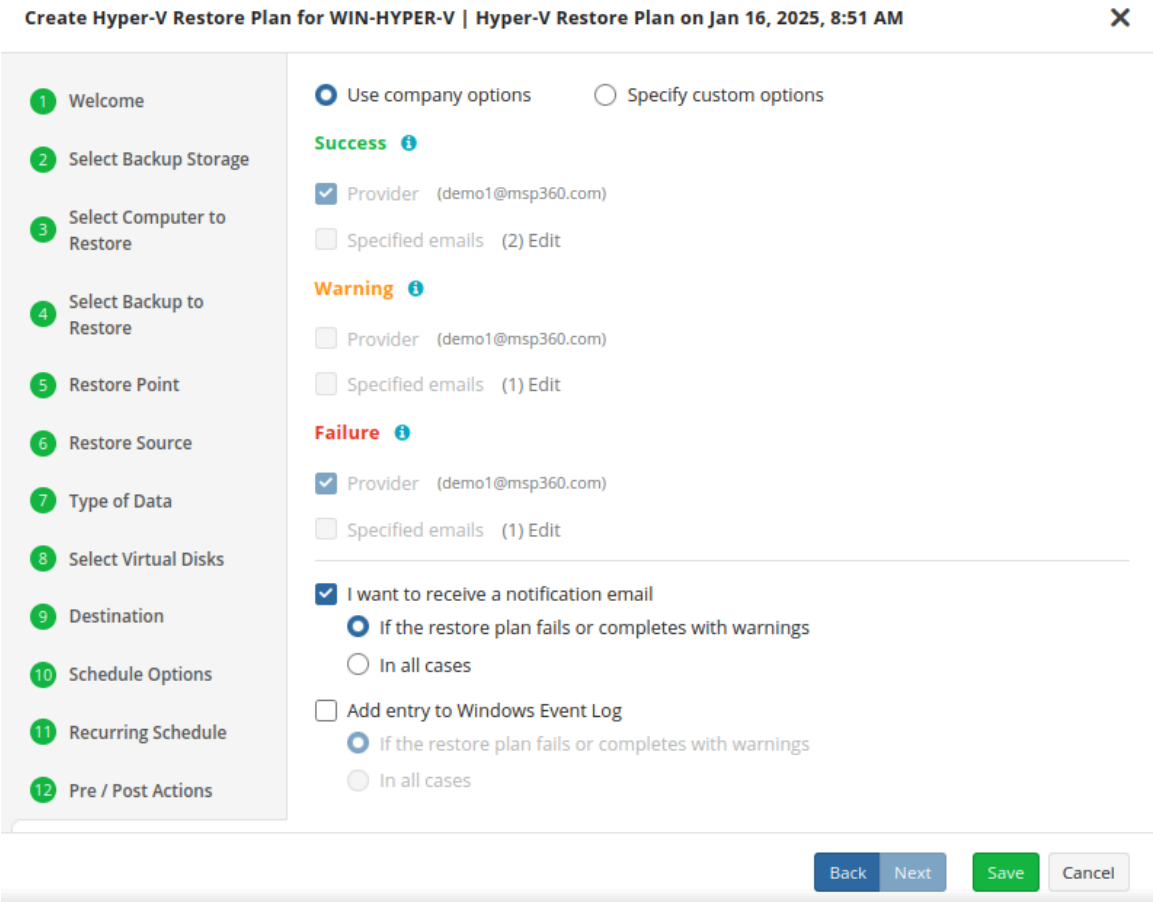
Step 15. If a recurring schedule was selected, now you can set up the frequency for the restore plan to be executed.



Step 16. Next, specify the pre/post actions if required.



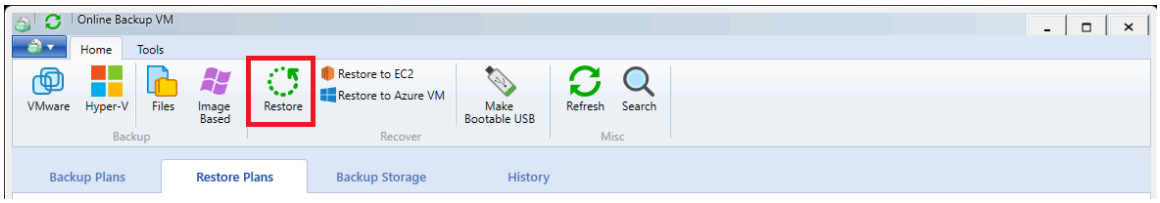
Step 17. After pre-post actions, you can configure the notifications for this restore plan.



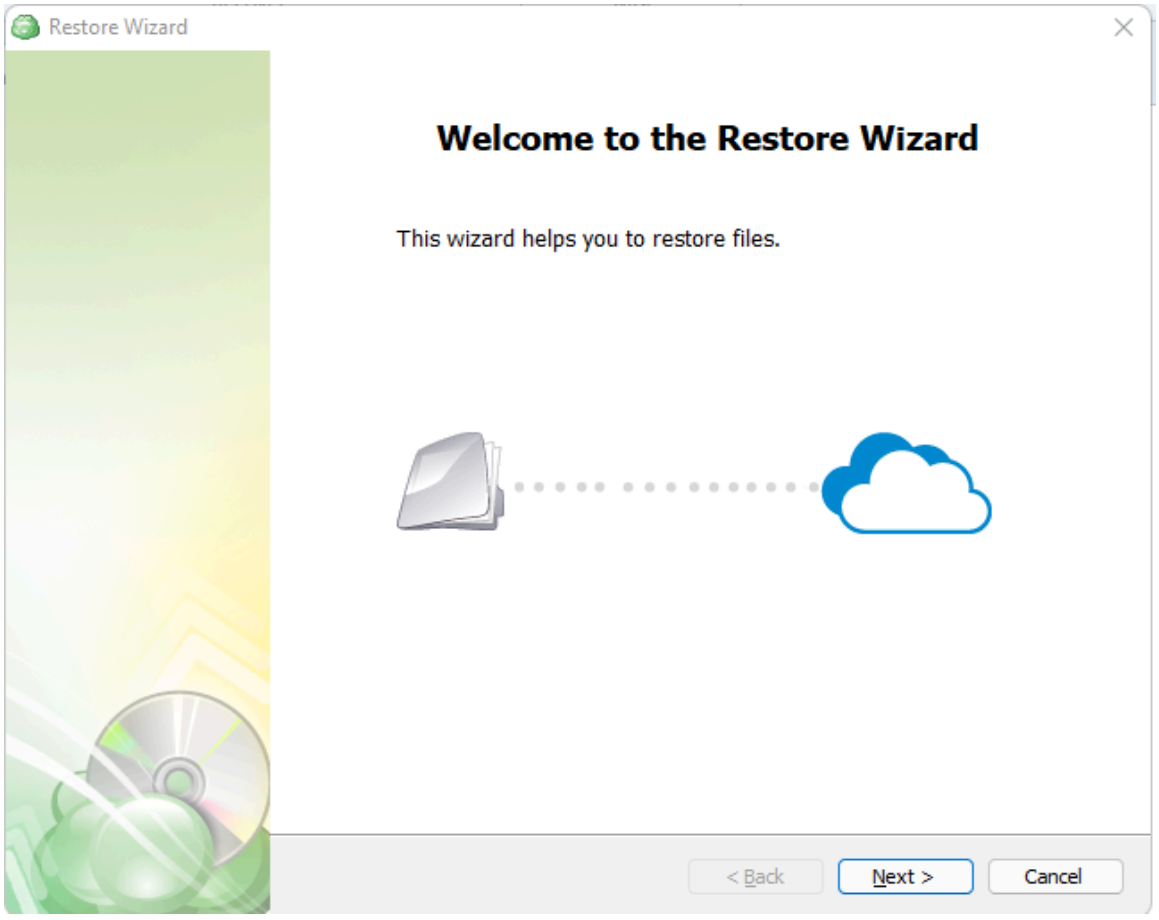
Step 18. Click on Save when you are happy with your selections. If the plan is set to run only a single time and has no set schedule, it will automatically start. Otherwise, if it is set to run only once and is scheduled, it will display in the list of plans until the scheduled time. If it is only set to run once, then when it completes successfully it will remove itself from the list of plans. Only Restore Plans which are saved will remain in the list for future use.

Restore as a Virtual Disk using the Agent

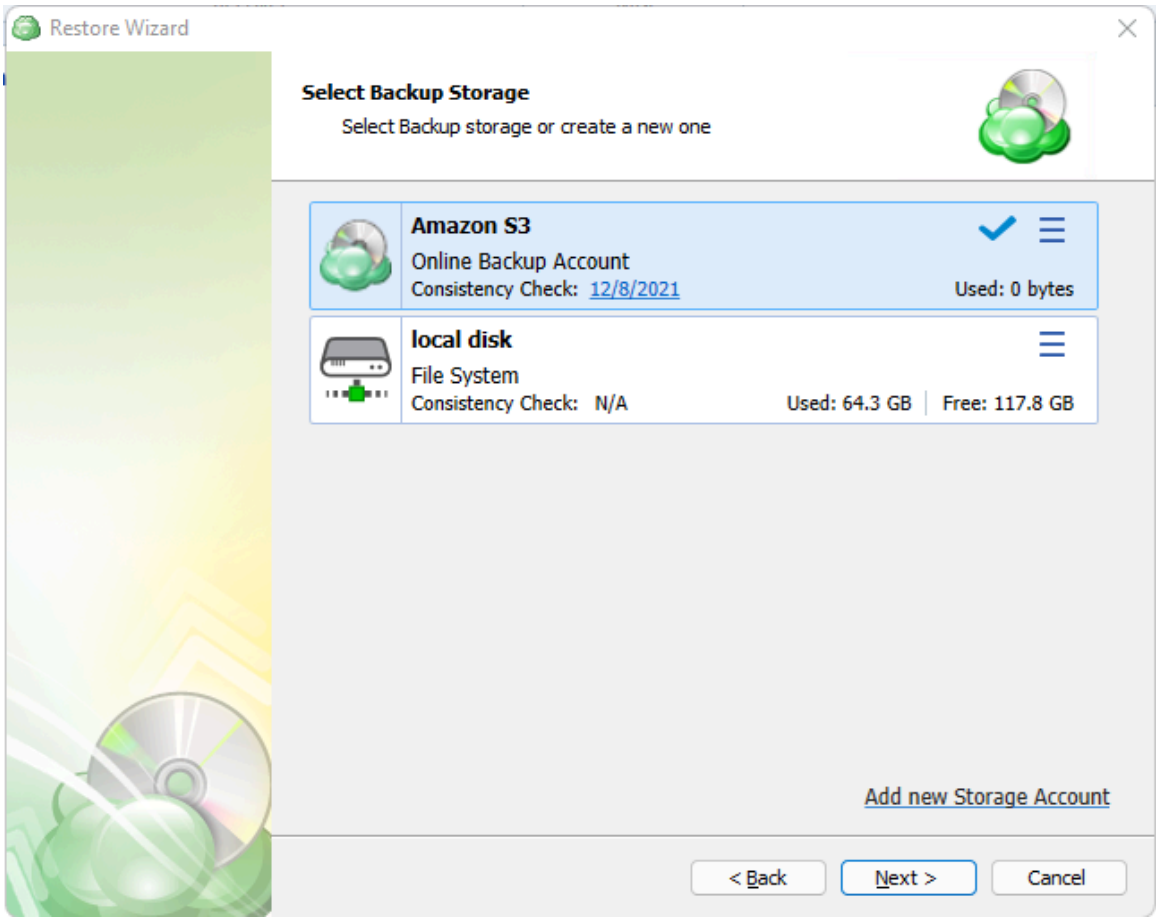
Step 1. Within the Online Backup Agent, click on “Restore”



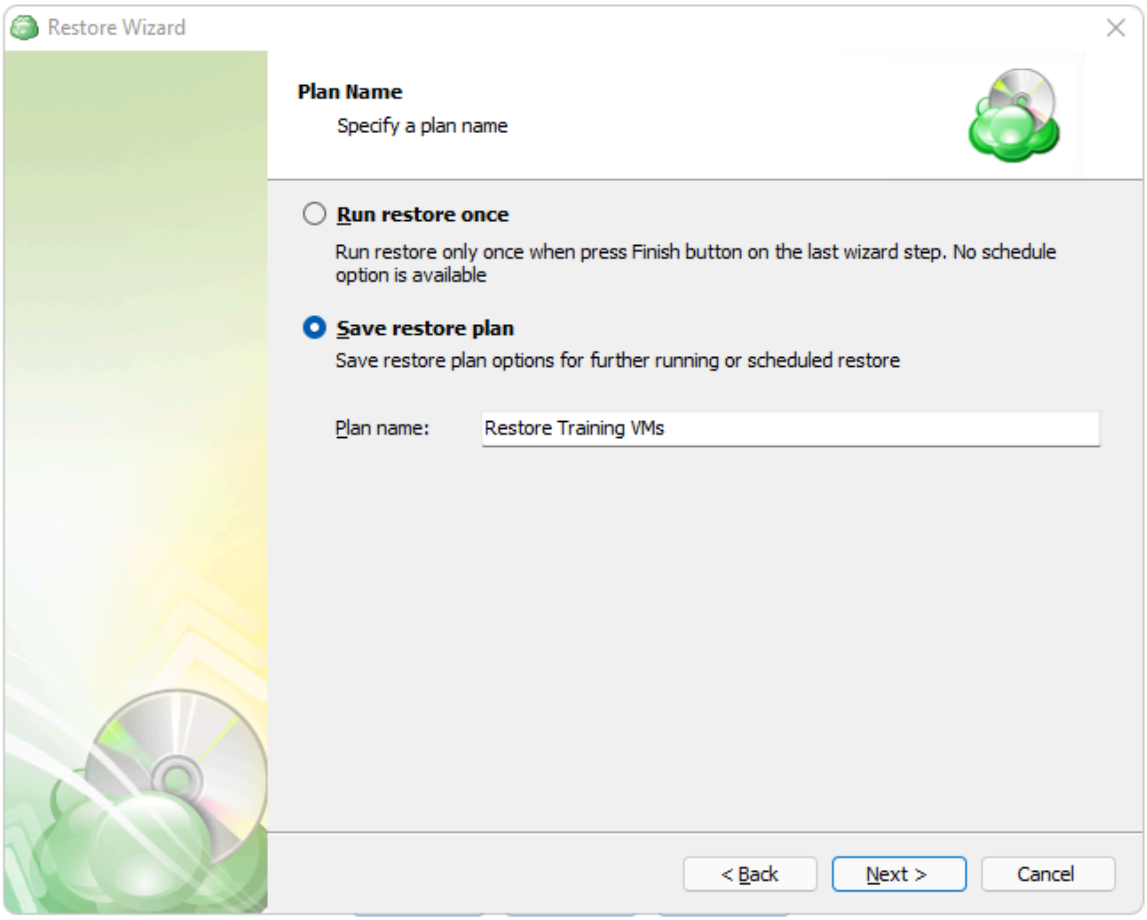
Step 2. Once the wizard starts, click on Next to advance to the next step.



Step 3. The next step will prompt you to select the source for the restore point.



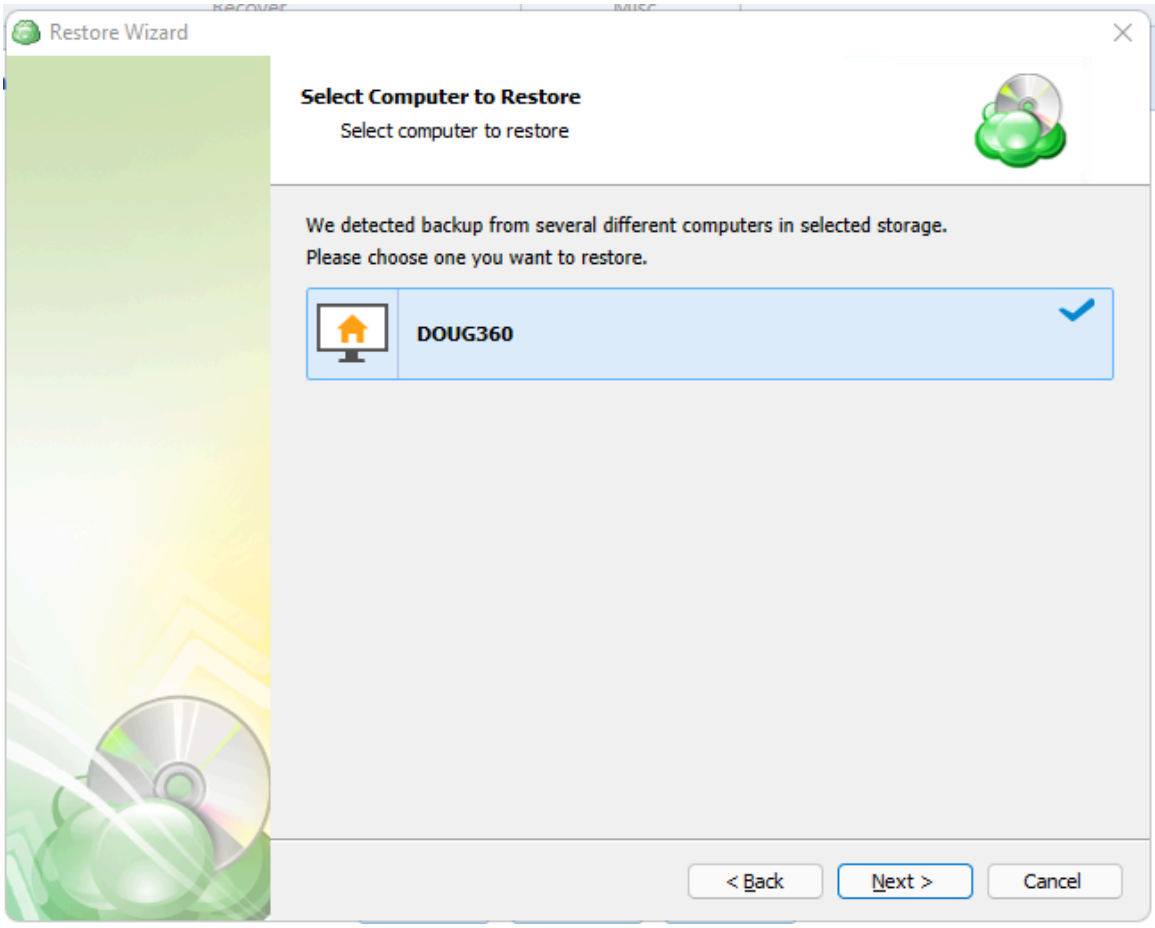
Step 4. Next, you will be given the option to either run the restore once or to save it to run later.



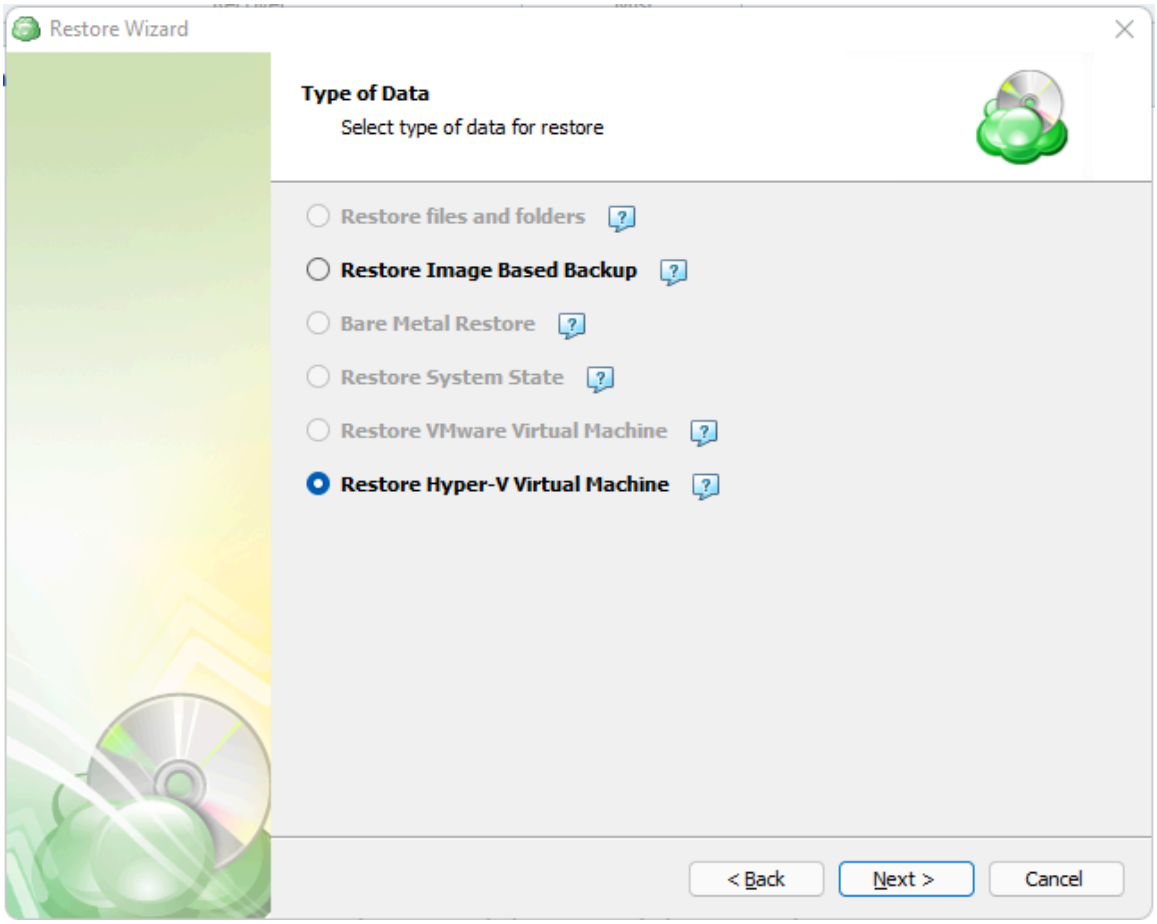
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

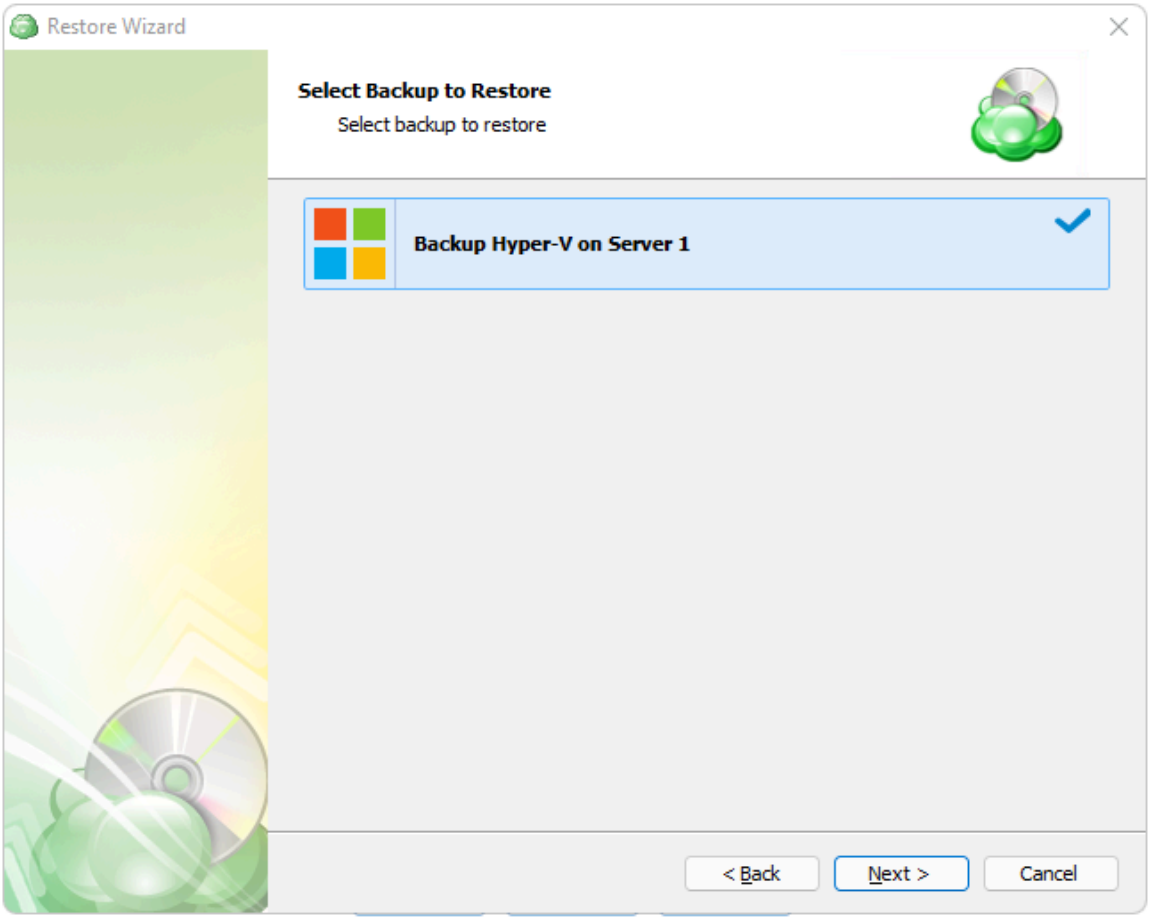
Step 5. With the type of restore selected, the next step is to select the correct Host server which the VM resides on.



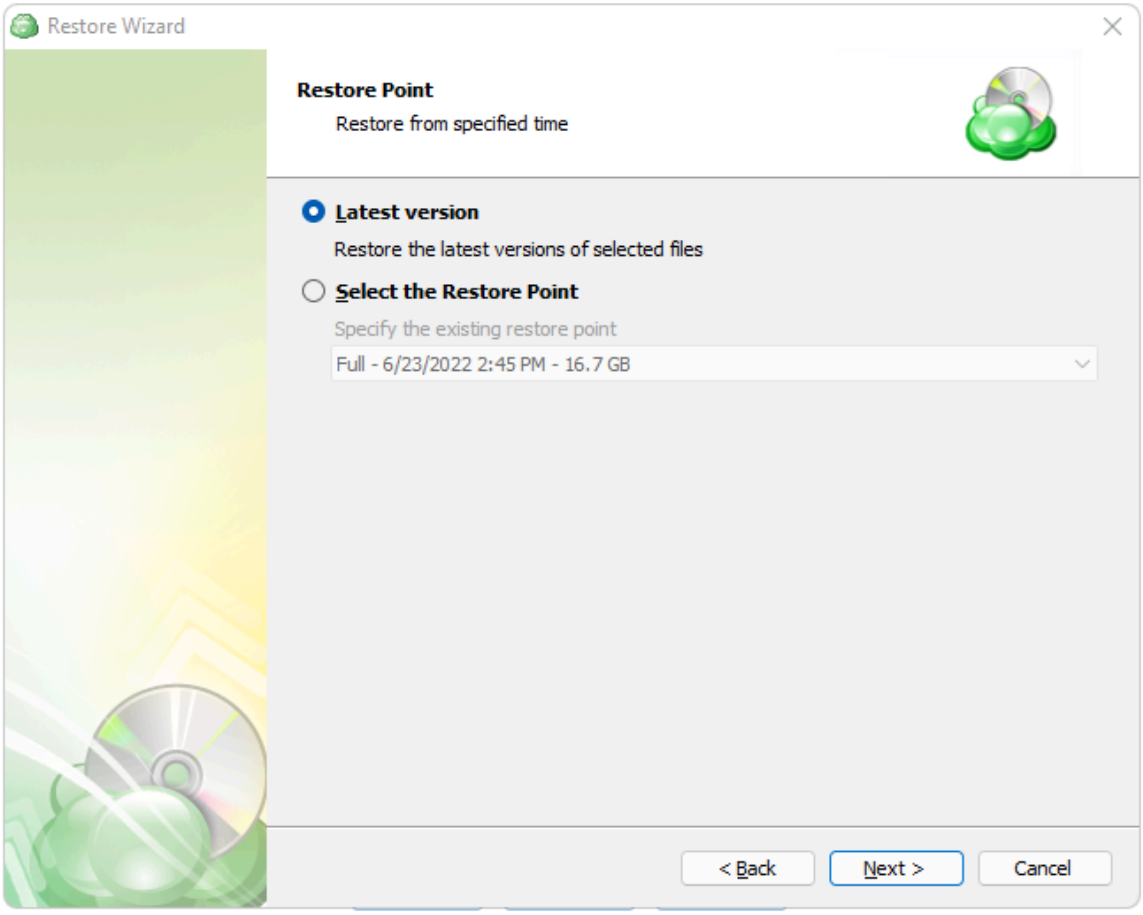
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore Hyper-V Virtual Machine” option to continue.



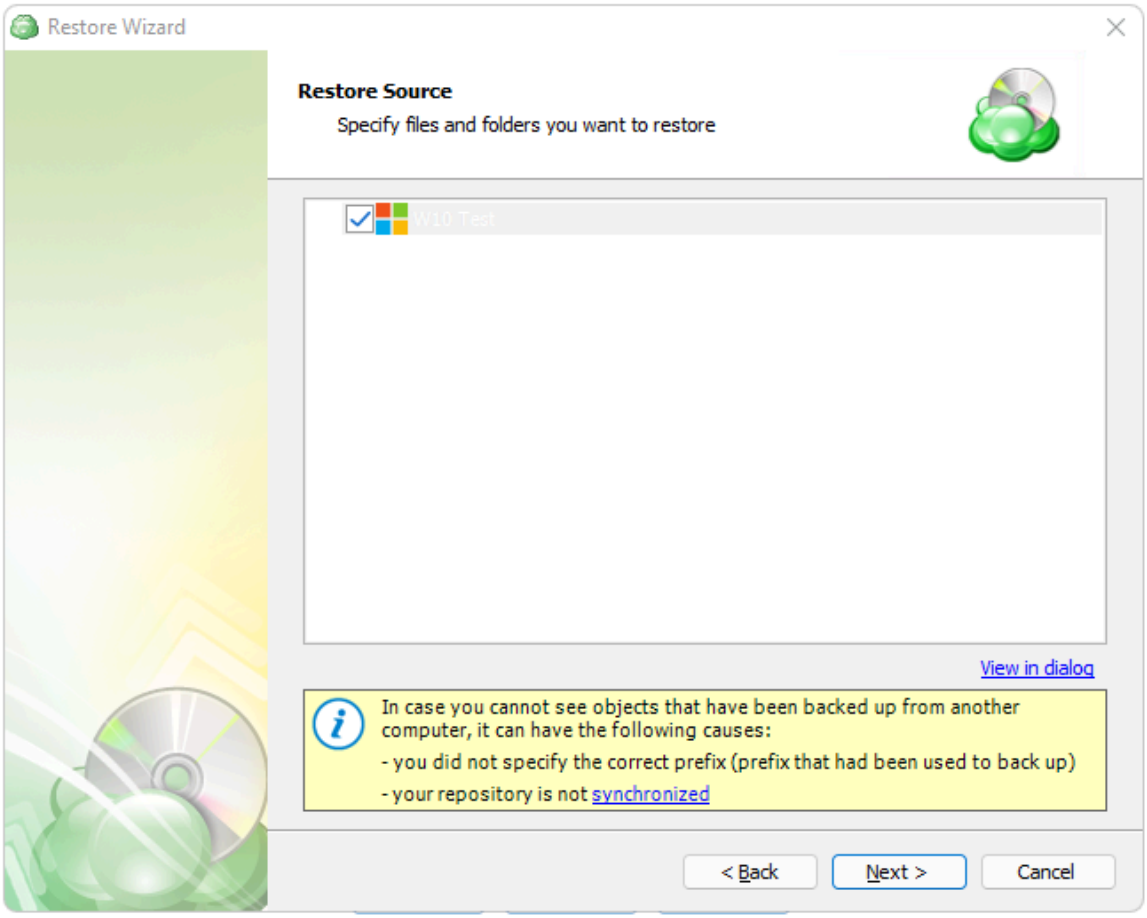
Step 7. With the correct type of data selected, the application will generate a list of available VM backup plans.



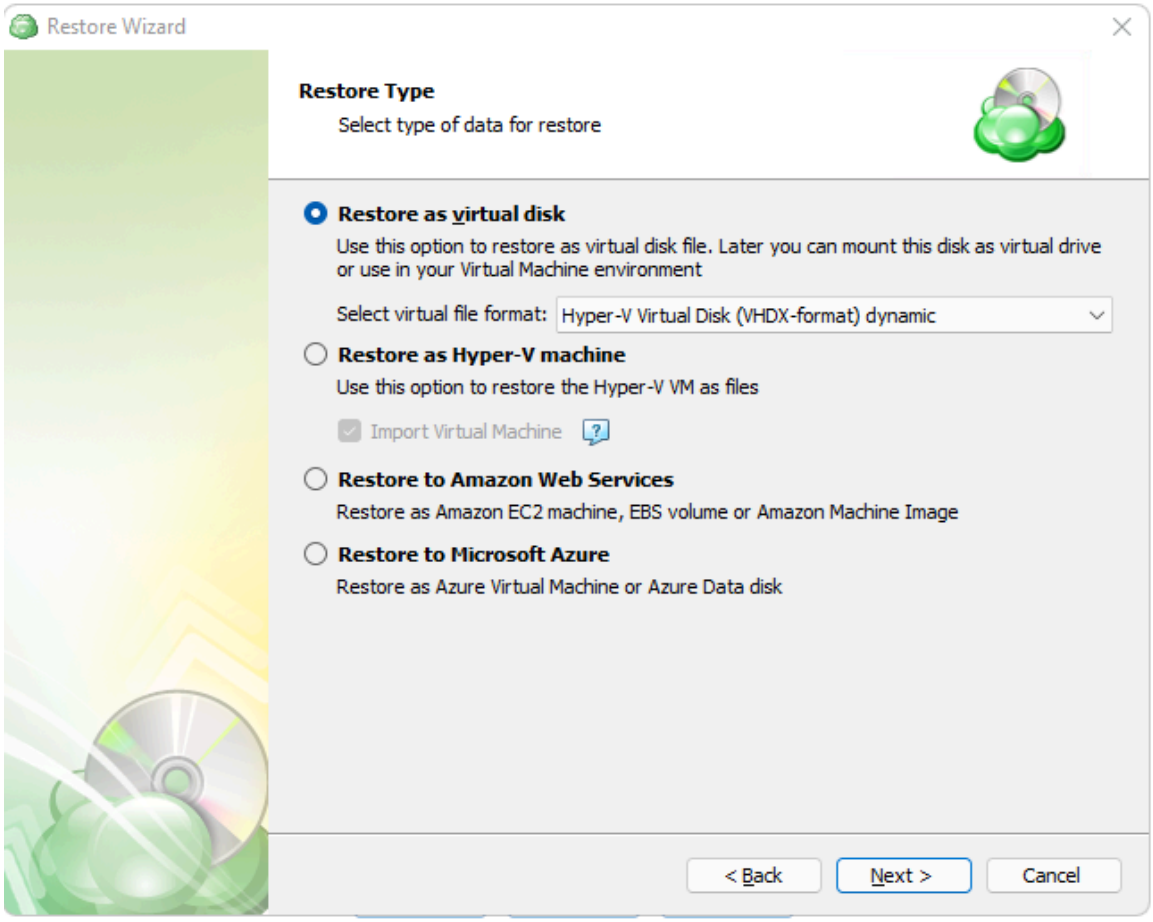
Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.



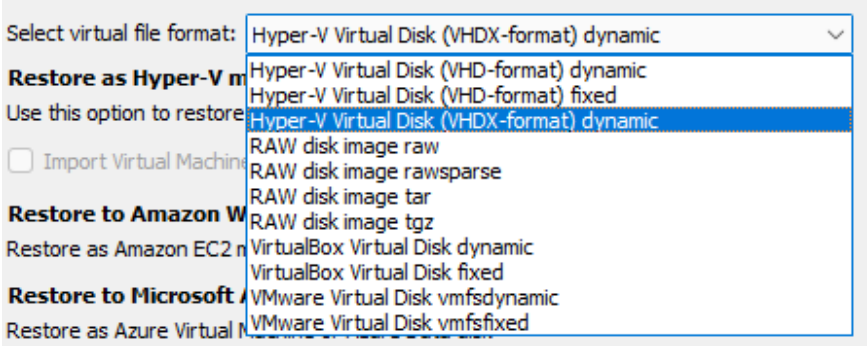
Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which to restore.



Step 10. The next step of the wizard allows you to choose how the VM data should be restored.

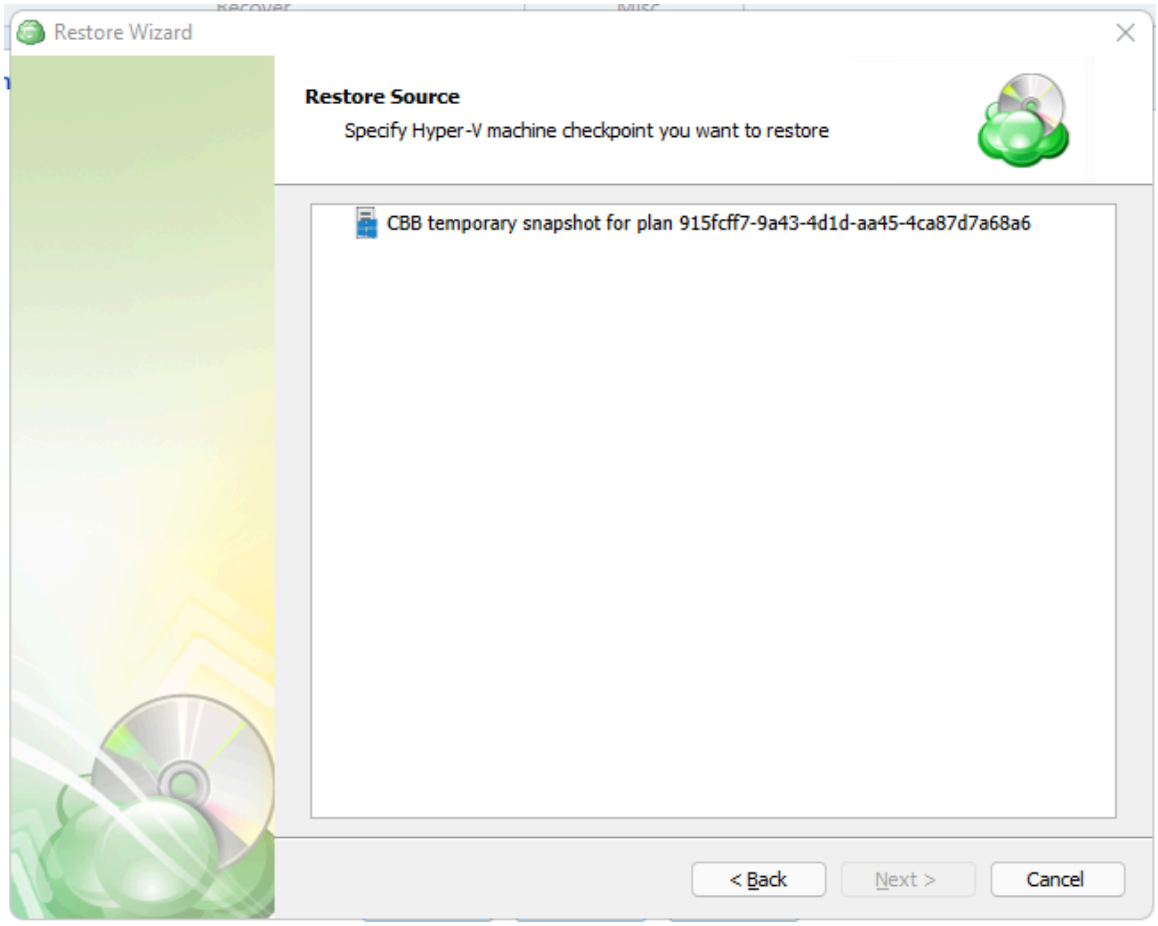


- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:

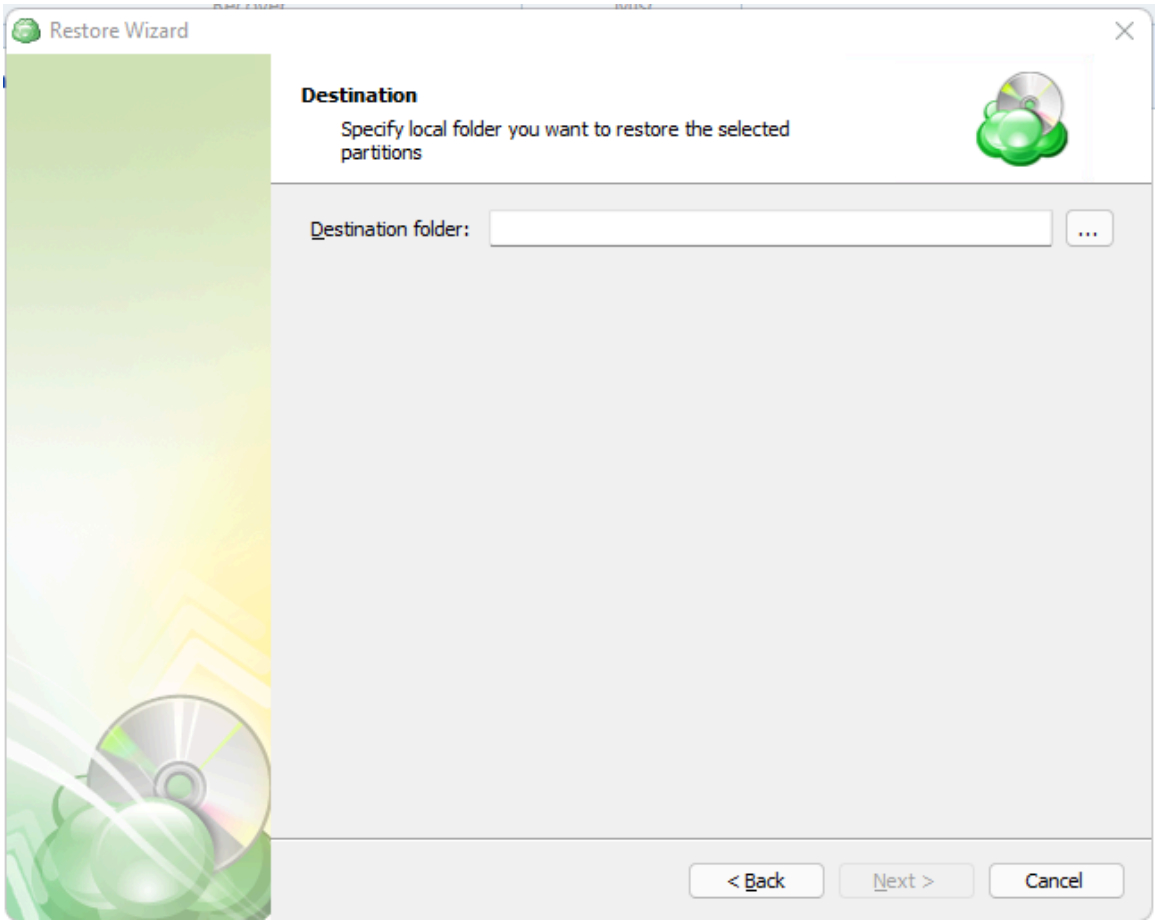


- **Restore as a Hyper-V machine:** Selecting this option restores the virtual machine configuration as well as the virtual disks as files, but does not import the VM into the hypervisor by default.
    - **Import Virtual Machine:** Use this option to have the VM automatically imported to the hypervisor.
- **Restore to Amazon Web Services:** If enabled, this will restore the selected VM directly to AWS Cloud either as an EC2 instance, EBS volume, or AMI.
- **Restore to Microsoft Azure:** This will restore the VM directly to Azure as either an Azure Virtual Machine or Azure Data disk.

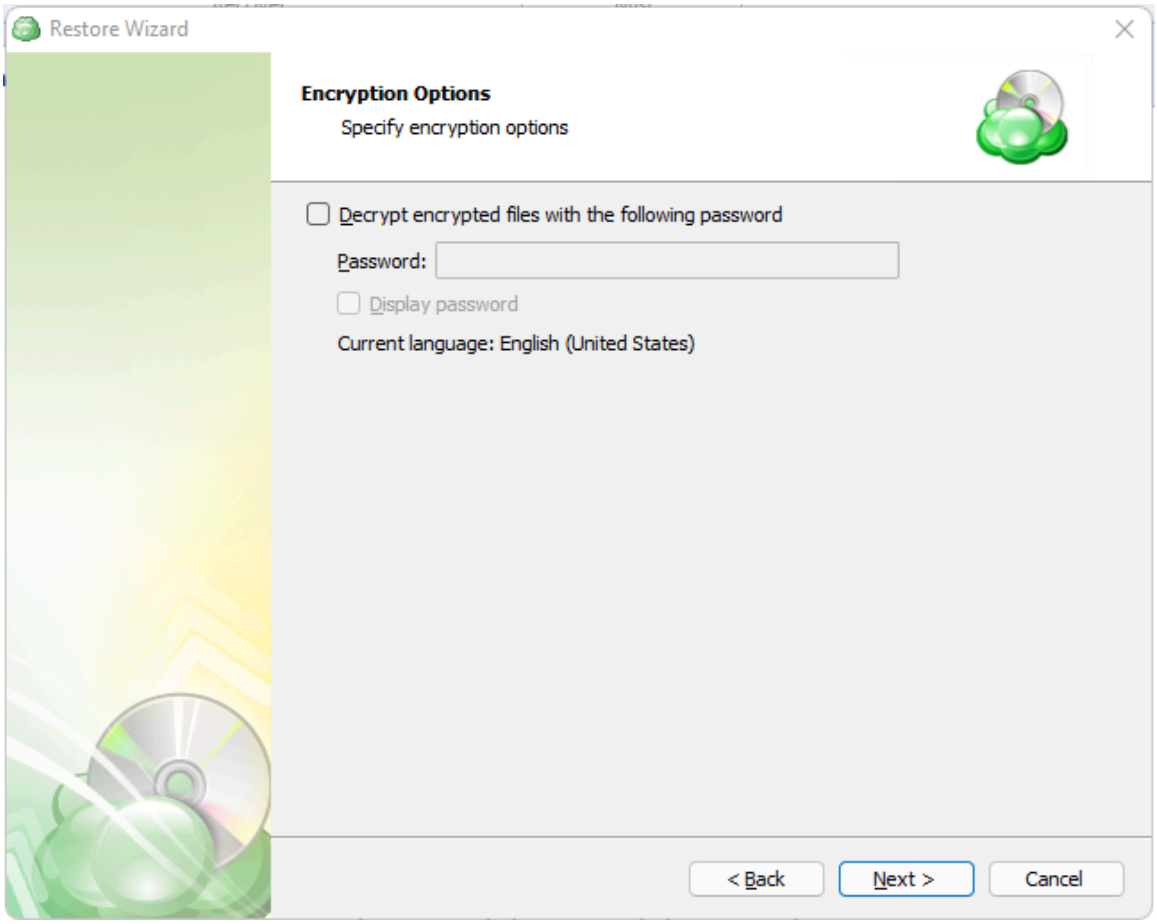
Step 11. Next you will need to determine which available checkpoint to restore for the virtual disk.



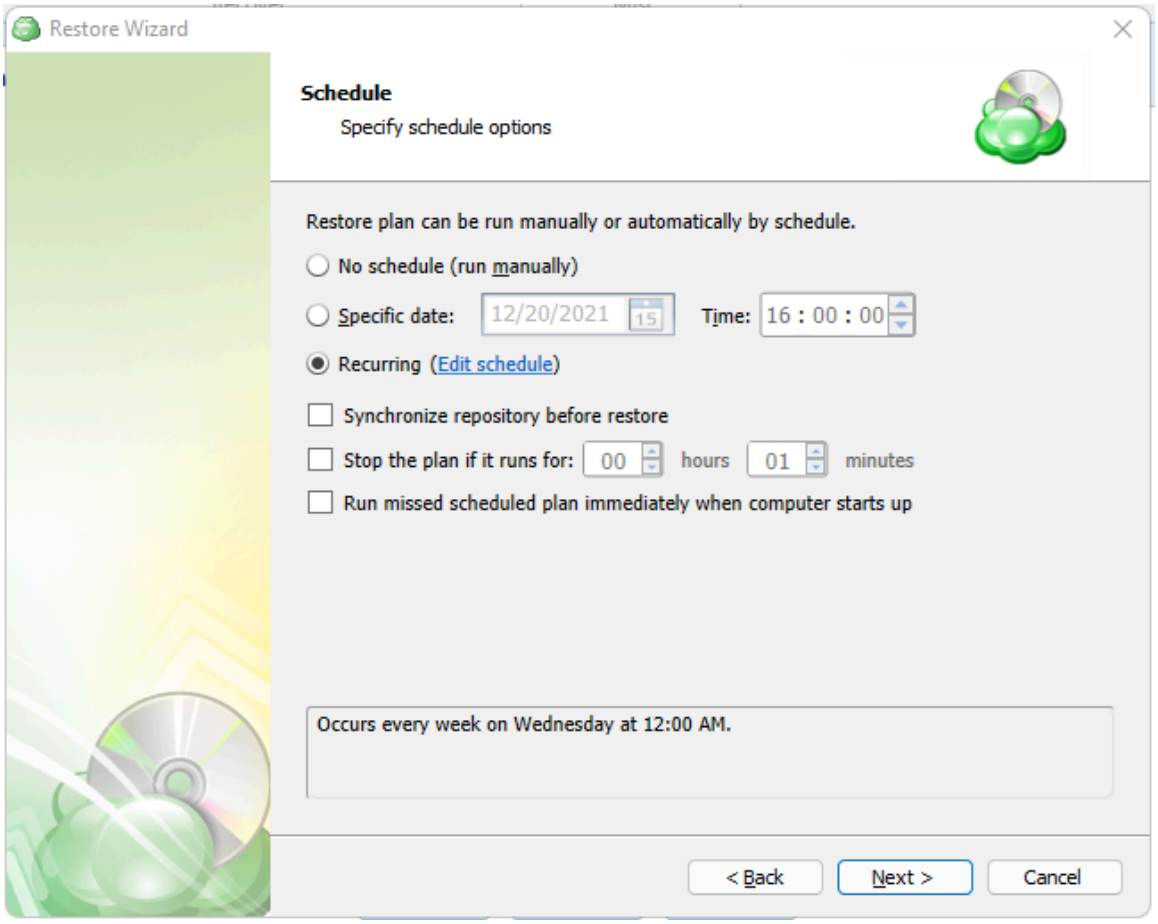
Step 12. With the checkpoint selected, you can now specify a destination folder for the virtual disk file.



Step 13. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the VM.



Step 14. With the decryption password entered, the next step is setting the schedule for the restore plan.

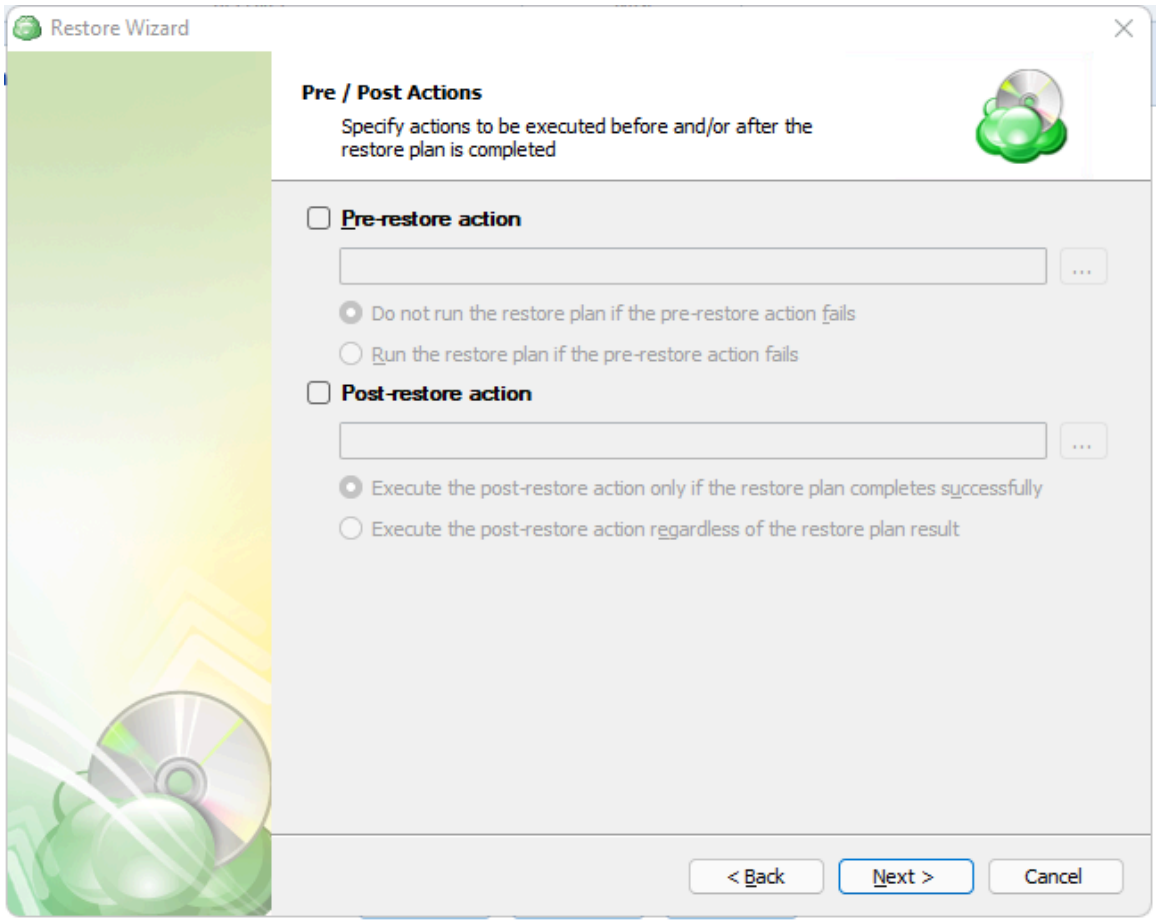


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

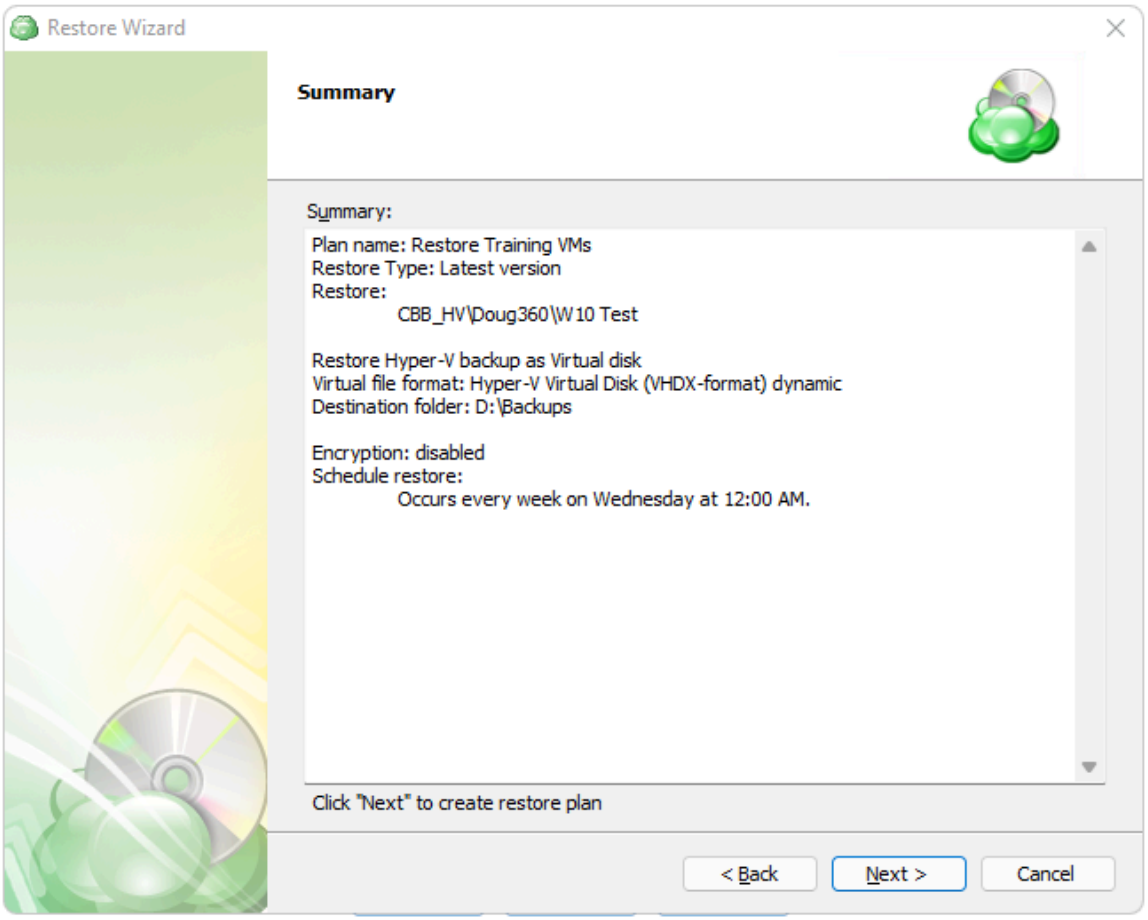
> Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 15. After setting the schedule, the next step allows pre and post actions to be defined.



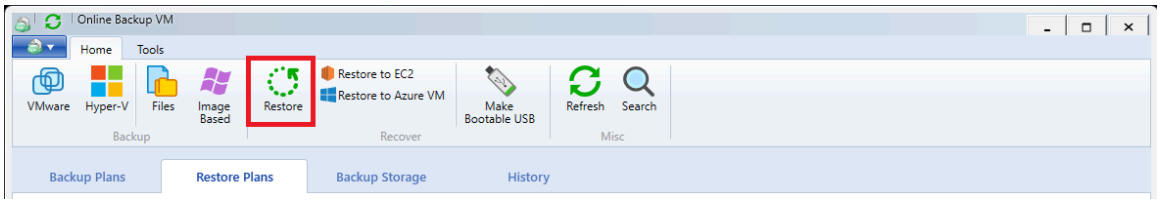
Step 16. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.



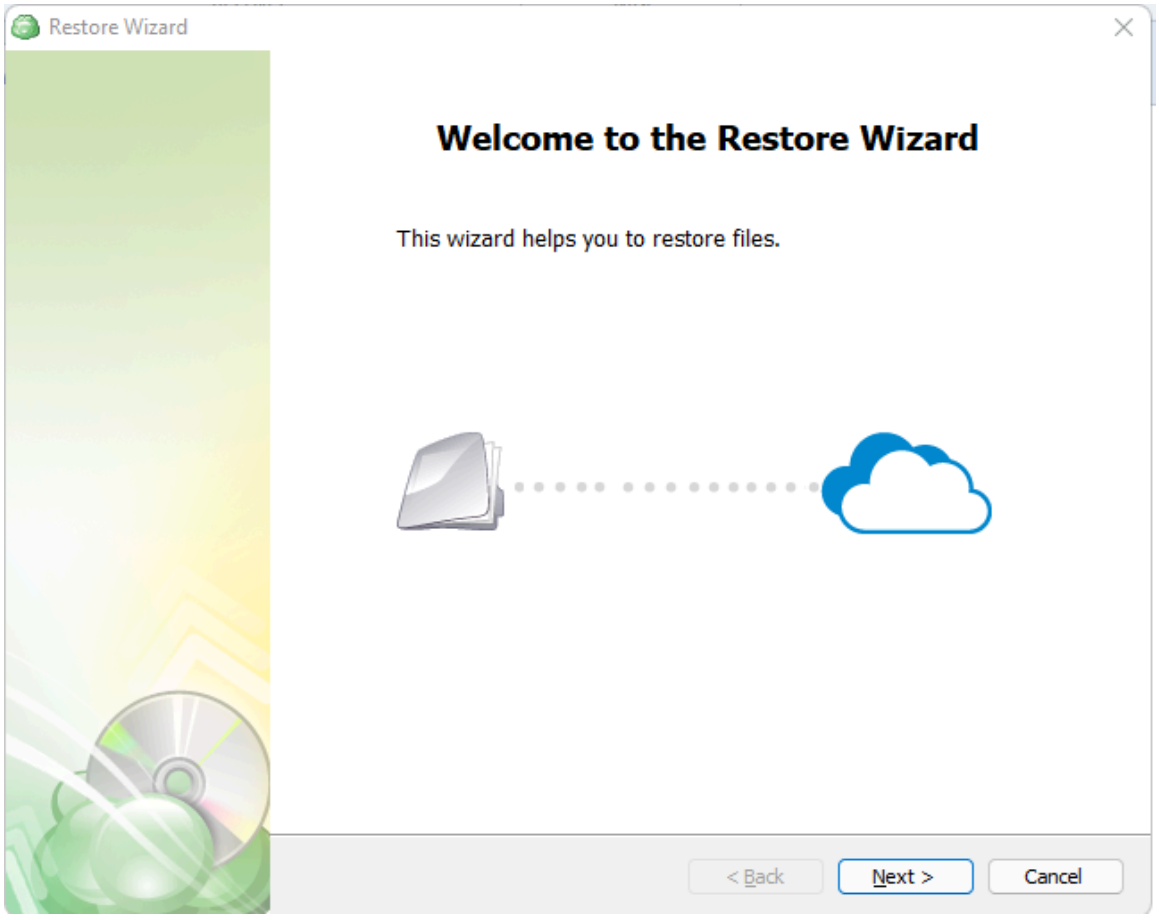
> If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

Restore as an Azure VM using the Agent

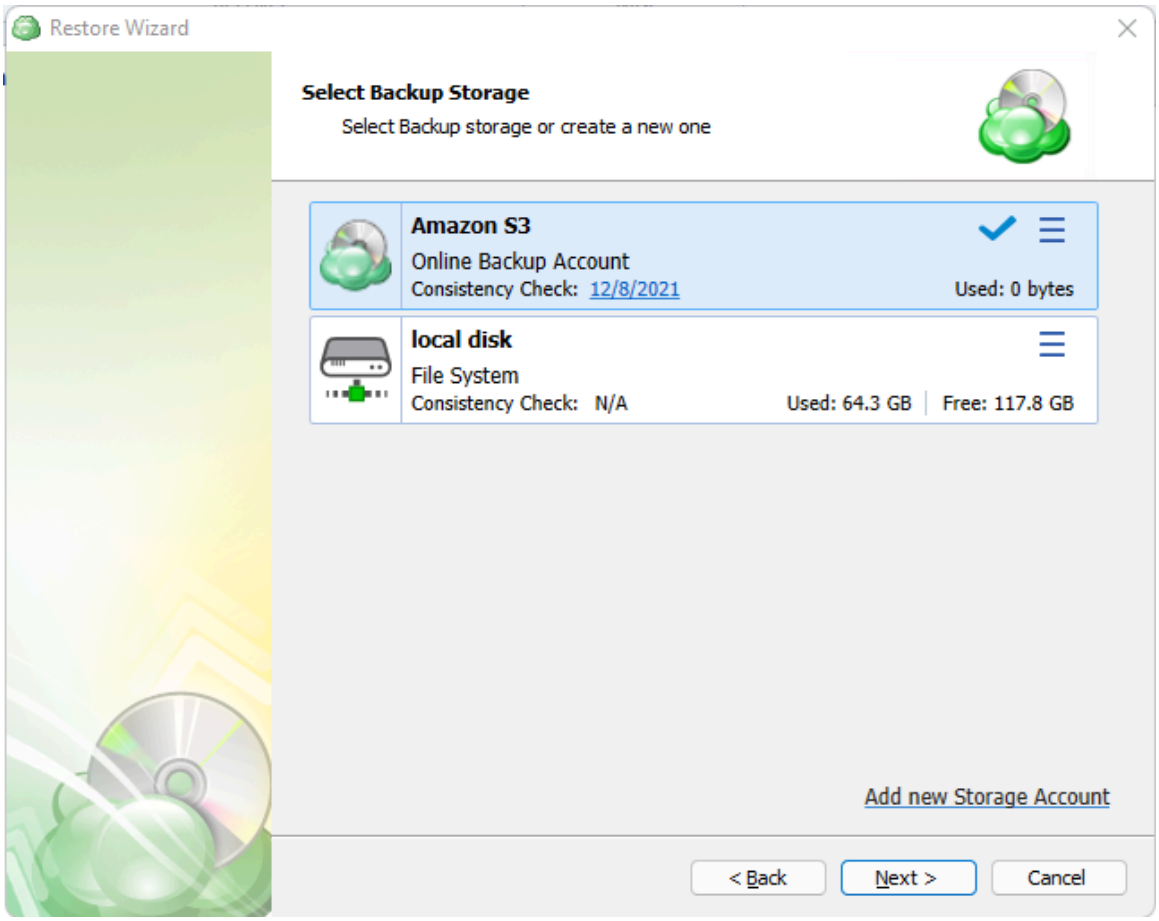
Step 1. Within the Online Backup Agent, click on “Restore”



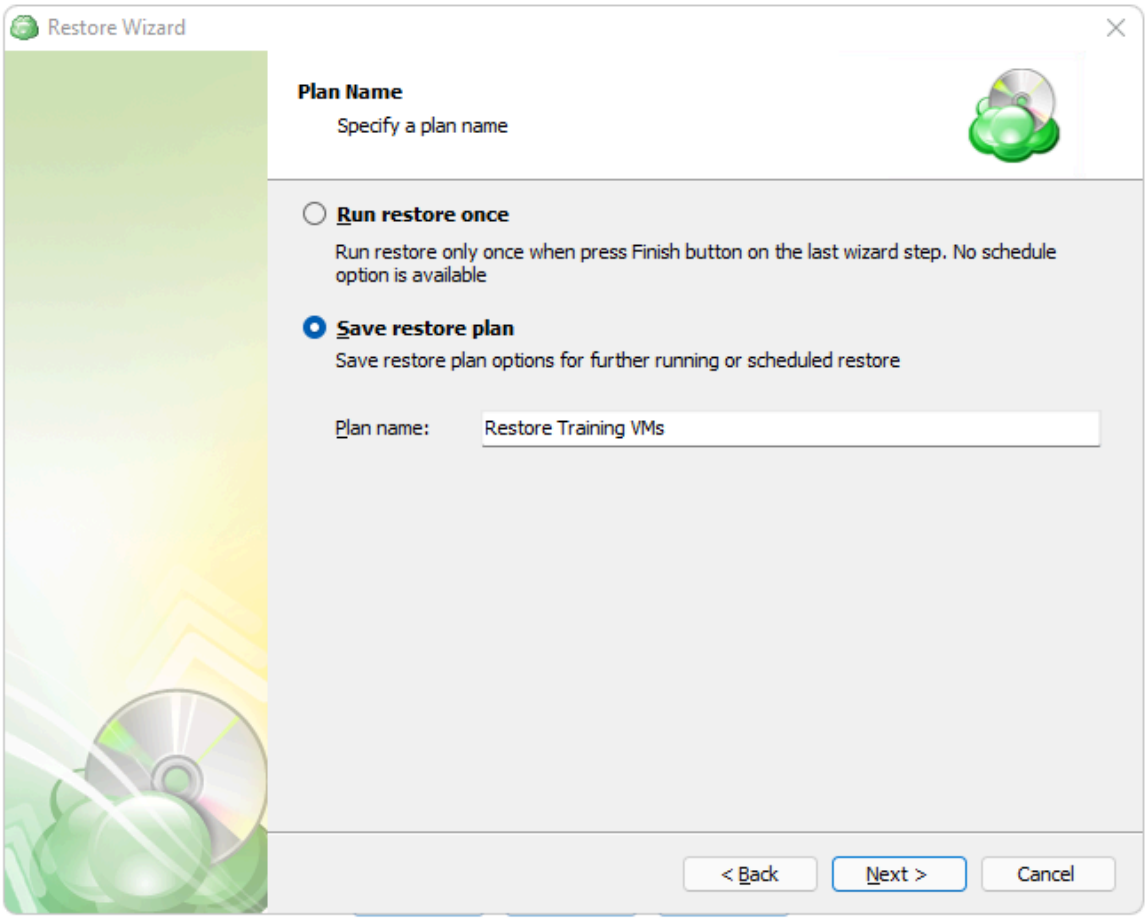
Step 2. Once the wizard starts, click on Next to advance to the next step.



Step 3. The next step will prompt you to select the source for the restore point.



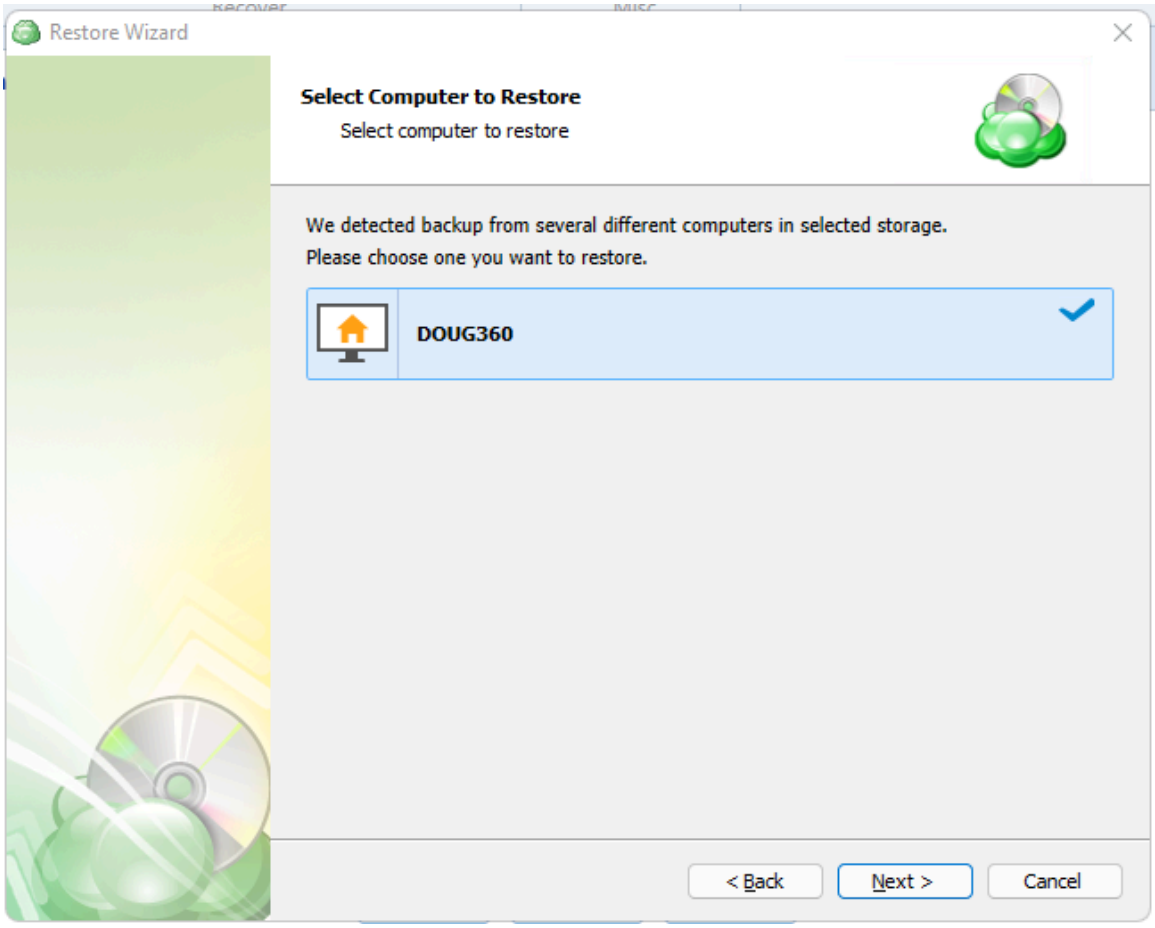
Step 4. Next, you will be given the option to either run the restore once or to save it to run later.



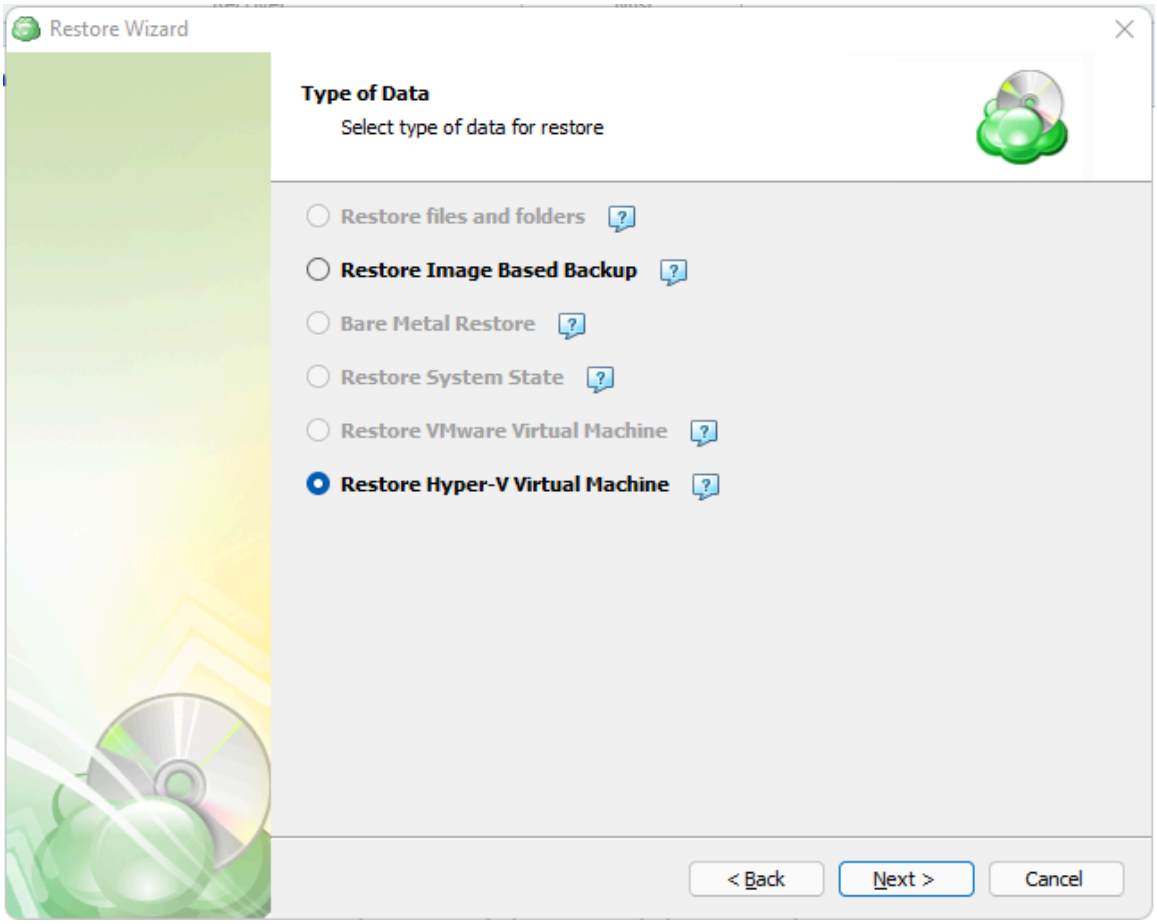
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

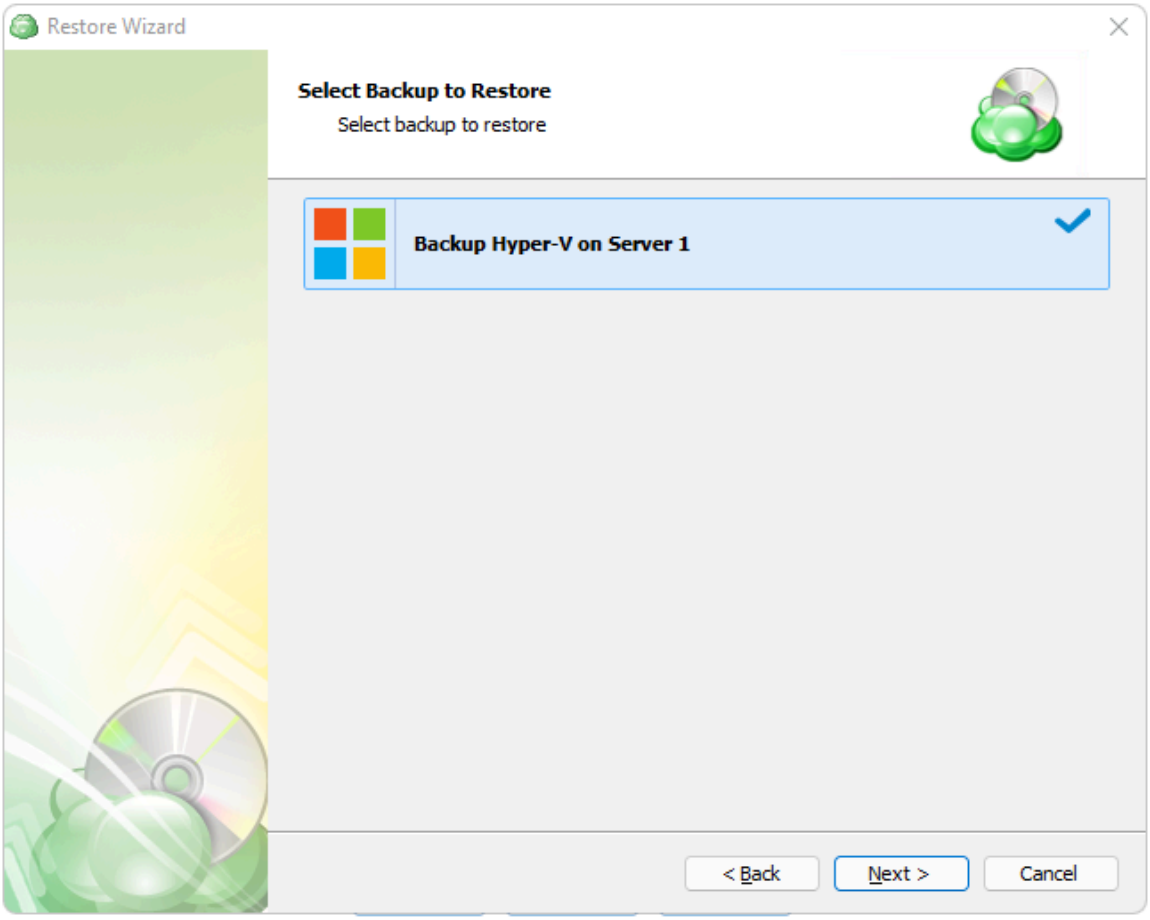
Step 5. With the type of restore selected, the next step is to select the correct Host server which the VM resides on.



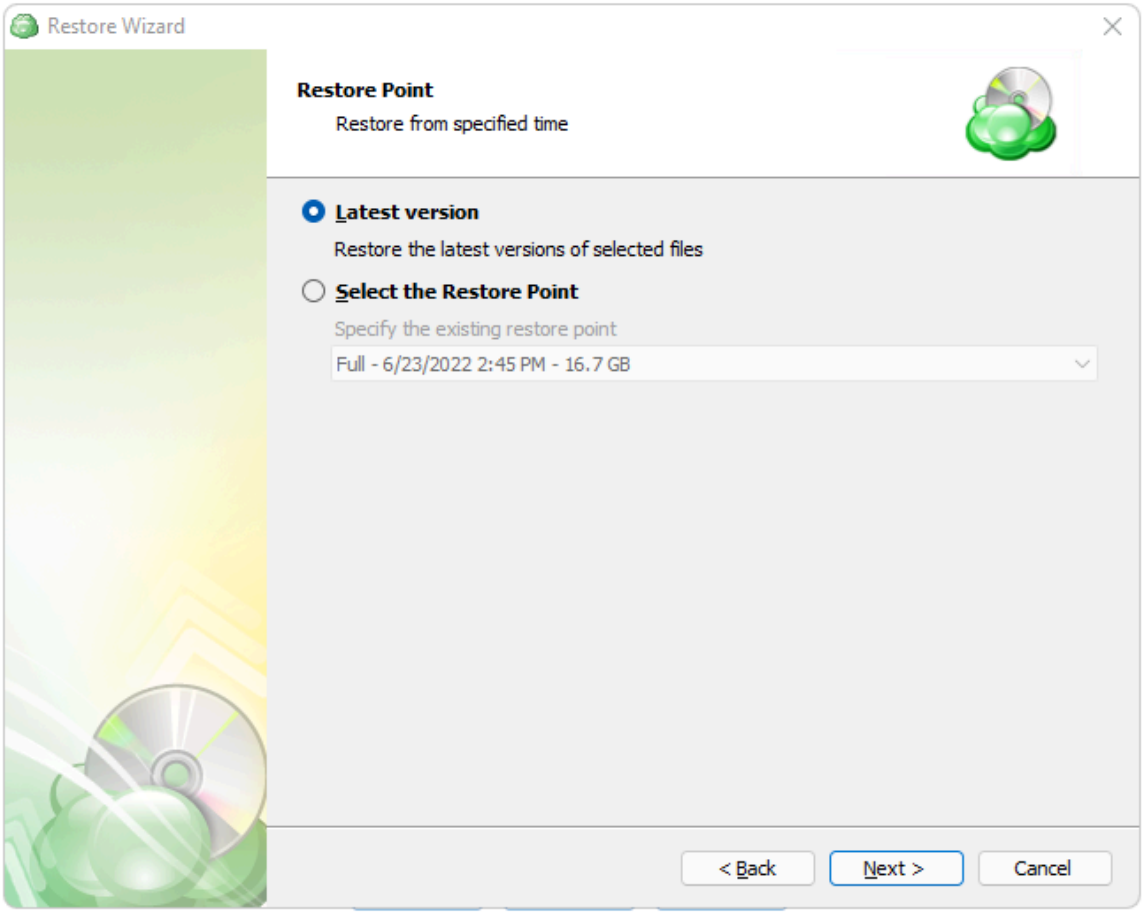
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore Hyper-V Virtual Machine” option to continue.



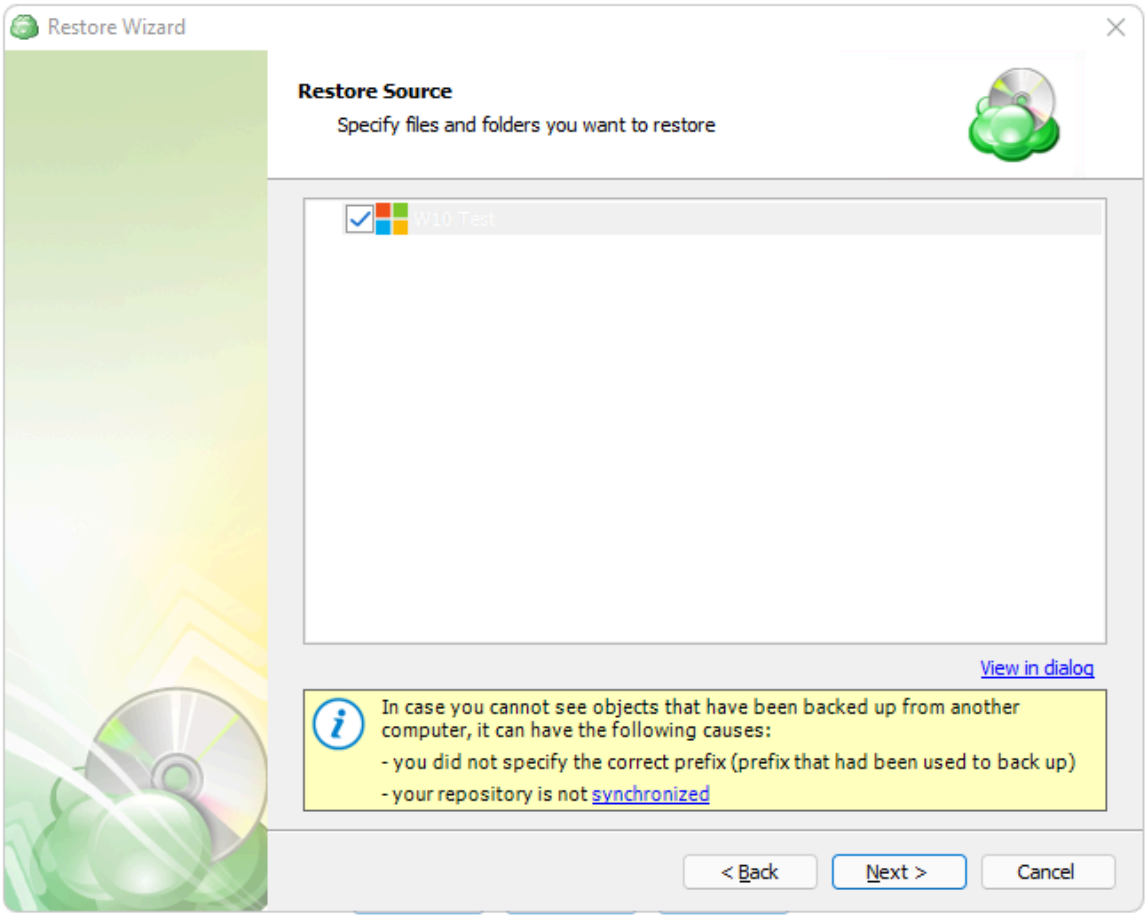
Step 7. With the correct type of data selected, the application will generate a list of available VM backup plans.



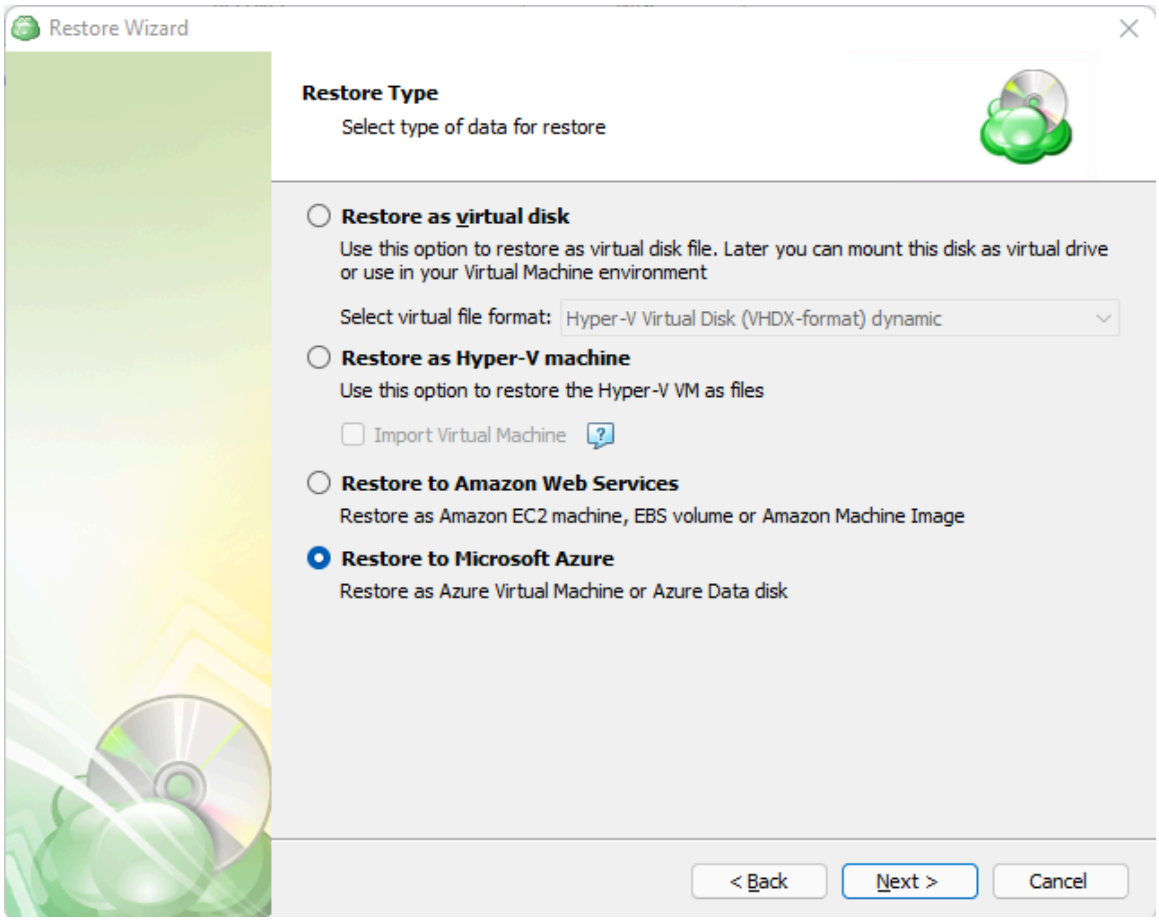
Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.



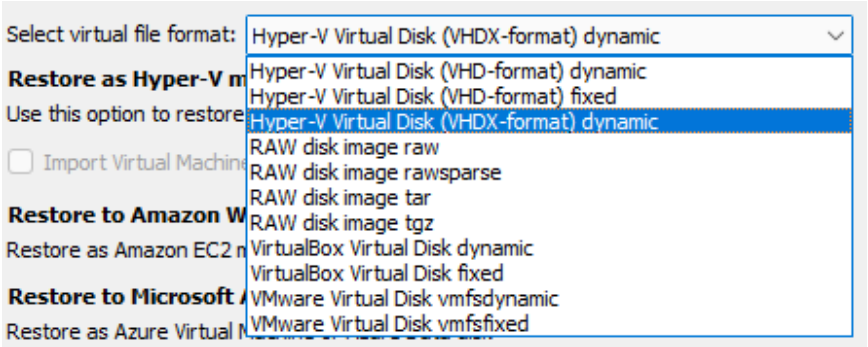
Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which to restore.



Step 10. The next step of the wizard allows you to choose how the VM data should be restored.

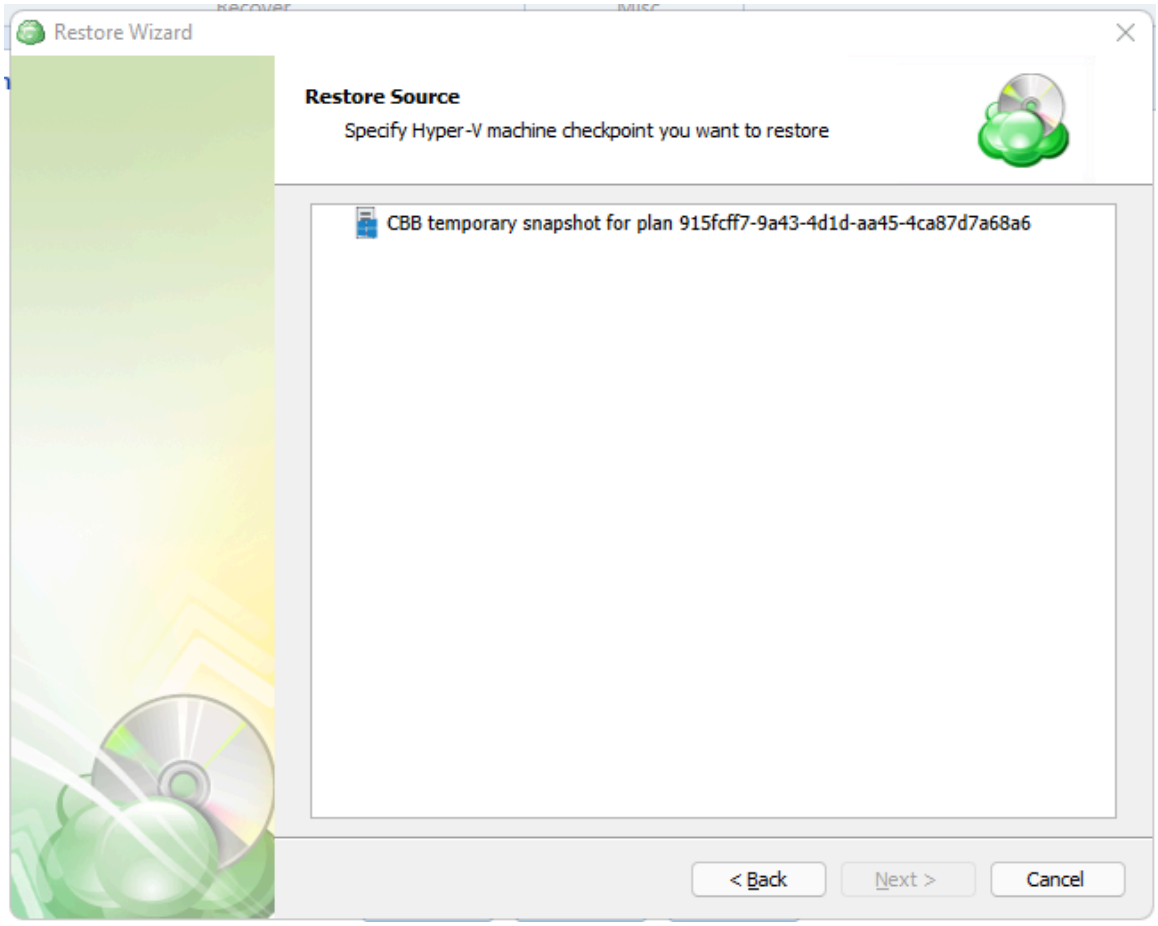


- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:

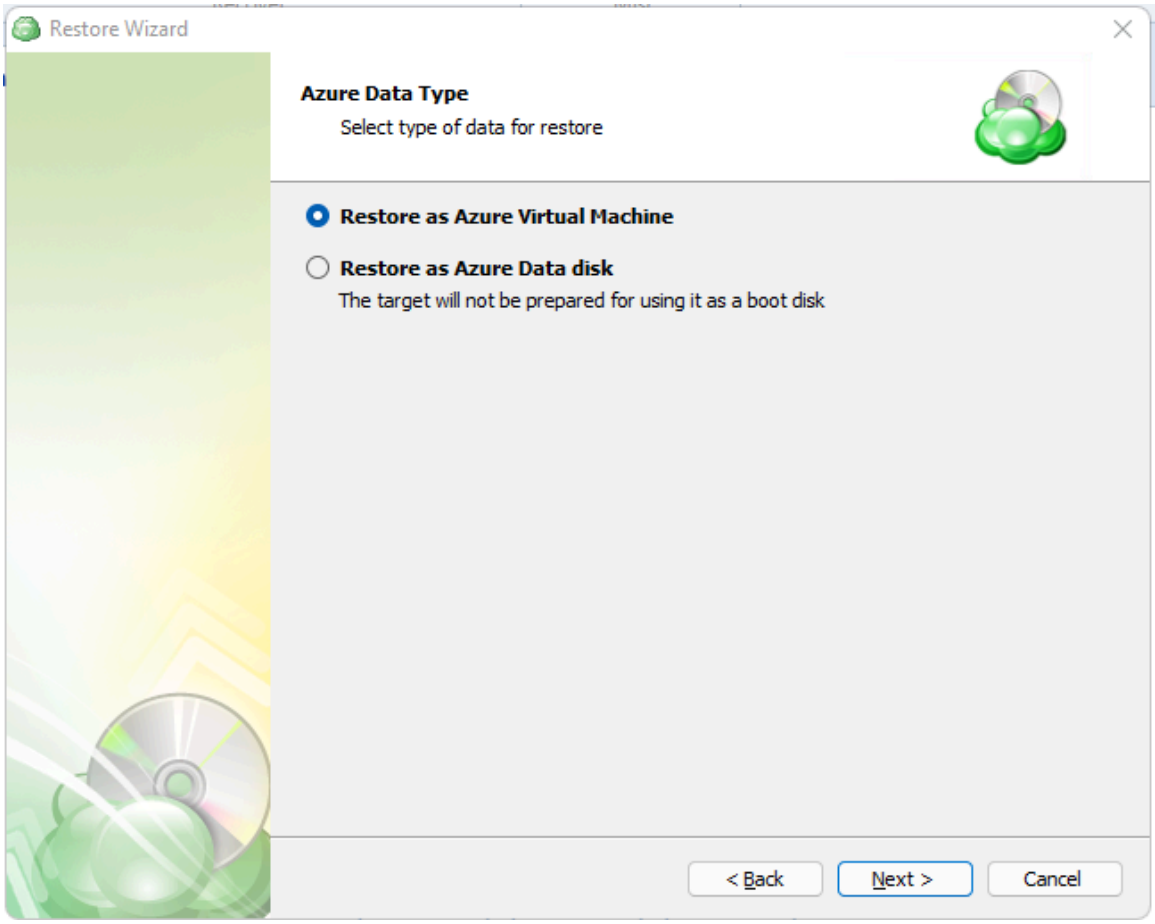


- **Restore as a Hyper-V machine:** Selecting this option restores the virtual machine configuration as well as the virtual disks as files, but does not import the VM into the hypervisor by default.
    - **Import Virtual Machine:** Use this option to have the VM automatically imported to the hypervisor.
- **Restore to Amazon Web Services:** If enabled, this will restore the selected VM directly to AWS Cloud either as an EC2 instance, EBS volume, or AMI.
- **Restore to Microsoft Azure:** This will restore the VM directly to Azure as either an Azure Virtual Machine or Azure Data disk.

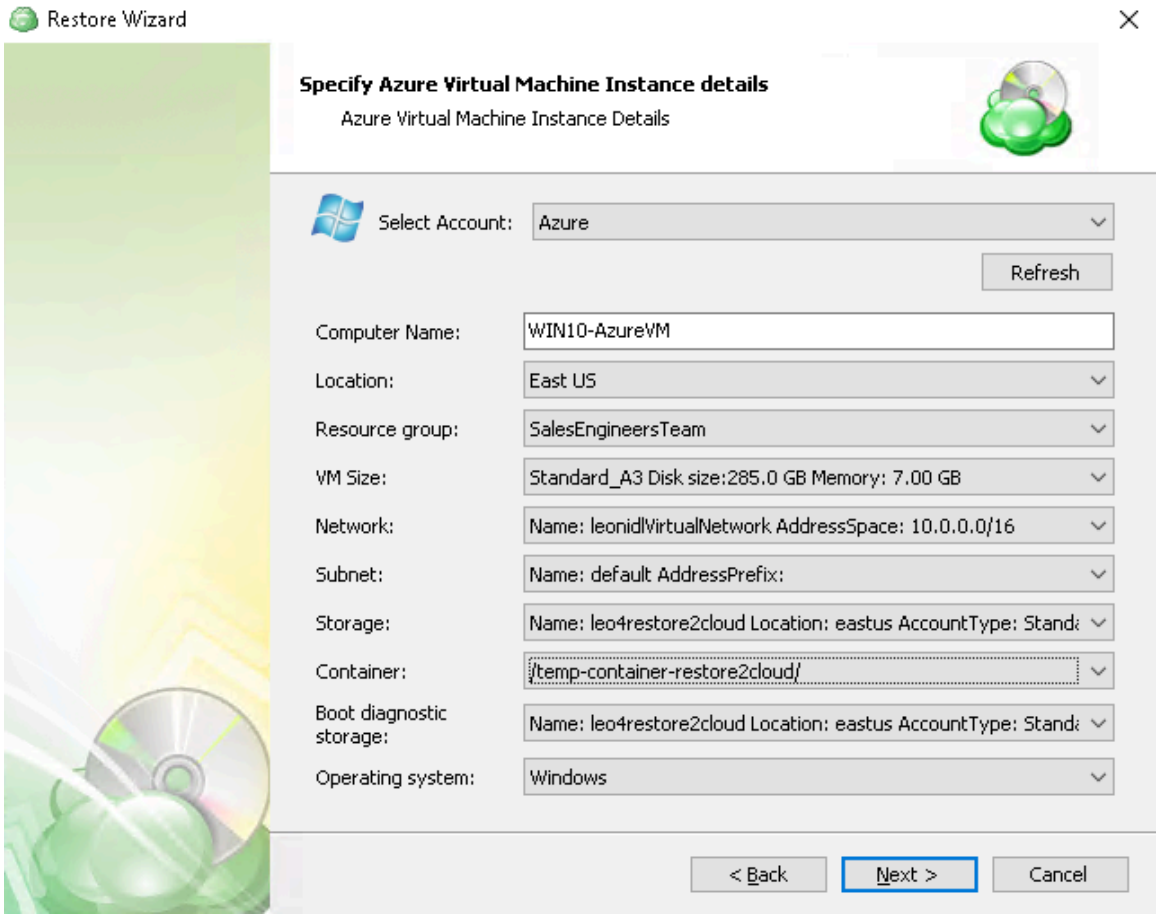
Step 11. Next you will need to determine which available checkpoint to restore for the virtual disk.



Step 12. With the checkpoint selected, you can now specify the type of instance you would like to create in Azure.



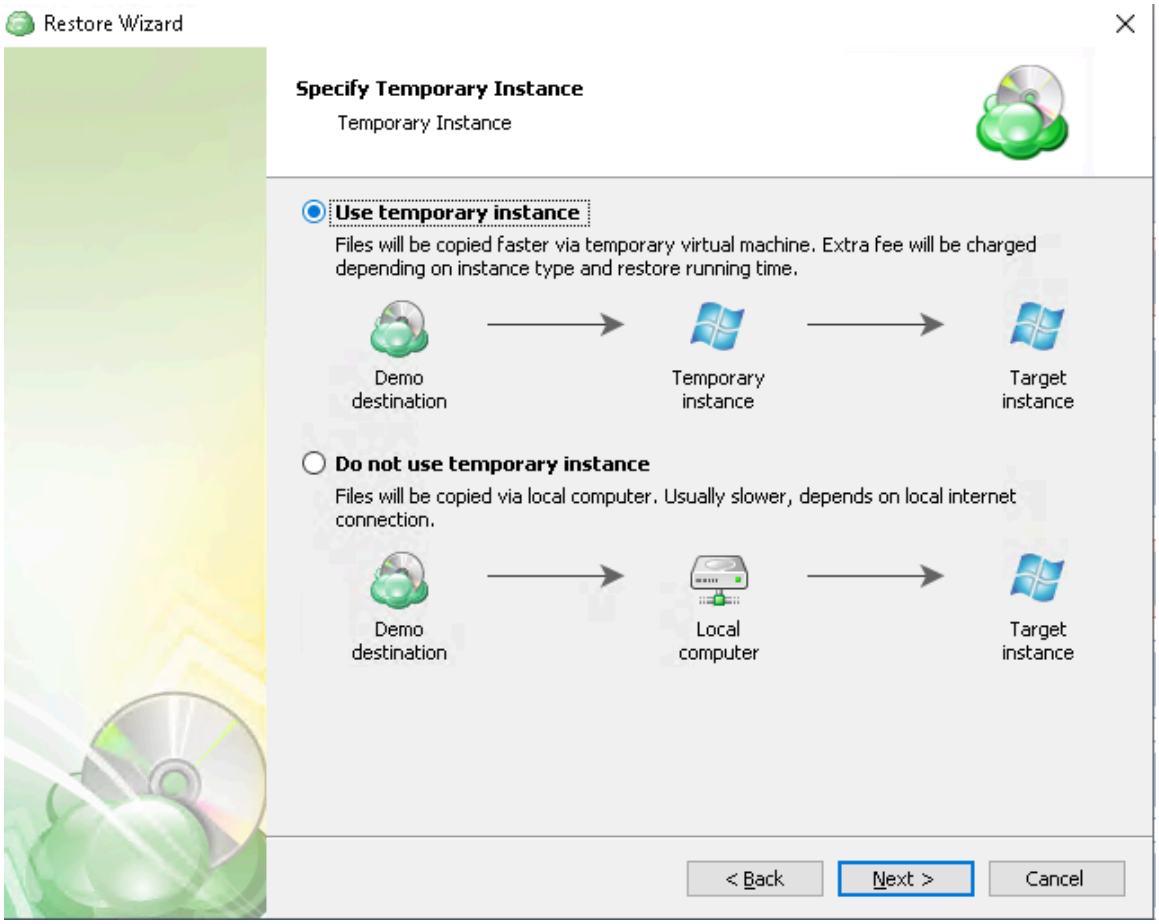
Step 13. If “Restore as Azure Virtual Machine” was selected: The next step allows you to select the appropriate Azure account from the upper dropdown box, and specify the configuration below. These options may vary depending on the type of instance selected in the previous step.



- **Computer Name:** Name to assign to the new virtual machine in Azure.
- **Location:** Azure region where the VM will be created (e.g., East US).
- **Resource group:** Azure Resource Group where the VM and associated resources will be deployed.
- **VM Size:** Specifies the virtual hardware profile (CPU, RAM, etc.) for the VM.
- **Network:** Azure virtual network to connect the VM. Defines subnet and IP range.
- **Use default AddressPrefix:** When enabled, uses the default IP address prefix for the selected network.
- **Storage**: Specifies the Azure storage account where the VM disk will be restored.
- **Container**: The storage container (within the selected storage account) where the VM disk will be stored.

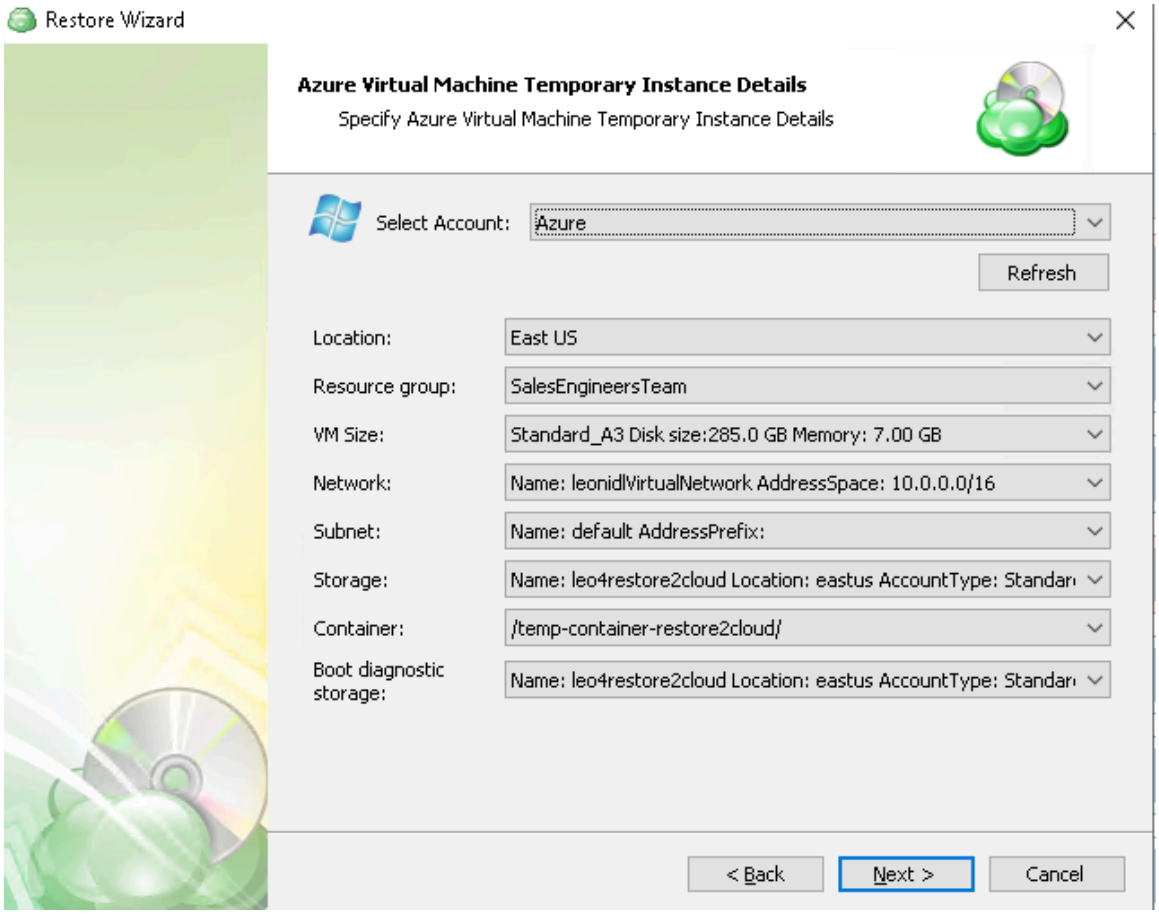
- **Boot diagnostic storage:** Storage account used by Azure to save diagnostic logs during VM boot.
- **Operating system:** OS of the restored VM (e.g., Windows or Linux). Used for compatibility and configuration during provisioning.

Step 14: After completing the Azure Virtual Machine, you'll have to choose if using a temporary instance or copy the files locally first.



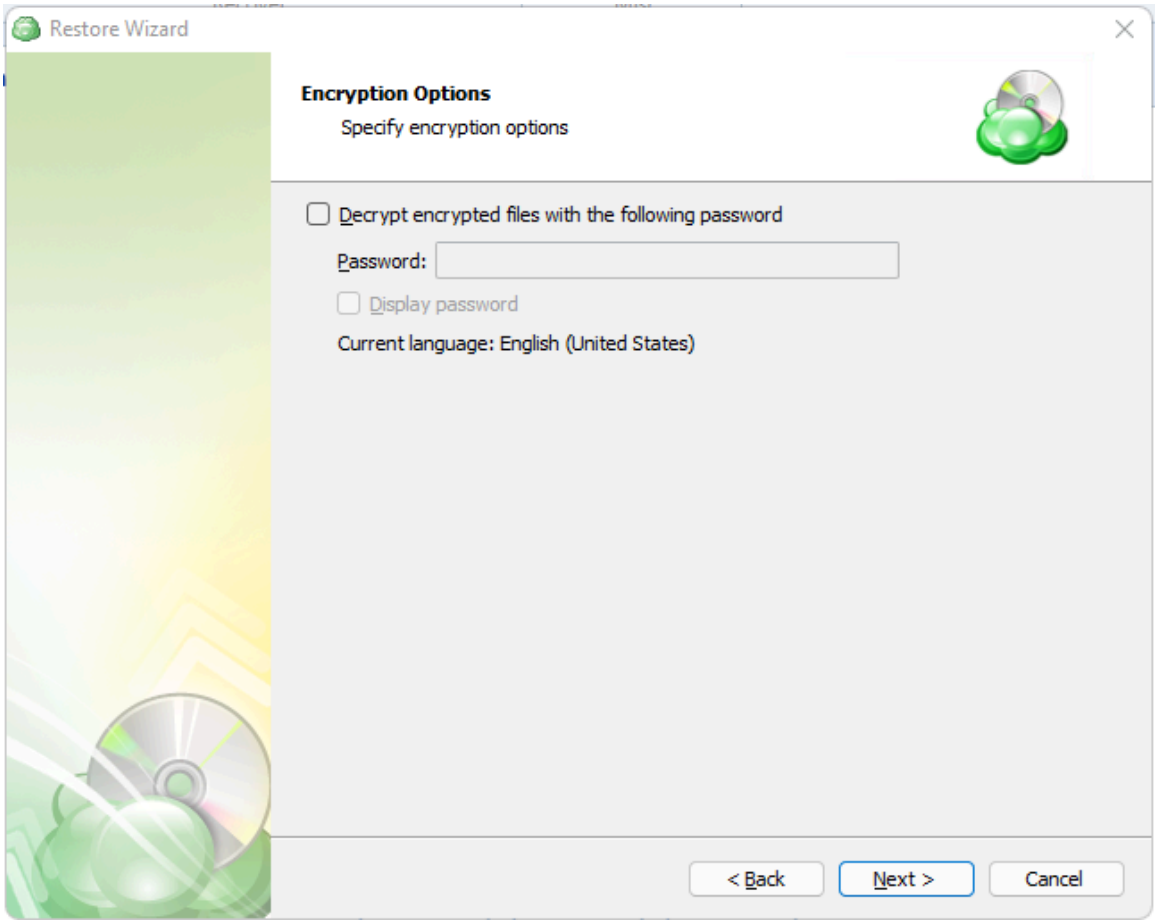
Use a temporary instance for faster cloud-to-cloud restores; avoid it to reduce cloud compute costs at the expense of speed.

Step 15. If “Use temporary Instance” was selected. You’ll need to specify the Temporary Instance Details

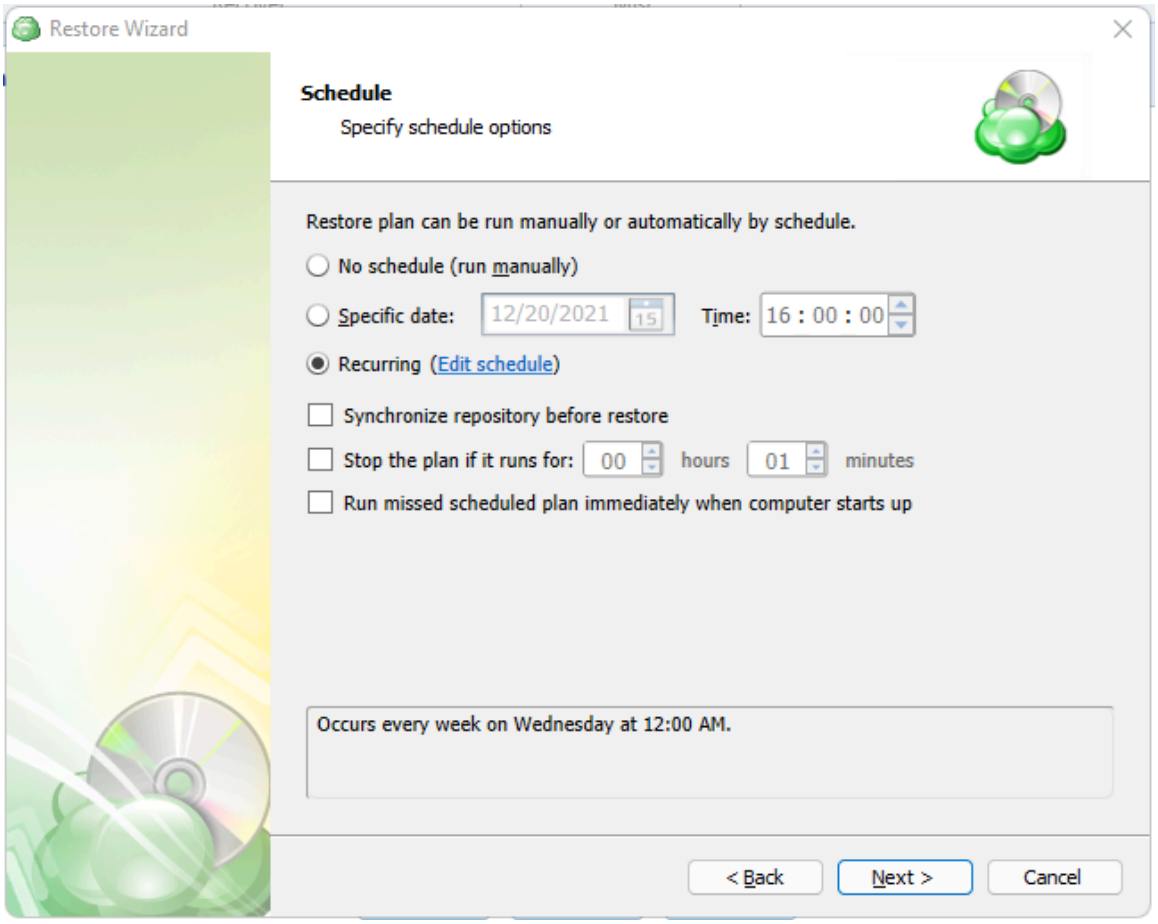


- **Location:** Azure region where the VM will be created (e.g., East US).
- **Resource group:** Azure Resource Group where the VM and associated resources will be deployed.
- **VM Size:** Specifies the virtual hardware profile (CPU, RAM, etc.) for the VM.
- **Network:** Azure virtual network to connect the VM. Defines subnet and IP range.
- **Storage**: Specifies the Azure storage account where the VM disk will be restored.
- **Container**: The storage container (within the selected storage account) where the VM disk will be stored.
- **Boot diagnostic storage:** Storage account used by Azure to save diagnostic logs during VM boot.

Step 16. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the VM.



Step 17. With the decryption password entered, the next step is setting the schedule for the restore plan.

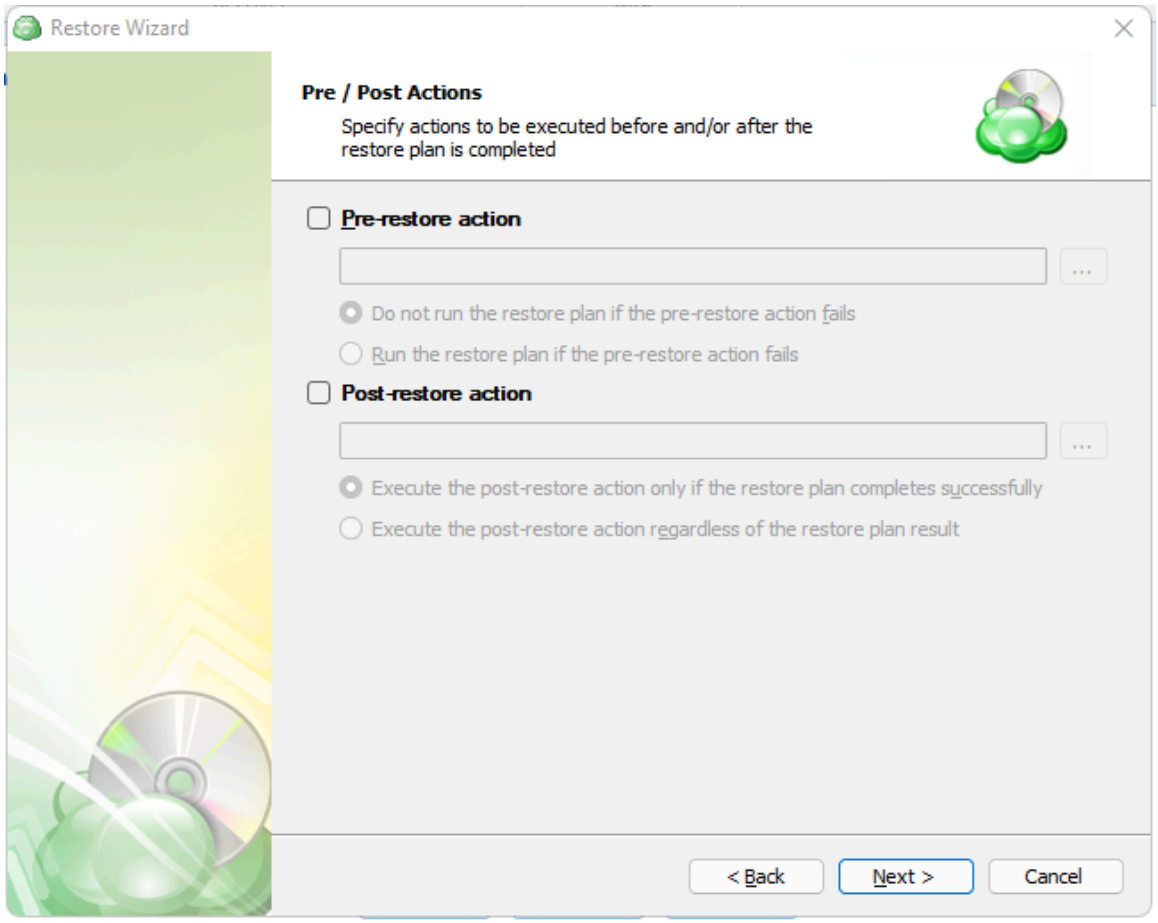


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

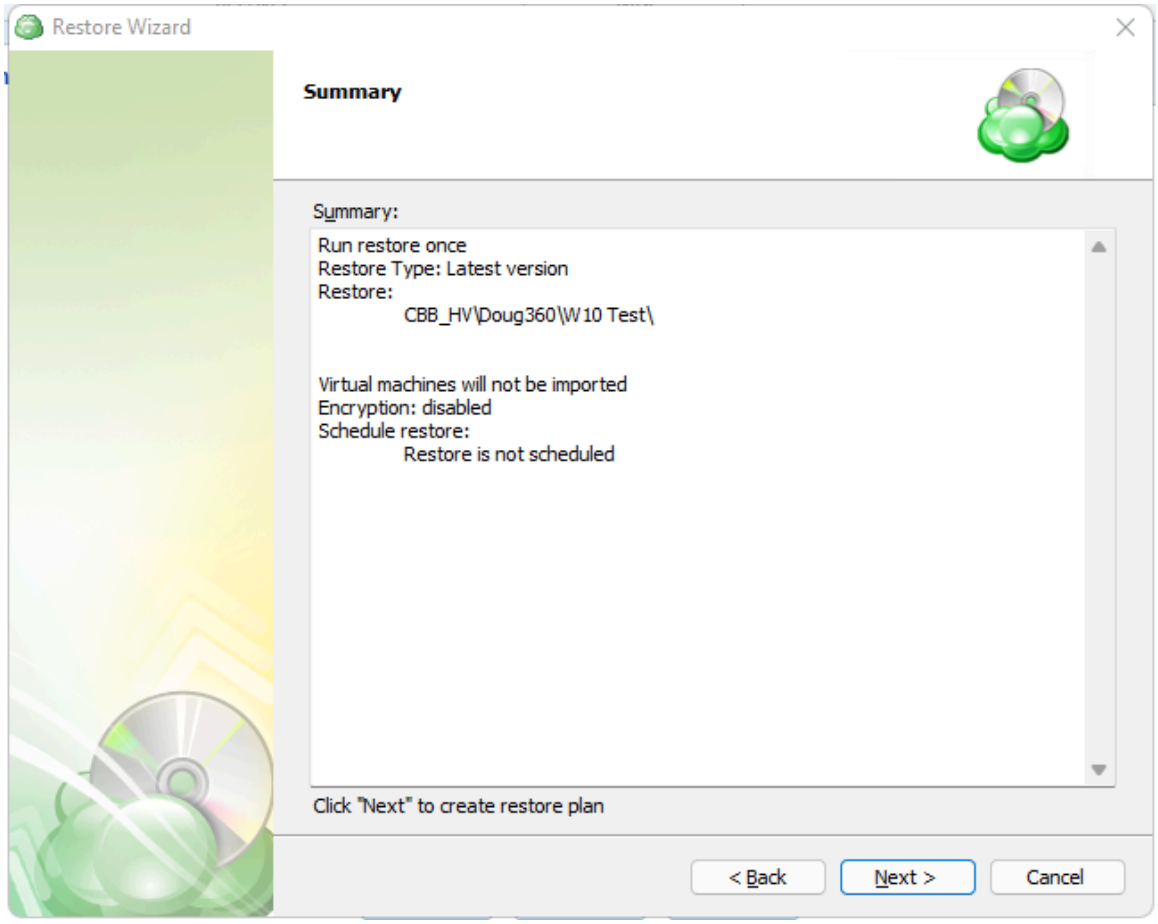
> Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

> Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 18. After setting the schedule, the next step allows pre and post actions to be defined.



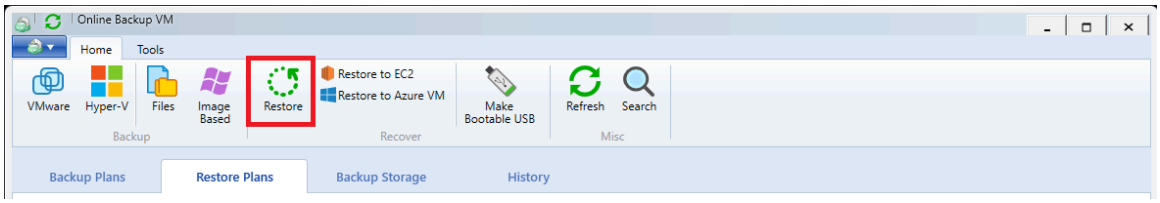
Step 19. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.



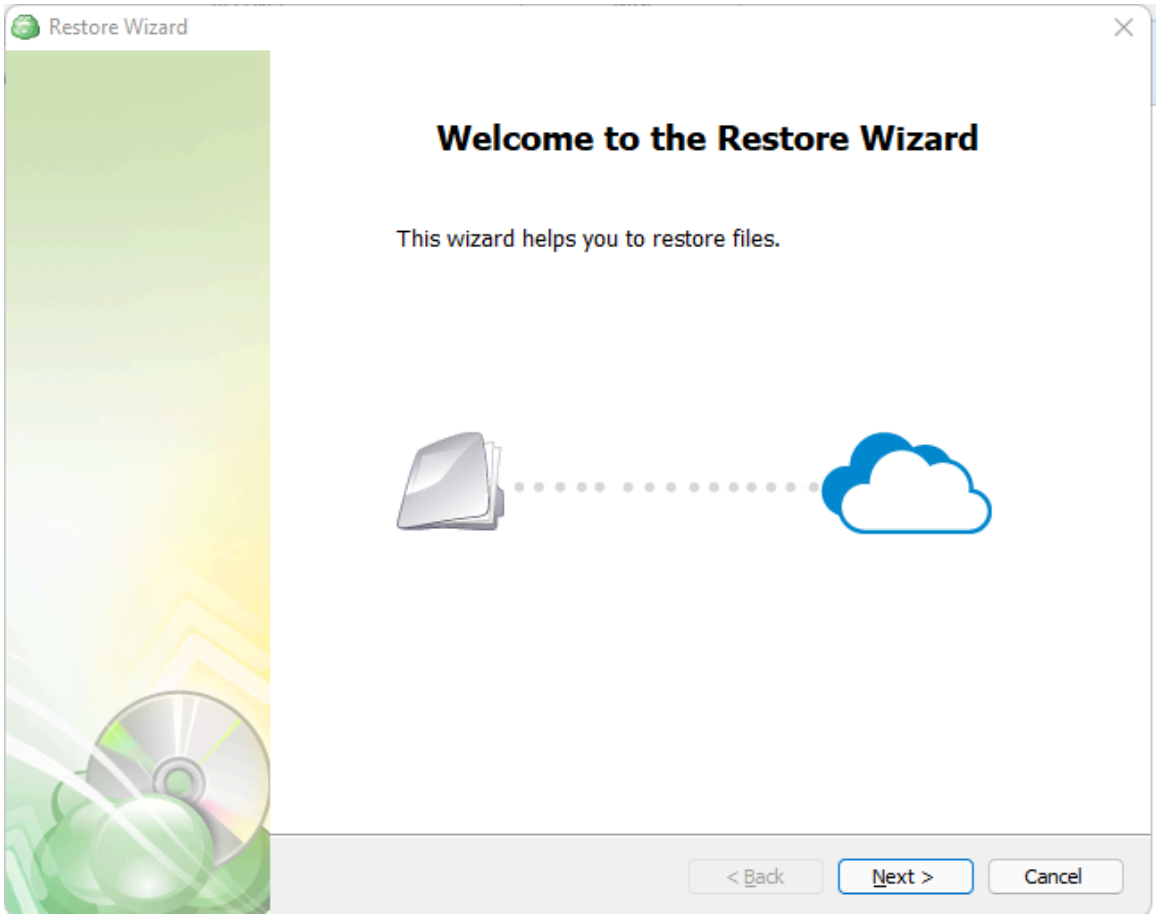
> If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

Restore as an AWS EC2 Instance using the Agent

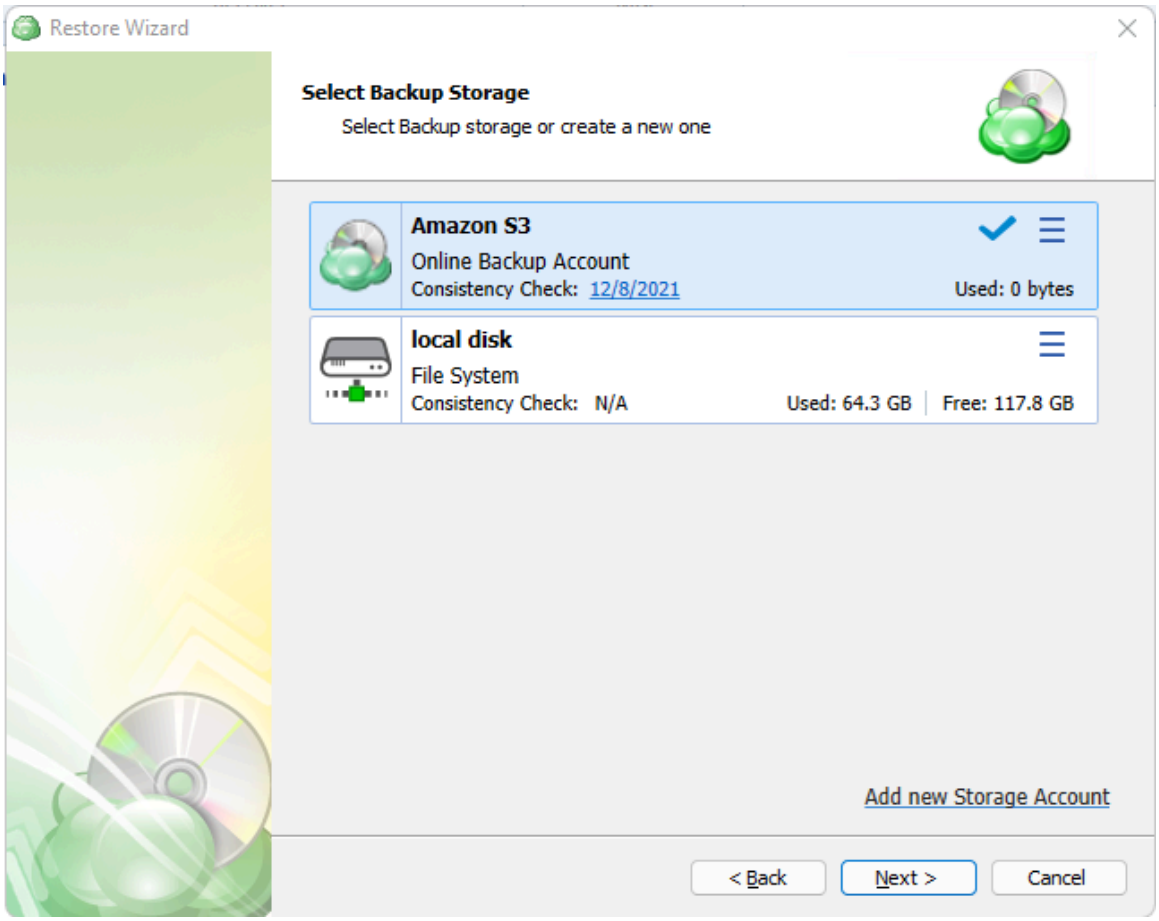
Step 1. Within the Online Backup Agent, click on “Restore”



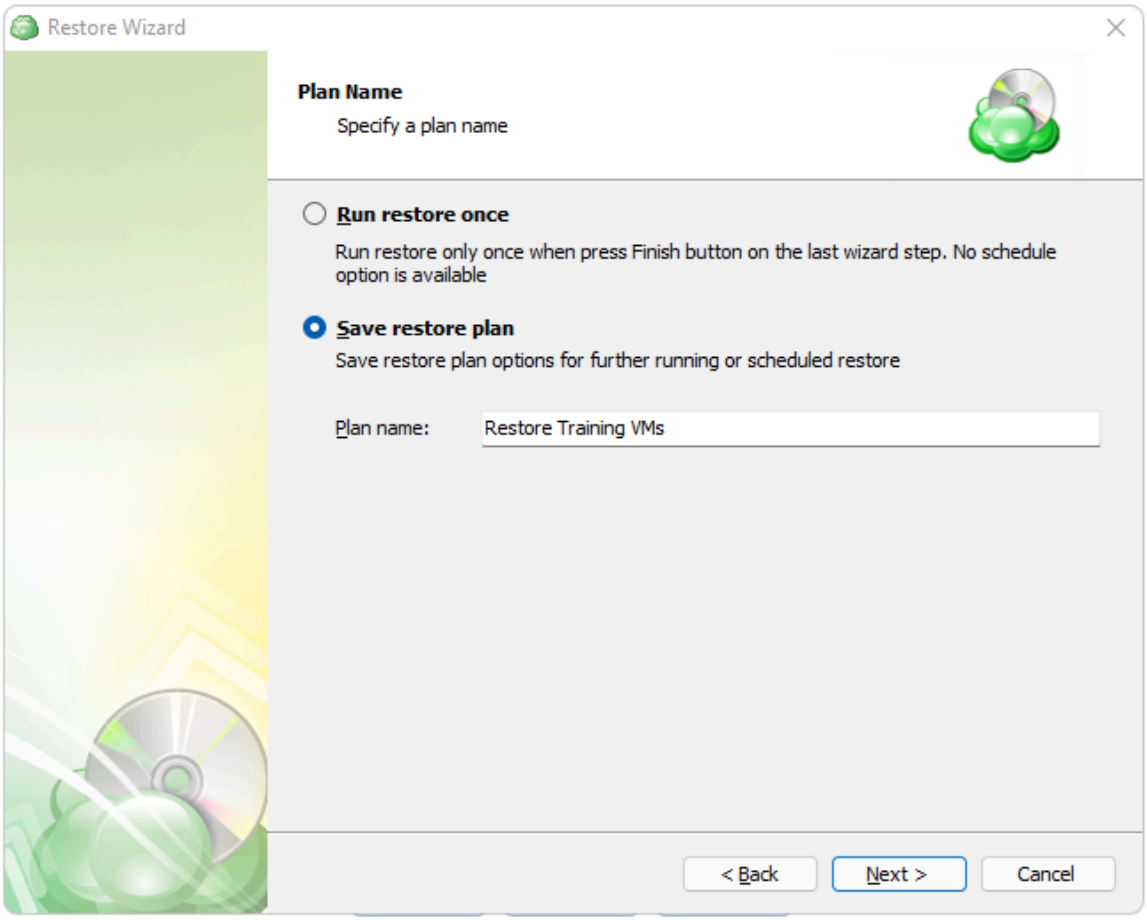
Step 2. Once the wizard starts, click on Next to advance to the next step.



Step 3. The next step will prompt you to select the source for the restore point.



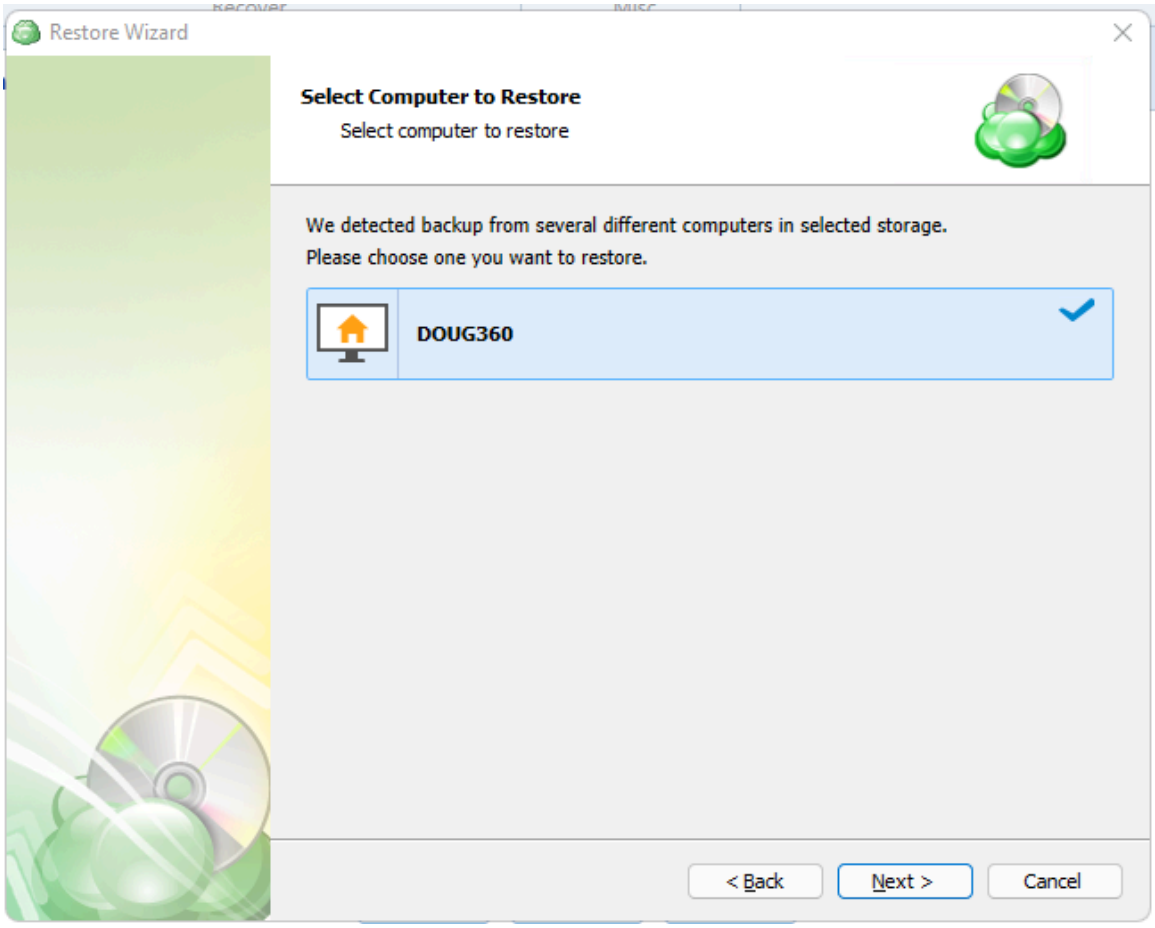
Step 4. Next, you will be given the option to either run the restore once or to save it to run later.



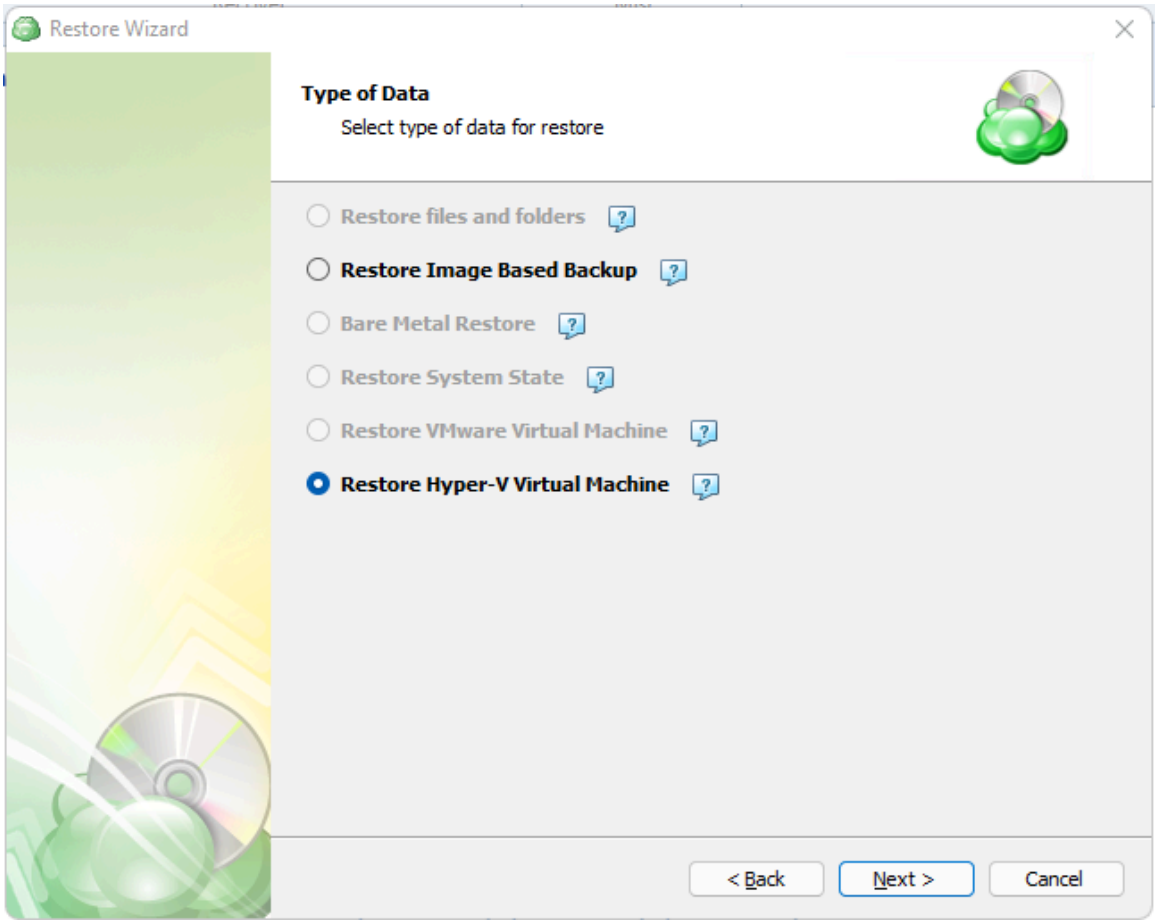
"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

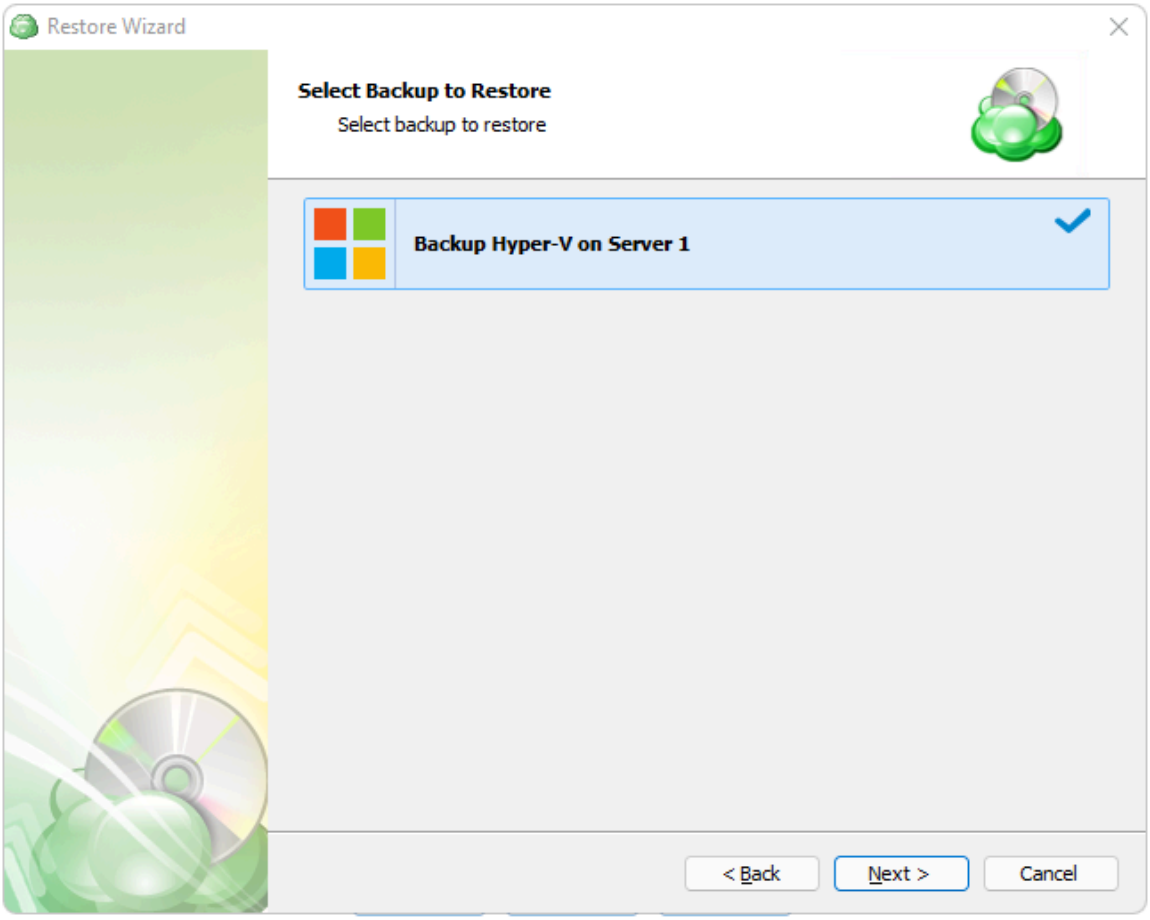
Step 5. With the type of restore selected, the next step is to select the correct Host server which the VM resides on.



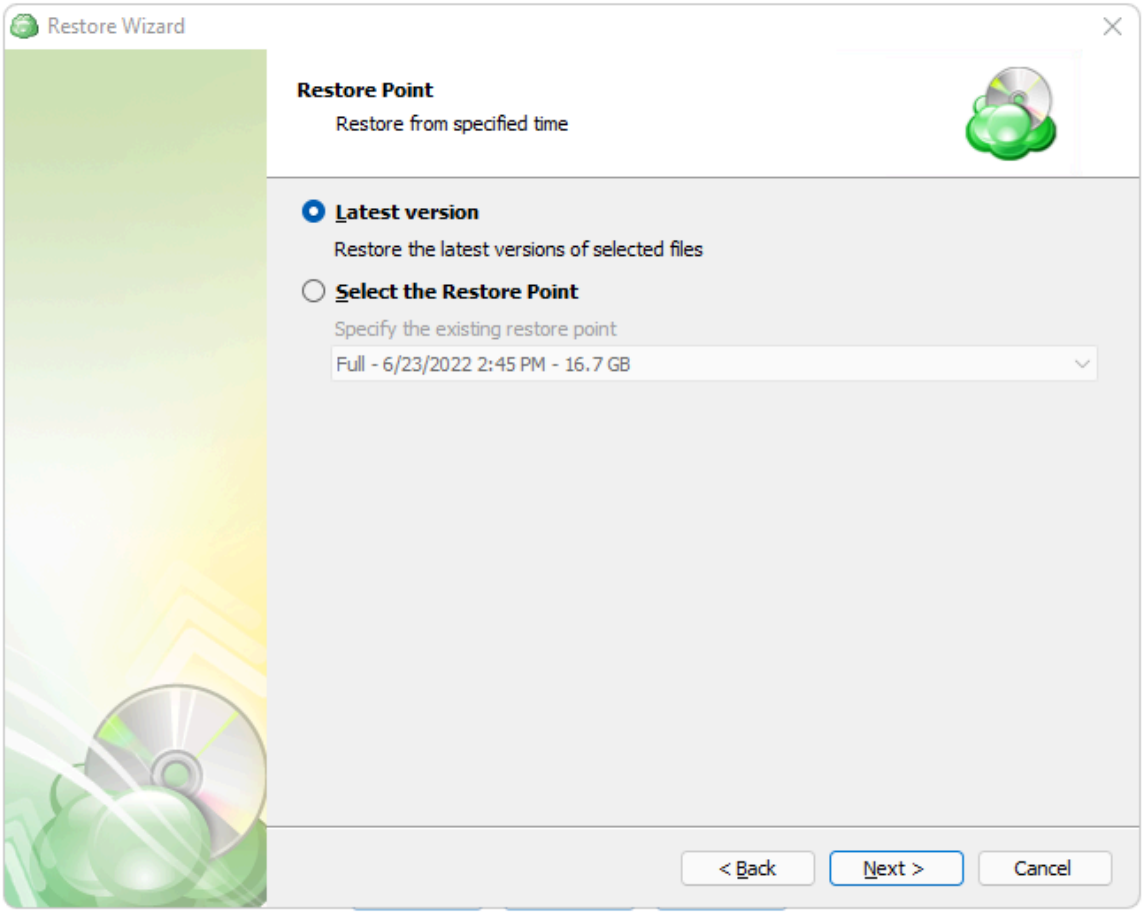
Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “Restore Hyper-V Virtual Machine” option to continue.



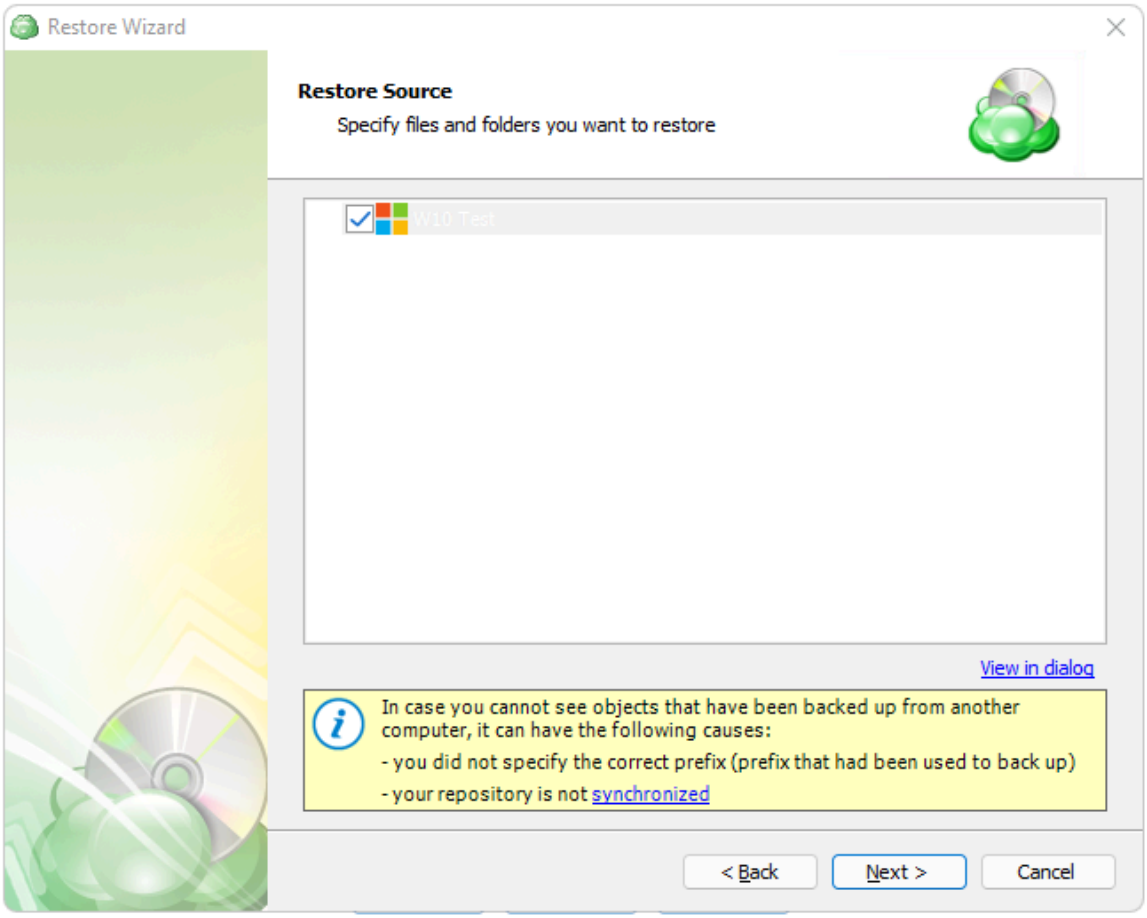
Step 7. With the correct type of data selected, the application will generate a list of available VM backup plans.



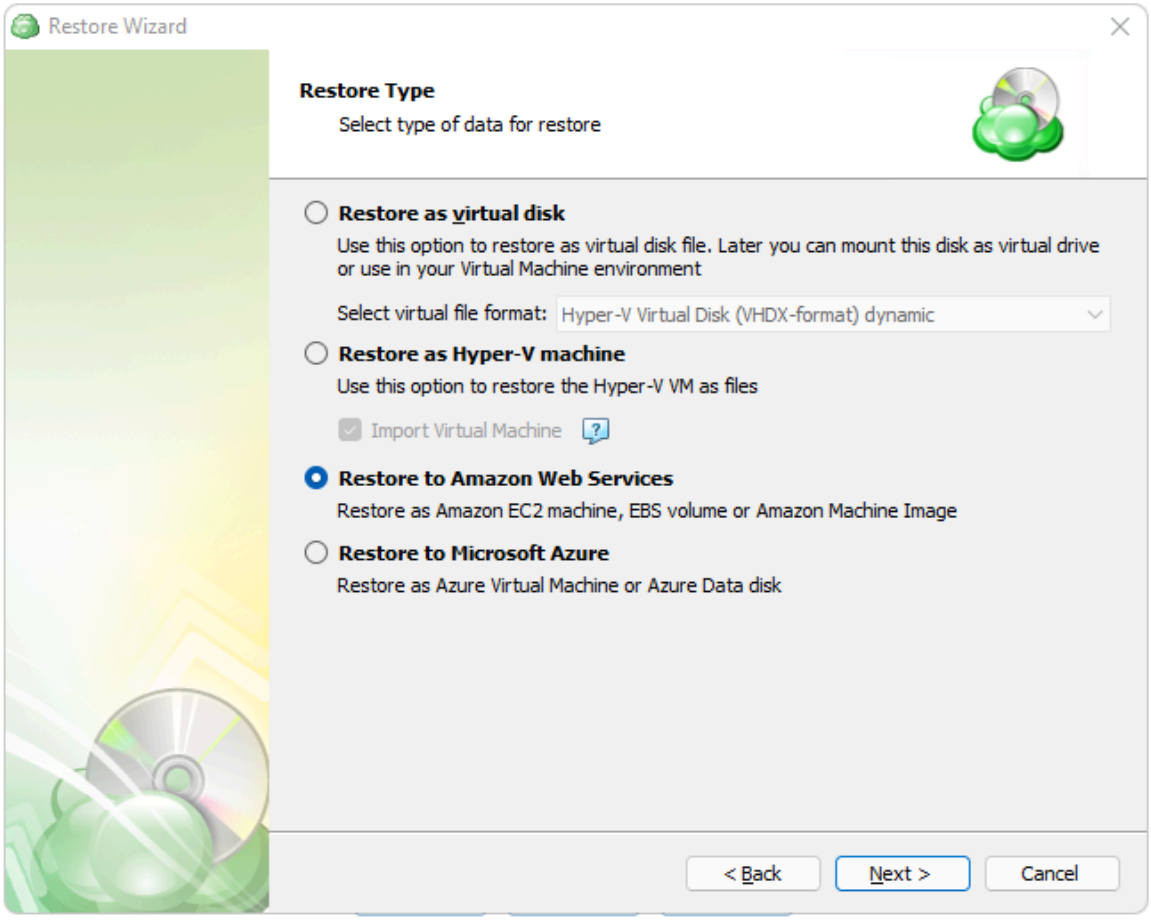
Step 8. Next you will be given a choice for what point in time you would like to restore the VM to.



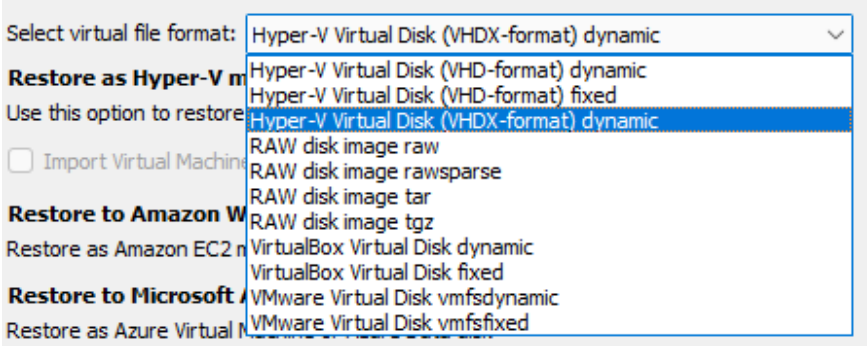
Step 9. Next, you will be able to expand the list of VM backups on the selected host and choose which to restore.



Step 10. The next step of the wizard allows you to choose how the VM data should be restored.

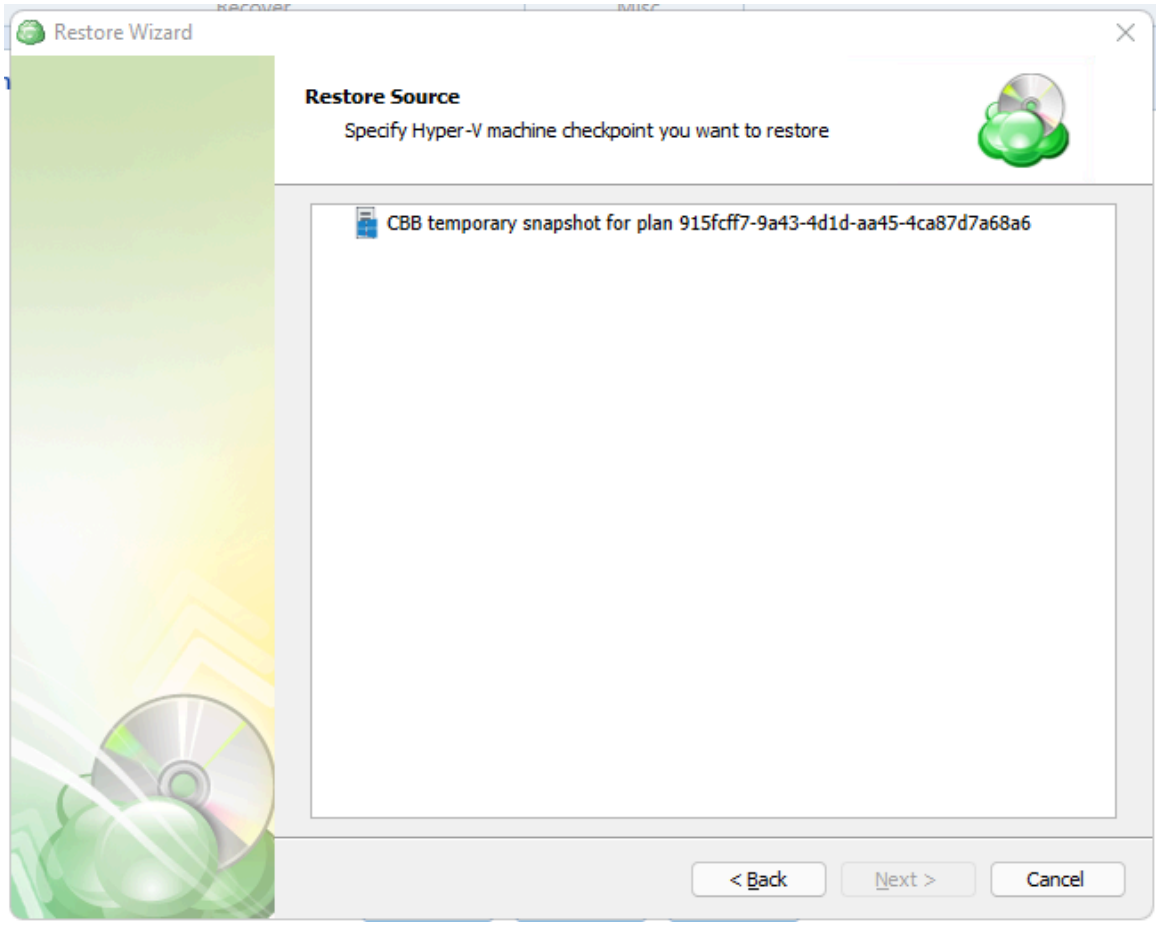


- **Restore as virtual disk:** Restores the virtual disks in the backup as a file which can later be mounted to a VM. No configuration files are included. Several formats are available:

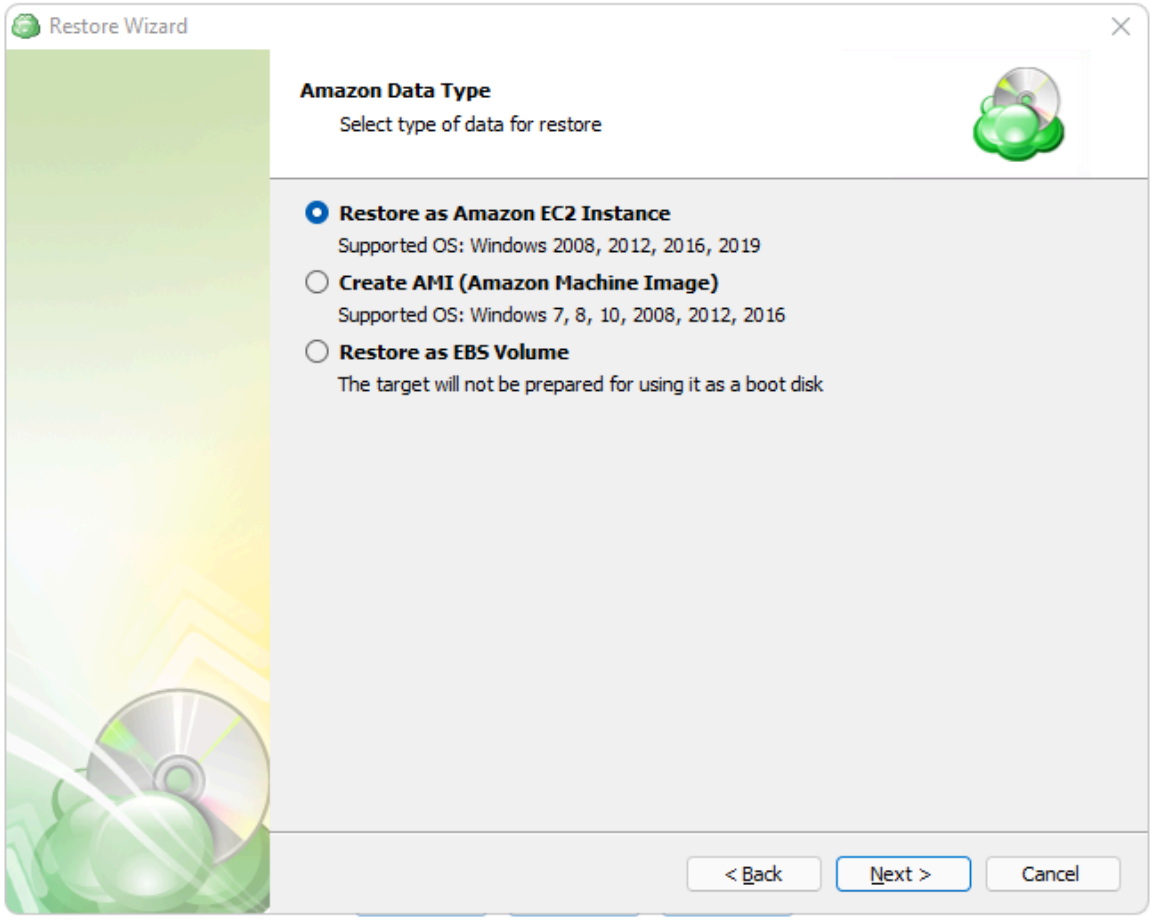


- **Restore as a Hyper-V machine:** Selecting this option restores the virtual machine configuration as well as the virtual disks as files, but does not import the VM into the hypervisor by default.
    - **Import Virtual Machine:** Use this option to have the VM automatically imported to the hypervisor.
- **Restore to Amazon Web Services:** If enabled, this will restore the selected VM directly to AWS Cloud either as an EC2 instance, EBS volume, or AMI.
- **Restore to Microsoft Azure:** This will restore the VM directly to Azure as either an Azure Virtual Machine or Azure Data disk.

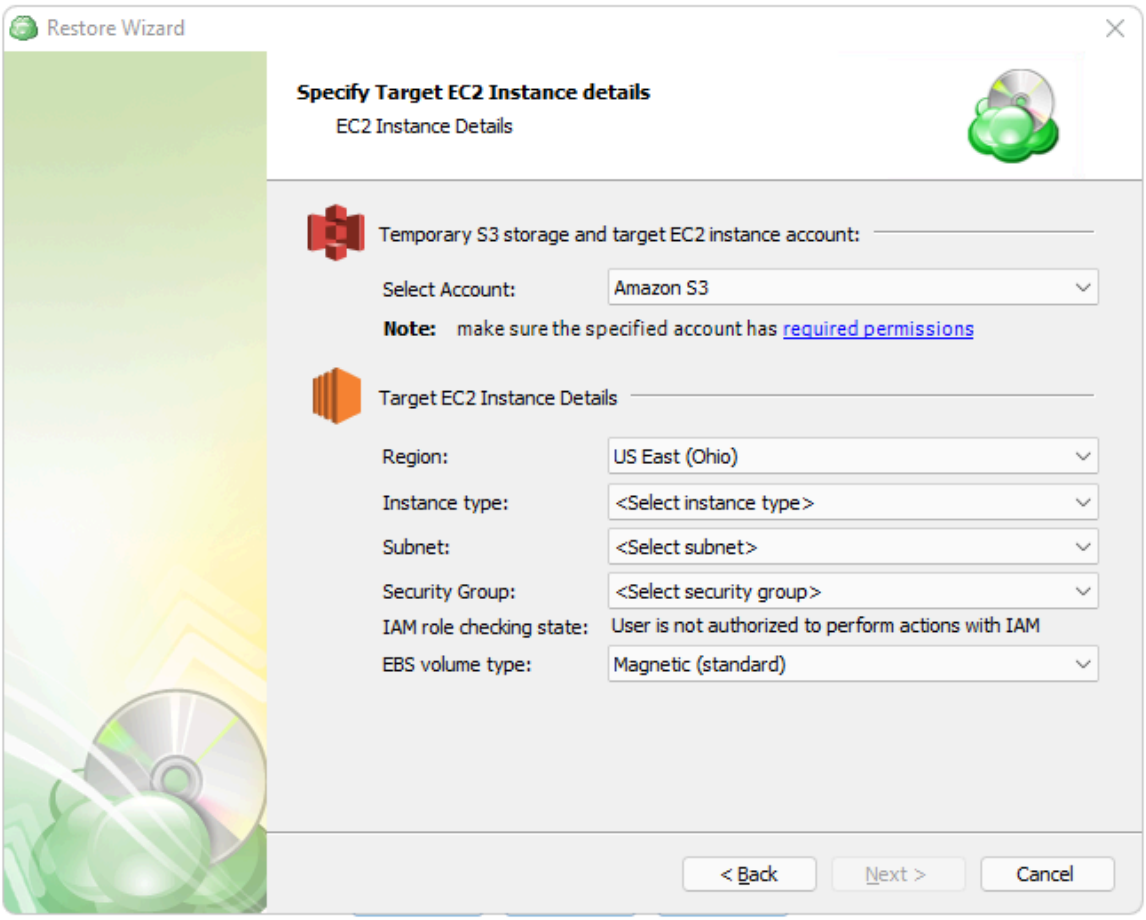
Step 11. Next you will need to determine which available checkpoint to restore for the virtual disk.



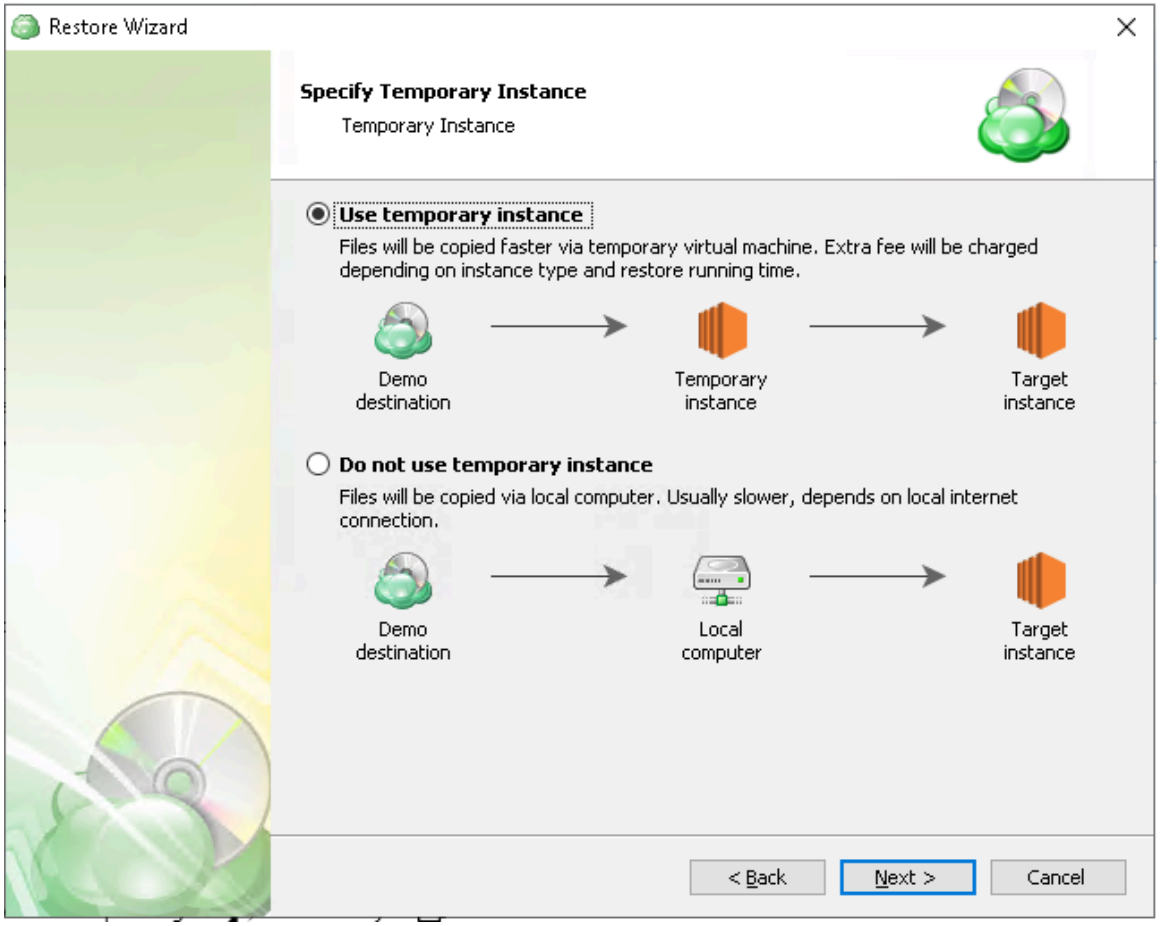
Step 12. With the checkpoint selected, you can now specify the type of instance you would like to create in AWS.



Step 13. The next step allows you to select the appropriate Azure account from the upper dropdown box, and specify the configuration below. These options may vary depending on the type of instance selected in the previous step.

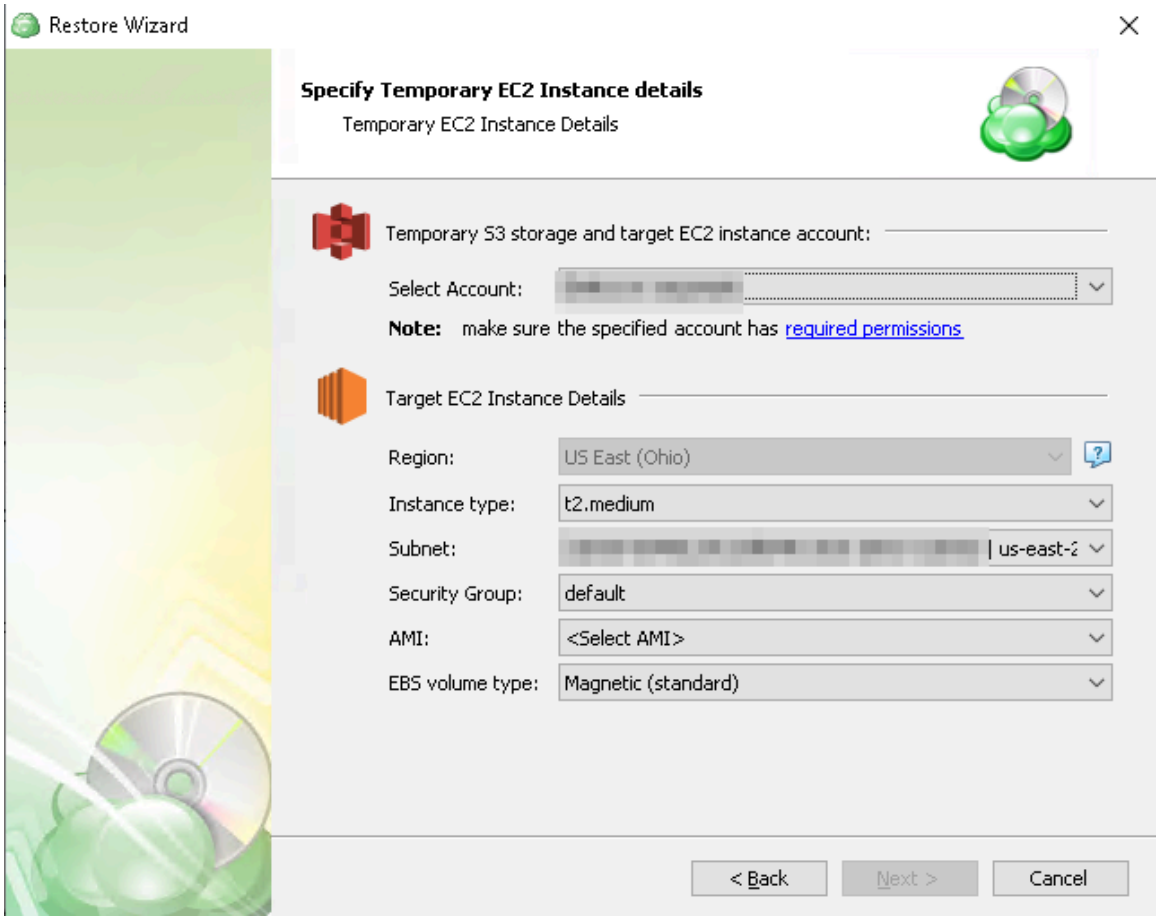


Step 14. After completing the AWS account/Instance details you'll have to choose whether to use a temporary instance or copy the files locally first.

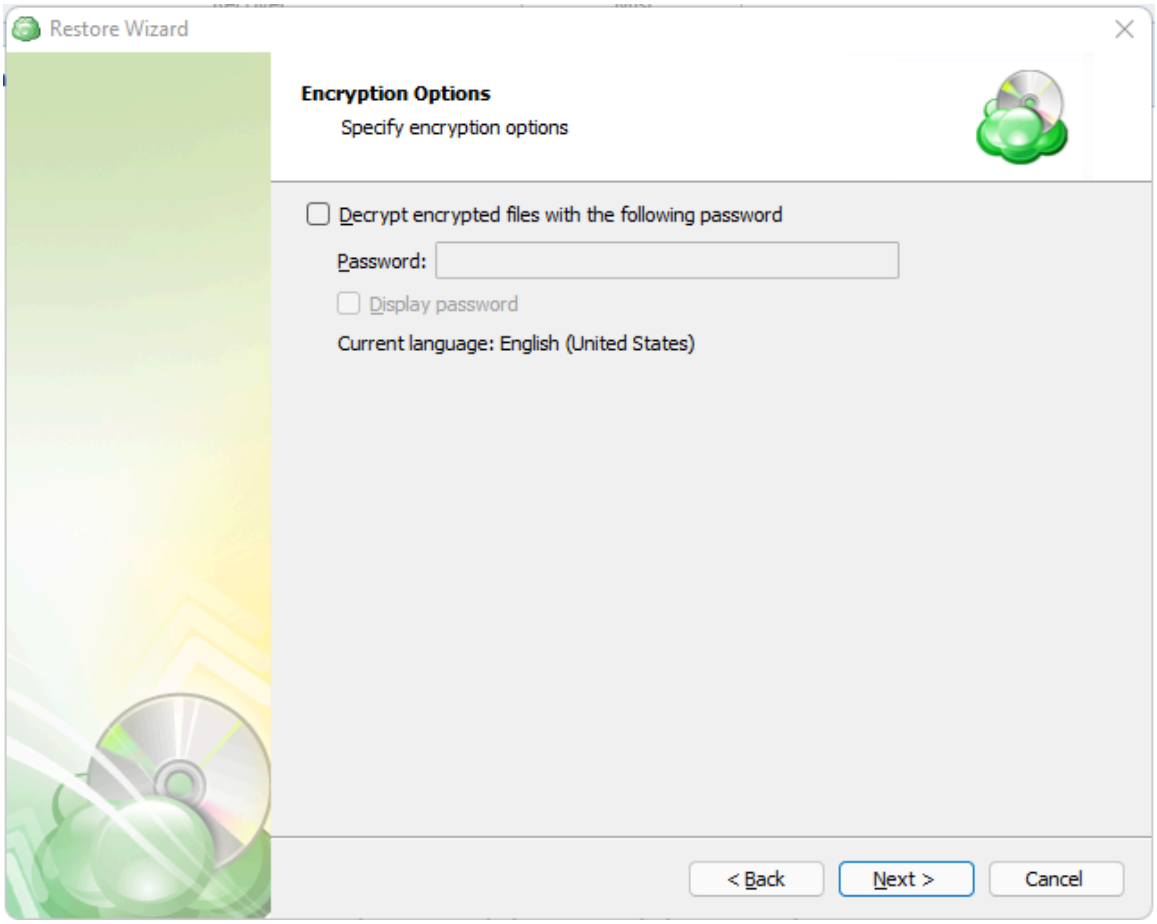


Use a temporary instance for faster cloud-to-cloud restores; avoid it to reduce cloud compute costs at the expense of speed.

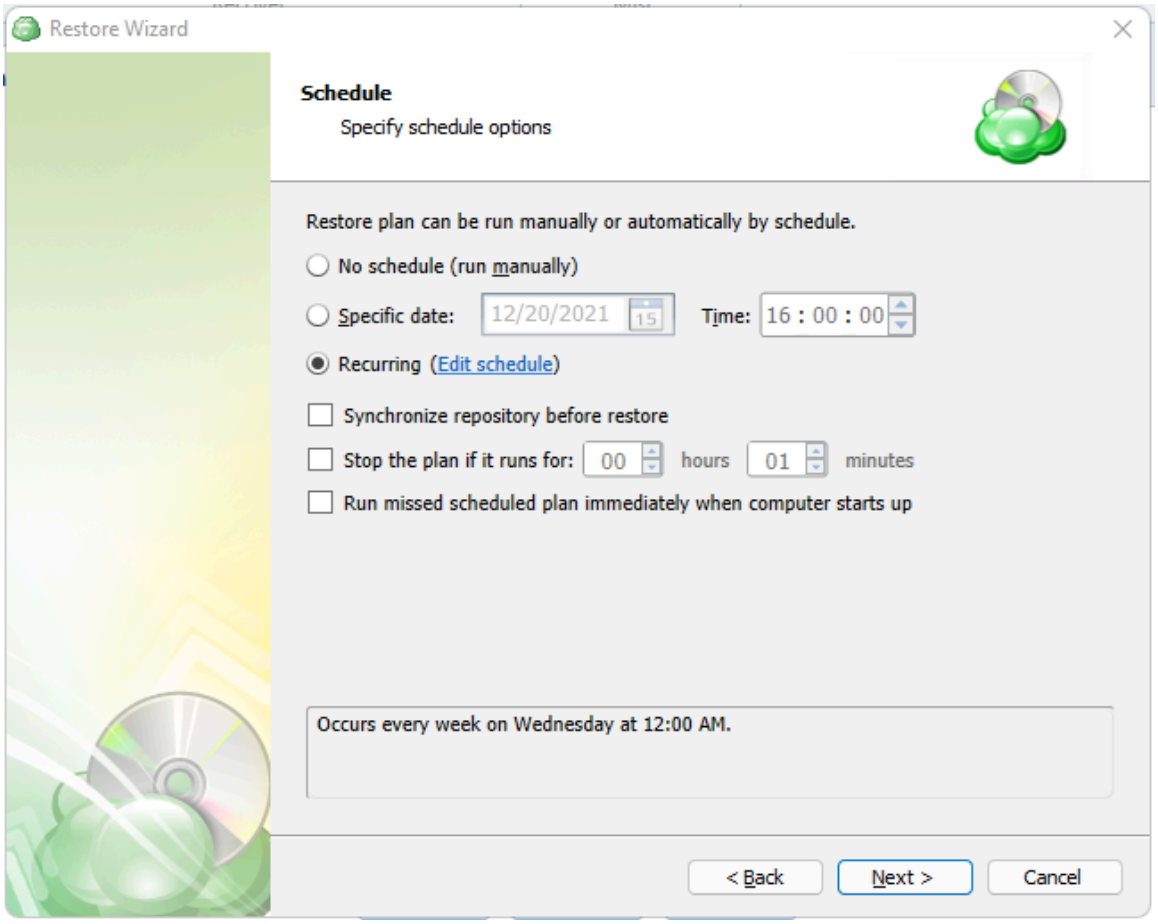
Step 15. If “Use temporary Instance” was selected. You’ll need to specify the AWS Temporary EC2 Instance Details



Step 16. After selecting the destination and any associated options, you will be prompted to provide the password to decrypt the VM.



Step 17. With the decryption password entered, the next step is setting the schedule for the restore plan.

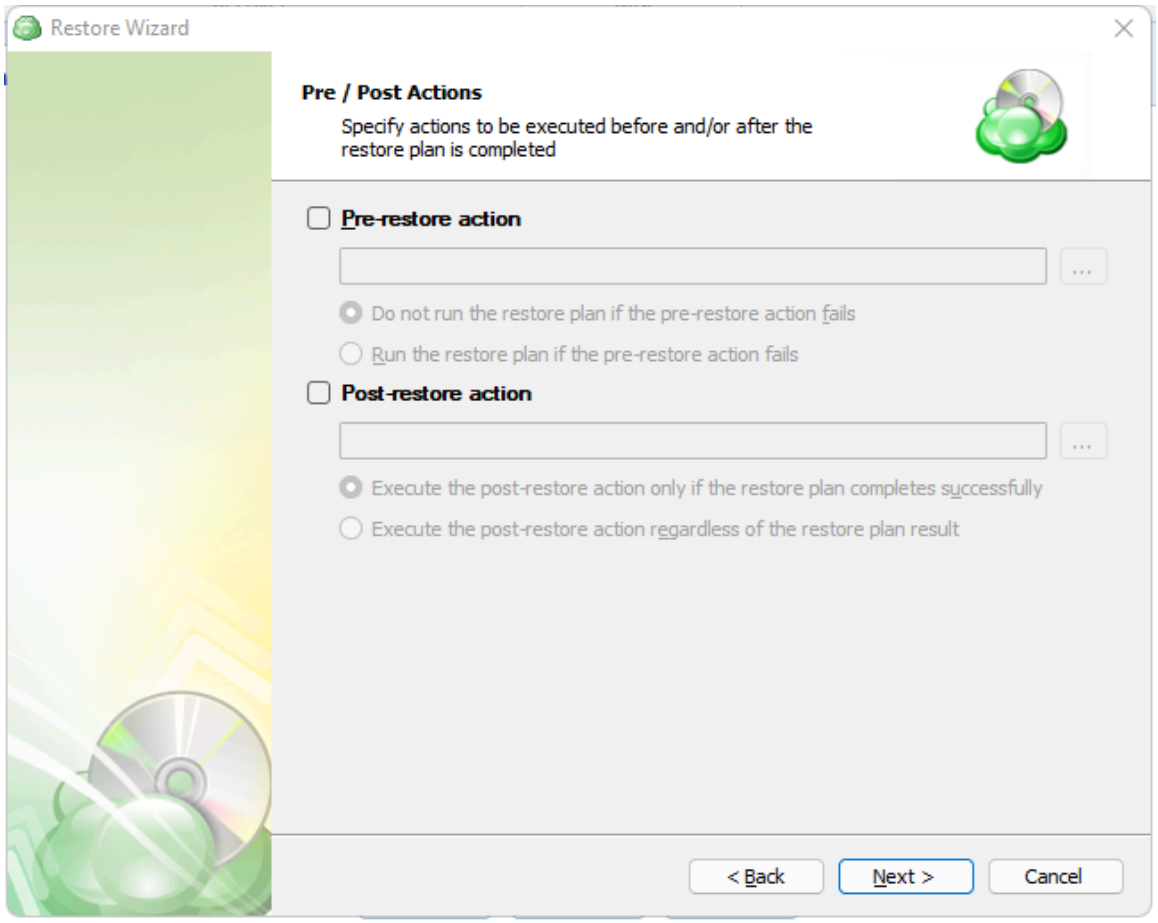


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

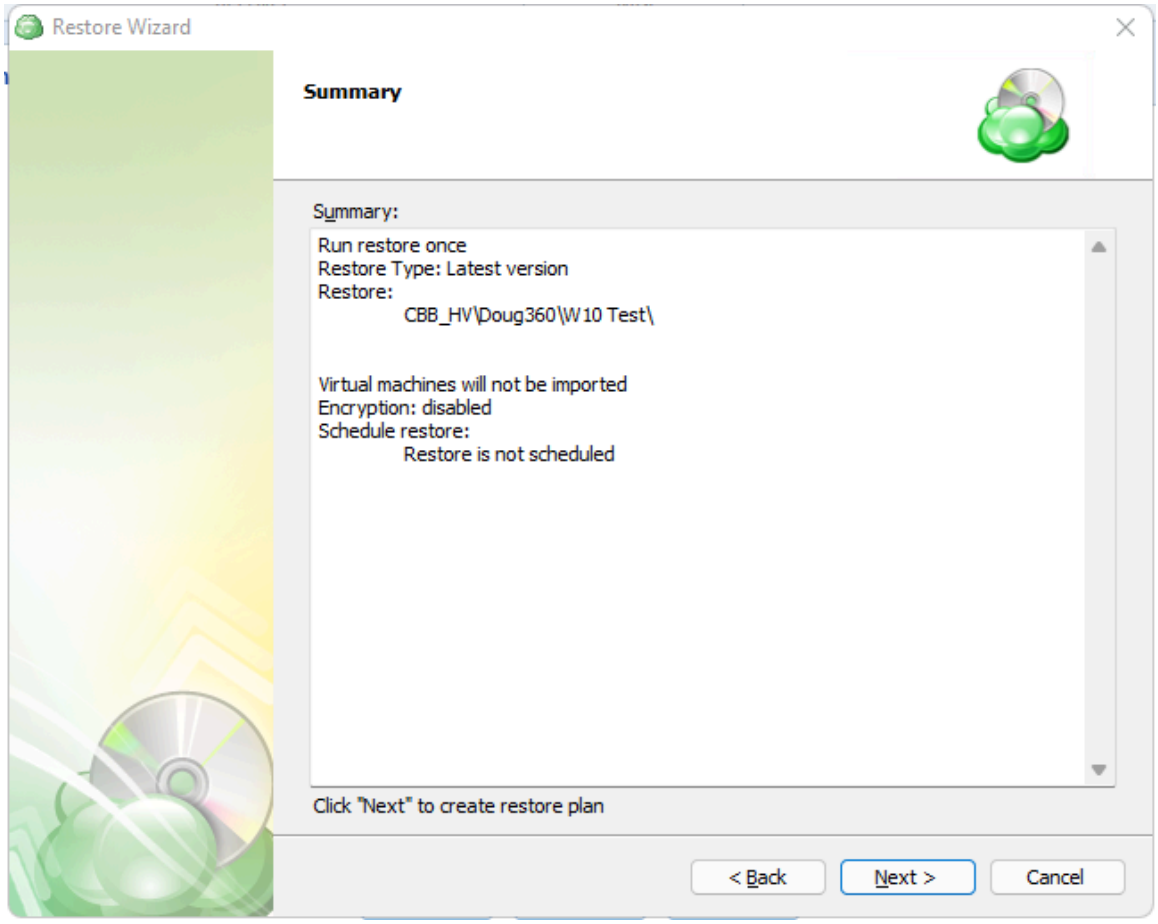
> Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 18. After setting the schedule, the next step allows pre and post actions to be defined.



Step 19. The final step of the wizard displays a summary of all selections for your review. Once read, click on “Next” to create the plan.

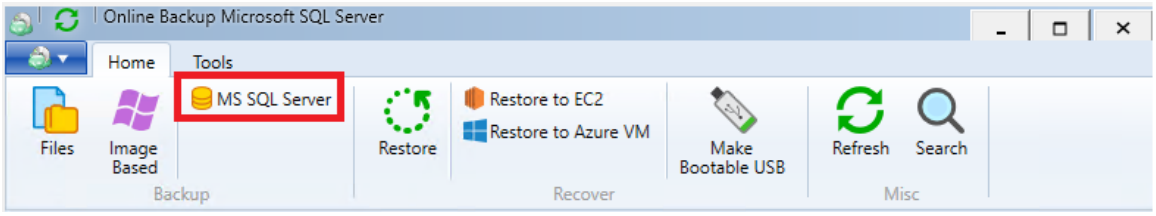


If “Run restore once” was selected at the beginning of the wizard, the plan will immediately execute once you click “Next”.

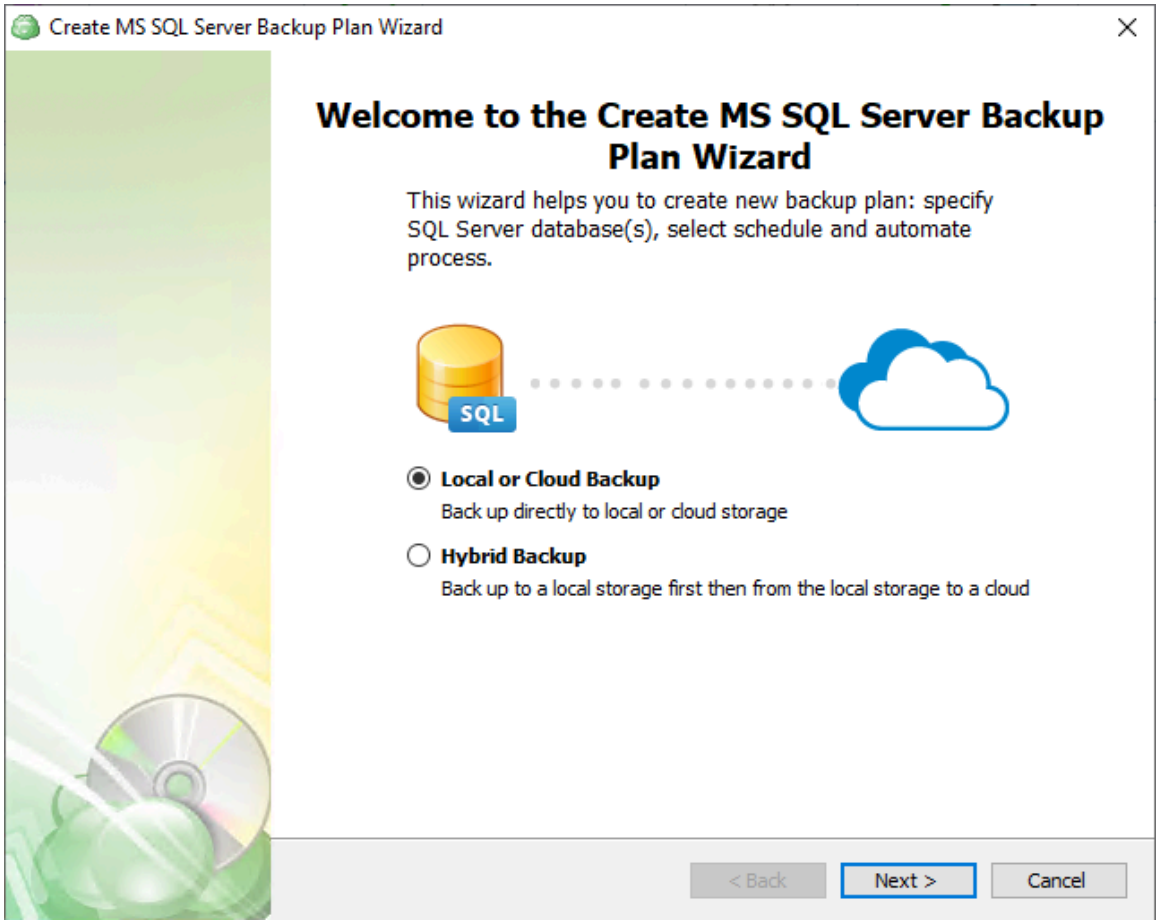
MS SQL Backup Plans

Backup Databases using the Agent

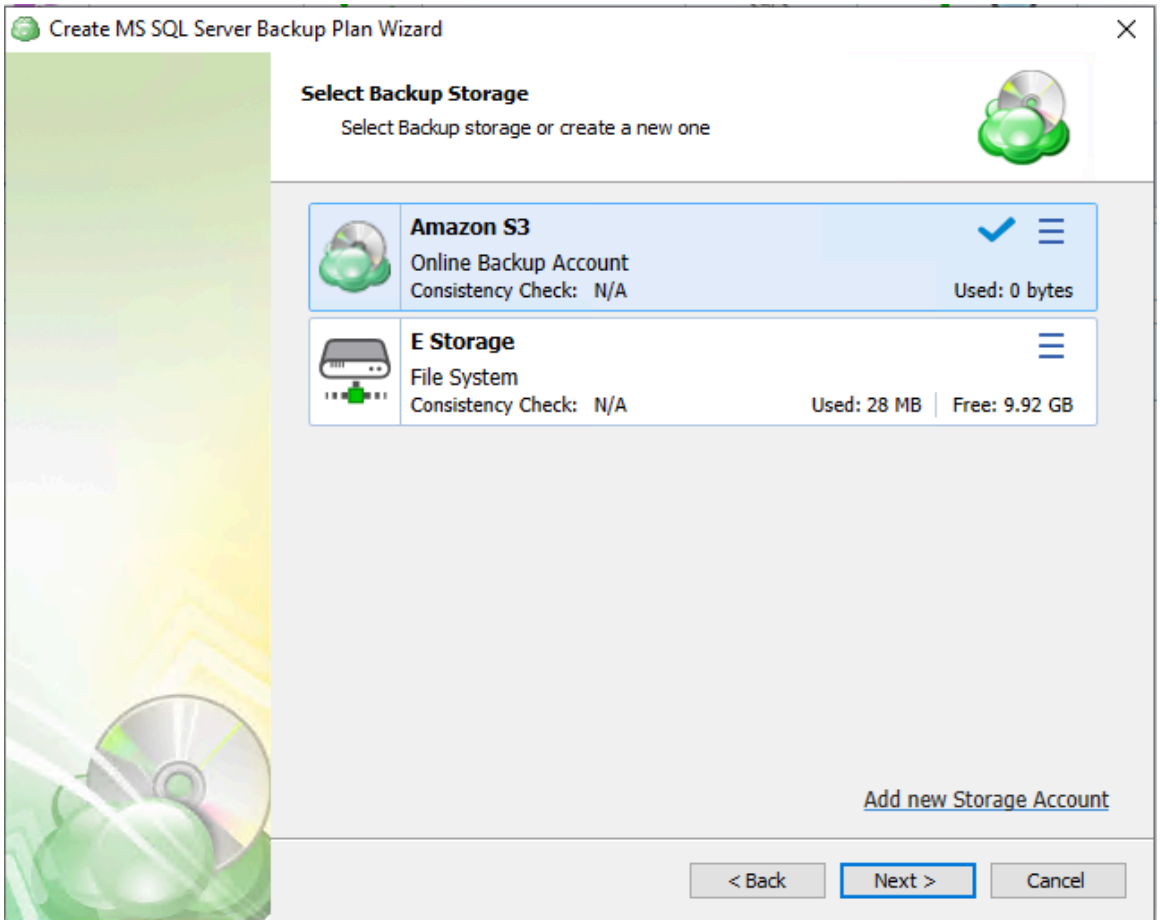
Step 1. Within the Online Backup Agent, click on “MS SQL Server”



Step 2. You will then be prompted to select the type of backup to create, either a standard Local/Cloud Backup, or a Hybrid Backup.

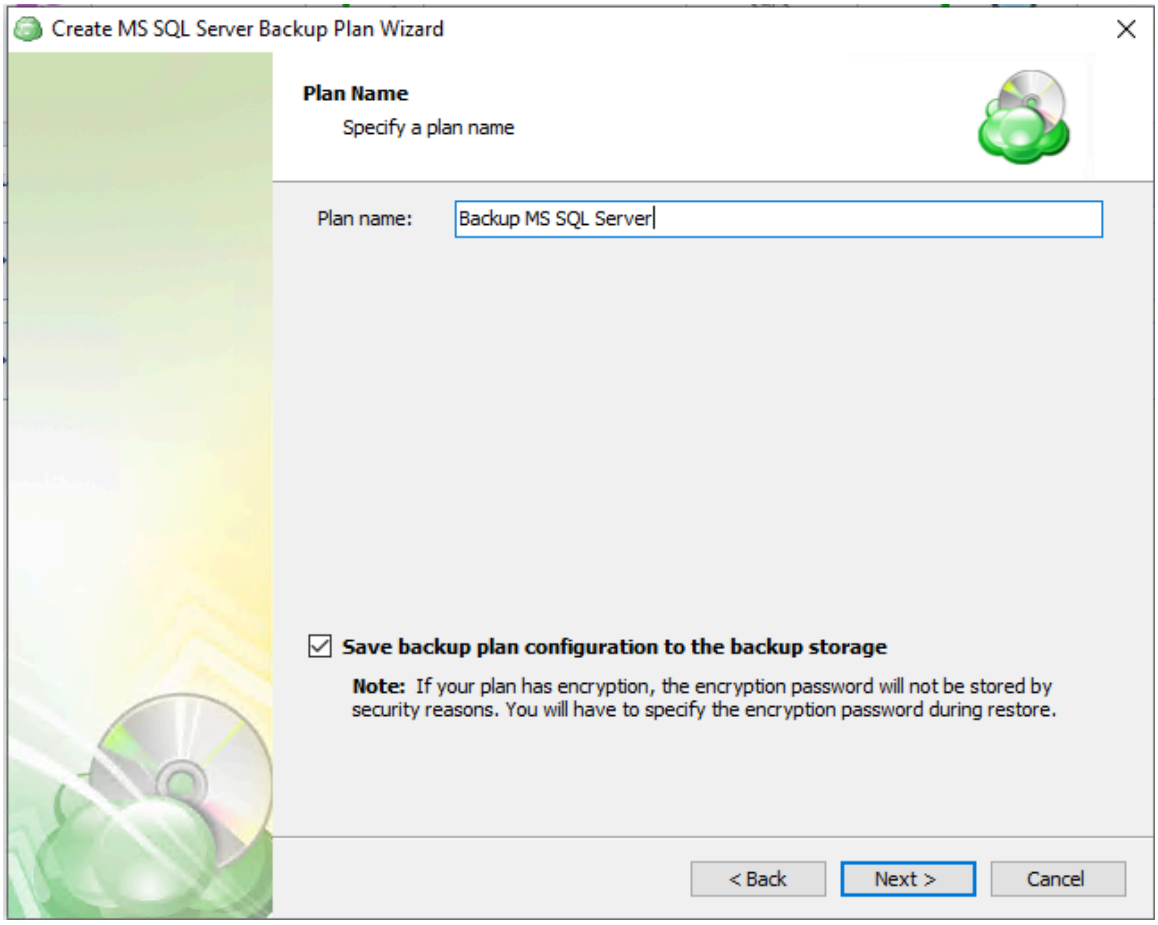


Step 3. The next step will prompt you to select the destination for the backup. This screen will be repeated for the second location if you selected “Hybrid” on the previous screen.



If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

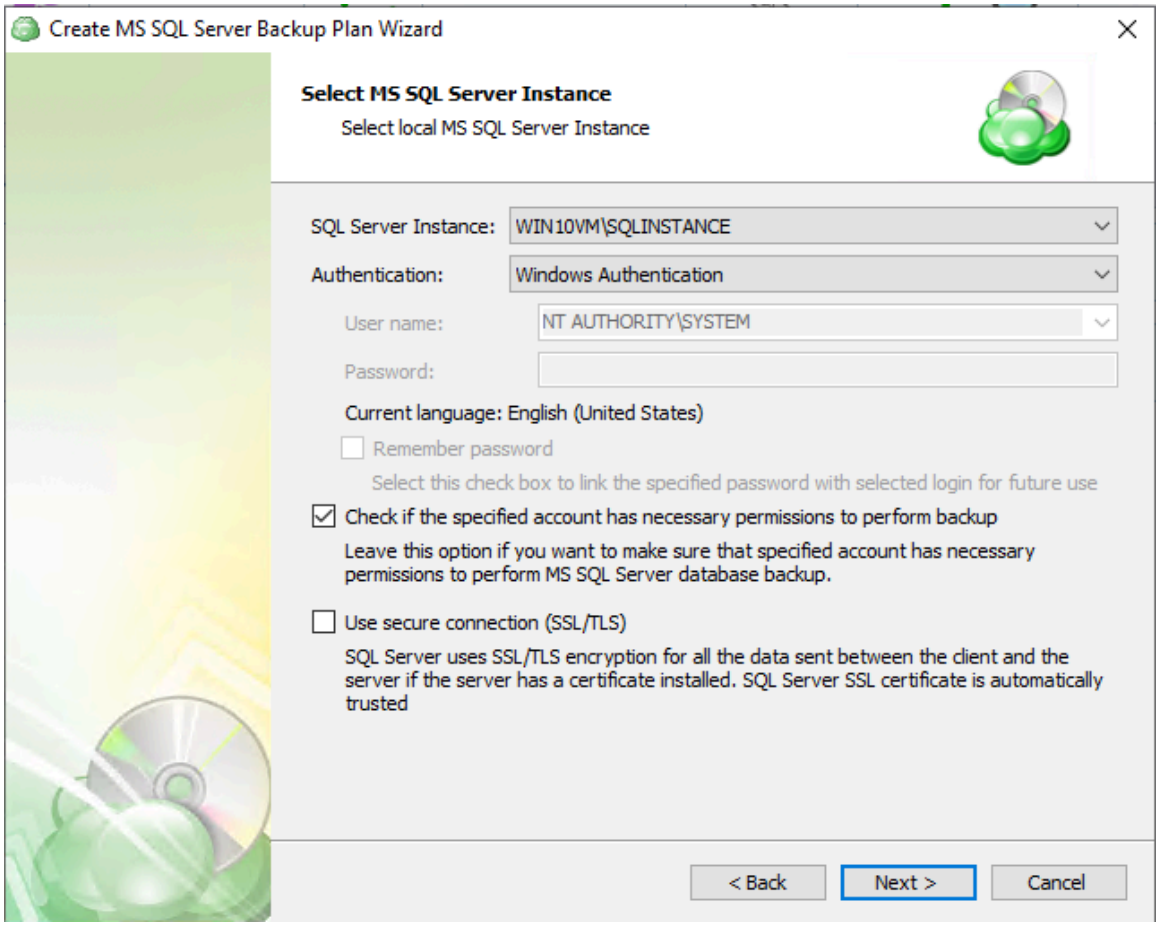
Step 4. Next, you will be prompted to name the plan.



It is recommended to use a descriptive name which will distinguish the backup from others.

“Save backup plan configuration to the backup storage” option allows you easily restore the backup plan to another destination if necessary.

Step 5. Next you will be prompted to select the SQL Server Instance as well as specify the credentials to be used by the backup service.



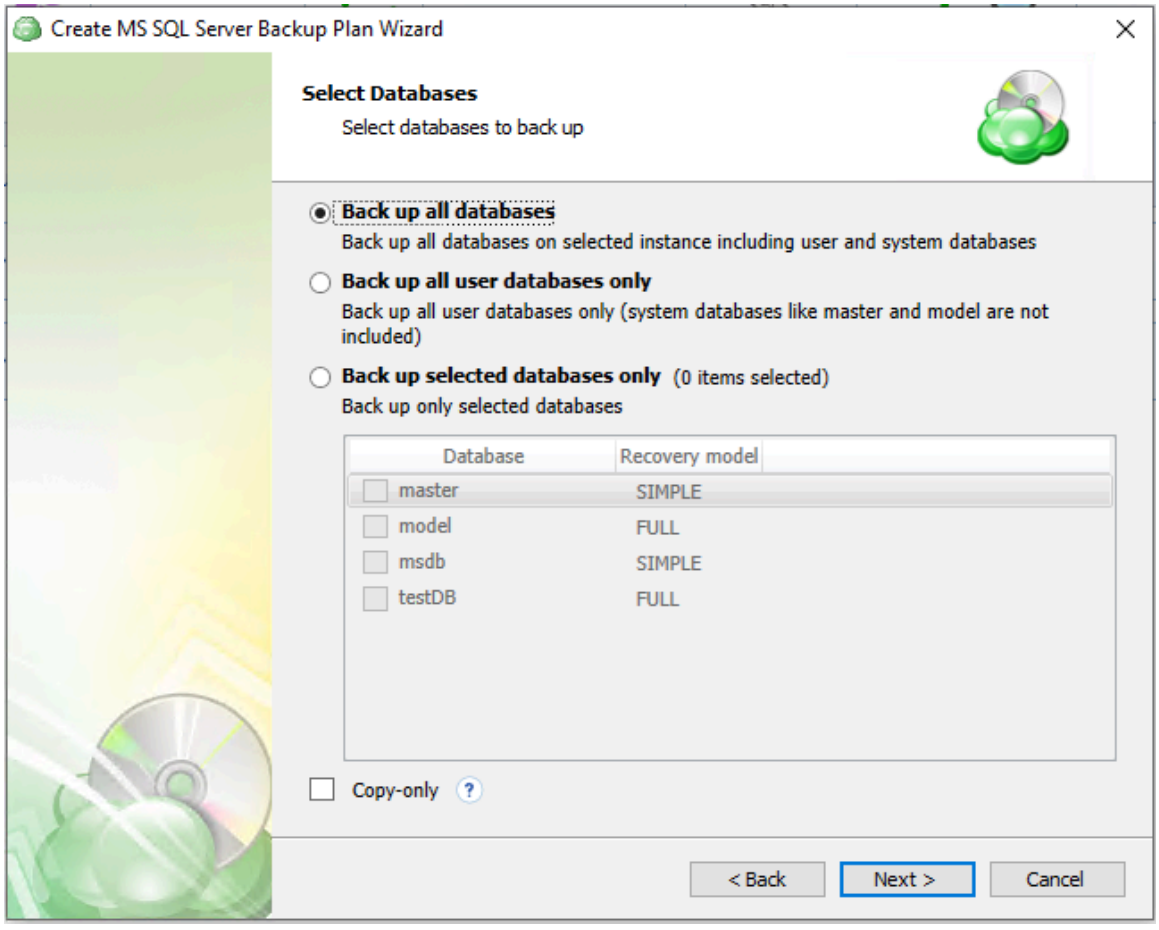
- **SQL Server Instance:** Select the instance containing the database to be backed up from the list. Note that only local instances can be selected.
- **Authentication Type:** Choose between Windows or SQL Authentication. If “Windows Authentication” is selected, the application will run the backup as the local service account.
- **User Name:** If “SQL Server Authentication” was selected, enter the user name in this field.
- **Password:** If “SQL Server Authentication” was selected, enter the password for the specified SQL user here.
- **Check if the specified account has necessary permissions to perform backup:** The application will check for the appropriate permissions prior to attempting to backup the database. It is recommended to use this option to prevent unexpected backup failures.

- **Use secure connection (SSL/TLS):** Enabling this will allow the application to connect to the SQL instance using encryption, if configured on the database host.

> To utilize the Windows Authentication option, the Online Backup service account (typically NT AUTHORITY/SYSTEM by default) must be assigned the “sysadmin” role within the MS SQL instance.

> Only local databases and instances can be backed up.

Step 6. Select the databases within the instance which you would like to back up.

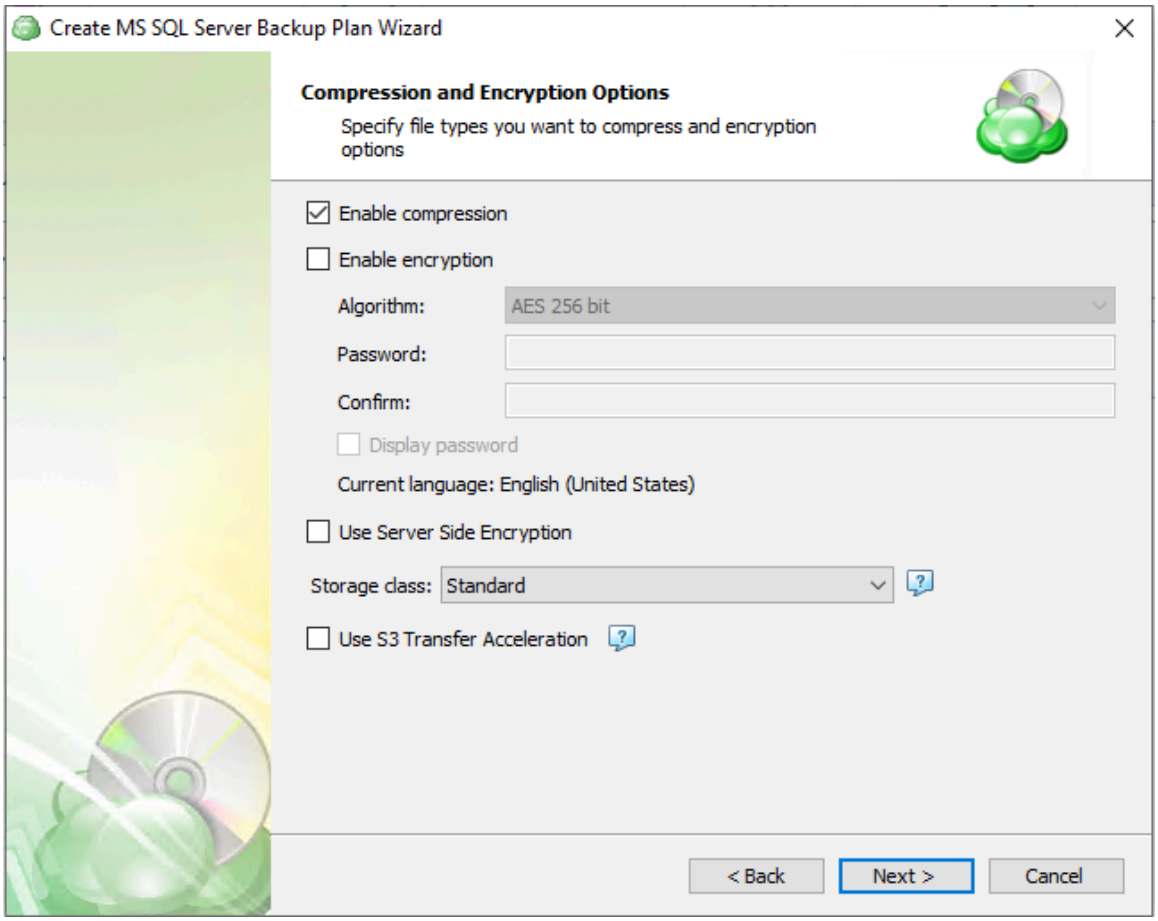


- **Back up all databases:** backs up all databases on the selected instance. Includes all user and system databases.

- **Back up all user databases only:** Will only backup the user databases while excluding the system databases.
- **Back up selected databases only:** Allows you to choose which database(s) from the list below you wish to include in this backup plan.
- **Copy-only:** Creates a backup which is independent of the sequence of conventional SQL backups.

> “Copy-only” backups cannot serve as a differential backup base or differential backup.

Step 7. After selecting the database(s) to be backed up, you are now able to choose whether to compress or encrypt them. Additional options may be displayed depending on the capabilities of the selected backup destination.



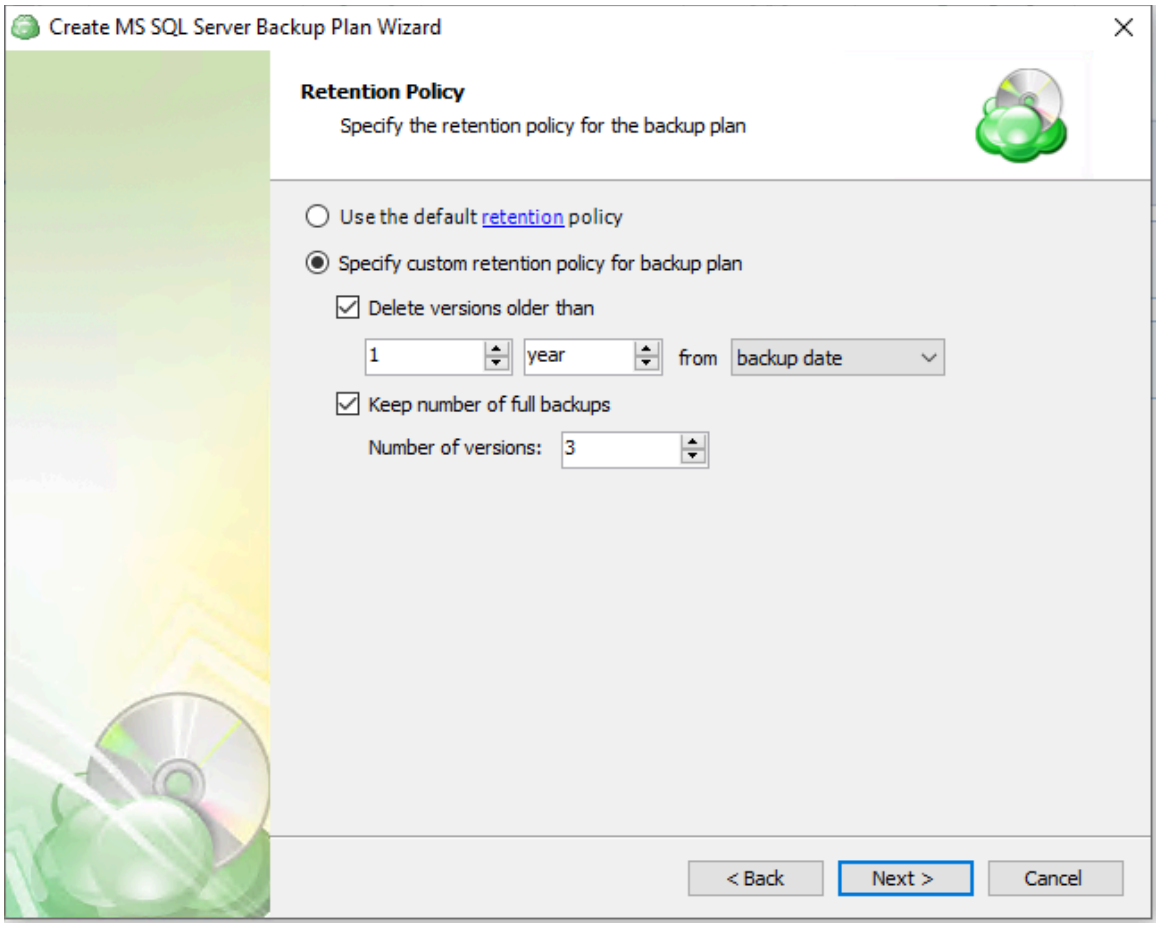
Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place.

“Server Side Encryption” is only available on certain cloud providers and is separate from the MSP360 encryption. The native encryption applies only to the data the application backs up, while the server side encryption refers to encrypting the bucket on the cloud service itself.

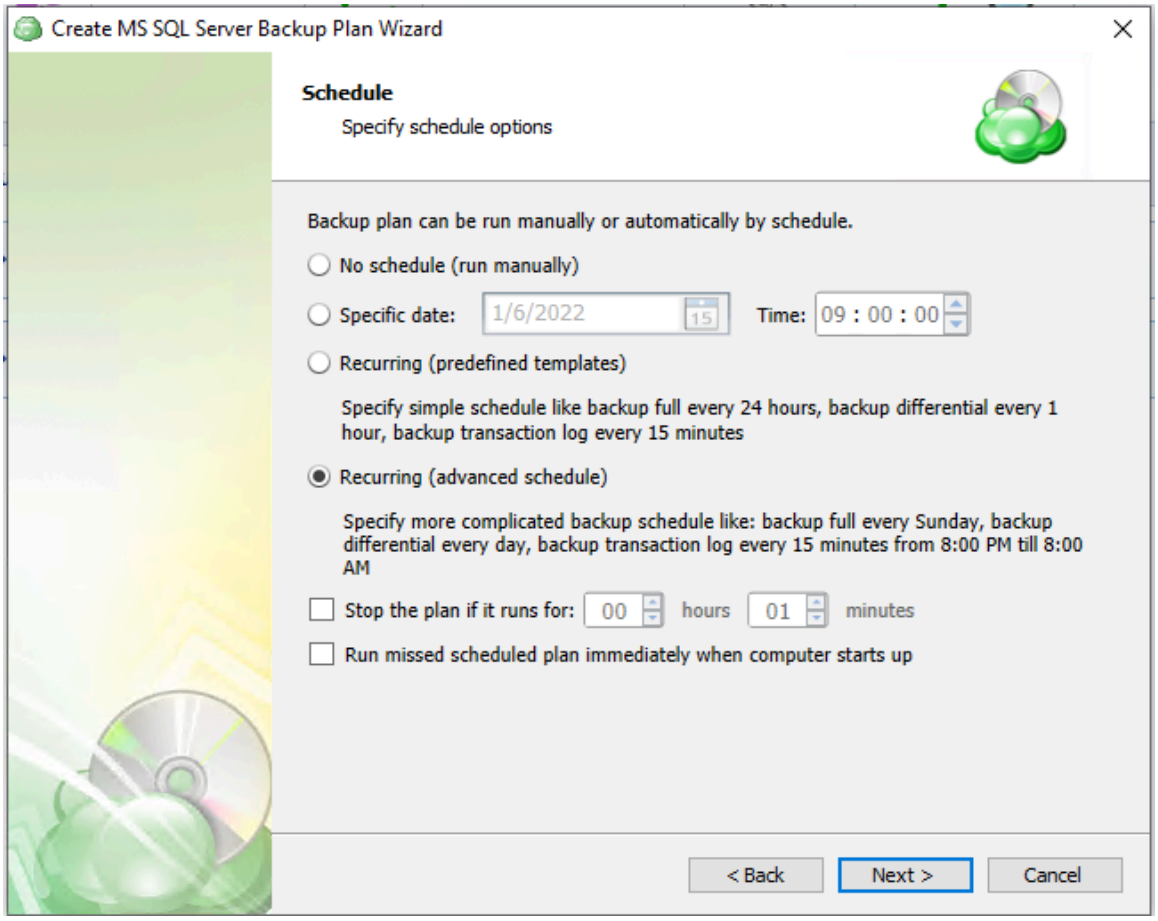
Step 8. The next step is to set up the retention policy for the backup plan.



- **Use the Default Retention Policy**. Select this option to apply the default retention policy settings. You can see them below, but cannot edit if this option is selected
- **Specify Custom Retention Policy for Backup Plan**. Select this option if you want to customize the retention policy settings for this backup plan
- **Keep number of full backups**. Select this check box to specify the number of full backups to be kept in backup storage, then specify the number of versions
- **Delete versions older than**. Select this option to enable retention by age instead of number of restore points. Backups which are older than the specified age will automatically be deleted.

> When both the “Delete versions older than”” and “Keep number of versions” options are enabled, a file will be purged when any one of these conditions becomes true.

Step 9. Next you are prompted to set the schedule for your backup plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.

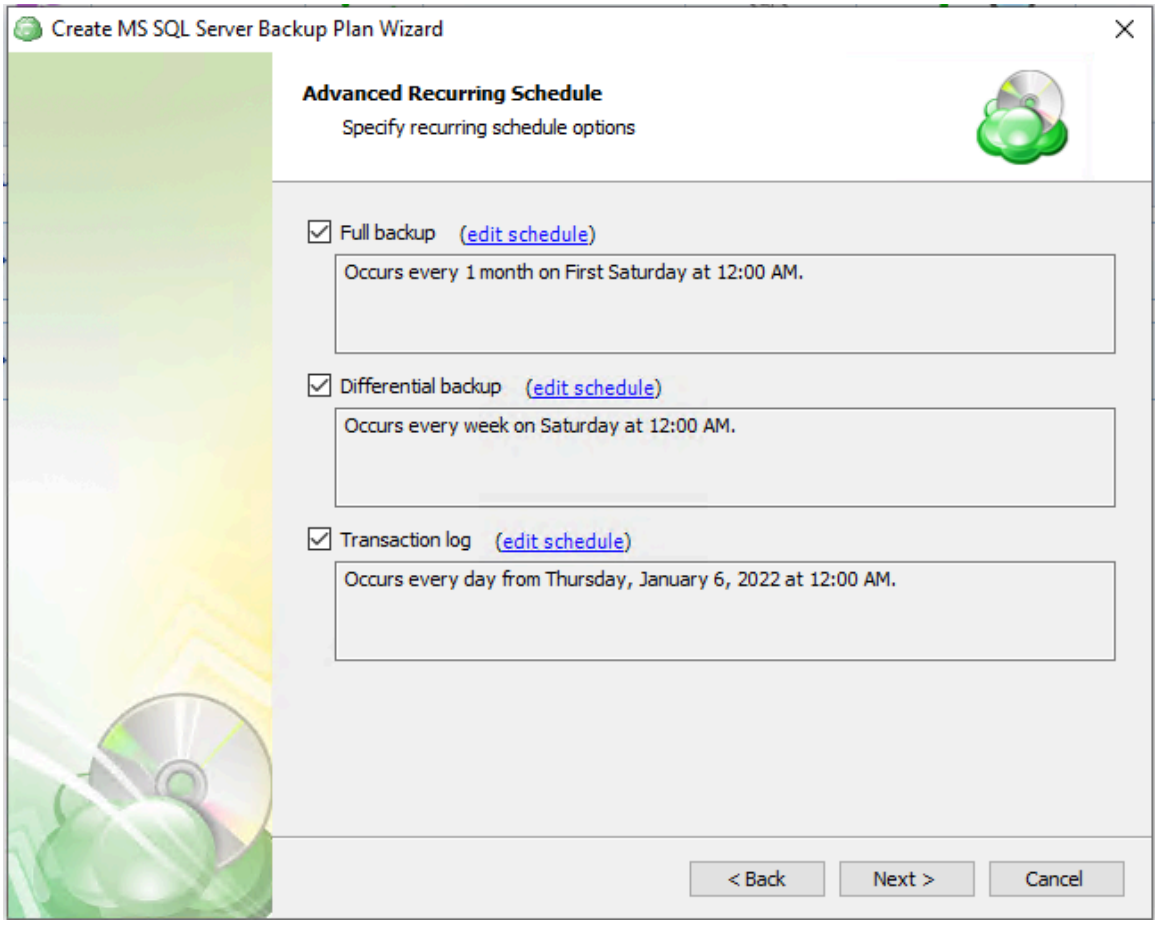


“Recurring (advanced schedule)” is the recommended selection for most backup plans

Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection.

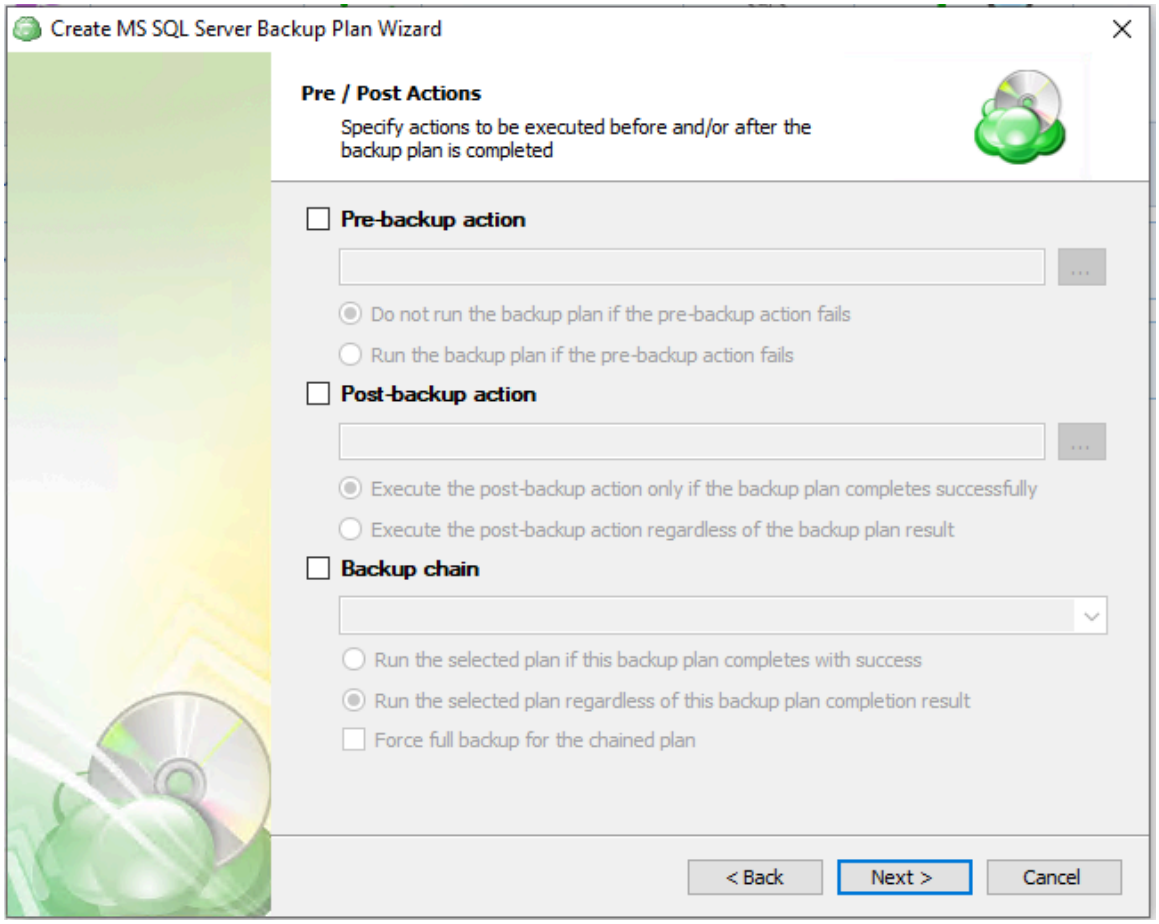
Step 10. Selecting the “Recurring (advanced schedule)” option on the previous step leads to detailed control over when different backup types run. Once checked, simply click on the “Edit Schedule” link to view the available options.



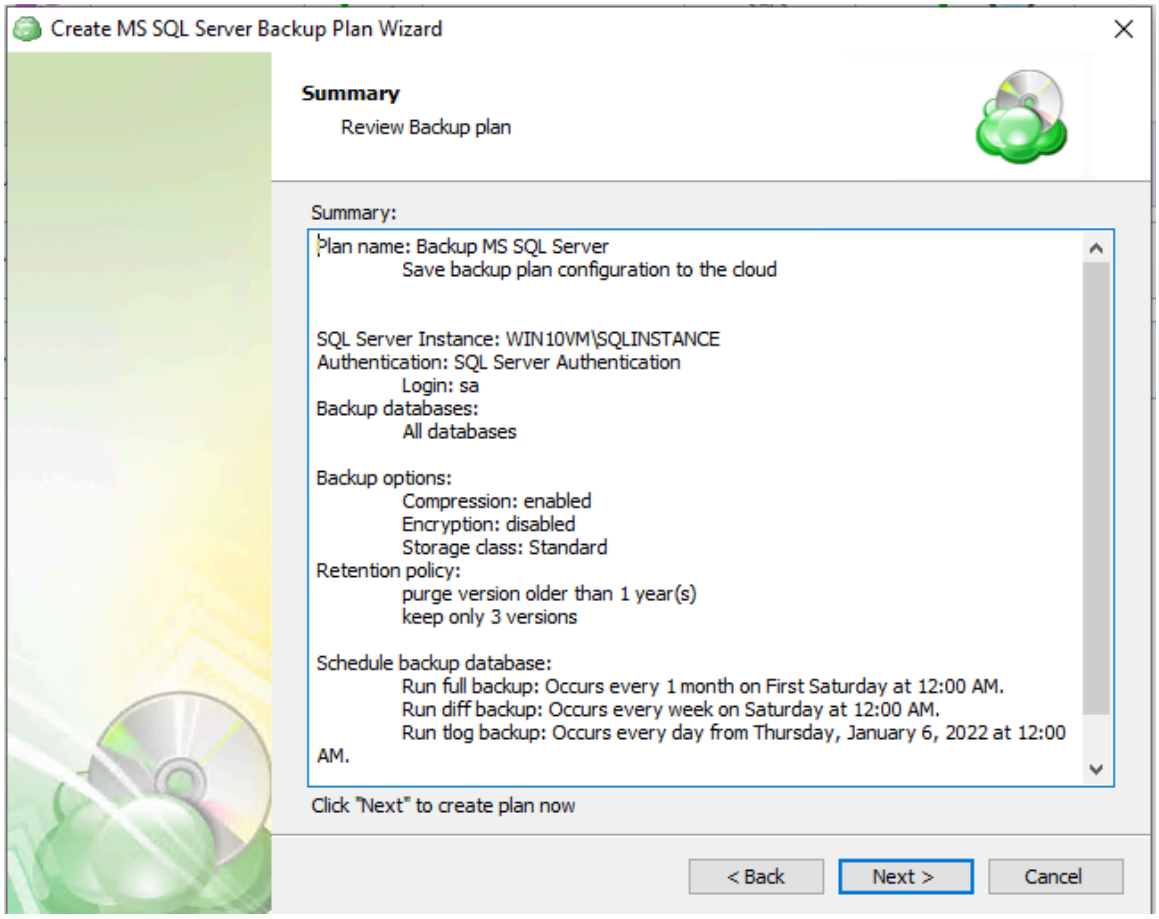
Schedule a **Full Backup** at regular periods, once a week will be suitable in most circumstances.

The retention policy will only perform properly with regular scheduled full backups.

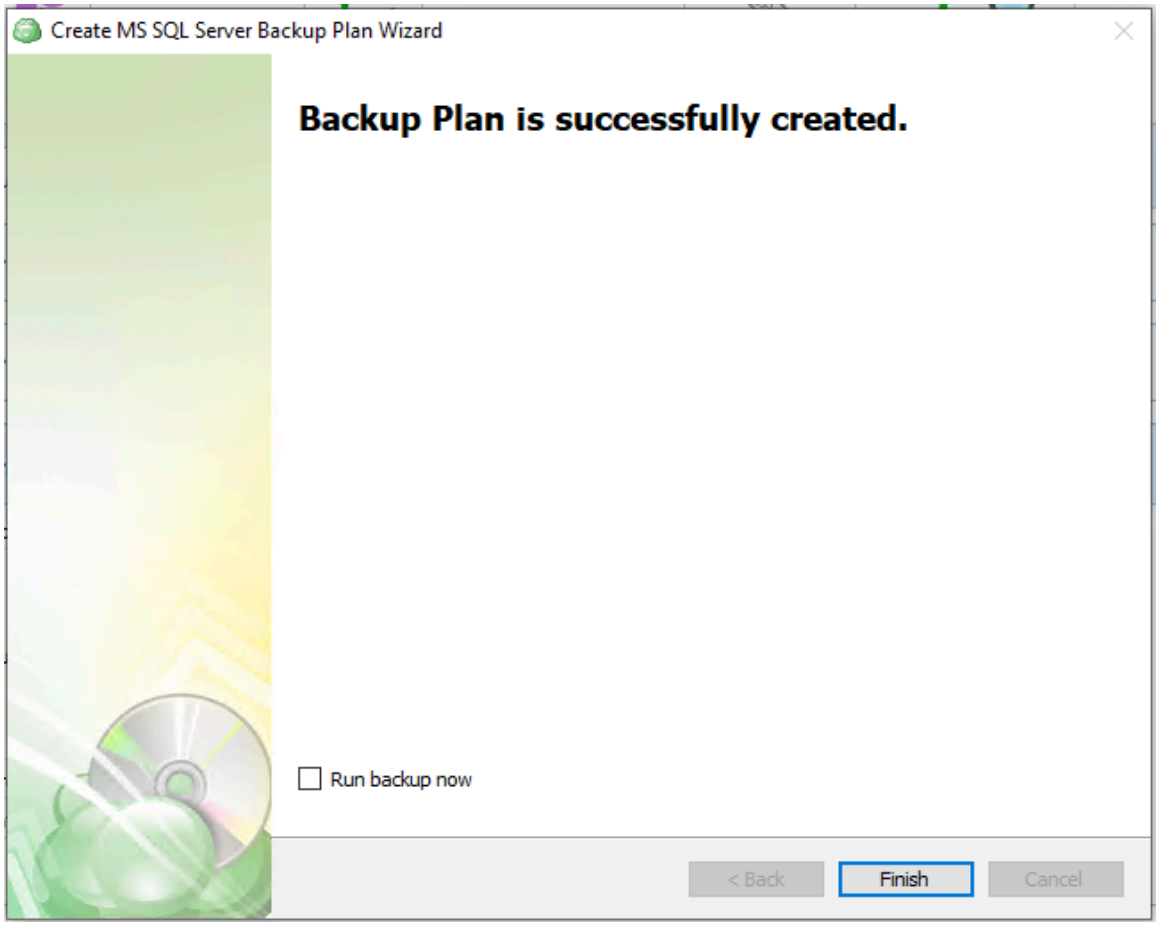
Step 11. The **Pre/Post Actions** page allows the execution of custom scripts before and/or after the running of a backup task, and can chain multiple backup tasks together for sequential execution.



Step 12. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.

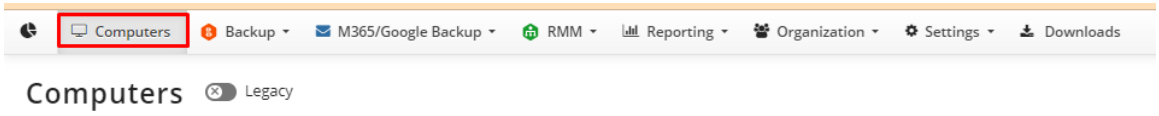


Step 13. After clicking next on the previous step, the Backup Plan is created. The final step is to acknowledge this and determine whether to run the backup immediately or for it to wait until the next scheduled occurrence.

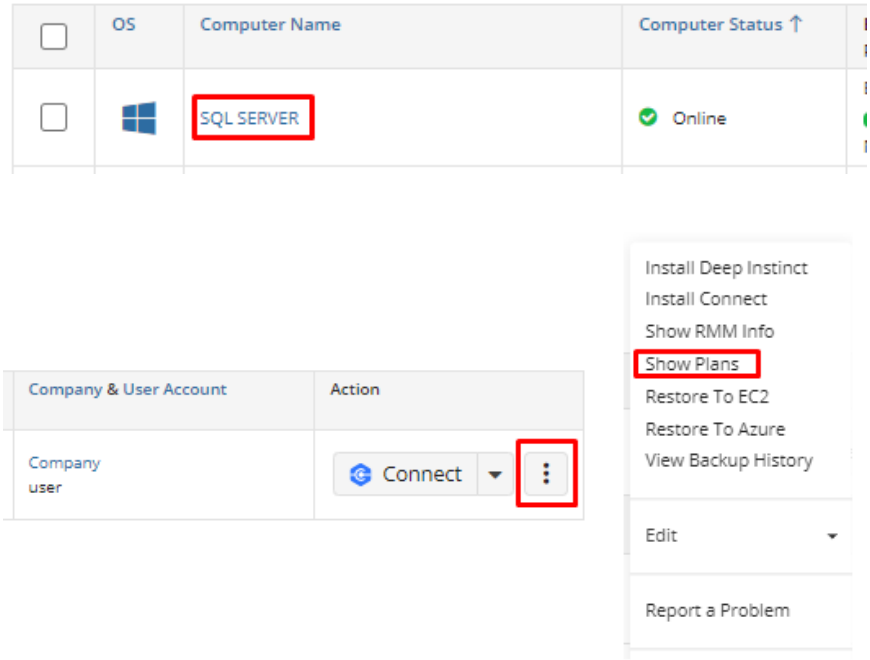


Backup Databases using MBS

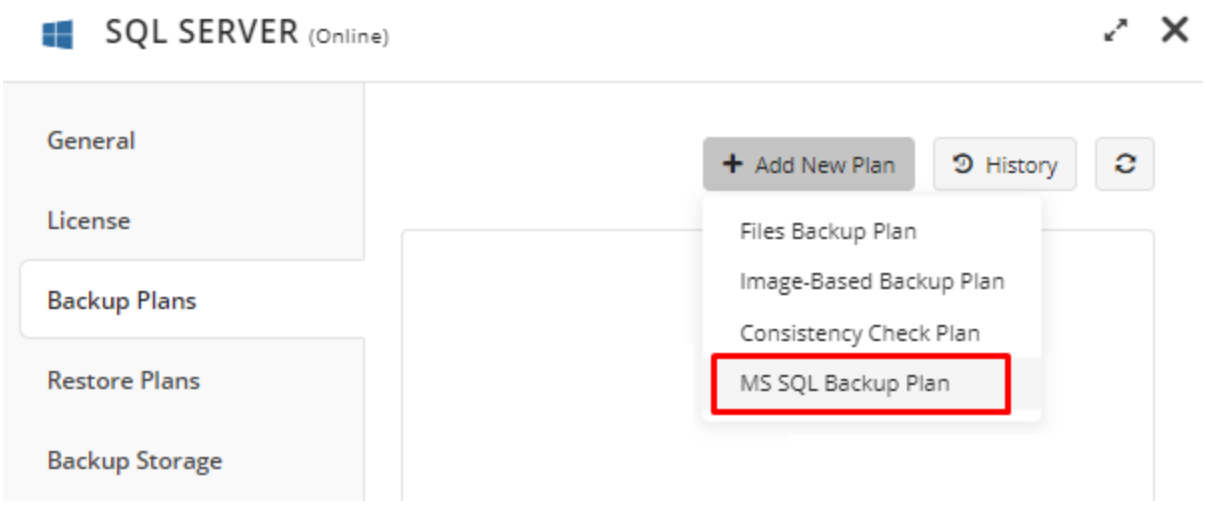
Step 1. From the MBS Portal, left-click Computers on the menu.



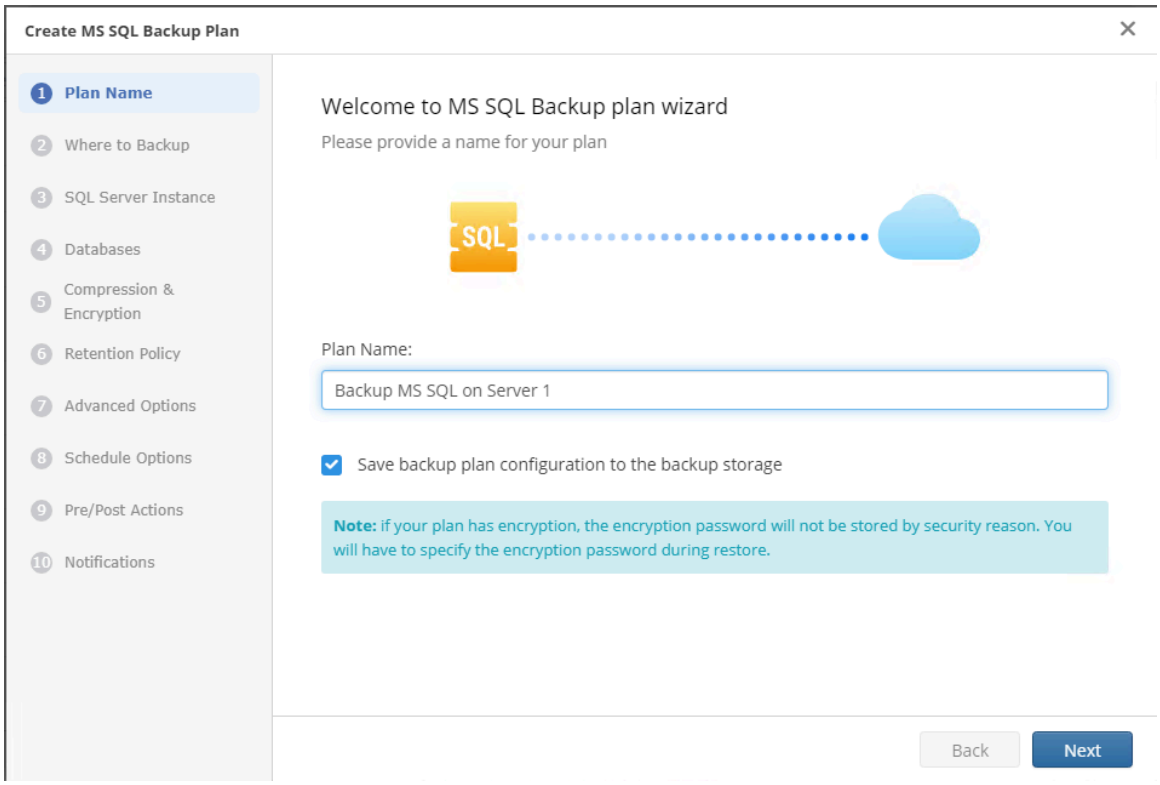
Step 2. Find the computer hosting the MS SQL instance you want to back up on the list and access the current list of plans either by clicking on the computer name or selecting "Show Plans" from the three-dot drop-down menu.



Step 3. In the appeared side panel, make sure you are within the “Backup Plans” section. Click on the “Add New Plan” button and select “MS SQL Backup Plan” from the drop-down menu.



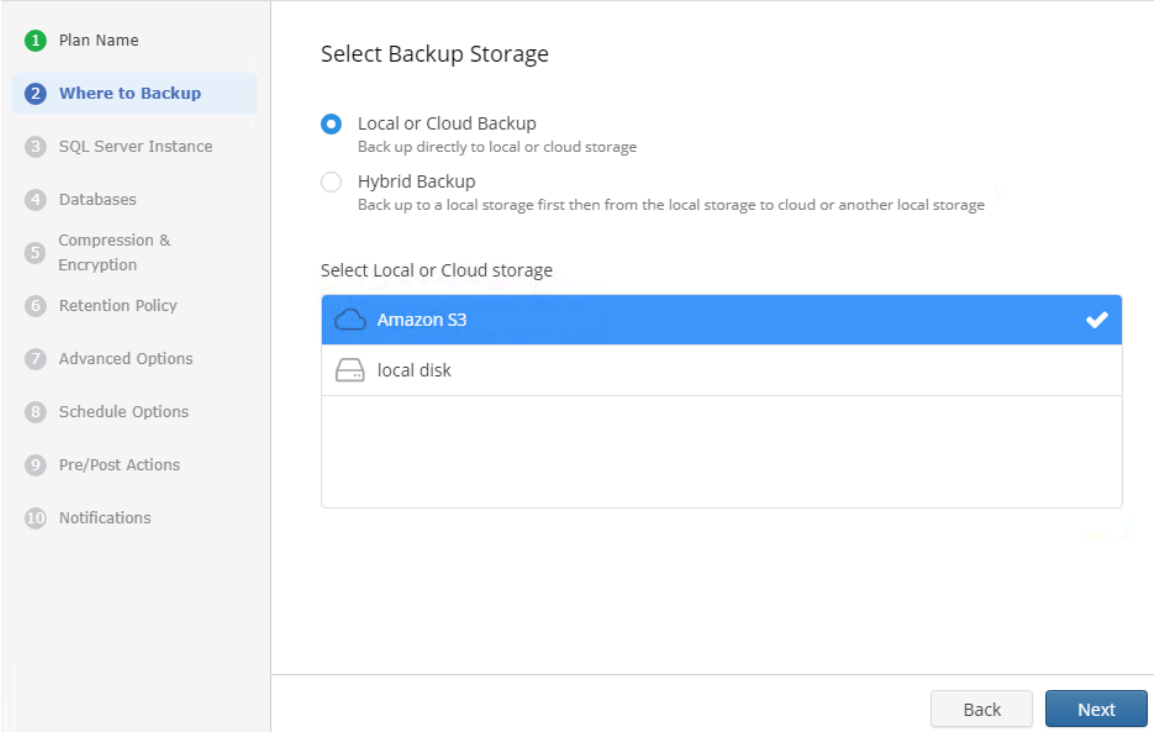
Step 4. The first step when creating a new MS SQL backup plan is to give the plan a name.



It is recommended to use a descriptive name which will distinguish the backup from others.

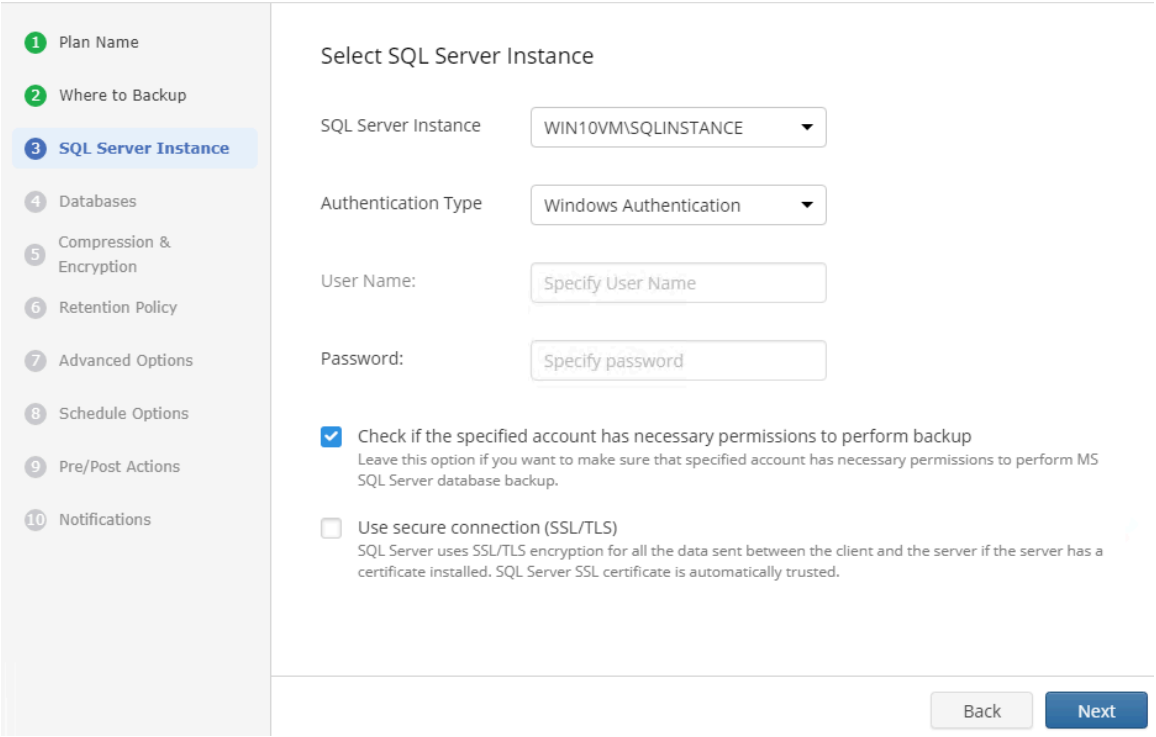
“Save backup plan configuration to the backup storage” option allows you easily restore the backup plan to another destination if necessary.

Step 5. After naming the backup plan, the next step is to select where you would like the backup to be stored.



If you choose to create a “Hybrid Backup” the wizard will prompt you to select a second location.

Step 6. Next you will be prompted to select the SQL Server Instance as well as specify the credentials to be used by the backup service.



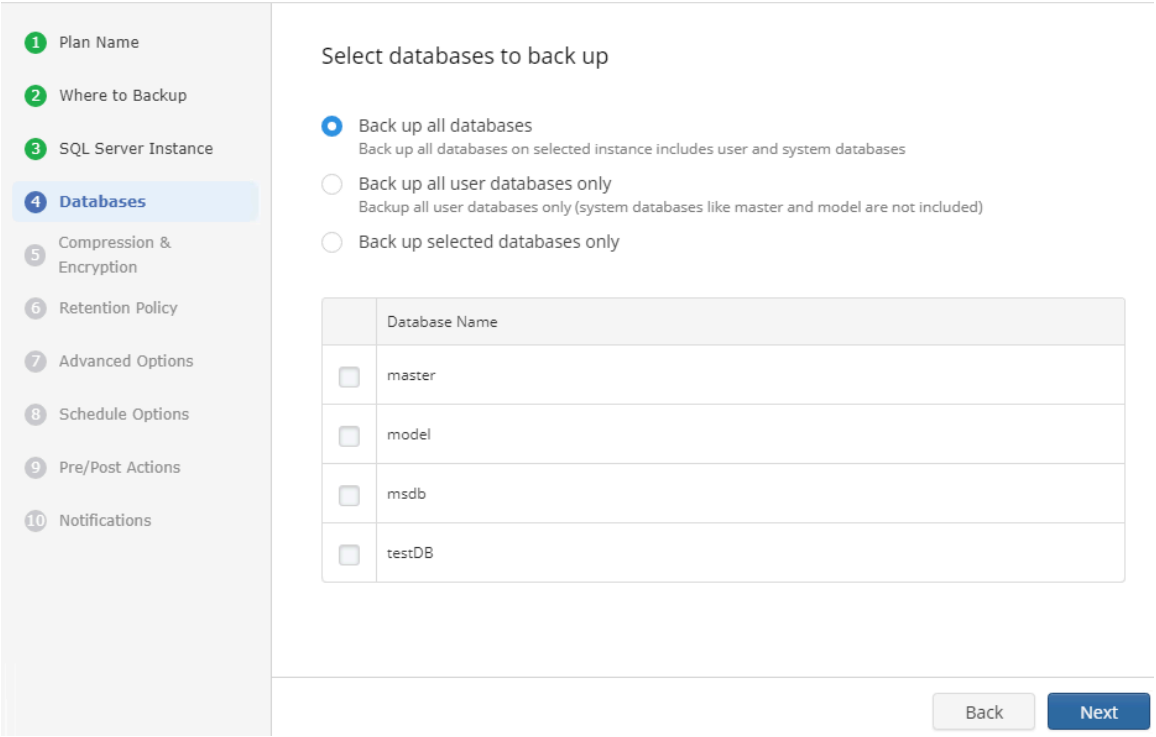
- **SQL Server Instance:** Select the instance containing the database to be backed up from the list. Note that only local instances can be selected.
- **Authentication Type:** Choose between Windows or SQL Authentication. If “Windows Authentication” is selected, the application will run the backup as the local service account.
- **User Name:** If “SQL Server Authentication” was selected, enter the user name in this field.
- **Password:** If “SQL Server Authentication” was selected, enter the password for the specified SQL user here.
- **Check if the specified account has necessary permissions to perform backup:** The application will check for the appropriate permissions prior to attempting to backup the database. It is recommended to use this option to prevent unexpected backup failures.
- **Use secure connection (SSL/TLS):** Enabling this will allow the application to connect to the SQL instance using encryption, if configured on the database host.

> To utilize the Windows Authentication option, the Online Backup service account (typically NT AUTHORITY/SYSTEM by default) must be assigned the

"sysadmin" role within the MS SQL instance.

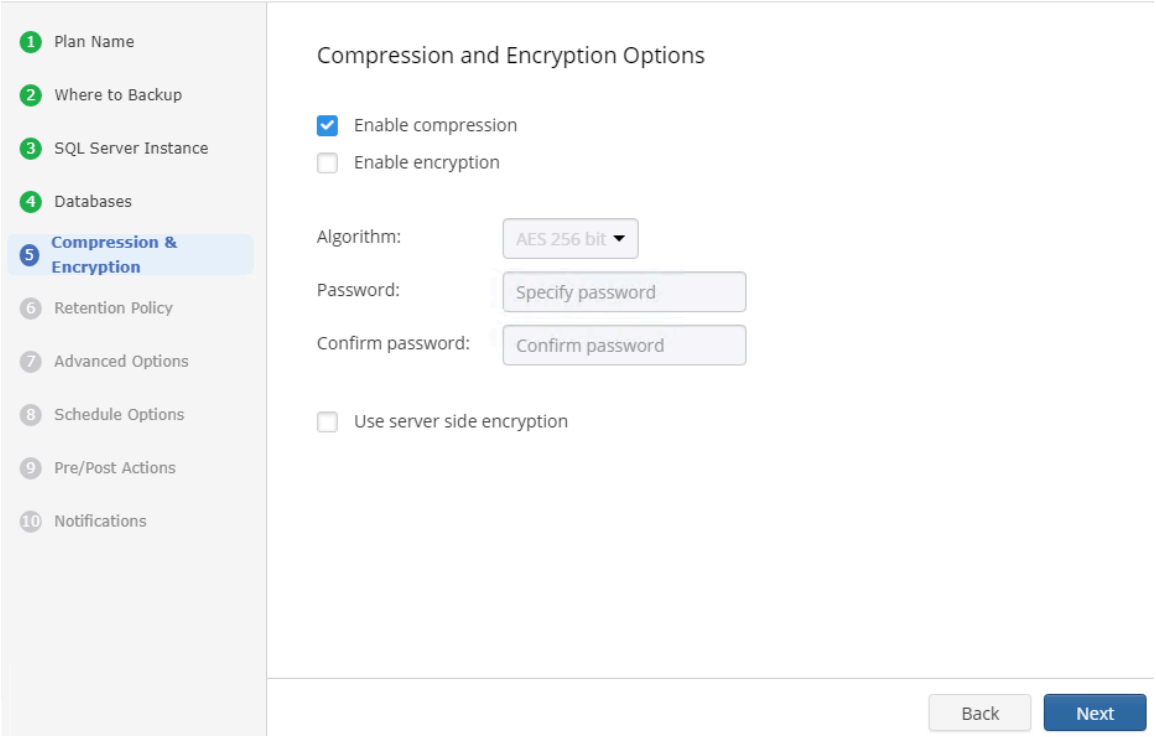
Only local databases and instances can be backed up.

Step 7. Select the databases within the instance which you would like to back up.



- **Back up all databases:** backs up all databases on the selected instance. Includes all user and system databases.
- **Back up all user databases only:** Will only backup the user databases while excluding the system databases.
- **Back up selected databases only:** Allows you to choose which database(s) from the list below you wish to include in this backup plan.

Step 8. After selecting the database(s) to be backed up, you are now able to choose whether to compress or encrypt them.



Enabling compression will reduce the size of the backup, reduce the time to upload it, both of which may decrease the cost of the backup.

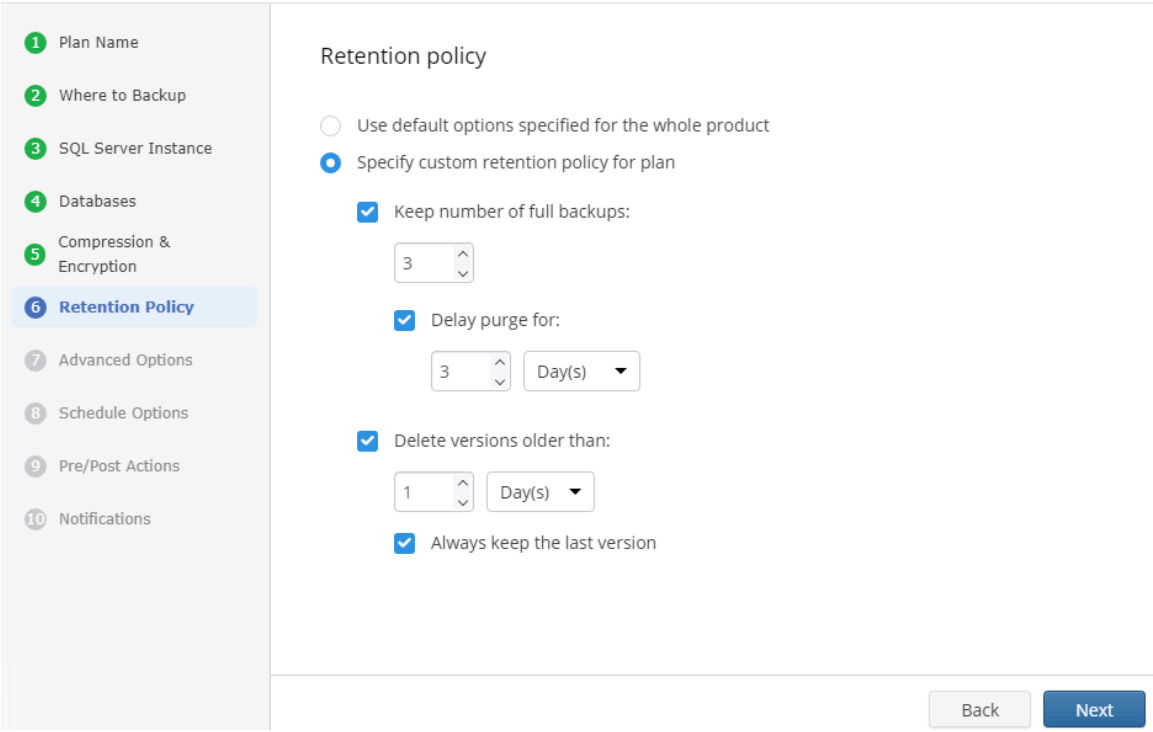
Encrypting the backup adds an additional layer of security to the data at the expense of increased processing resources during the backup process. Several types of encryption are available, with the most secure selected by default.

It is important to remember that MSP360 Support is not able to retrieve or reset the encryption password. It is recommended that you store the password in a secure place.

"Server Side Encryption" is only available on certain cloud providers and is separate from the MSP360 encryption. The native encryption applies only to the

data the application backs up, while the server side encryption refers to encrypting the bucket on the cloud service itself.

Step 9. On the **Retention Policy** page, you can choose if the backup plan should use the global retention policy settings defined at the application level, or use a customized retention policy.

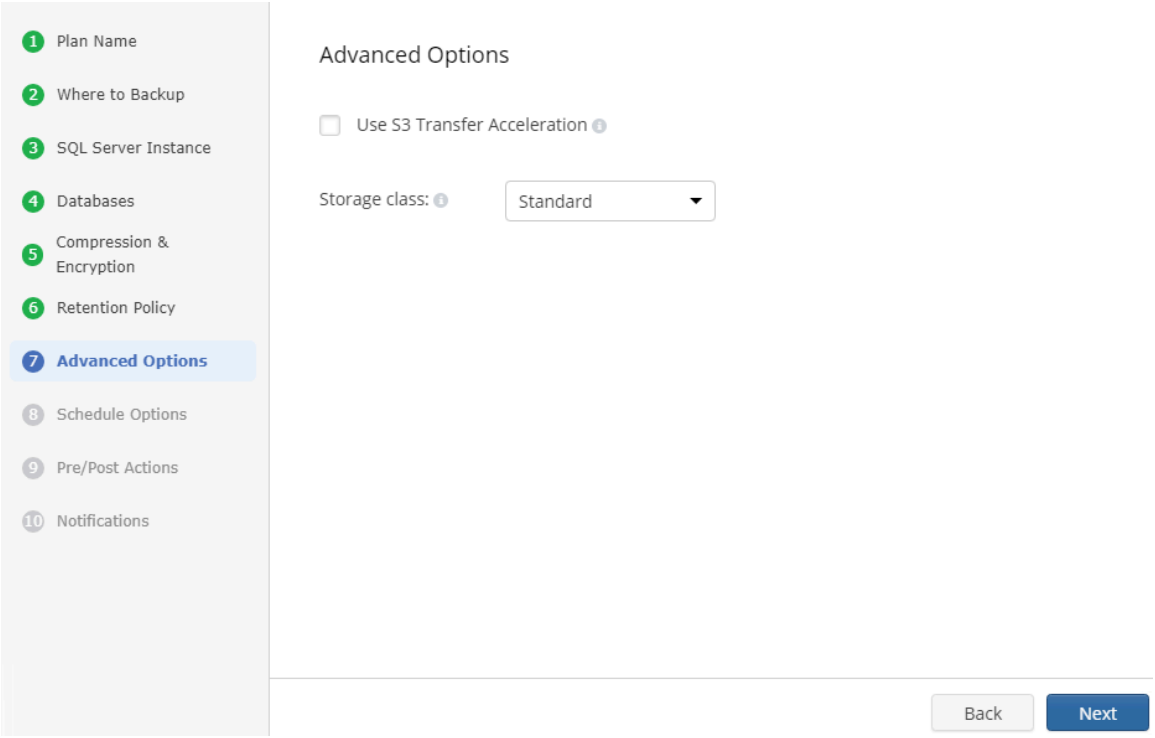


- **Use the Default Retention Policy**. Select this option to apply the default retention policy settings. You can see them below, but cannot edit if this option is selected
- **Specify Custom Retention Policy for Backup Plan**. Select this option if you want to customize the retention policy settings for this backup plan
- **Keep number of full backups**. Select this check box to specify the number of full backups to be kept in backup storage, then specify the number of versions
- **Delay purge for**. Specify the number of days after a full backup is out of retention before it is deleted. If no delay is set, the backup will be deleted immediately after aging out of the retention policy.
- **Delete versions older than**. Select this option to enable retention by age instead of number of restore points. Backups which are older than the specified age will automatically be deleted.

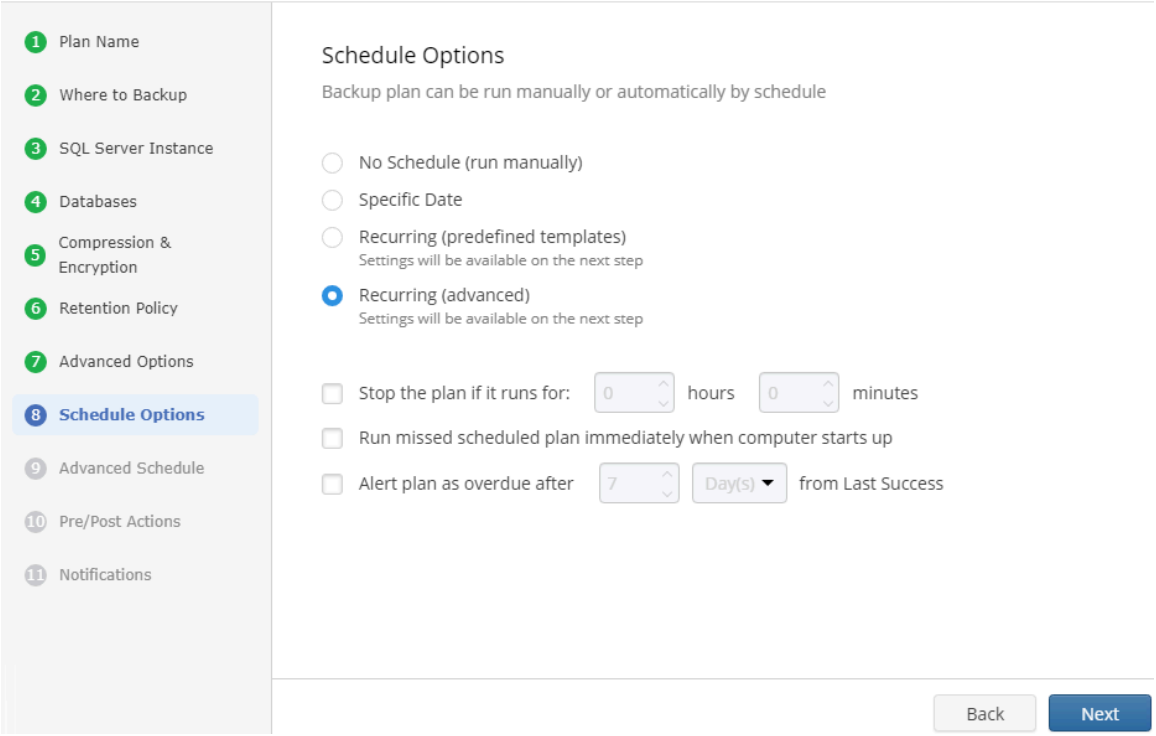
- **Always keep the last version**. Select this option to force the system to always keep the newest backup regardless of age.

> When both the “Delete versions older than”” and “Keep number of versions” options are enabled, a file will be purged when any one of these conditions becomes true.

Step 10. The next step displays any advanced options available for the plan storage. Options presented here will depend on the storage destination selected.



Step 11. Next you are prompted to set the schedule for your backup plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.

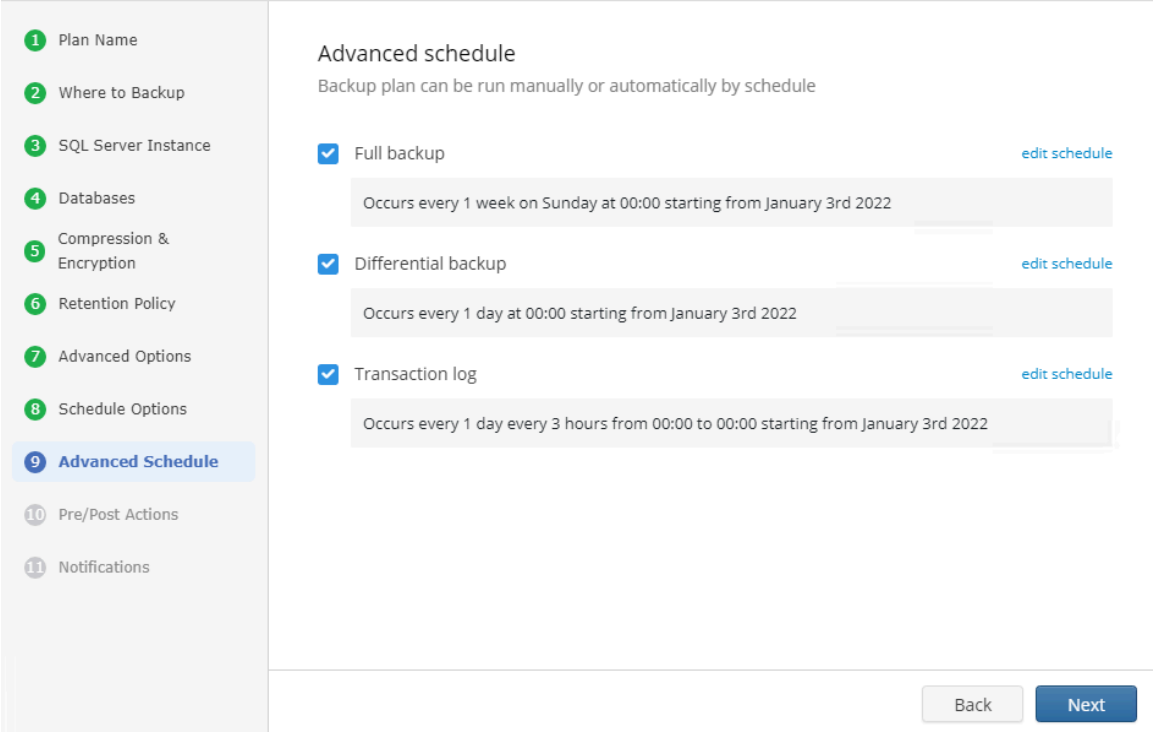


“Recurring (advanced schedule)” is the recommended selection for most backup plans

Enabling the “**Run missed scheduled backup immediately when computer starts up”** option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

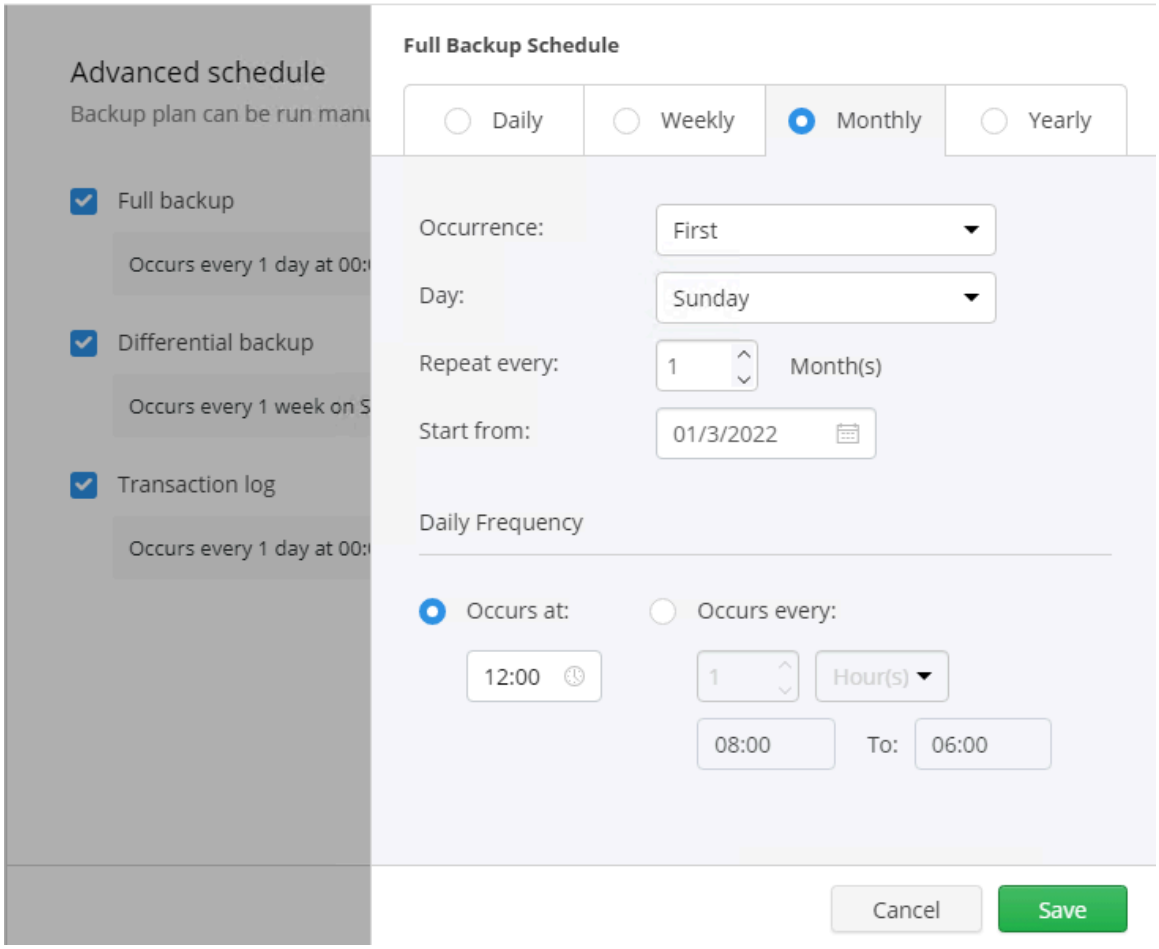
Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection. The first full backup can take a long time to upload, and it can be unexpectedly interrupted if this option is enabled.

Step 12. Selecting the “Recurring (advanced schedule)” option on the previous step leads to detailed control over when different backup types run, and when to run them.



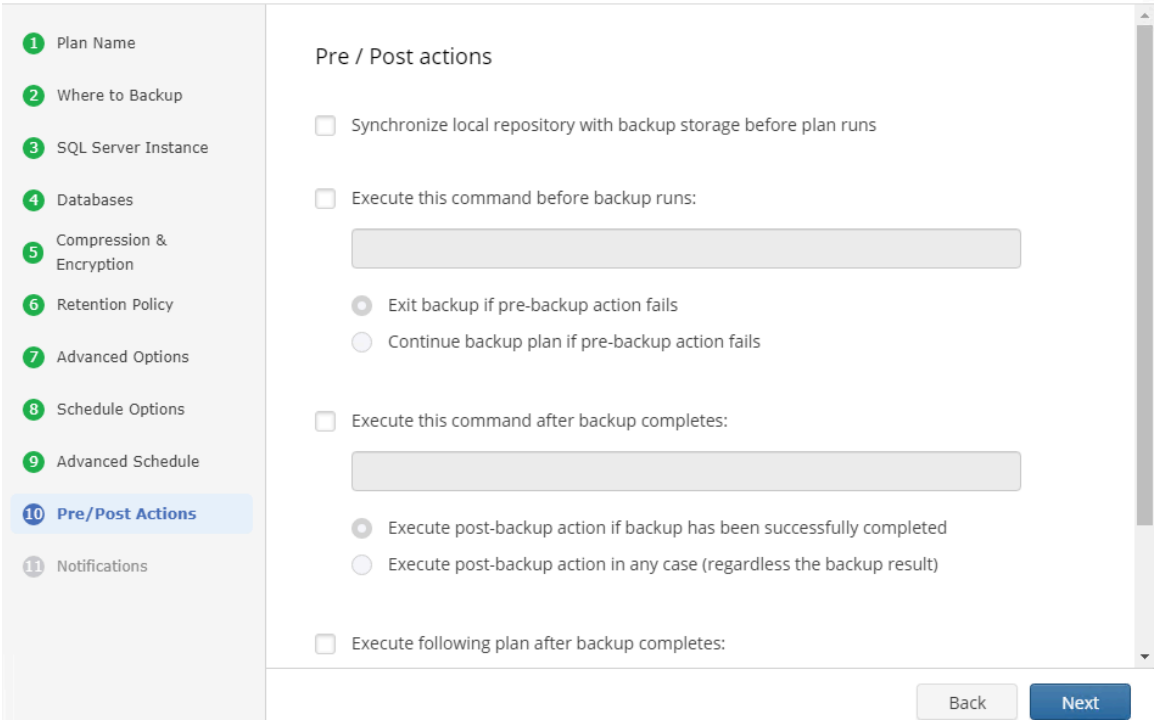
- **Full backup:** Clicking on this will open up the scheduling options for running a full backup. Full backups are required for the retention policy, Differential Backup, and restore operations to work.
- **Differential backup:** Clicking on this will open up the scheduling options for running a Differential Backup. A Differential Backup is similar to an incremental backup in that it only backs up new or changed data.
- **Transaction log:** Enable this to schedule transaction log backups of the selected databases.

Enable the type of backups you would like to run by clicking on the toggle. Each type will have similar scheduling options available.

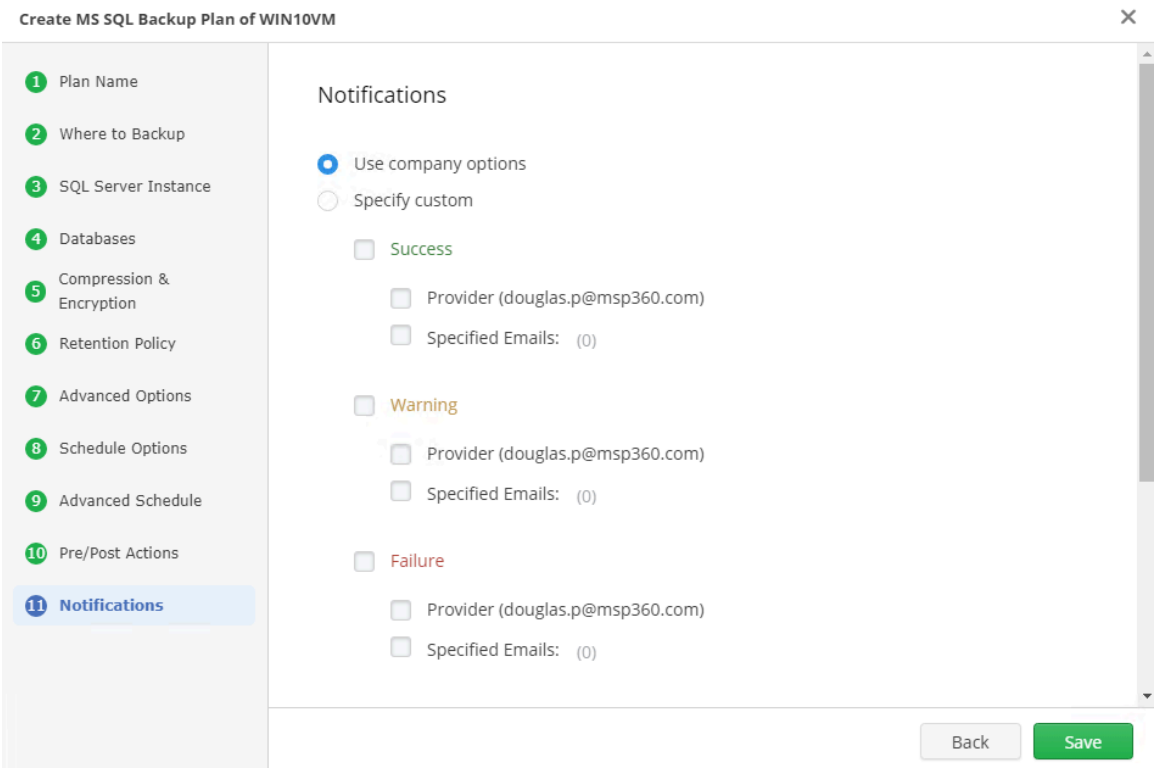


The retention policy will only perform properly with regular scheduled full backups.

Step 13. After the schedule is set, the next section is used to set the “Pre” and “Post” Actions



Step 14. The final step is to review the Notifications and Logging. The default settings applied at the Company level are selected by default, however you are also able to specify custom options per plan.

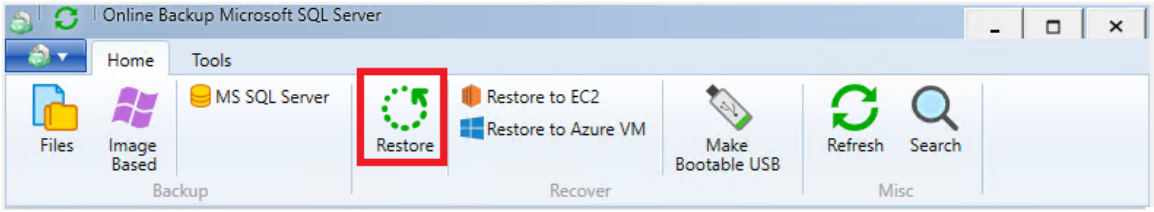


Once you are satisfied with the selected notifications and logging, clicking “Save” will create the new plan and close the wizard.

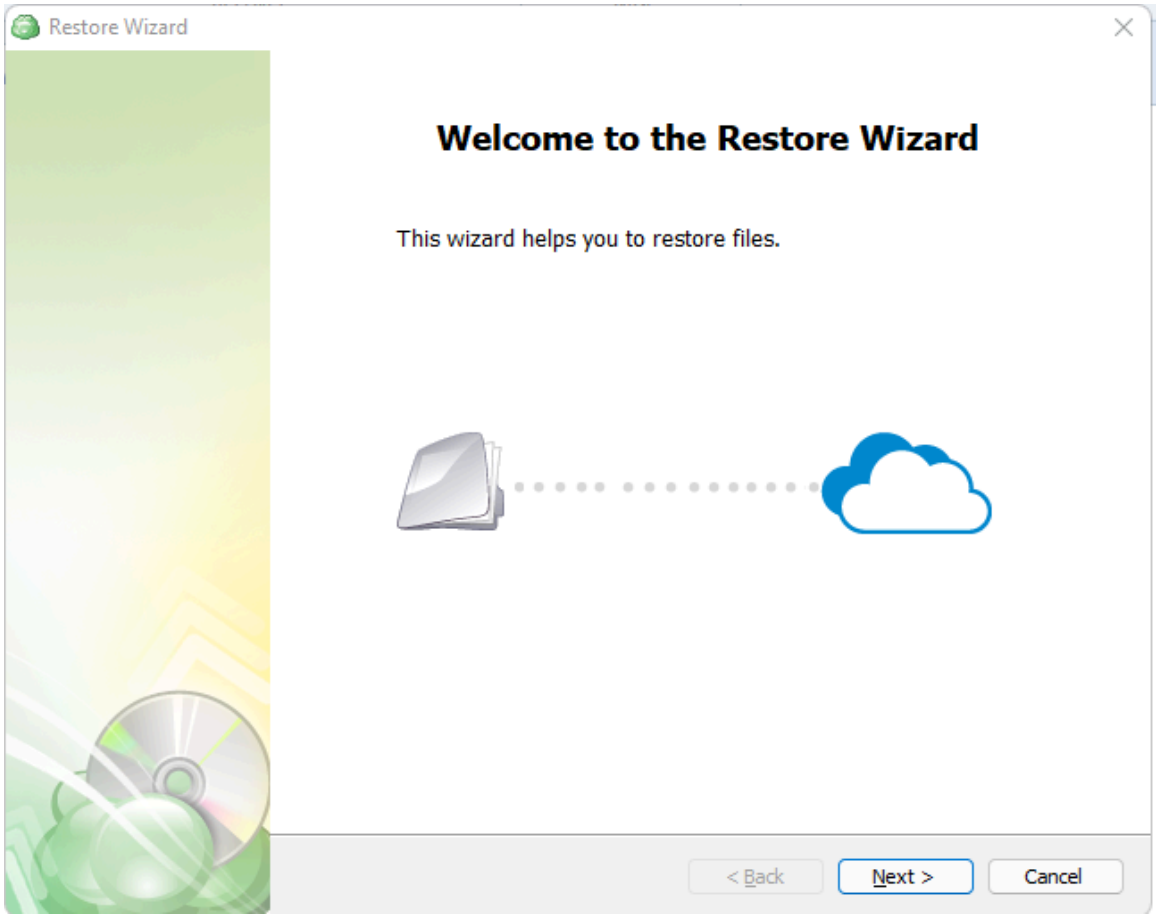
MS SQL Restore Plans

Restore Databases using the Agent

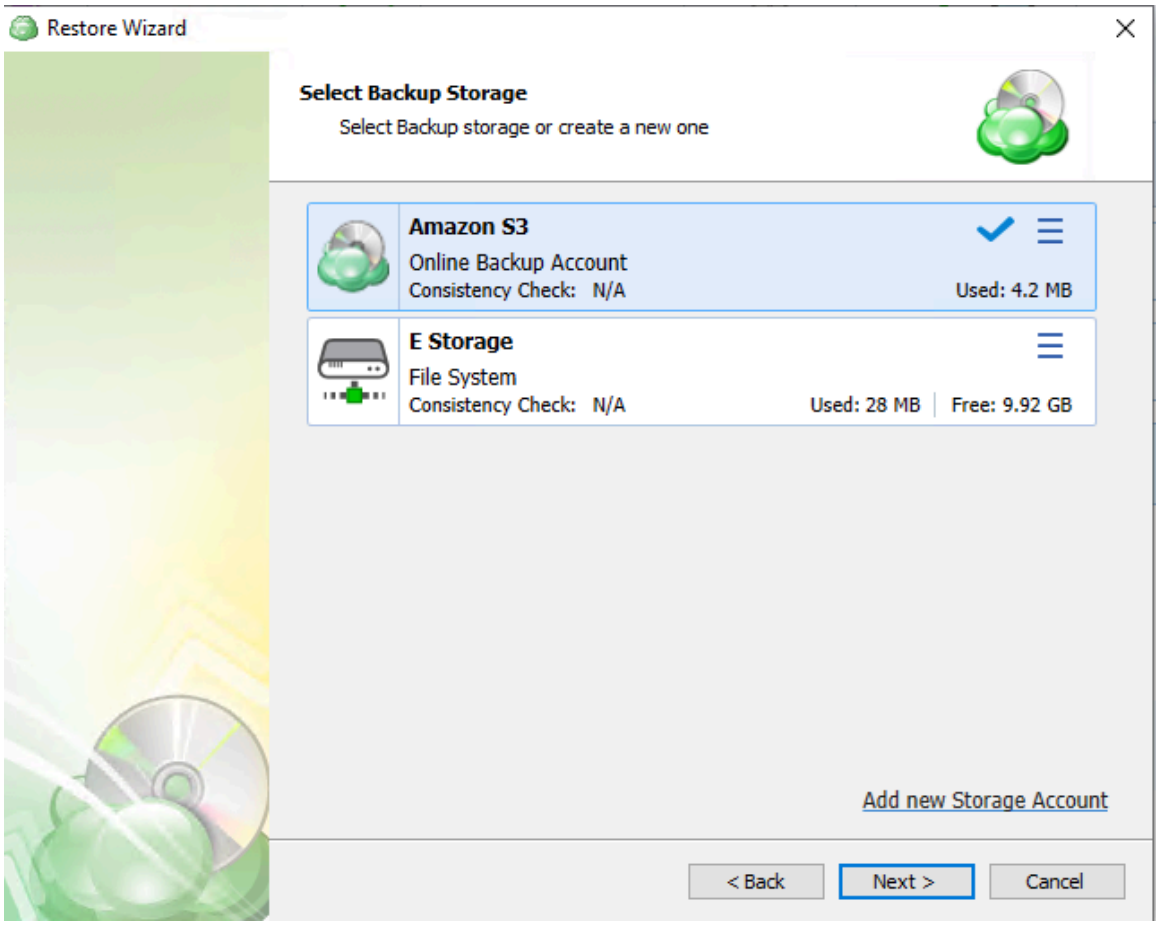
Step 1. Within the Online Backup Agent, click on “Restore”



Step 2. Once the wizard starts, click on Next to advance to the next step.

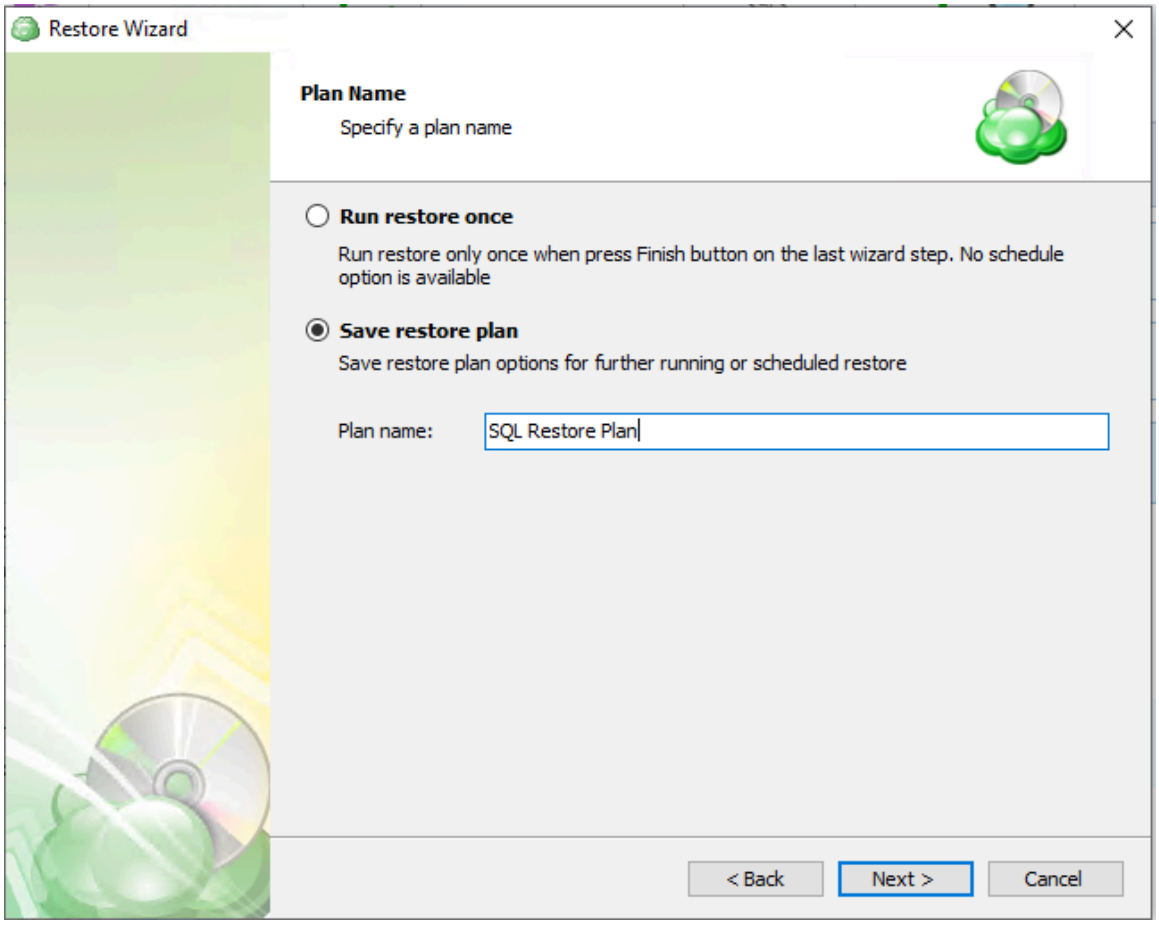


Step 3. The next step will prompt you to select the source for the restore.



If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

Step 4. Next, you will be given the option to either run the restore once or to save it to run later.

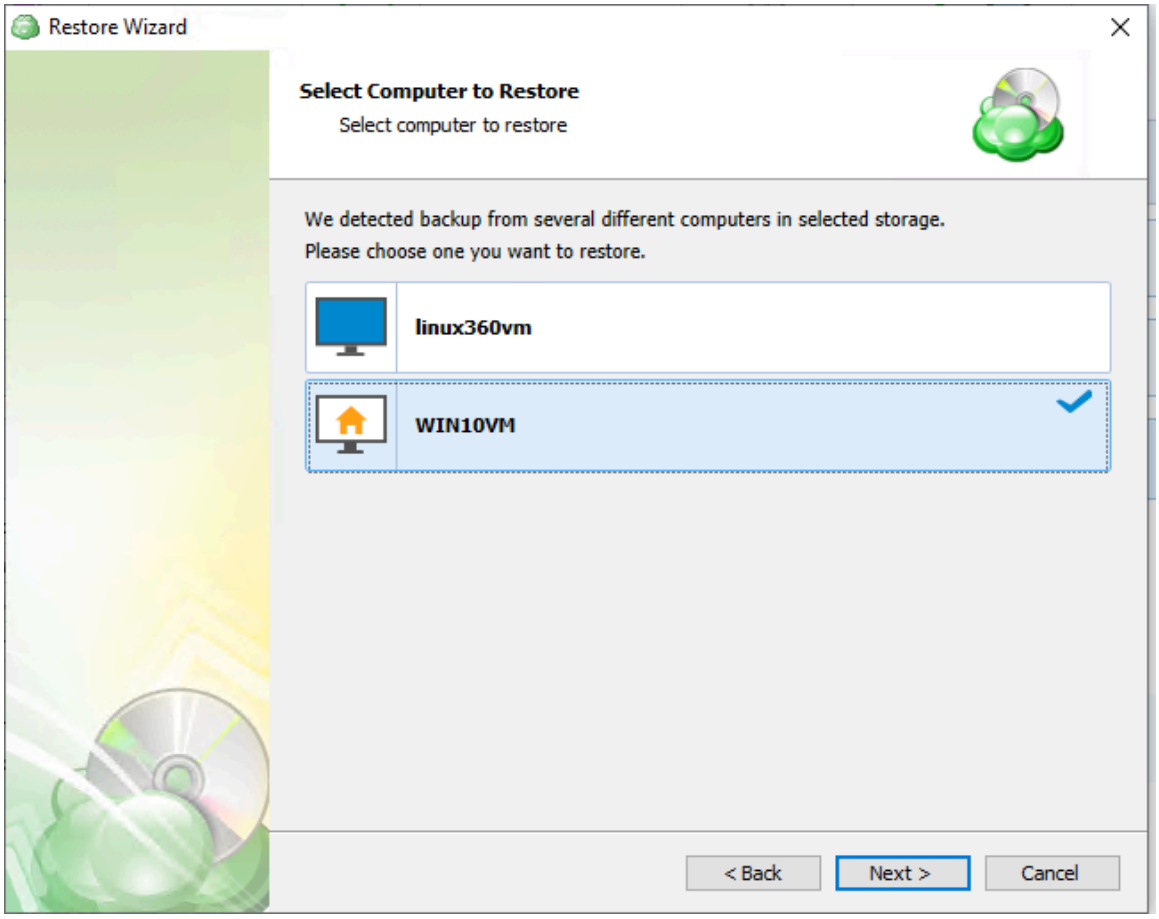


"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

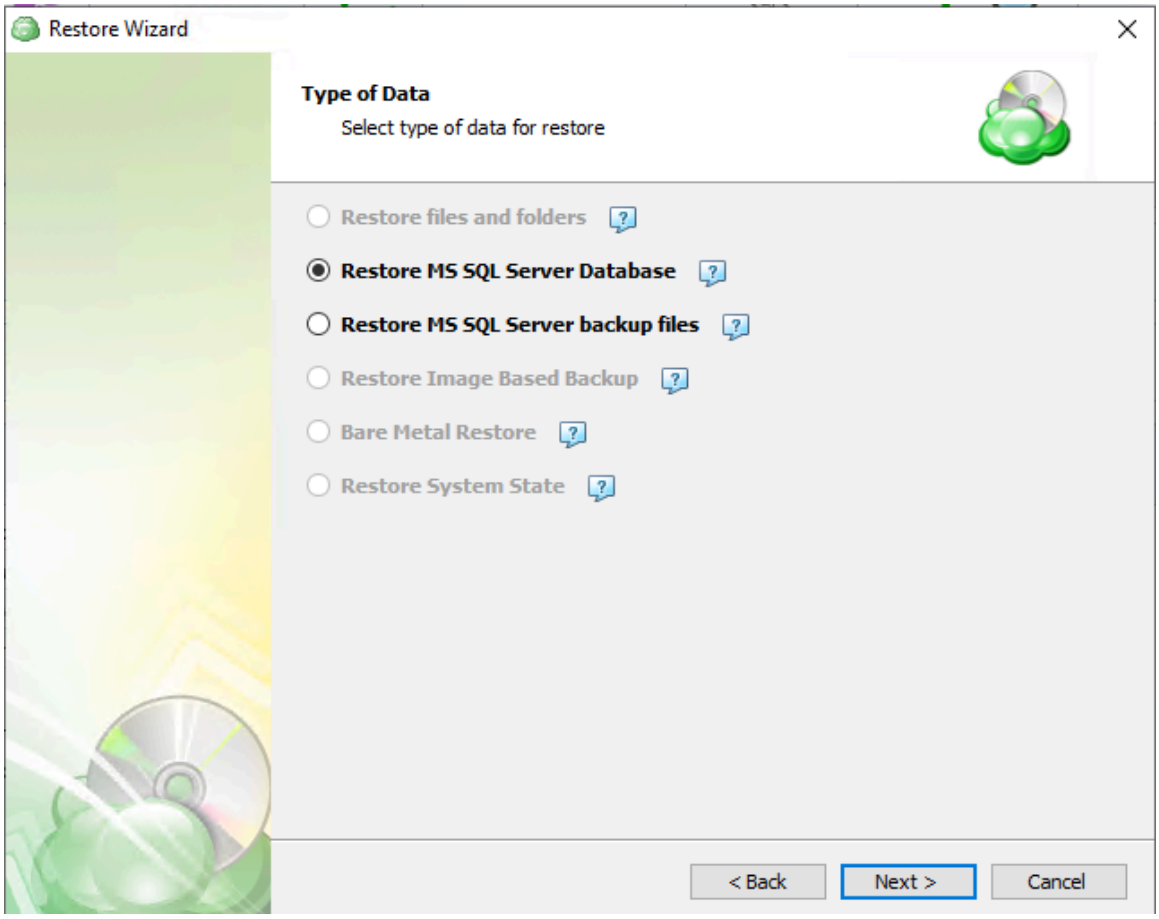
"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

It is recommended to use a descriptive name which will distinguish the backup from others.

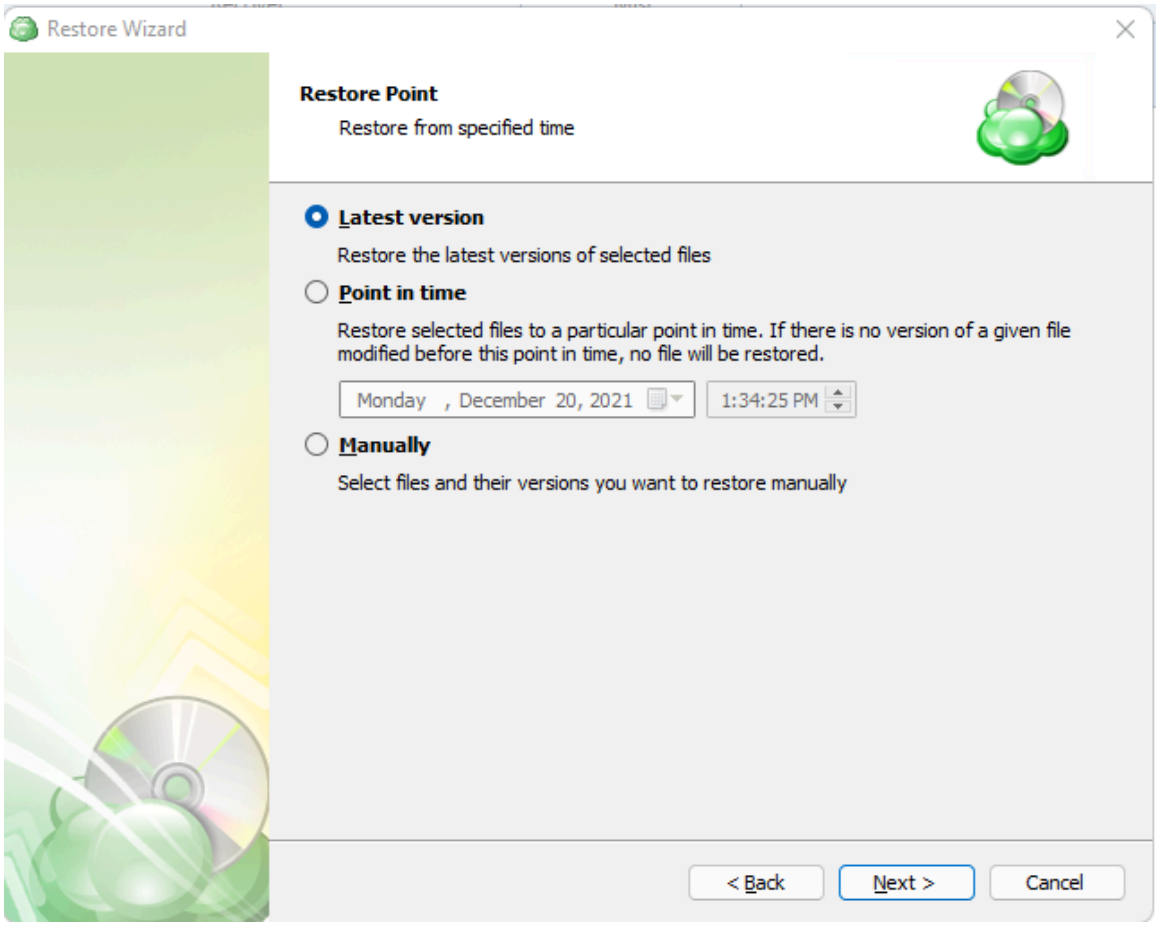
Step 5. With the type of restore selected, the next step is to select the computer associated with the backup which you would like to restore.



Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “MS SQL Server Database” option to continue.

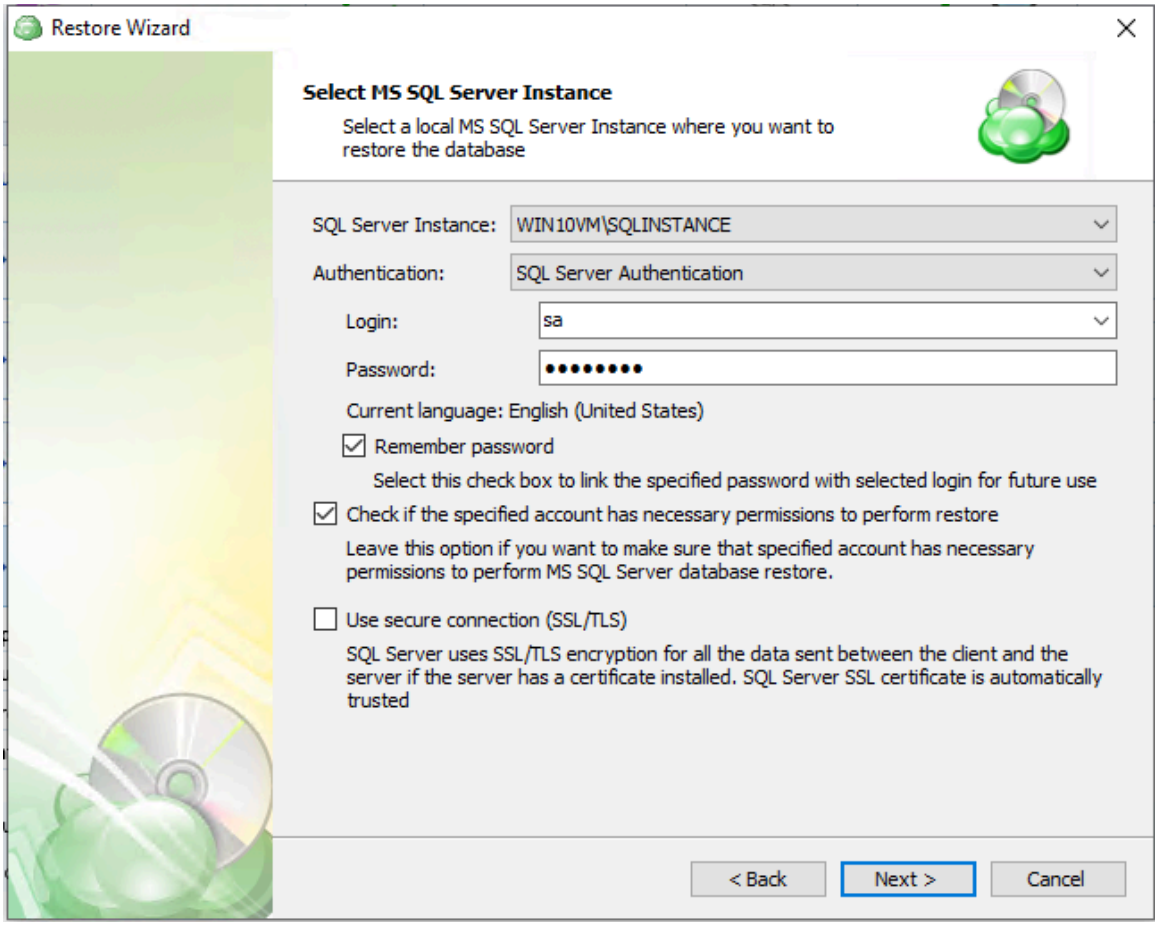


Step 7. Next you will be given a choice for what point in time you would like to restore the VM to.



> If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

Step 8. Next you will be prompted to select the SQL Server Instance as well as specify the credentials to be used by the backup service.

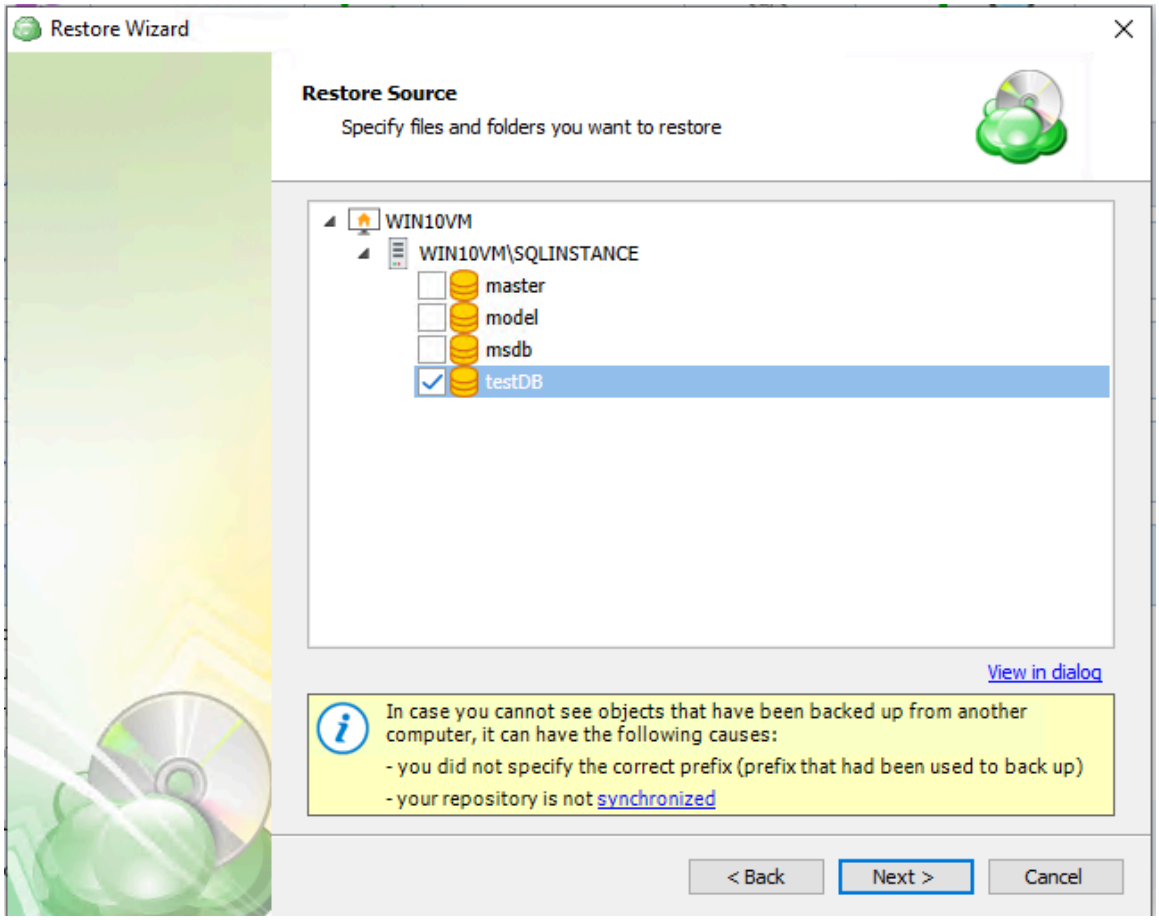


- **SQL Server Instance:** Select the instance containing the database to be backed up from the list. Note that only local instances can be selected.
- **Authentication Type:** Choose between Windows or SQL Authentication. If “Windows Authentication” is selected, the application will run the backup as the local service account.
- **User Name:** If “SQL Server Authentication” was selected, enter the user name in this field.
- **Password:** If “SQL Server Authentication” was selected, enter the password for the specified SQL user here.
- **Check if the specified account has necessary permissions to perform backup:** The application will check for the appropriate permissions prior to attempting to backup the database. It is recommended to use this option to prevent unexpected backup failures.

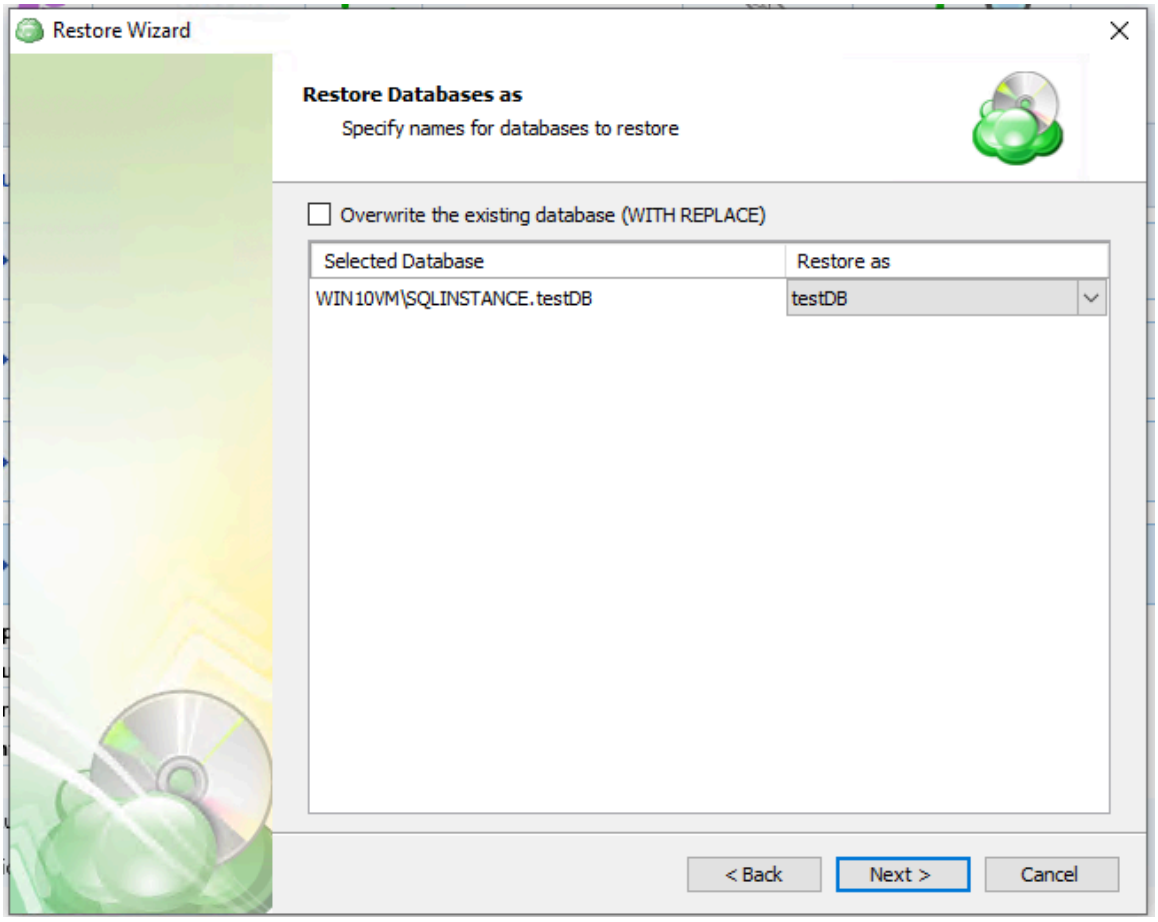
- **Use secure connection (SSL/TLS):** Enabling this will allow the application to connect to the SQL instance using encryption, if configured on the database host.

> Only local databases and instances can be restored to.

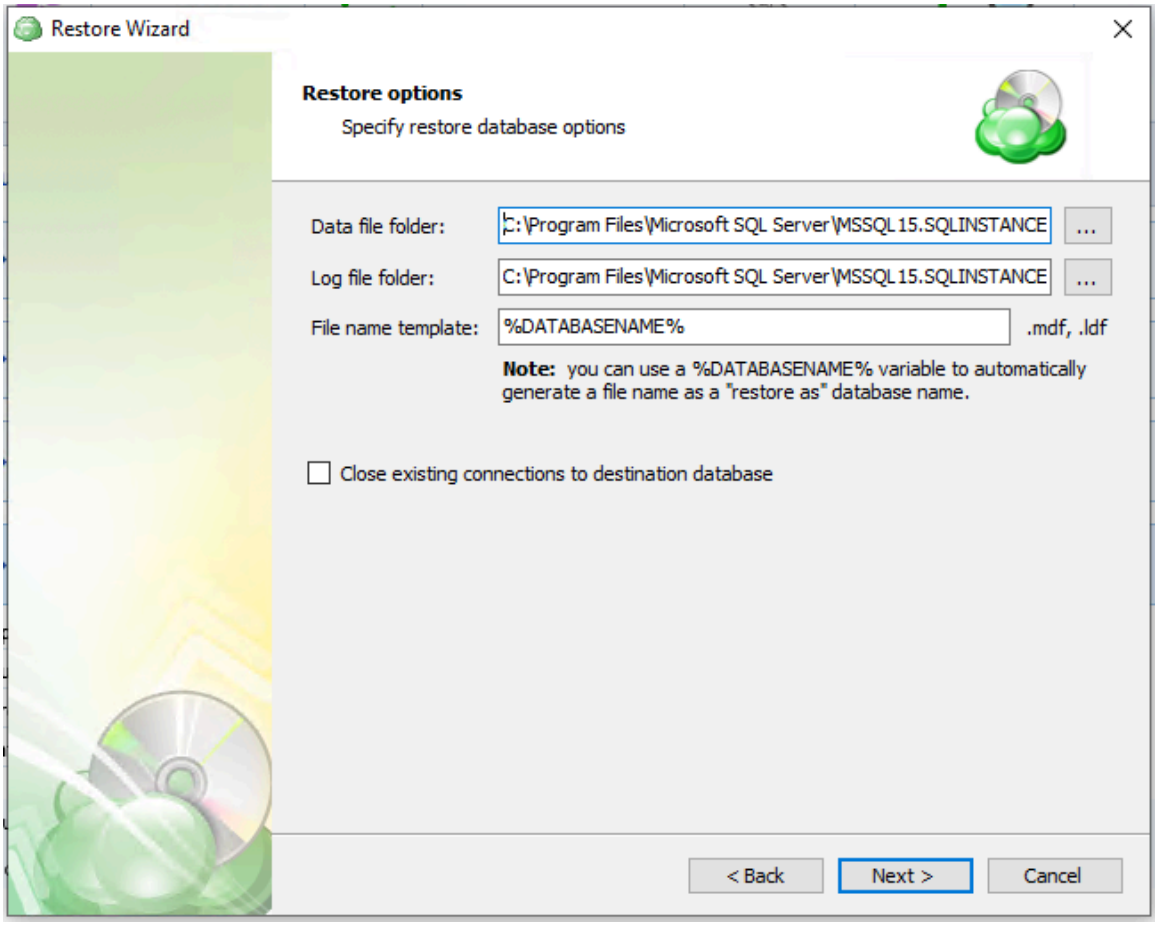
Step 9. Select the databases within the instance which you would like to restore.



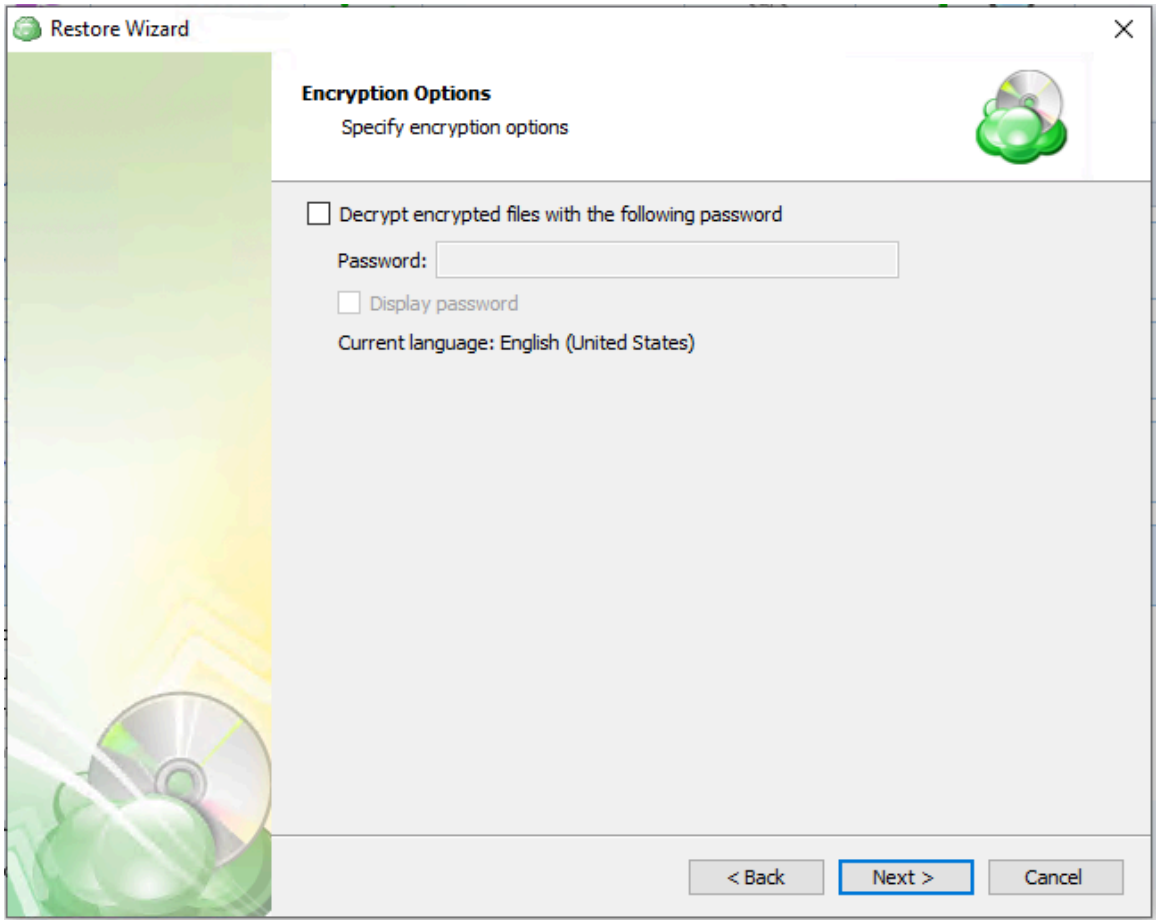
Step 10. After selecting the database(s) to be restored, you will be given options to overwrite an existing database or restore the database with a new name.



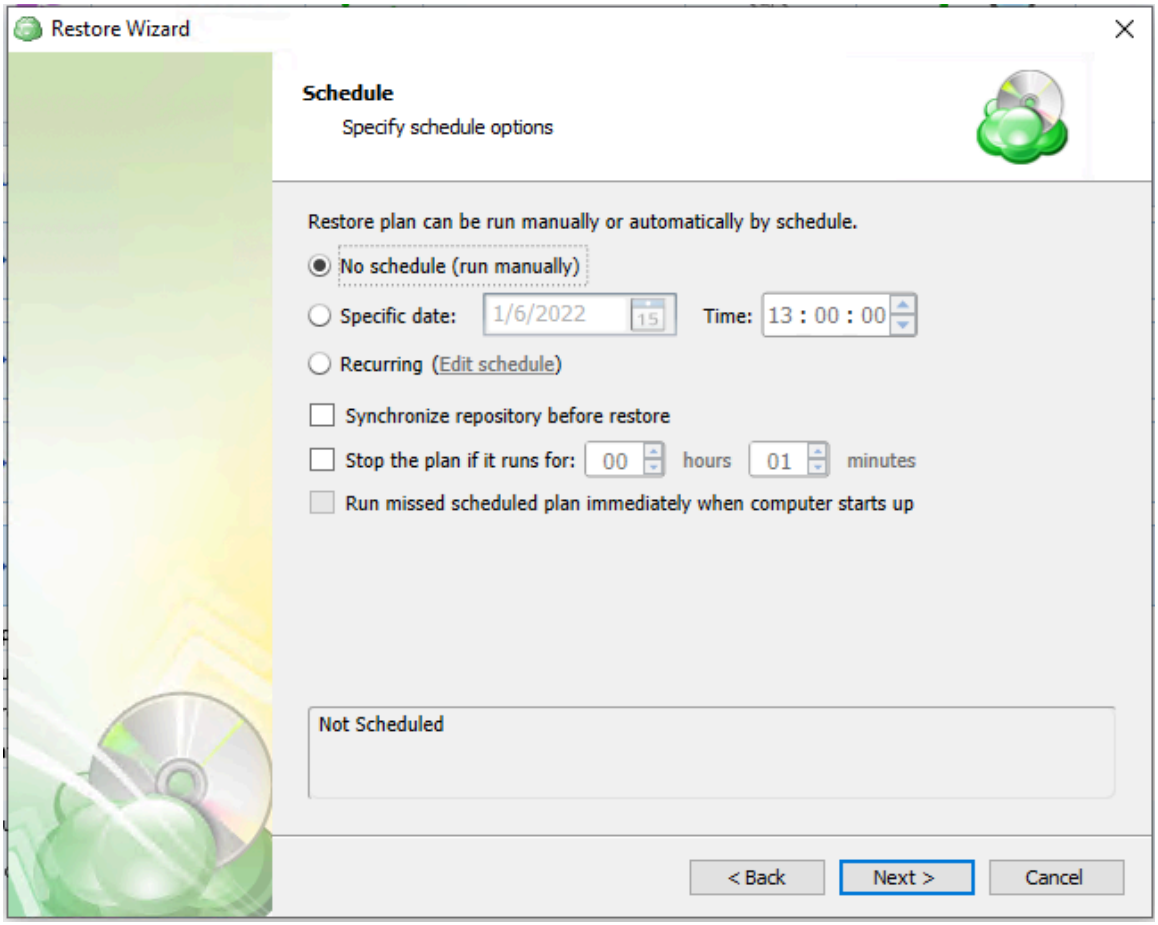
Step 11. The next step asks you to provide the paths the database files will be restored to.



Step 12. Next the application will prompt you to enter the credentials used if the backup was encrypted. If it was not encrypted, simply click “Next”.



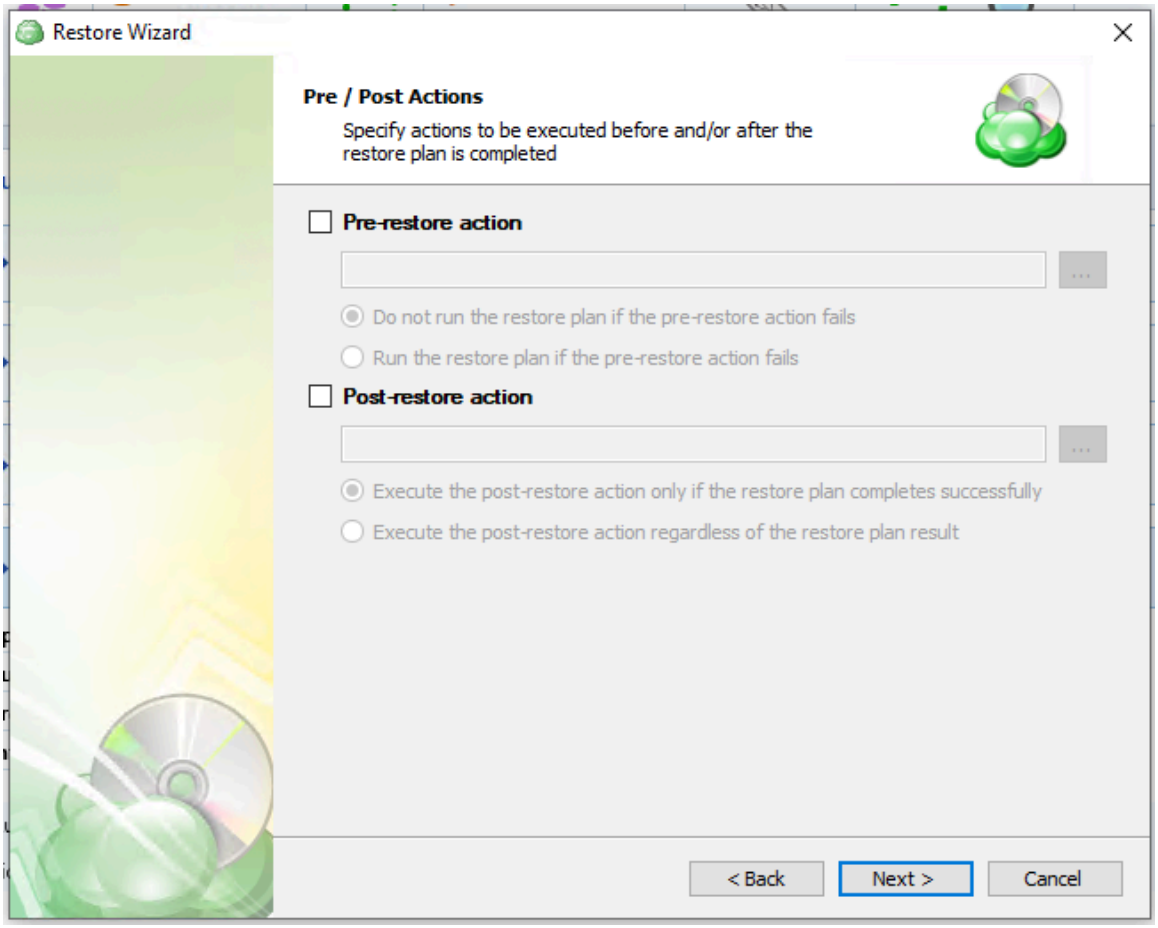
Step 13. Next you are prompted to set the schedule for your restore plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.



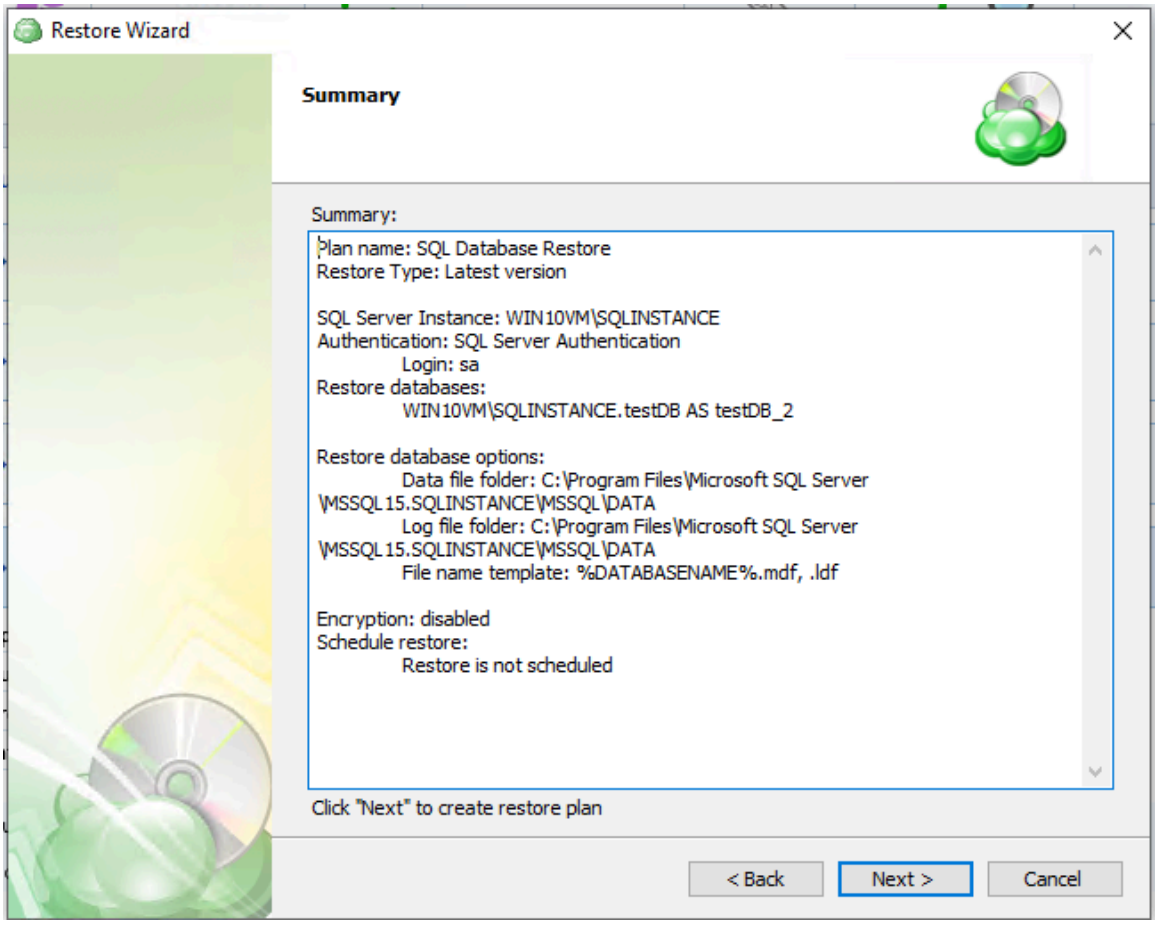
Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection.

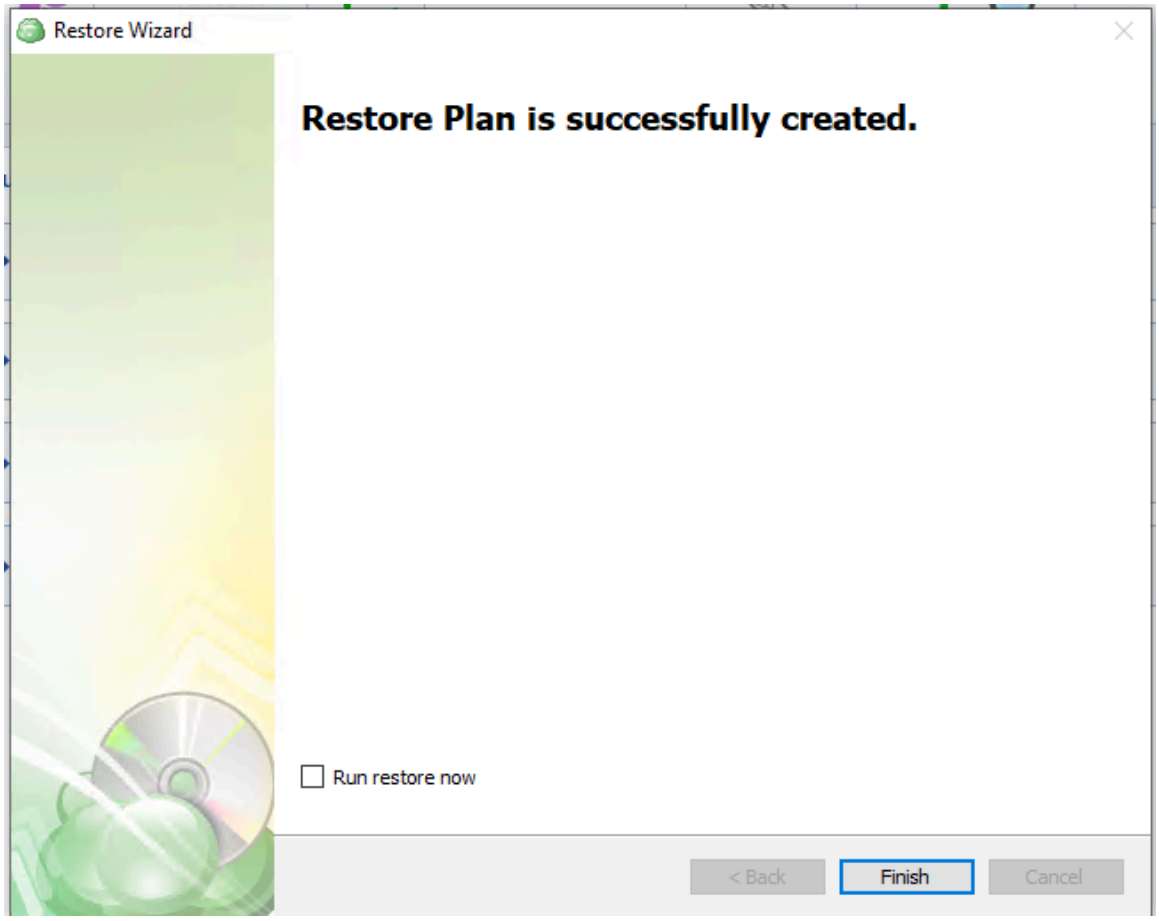
Step 14. The **Pre/Post Actions** page allows the execution of custom scripts before and/or after the running of a backup task.



Step 15. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.

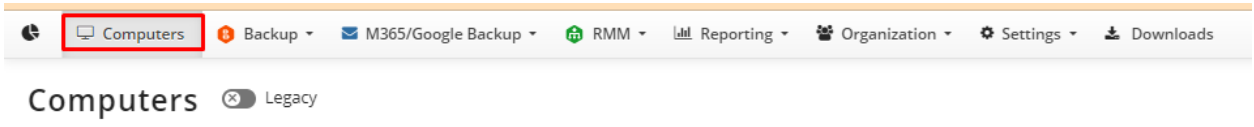


Step 16. After clicking next on the previous step, the Restore Plan is created. The final step is to acknowledge this and determine whether to run the backup immediately or for it to wait until the next scheduled occurrence.



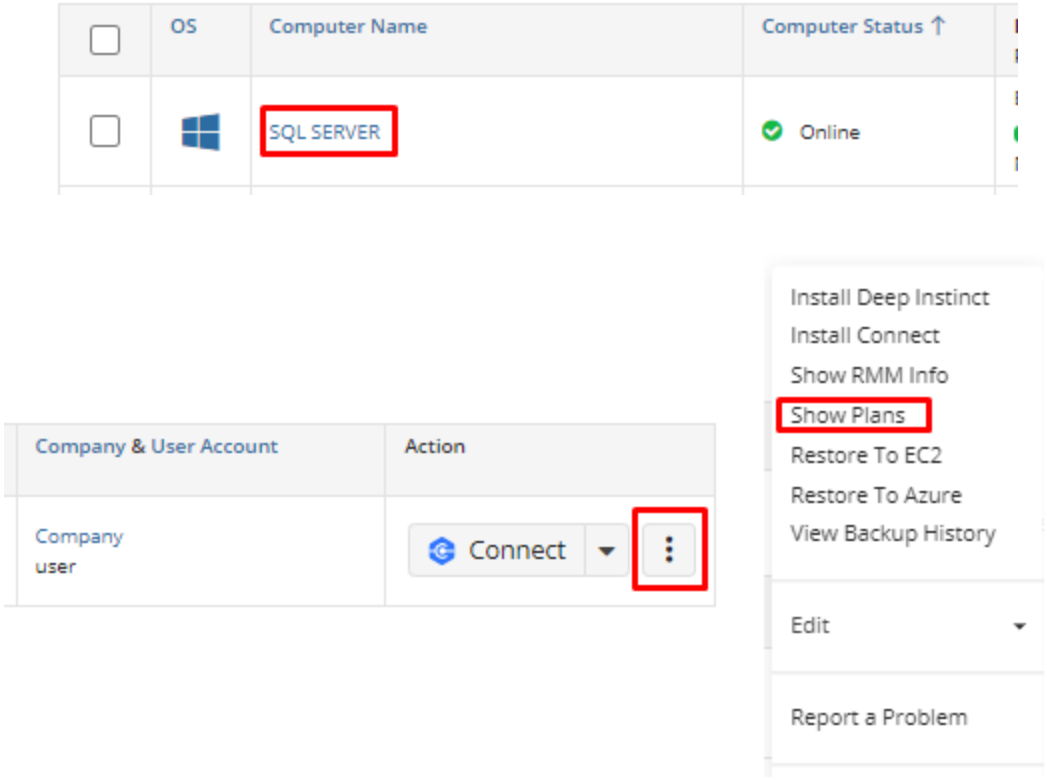
Restore Databases using MBS

Step 1. From the MBS Portal, left-click Computers on the menu.

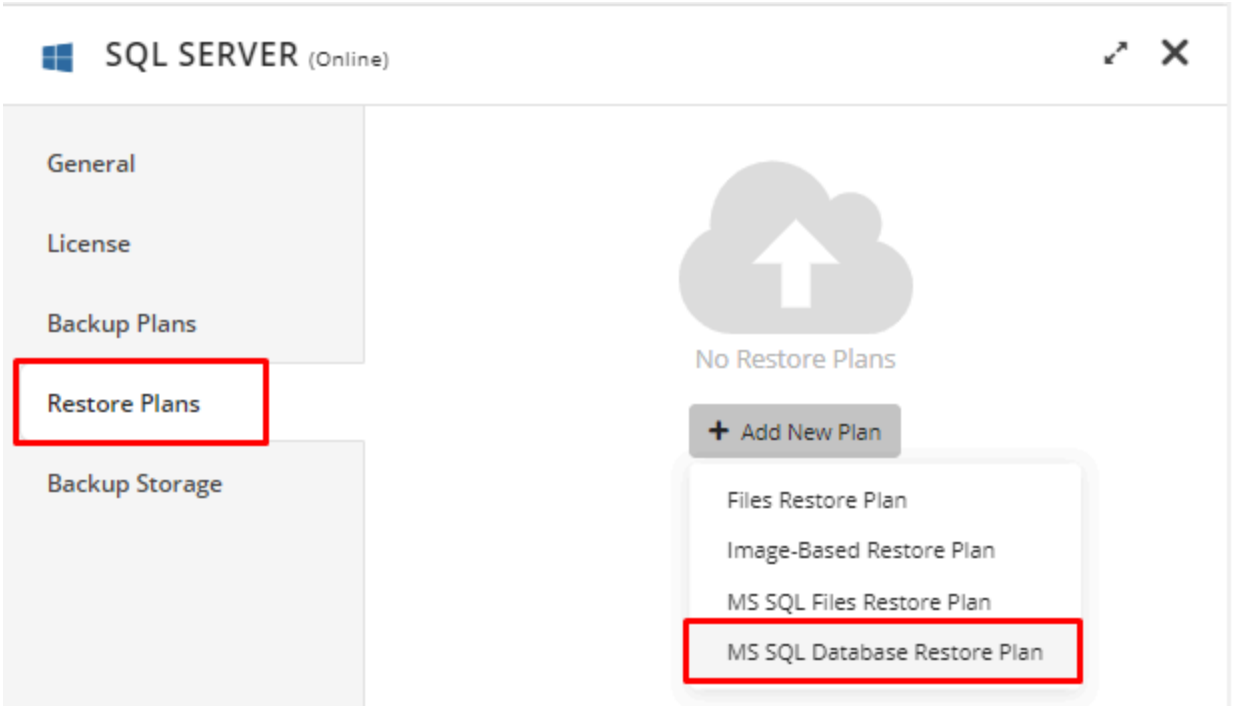


Step 2. Find the computer hosting the MS SQL instance to which you want to restore a previously backed up database or databases.

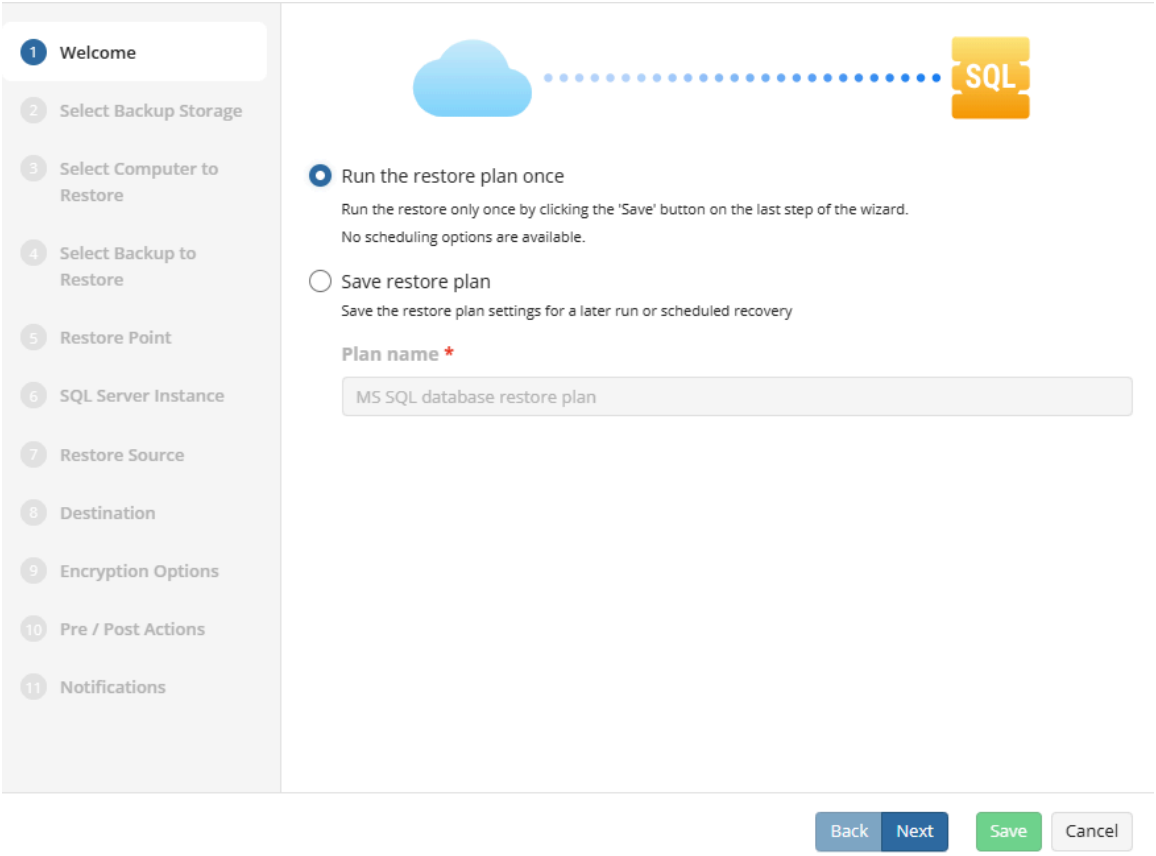
Click on the computer name or select "Show Plans" from the three-dot drop-down menu.



Step 3. In the side panel, navigate to the “Restore Plans” section. Click on the “Add New Plan” button and select “MS SQL Database Restore Plan” from the drop-down menu.



Step 4. The first step when creating a new MS SQL restore plan is to decide whether to run it a single time immediately after plan creation, or give it a name and save it for later.

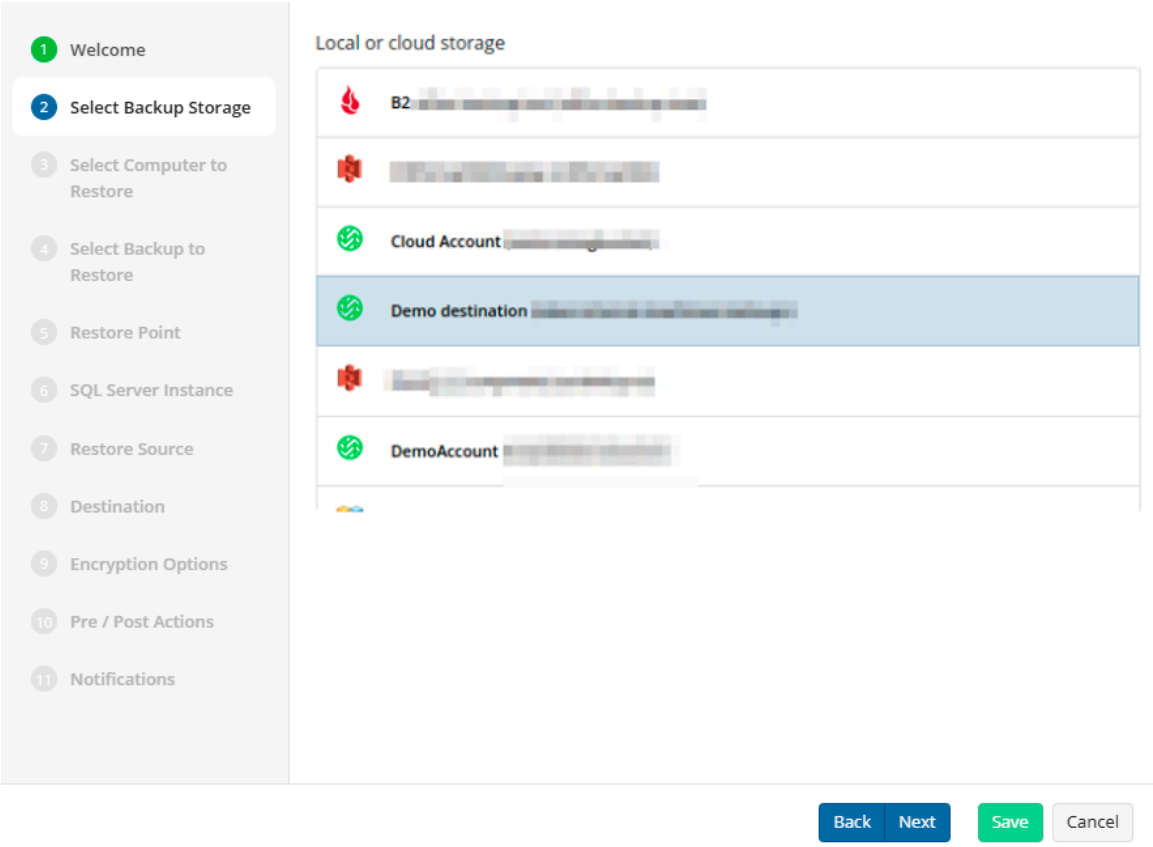


"Run restore once" will execute the restore immediately upon completing the wizard.

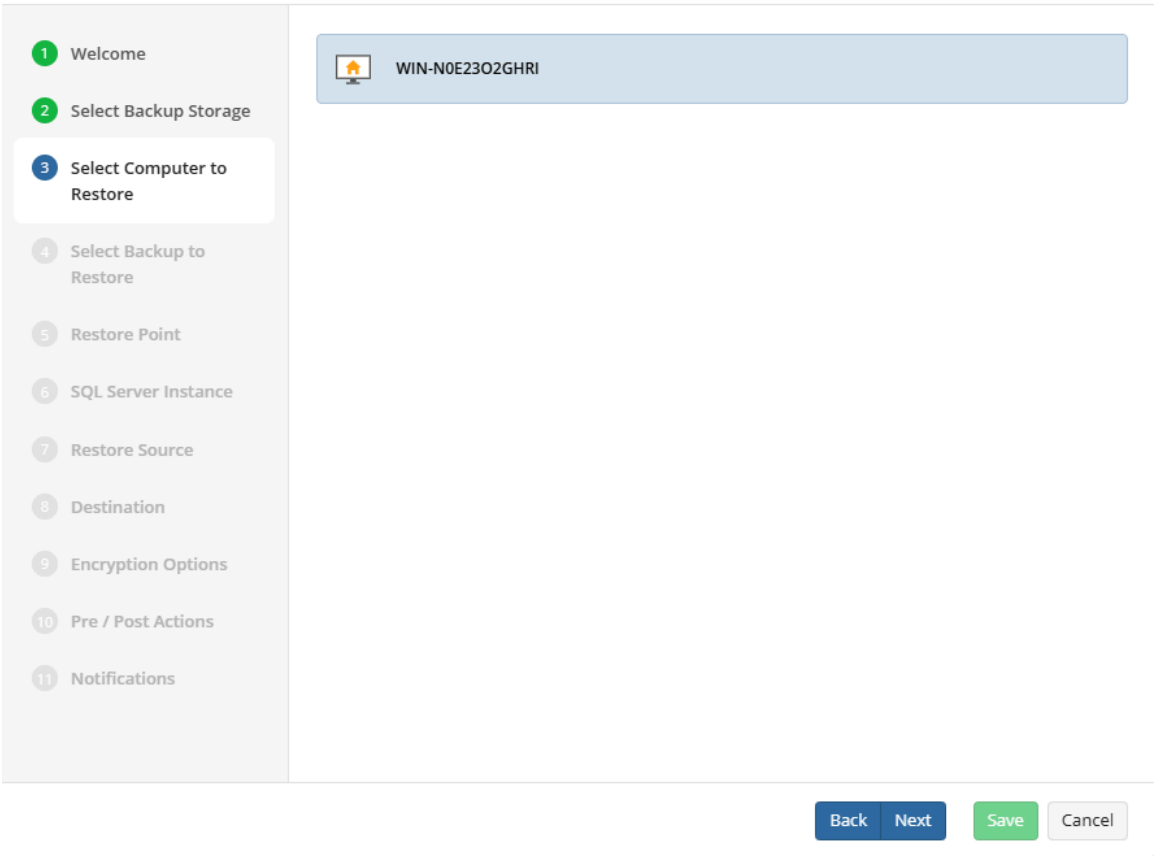
"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

It is recommended to use a descriptive name which will distinguish the plan from others.

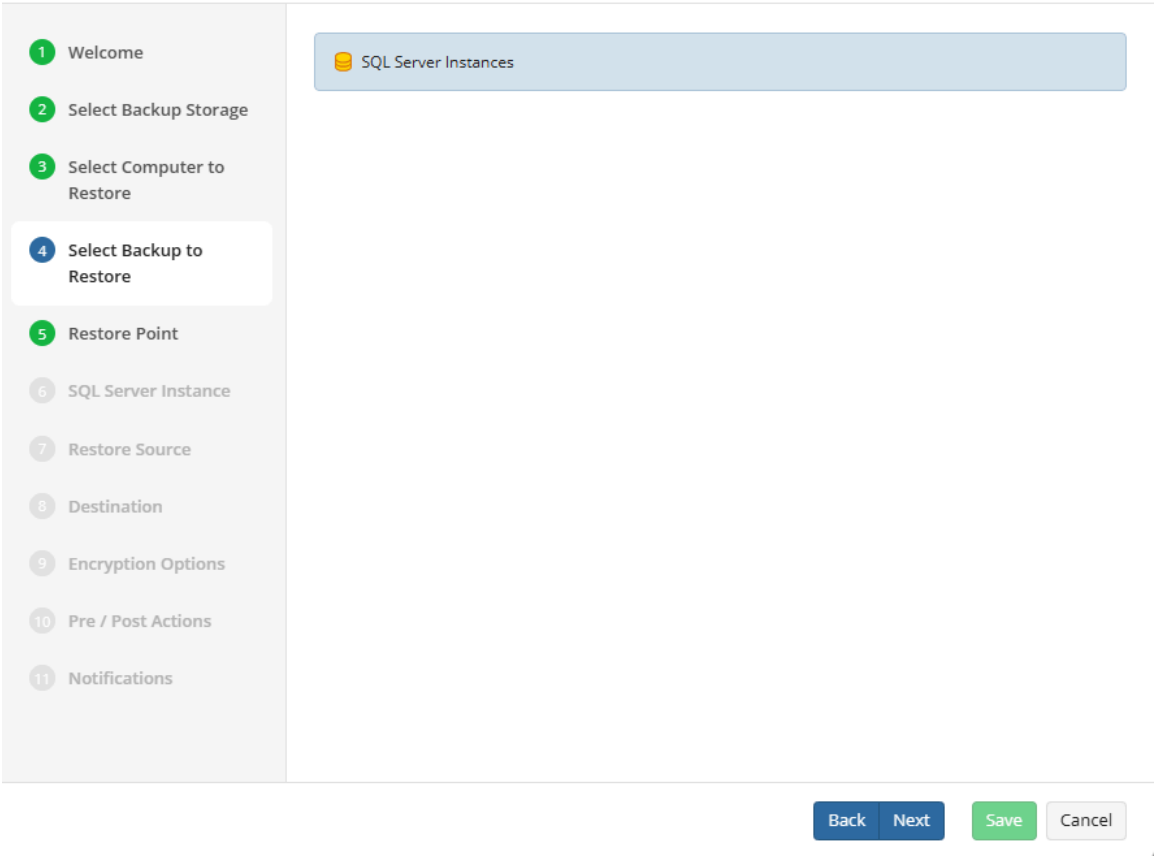
Step 5. Next, select the storage which contains the desired data.



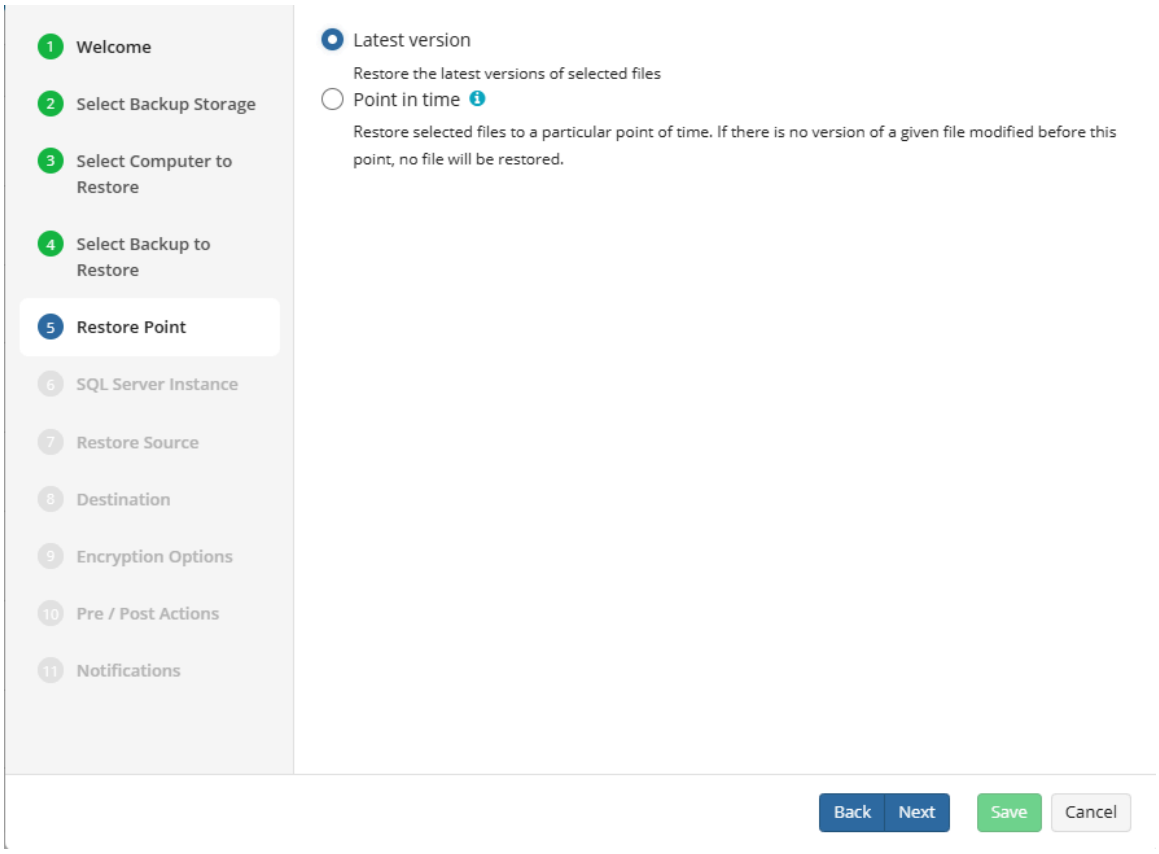
Step 6. With the Backup Storage selected, the next step is to select the computer associated with the backup which you would like to restore.



Step 7. Next, you will be presented with a list of available backup types for the selected host. Select the “SQL Server Instances” option to continue.

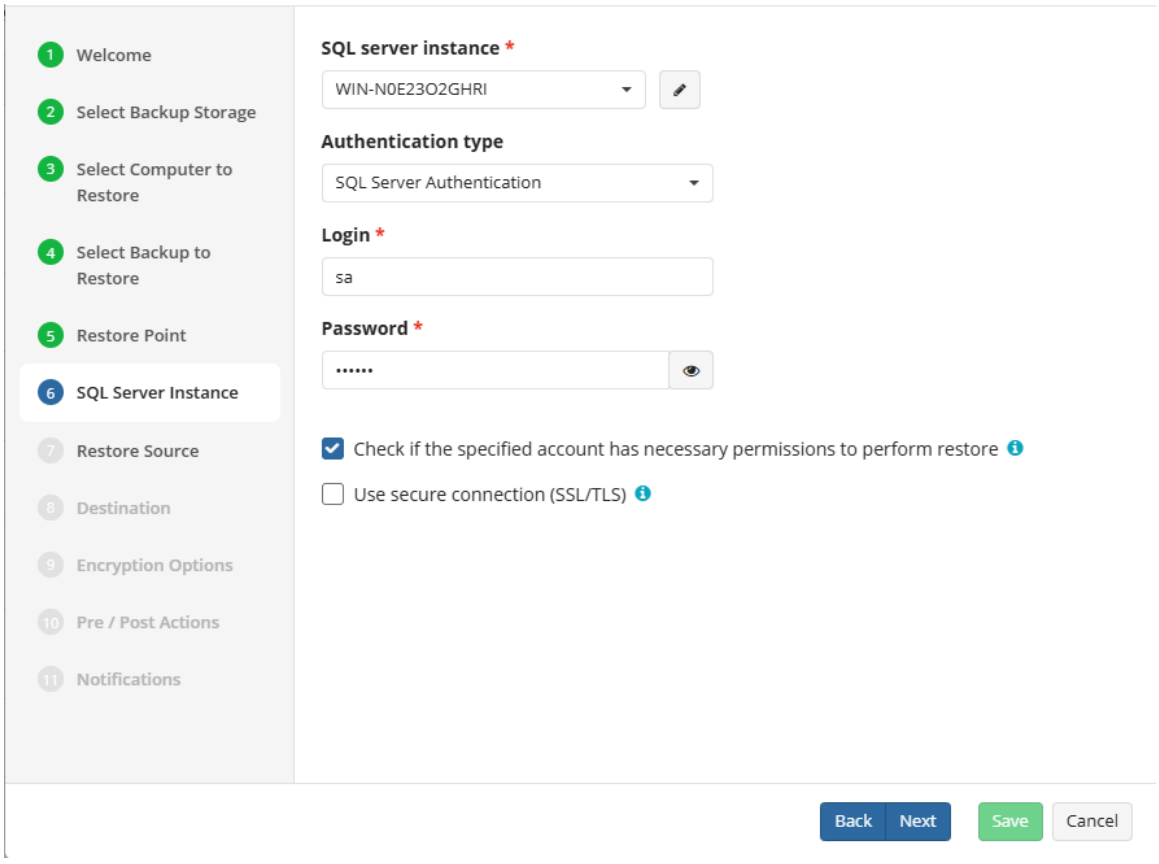


Step 8. The next step is to select the desired point in time to restore to.



If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

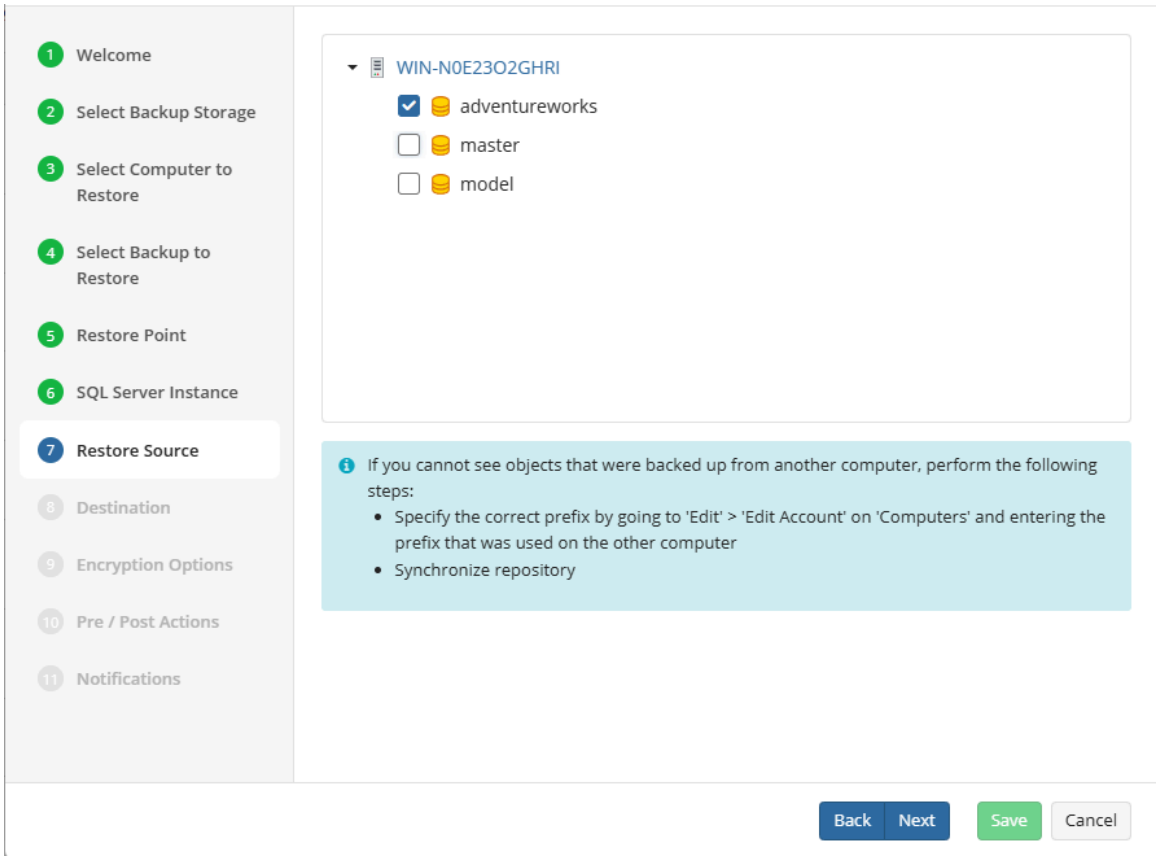
Step 9. Next you will be prompted to select the SQL Server Instance as well as specify the credentials to be used by the application.



- **SQL Server Instance:** Select the instance containing the database to be backed up from the list. Note that only local instances can be selected.
- **Authentication:** Choose between Windows or SQL Authentication. If “Windows Authentication” is selected, the application will run the backup as the local service account.
- **User Name:** If “SQL Server Authentication” was selected, enter the user name in this field.
- **Password:** If “SQL Server Authentication” was selected, enter the password for the specified SQL user here.

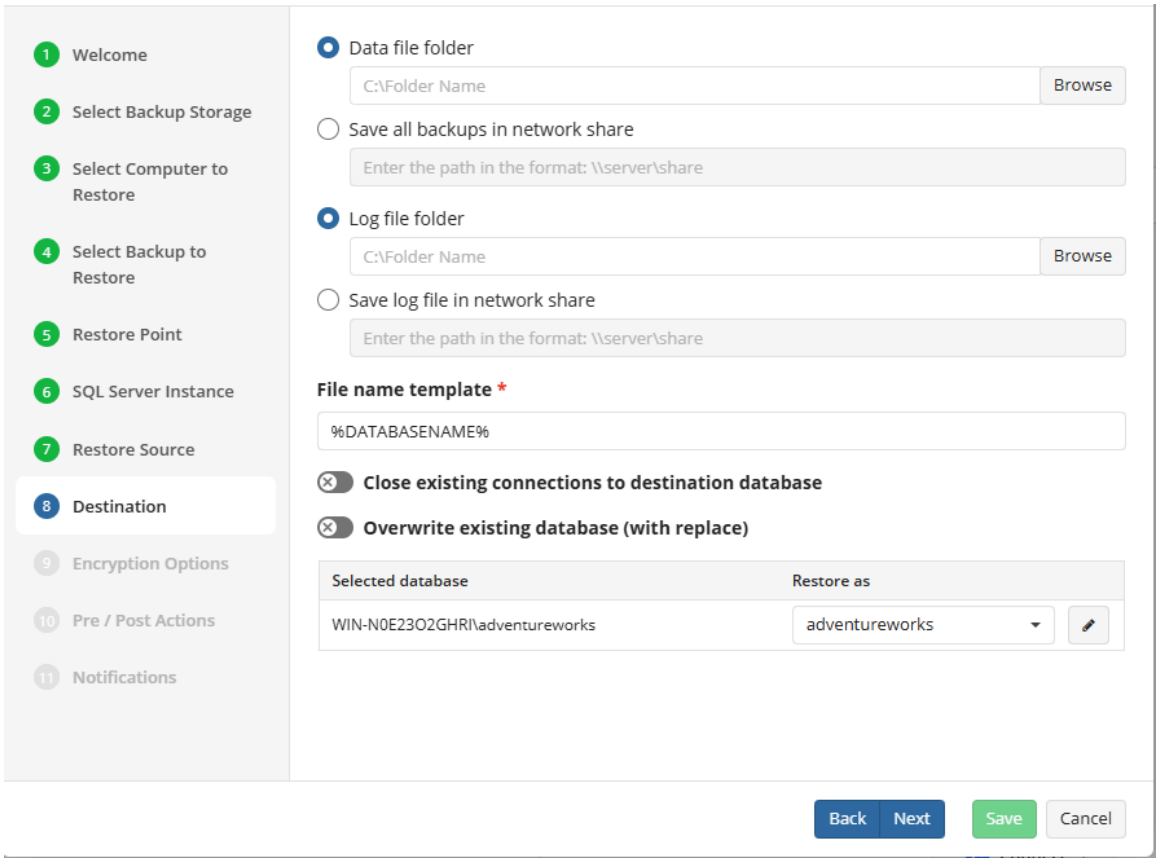
> Only local databases and instances can be restored to.

Step 10. Next, select the source of the backup to be restored, then select which databases to restore from the list.



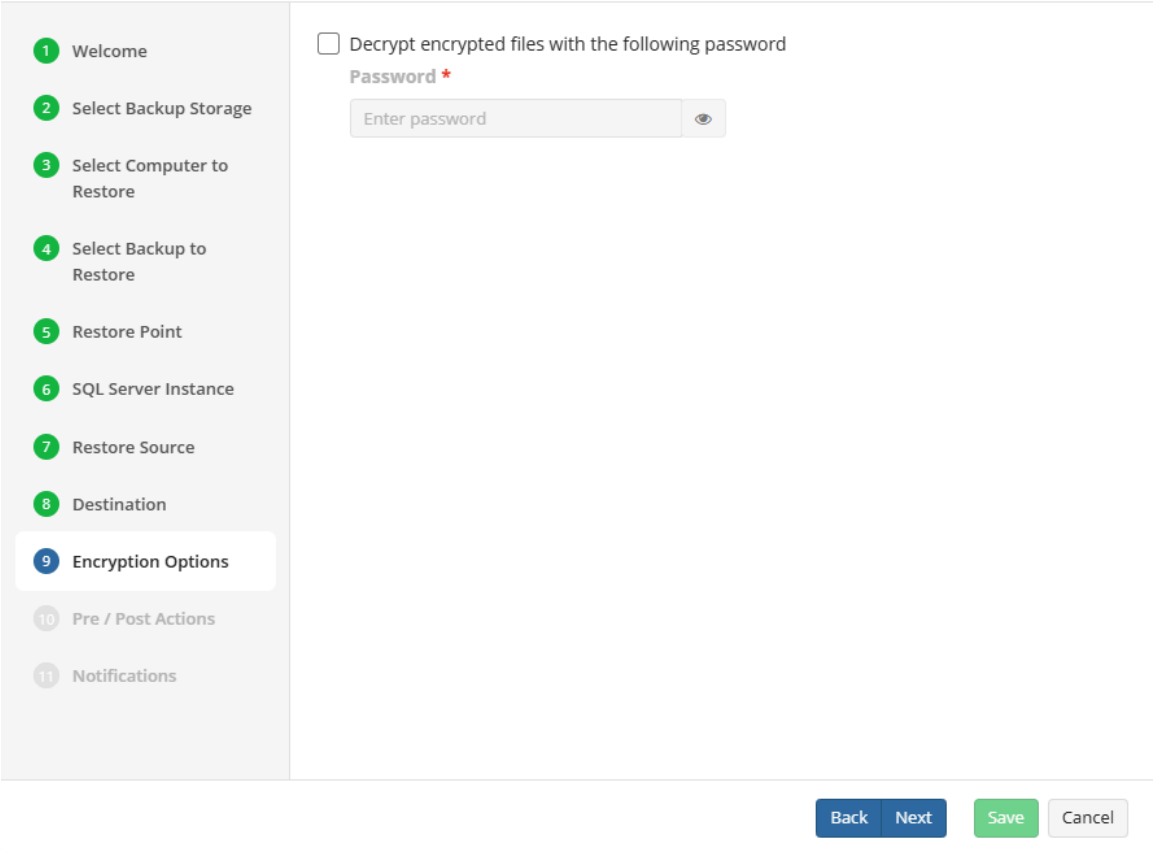
When selecting the databases from the list they will restore with their existing name by default, but if you would like to restore it as a new or different name, type the new name into the “Restore As” field.

Step 11. The next step asks you to provide the paths the database files will be restored to, and you will be given options to overwrite an existing database or restore the database with a new name.

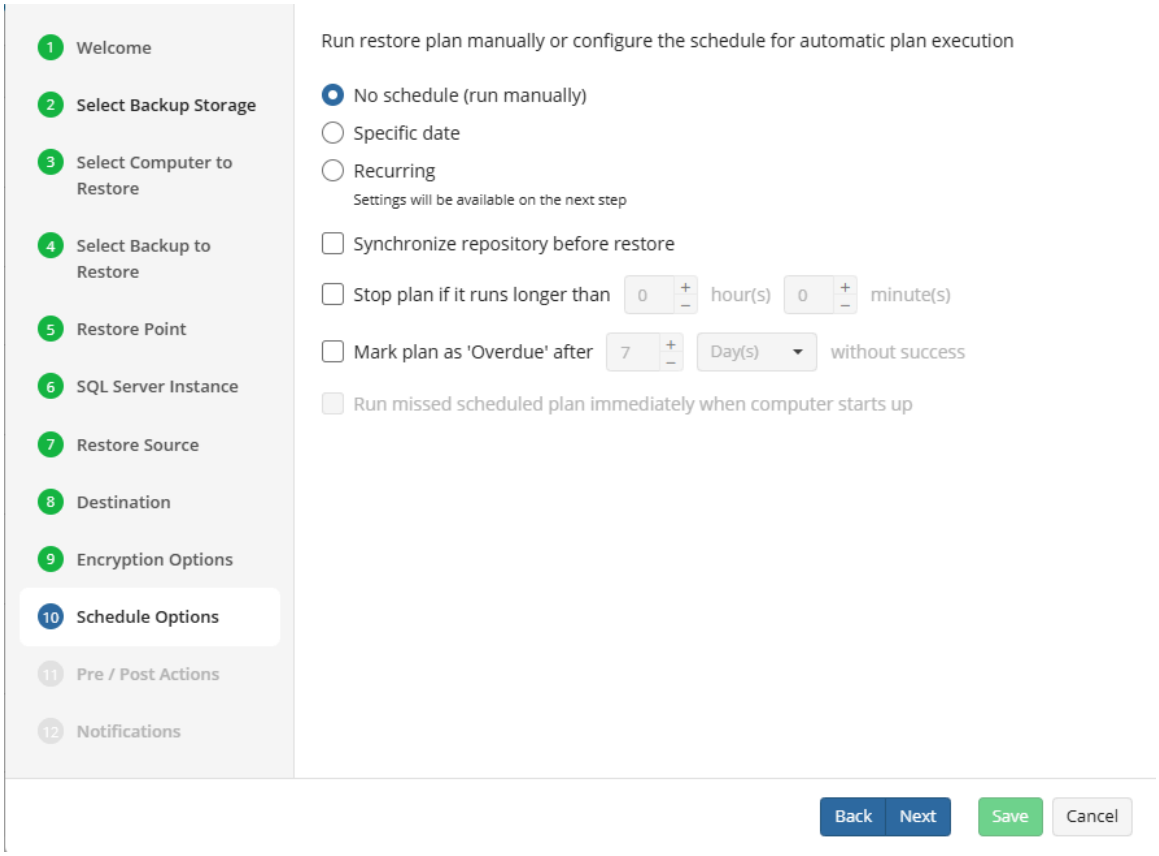


When selecting the databases from the list they will restore with their existing name by default, but if you would like to restore it as a new or different name, type the new name into the “Restore As” field.

Step 12. If the backed up data was encrypted, the next step will be to enter the password for decryption. If the password is incorrect or missing, the restore plan will fail and you will need to edit the plan to input the correct password.



Step 13. Next, if you opted to save the restore plan, the next step is to specify how the plan should be triggered.



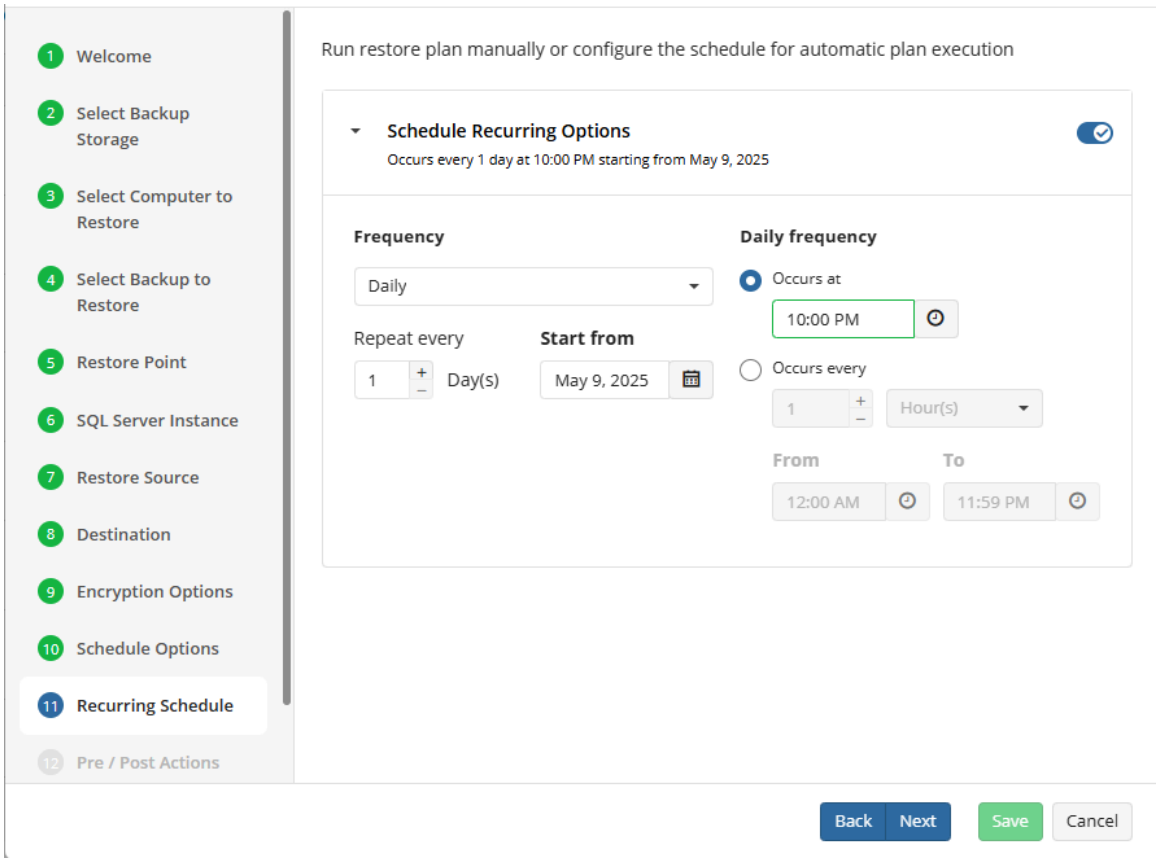
- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the fields below.

Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

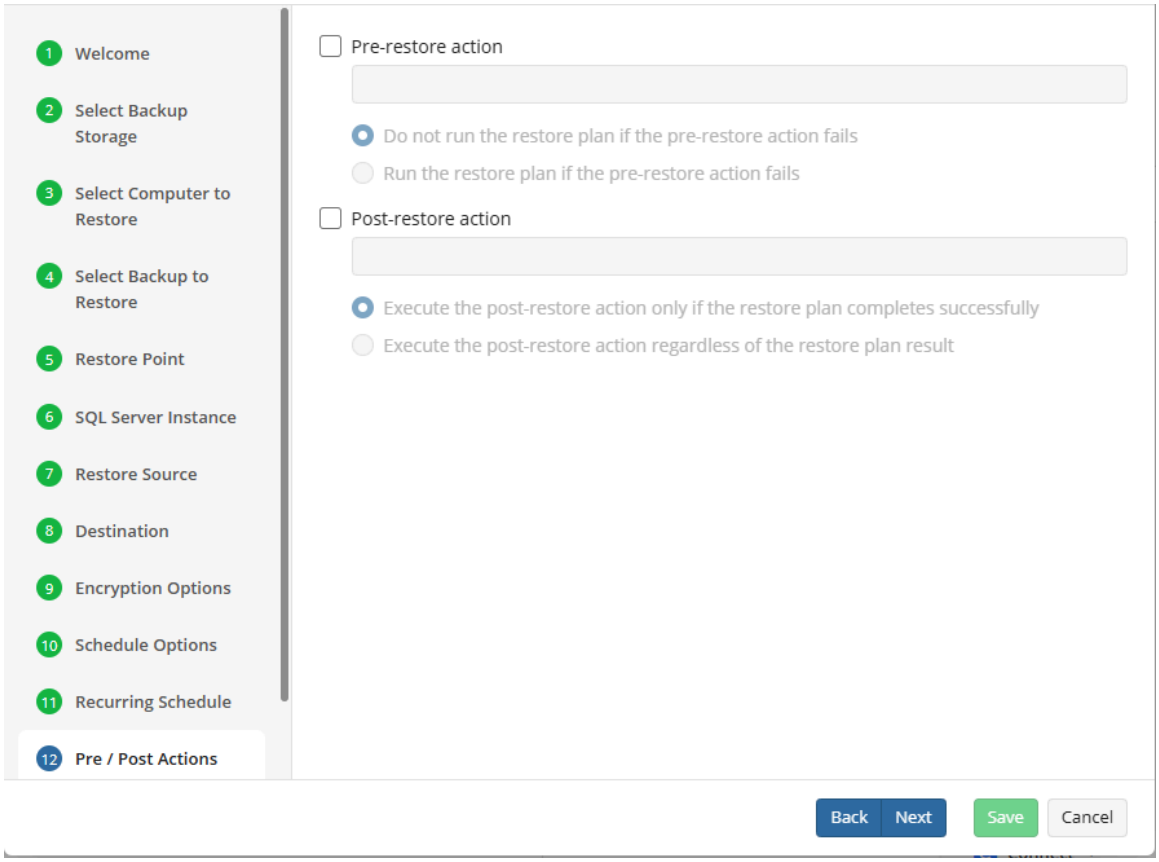
Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that

you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

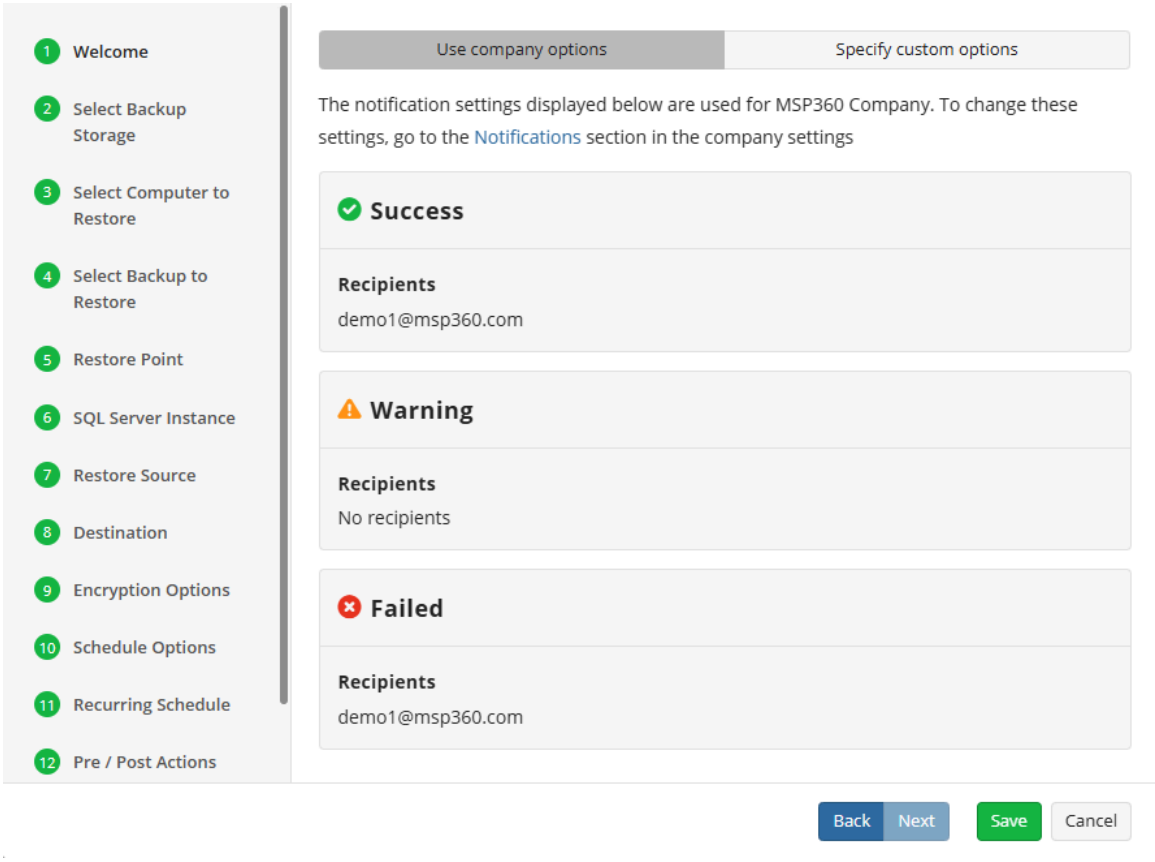
Step 14. With “Recurring” selected on the previous step, you are then prompted to define the time and frequency the plan should execute.



Step 15. The **Pre/Post Actions** page allows the execution of custom scripts before and/or after the running of a backup task.



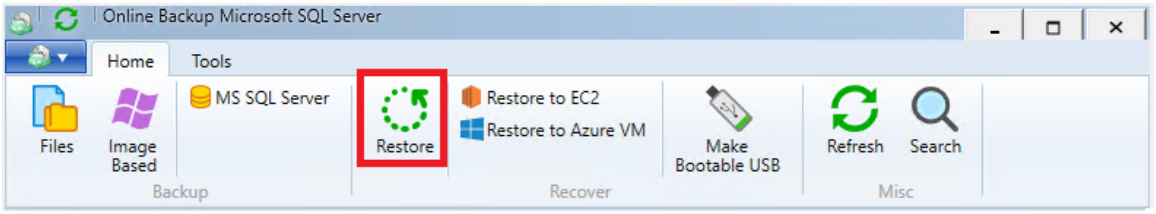
Step 16. The final step is to review the Notifications and Logging. The default settings applied at the Company level are selected by default, however you are also able to specify custom options per plan.



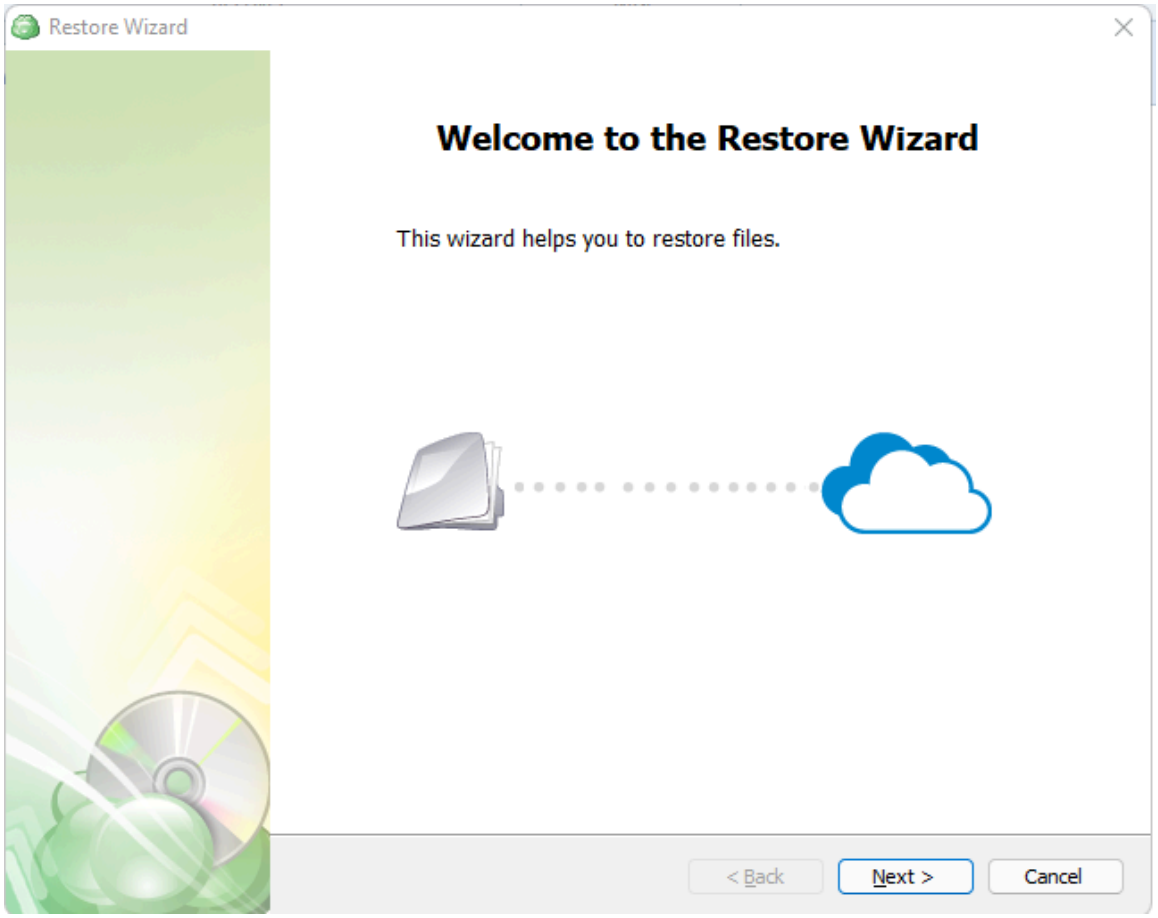
Step 17. Click on Save when you are happy with your selections. If the plan is set to run only a single time and has no set schedule, it will automatically start. Otherwise, if it is set to run only once and is scheduled, it will display in the list of plans until the scheduled time. If it is only set to run once, then when it completes successfully it will remove itself from the list of plans. Only Restore Plans which are saved will remain in the list for future use.

Restore Database Files using the Agent

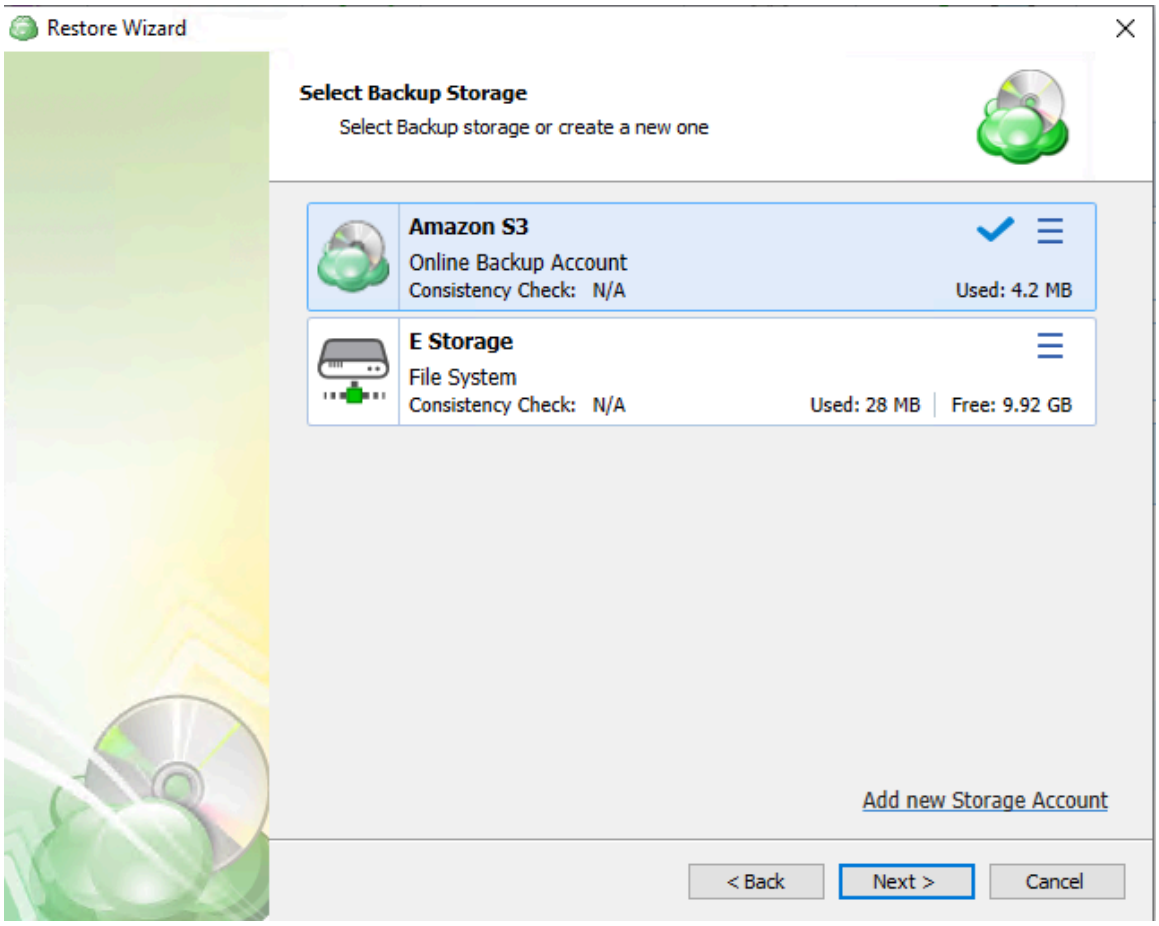
Step 1. Within the Online Backup Agent, click on “Restore”



Step 2. Once the wizard starts, click on Next to advance to the next step.

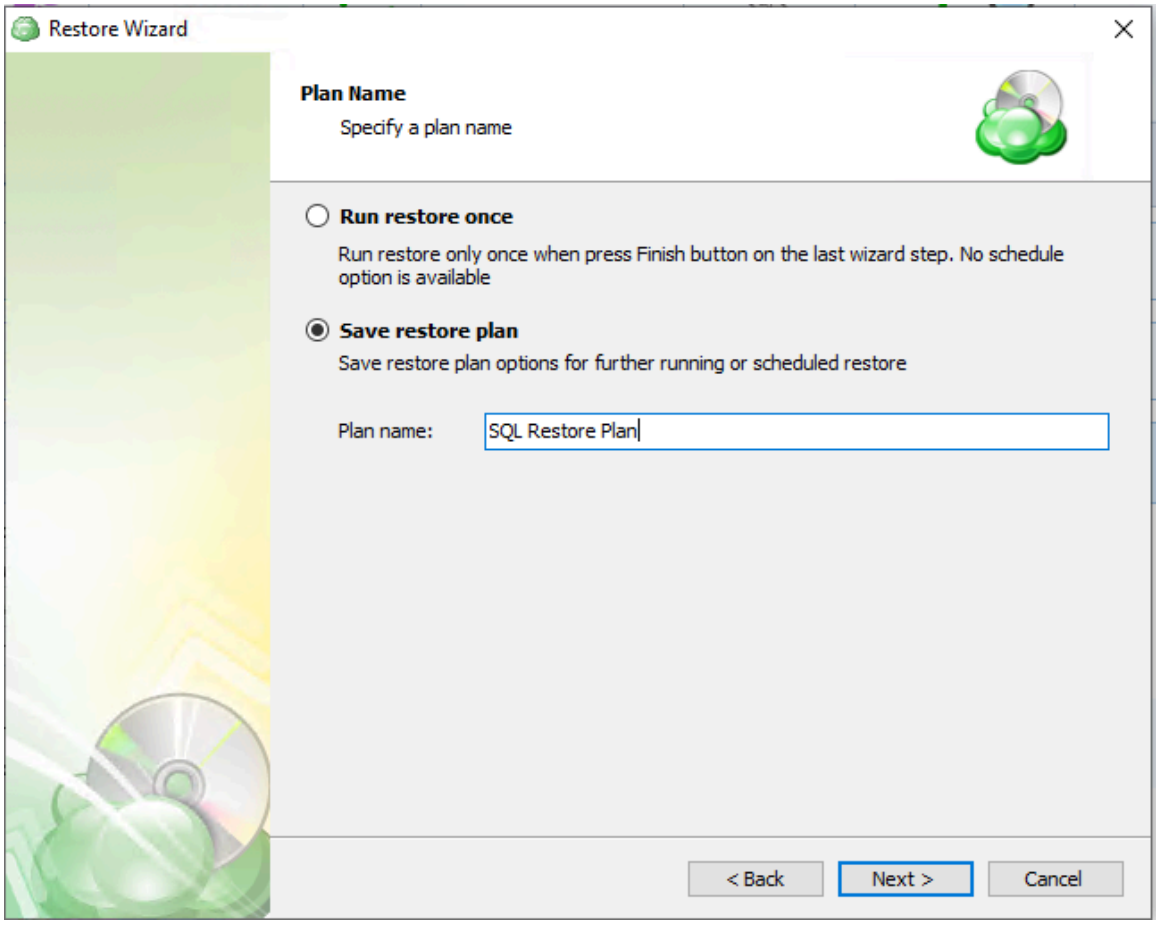


Step 3. The next step will prompt you to select the source for the restore.



If the desired destination is not in the list, you can click “Add new Storage Account” to add it.

Step 4. Next, you will be given the option to either run the restore once or to save it to run later.

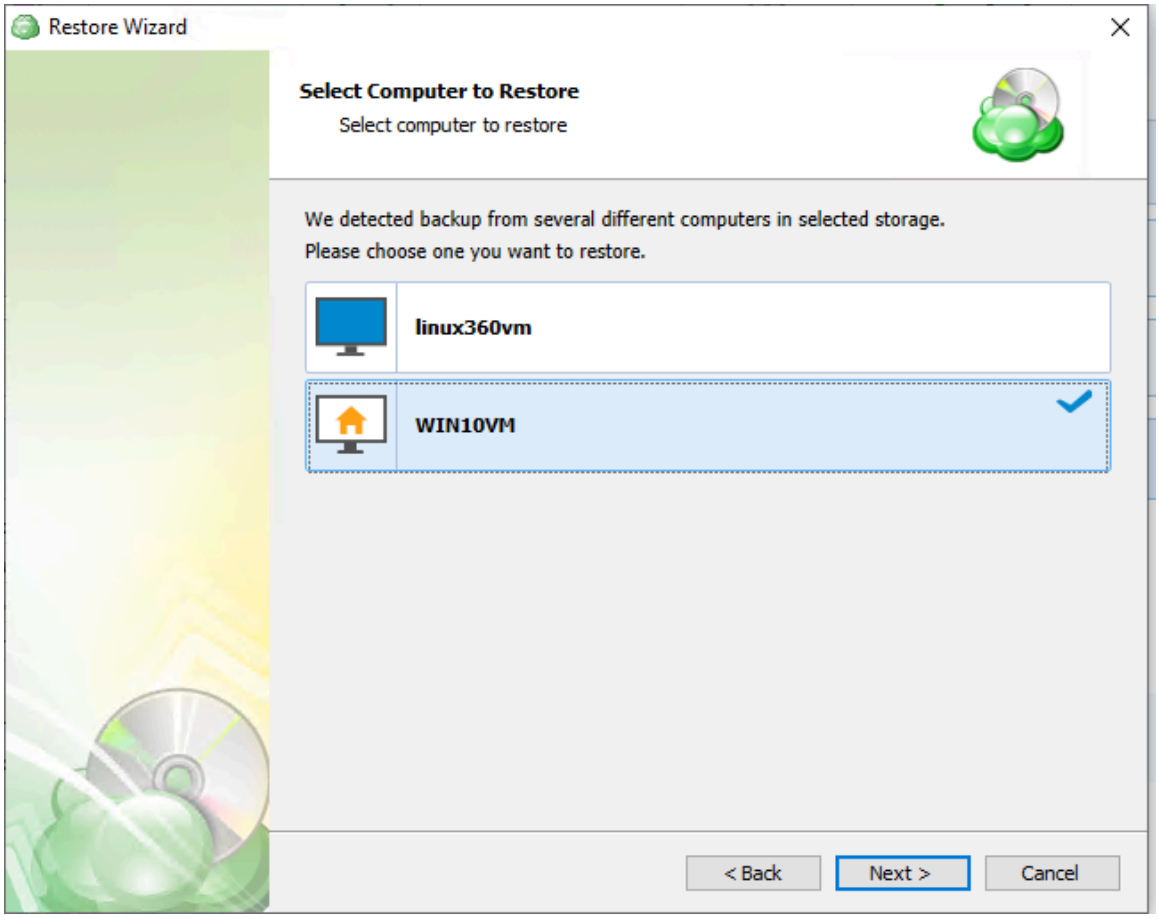


"Run restore once" will execute the restore immediately upon completing the wizard. There is no option to schedule this type of restore.

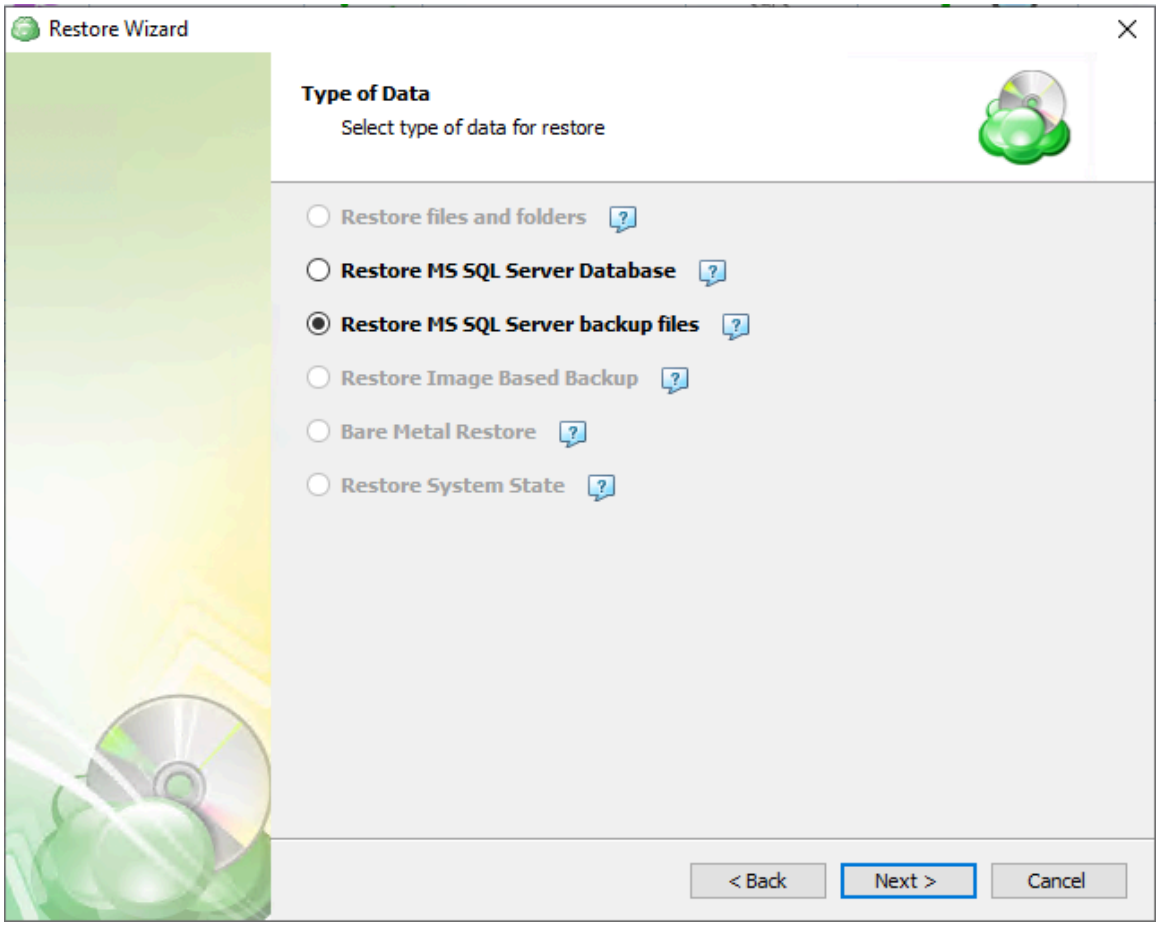
"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

It is recommended to use a descriptive name which will distinguish the backup from others.

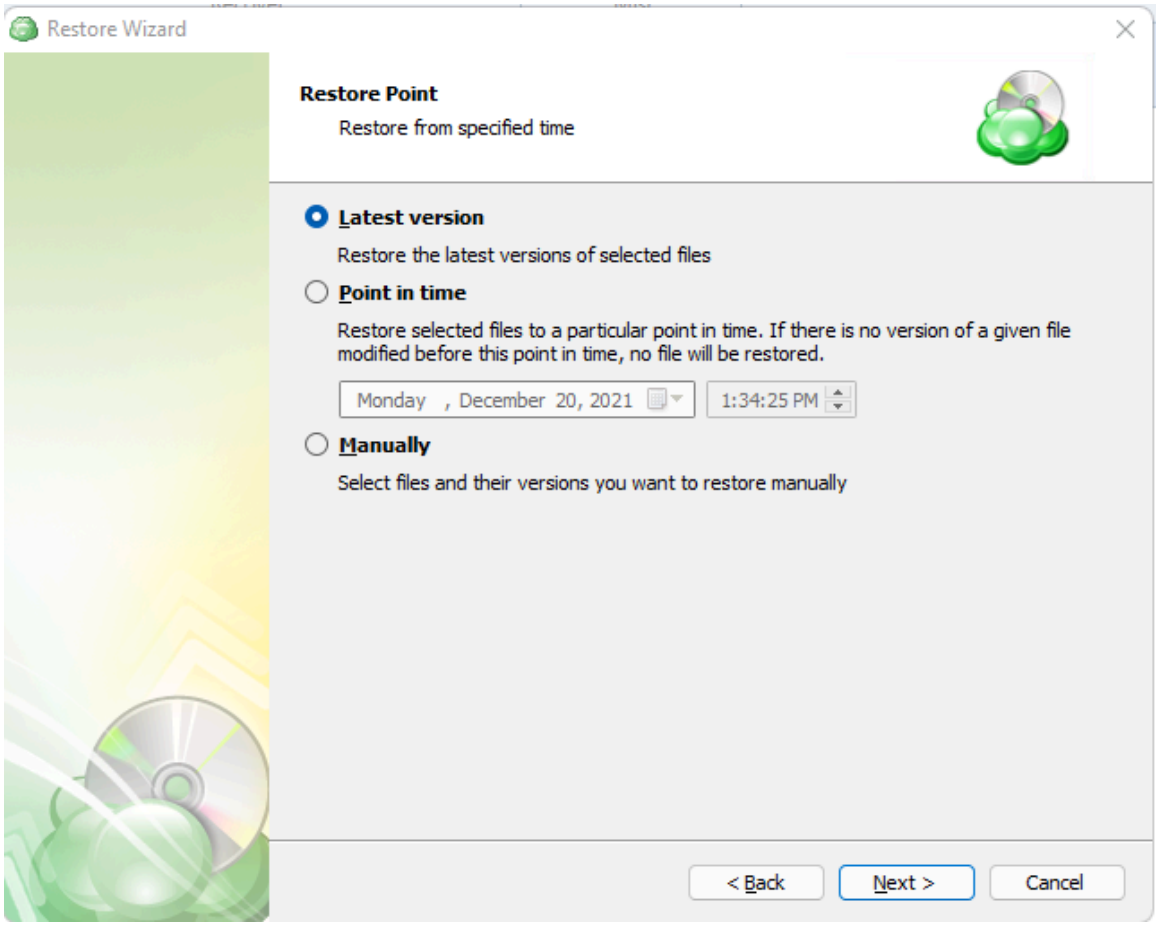
Step 5. With the type of restore selected, the next step is to select the computer associated with the backup which you would like to restore.



Step 6. Next, you will be presented with a list of available backup types for the selected host. Select the “MS SQL backup files” option to continue.

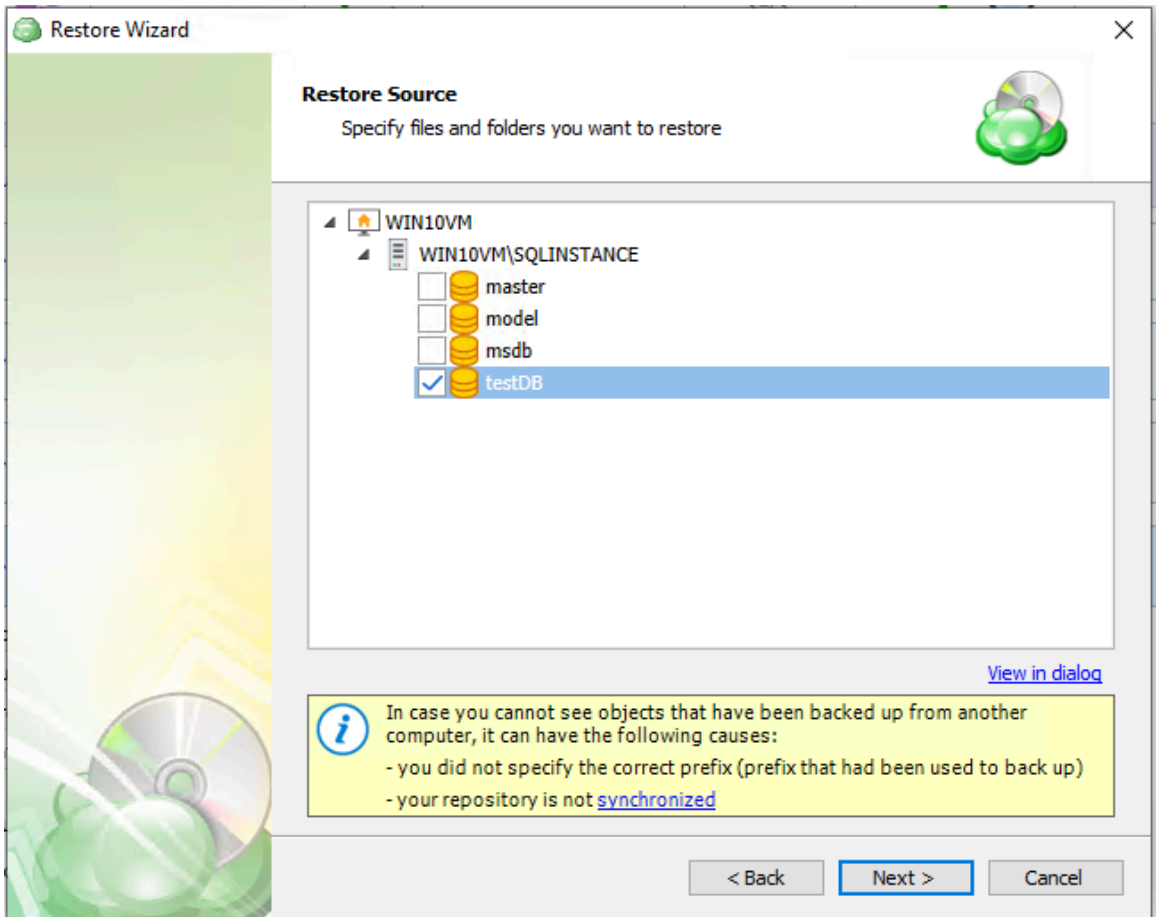


Step 7. Next you will be given a choice for what point in time you would like to restore the VM to.

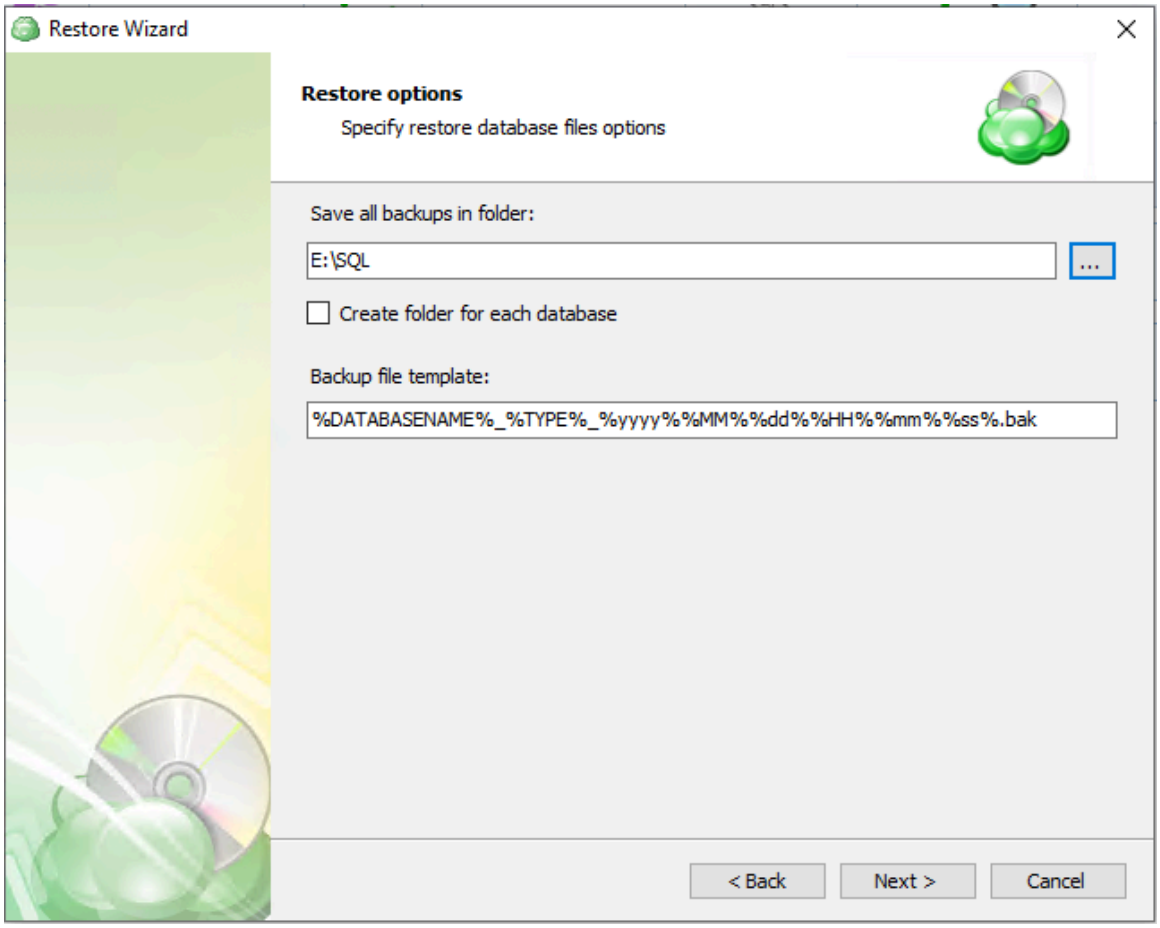


> If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

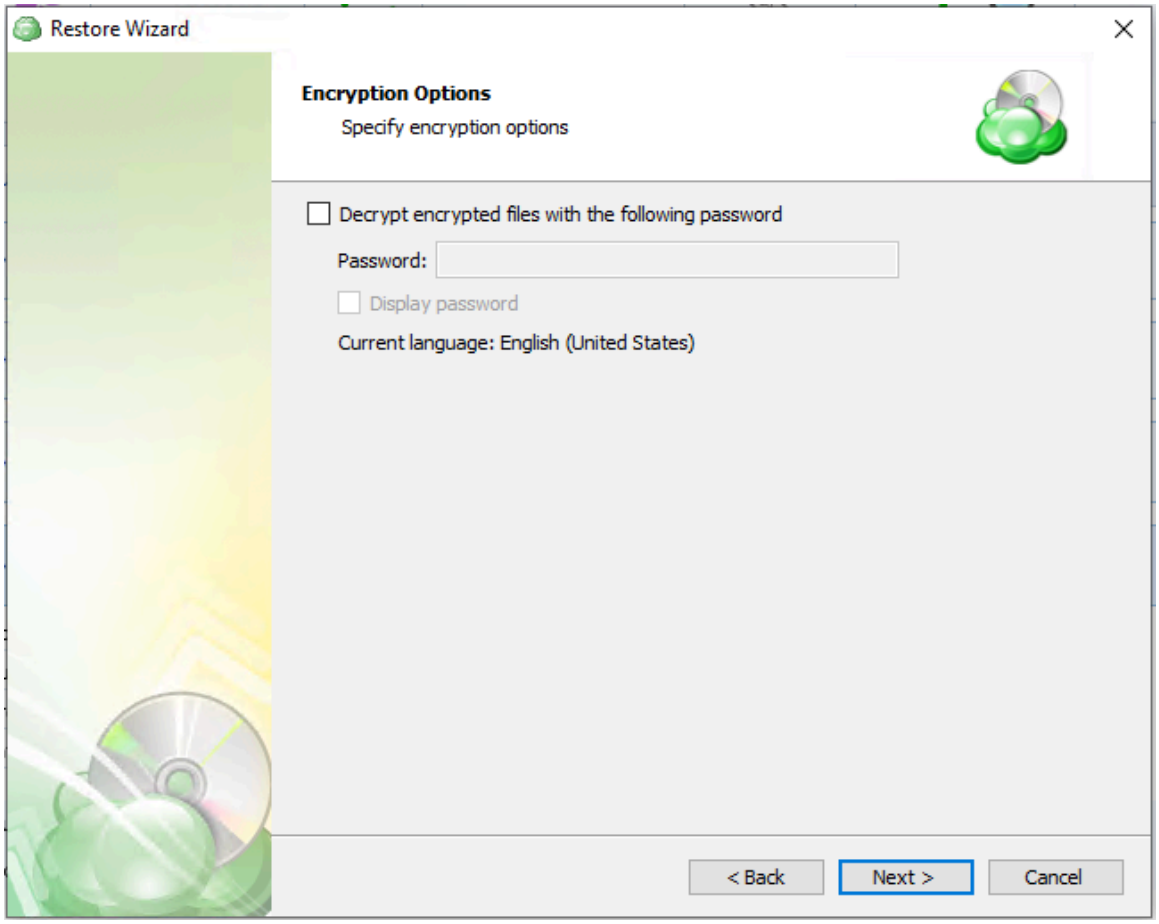
Step 8. Select the database backup which you would like to restore.



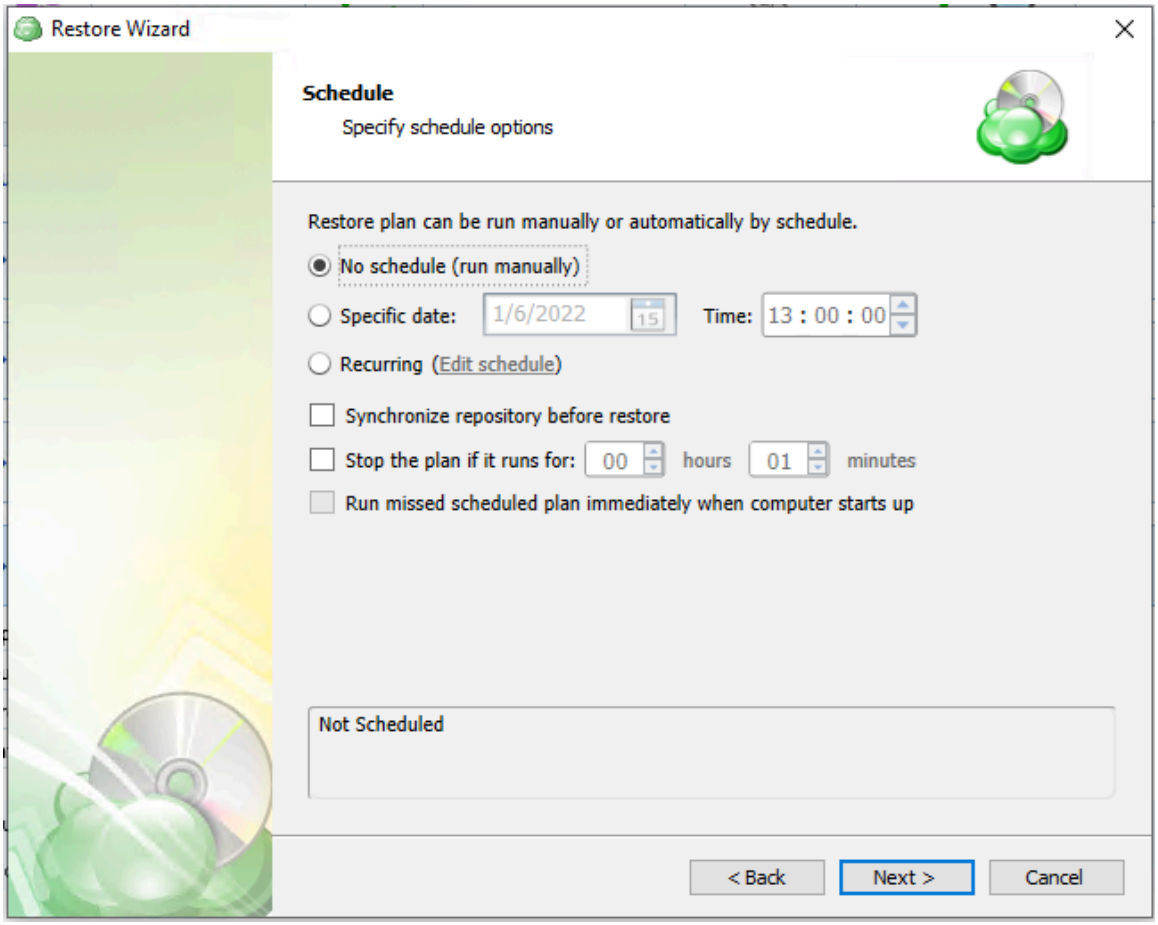
Step 9. The next step asks you to provide the paths the database files will be restored to.



Step 10. Next the application will prompt you to enter the credentials used if the backup was encrypted. If it was not encrypted, simply click “Next”.



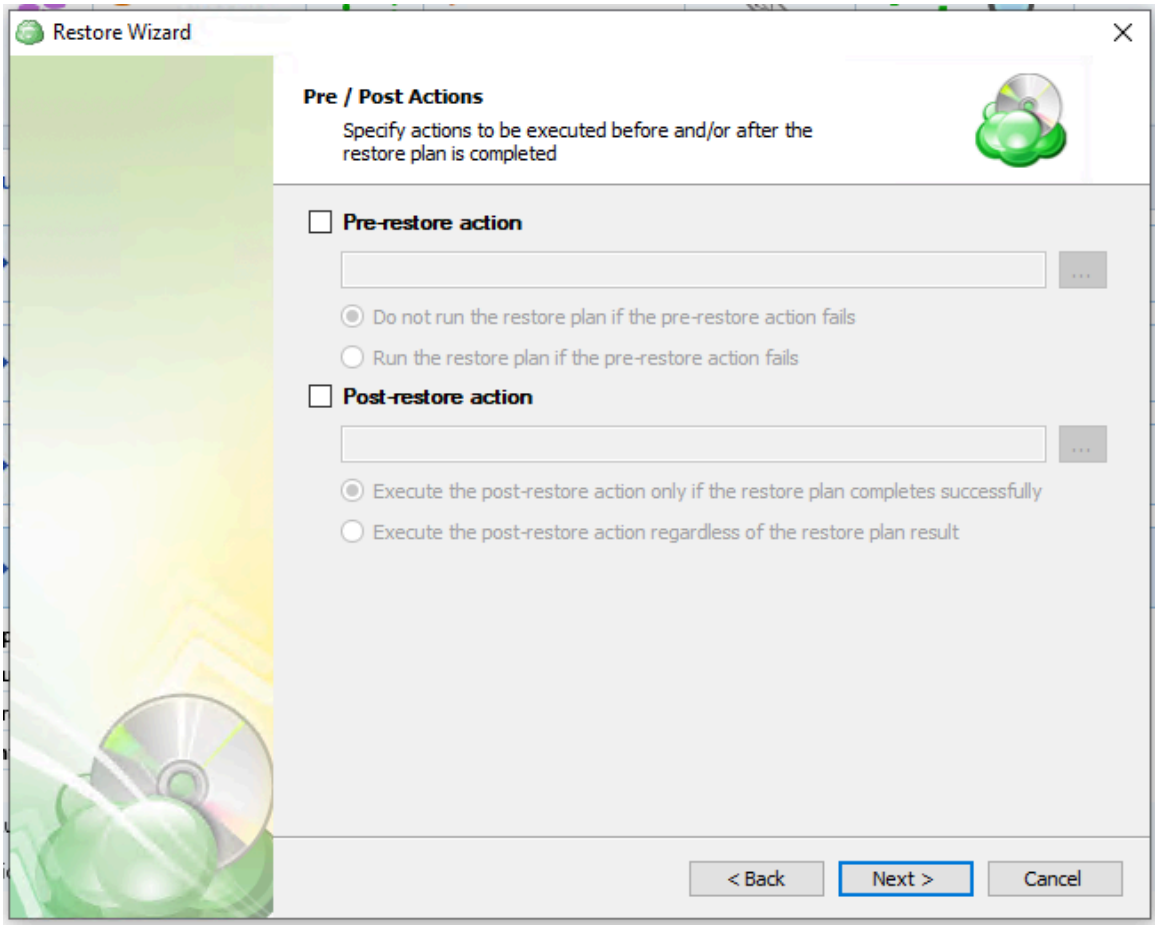
Step 11. Next you are prompted to set the schedule for your restore plan which will allow it to run autonomously, or you are able to select “No Schedule” for it to remain a manual process.



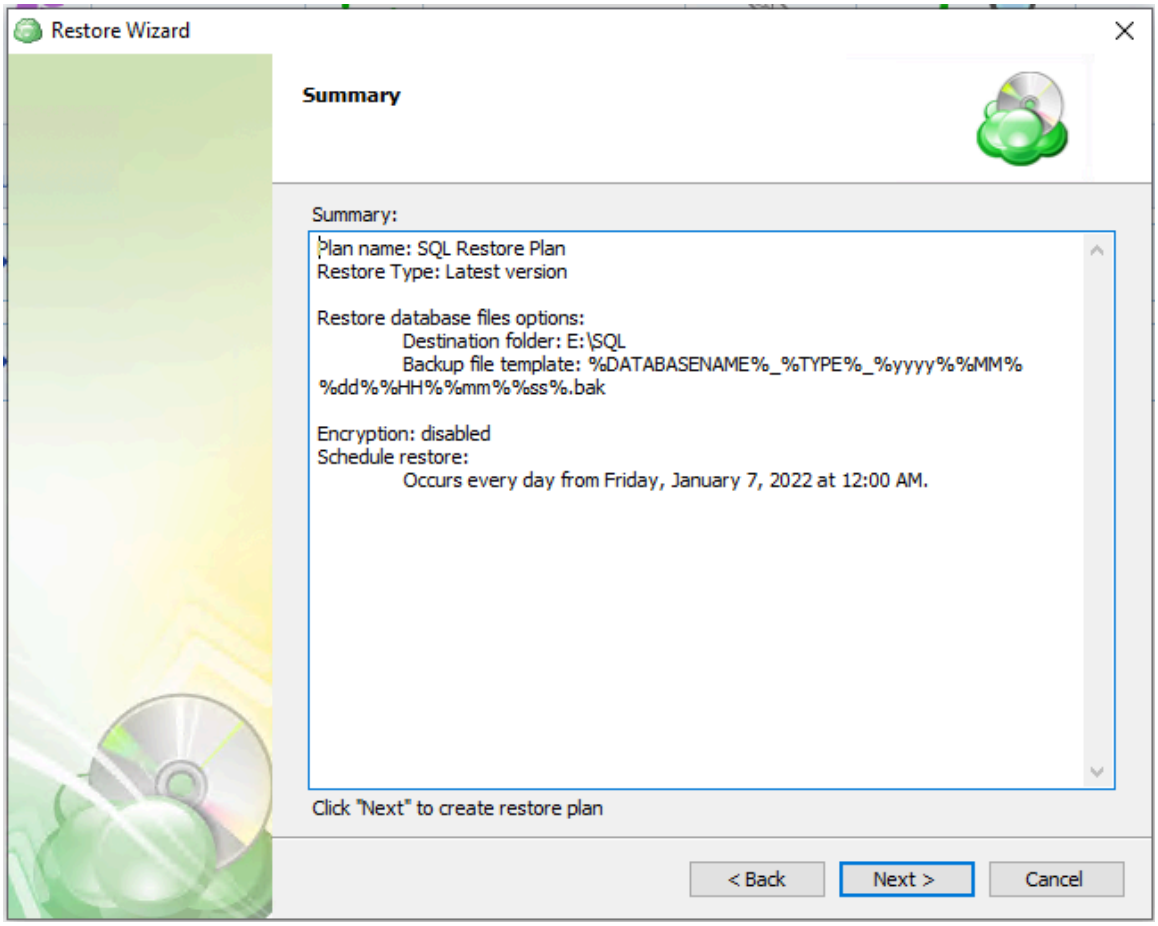
Enabling the “Run missed scheduled backup immediately when computer starts up” option will ensure that the backup process begins automatically upon startup if the last backup was not able to start at the scheduled time for any reason. This option is recommended for Desktops and Laptops.

Do not use the “Stop the plan if it runs for:” option if you have a slow or unstable internet connection.

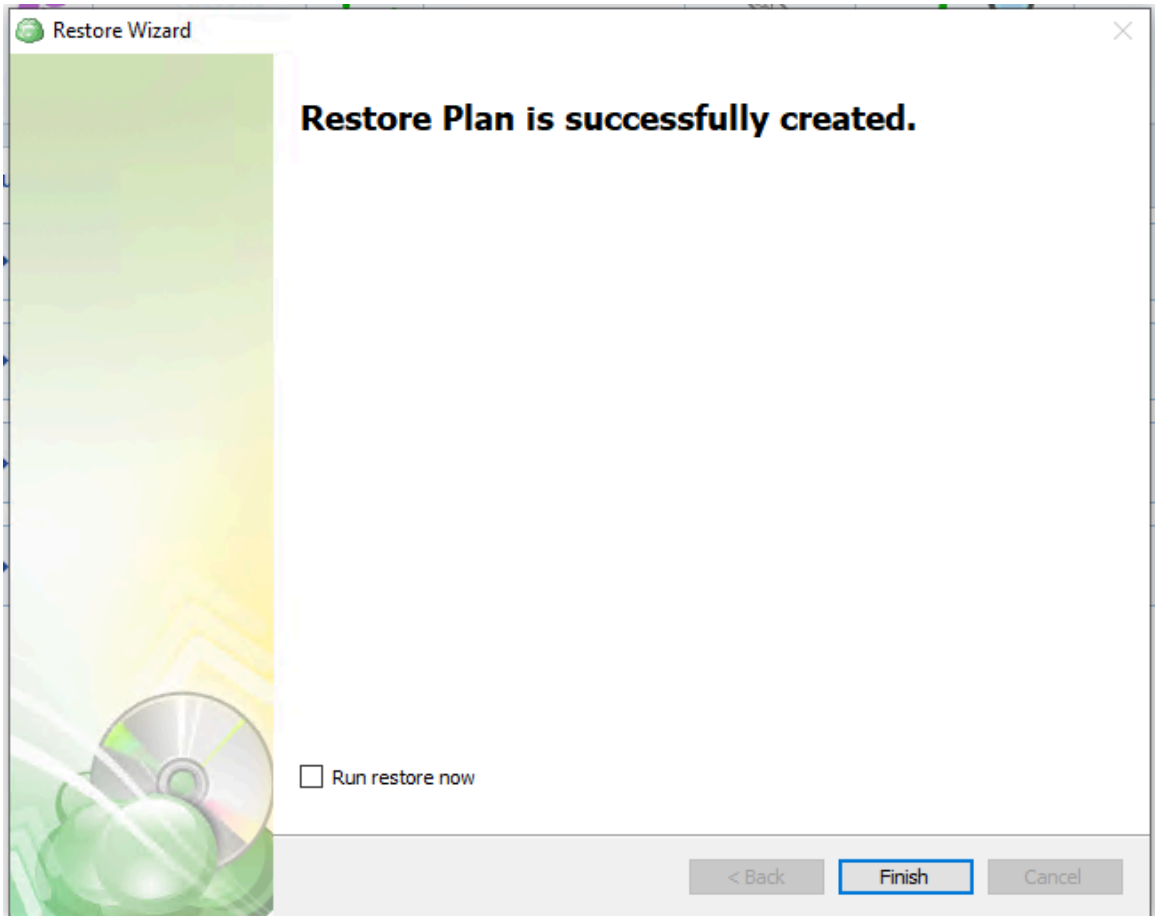
Step 12. The **Pre/Post Actions** page allows the execution of custom scripts before and/or after the running of a backup task.



Step 13. The next step of the Wizard displays a summary of the selections made throughout the process. Once you have reviewed your selections, click “Next”.

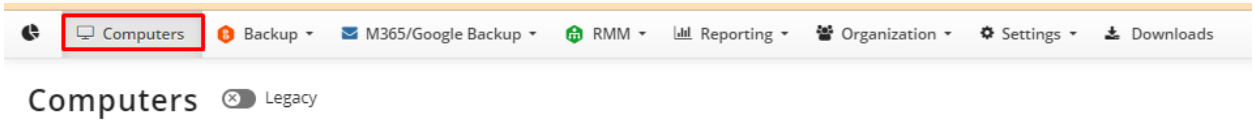


Step 14. After clicking next on the previous step, the Restore Plan is created. The final step is to acknowledge this and determine whether to run the backup immediately or for it to wait until the next scheduled occurrence.



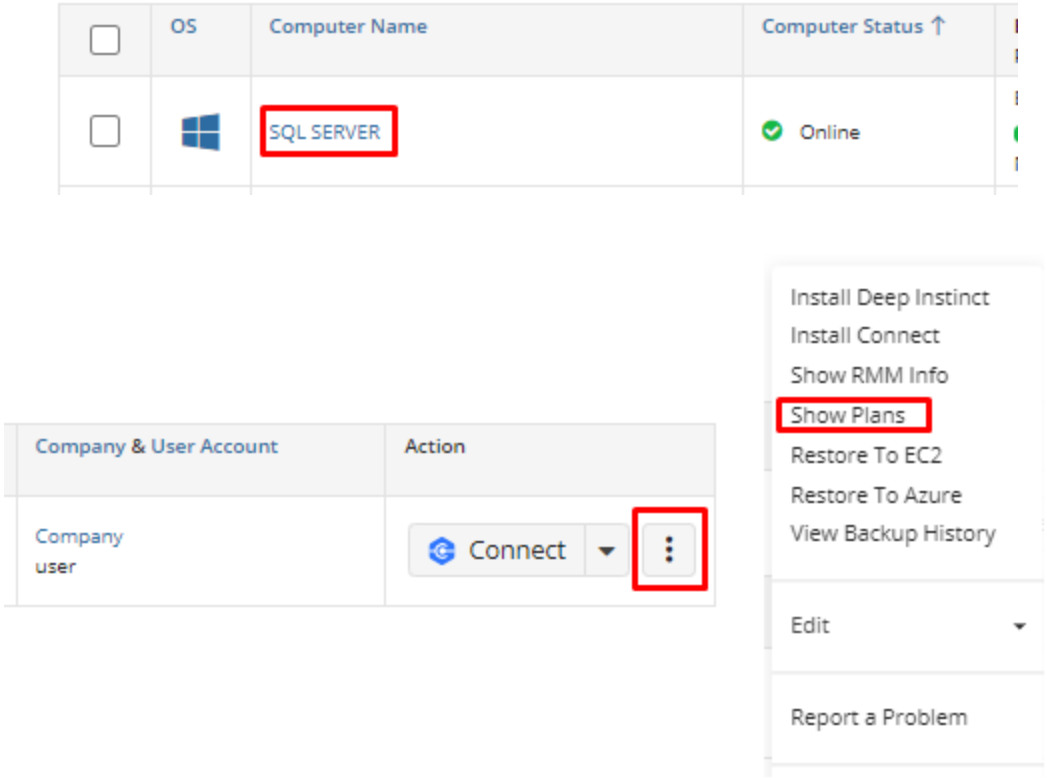
Restore Database files using MBS

Step 1. From the MBS Portal, left-click Computers on the menu.

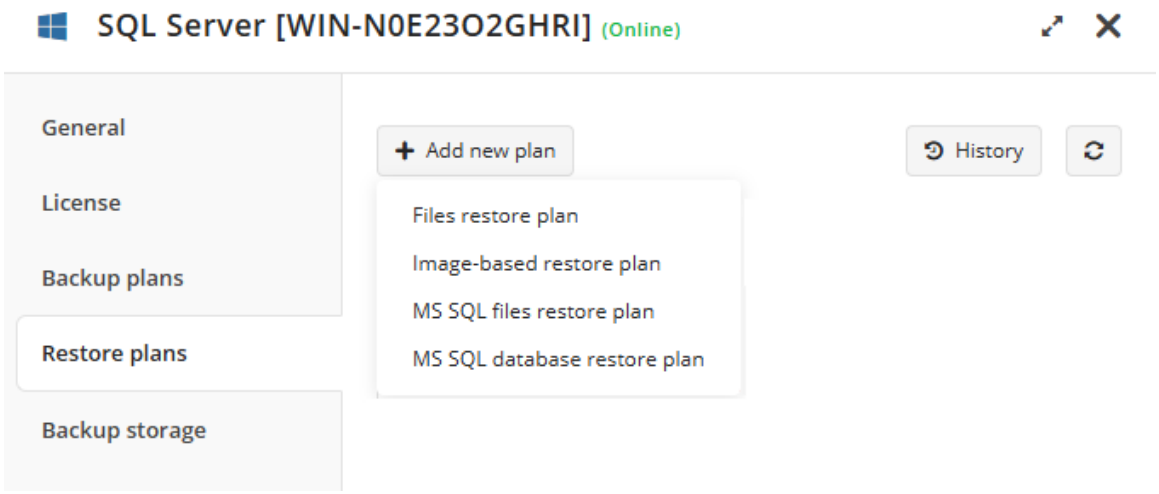


Step 2. Find the computer hosting the MS SQL instance to which you want to restore a previously backed up database or databases.

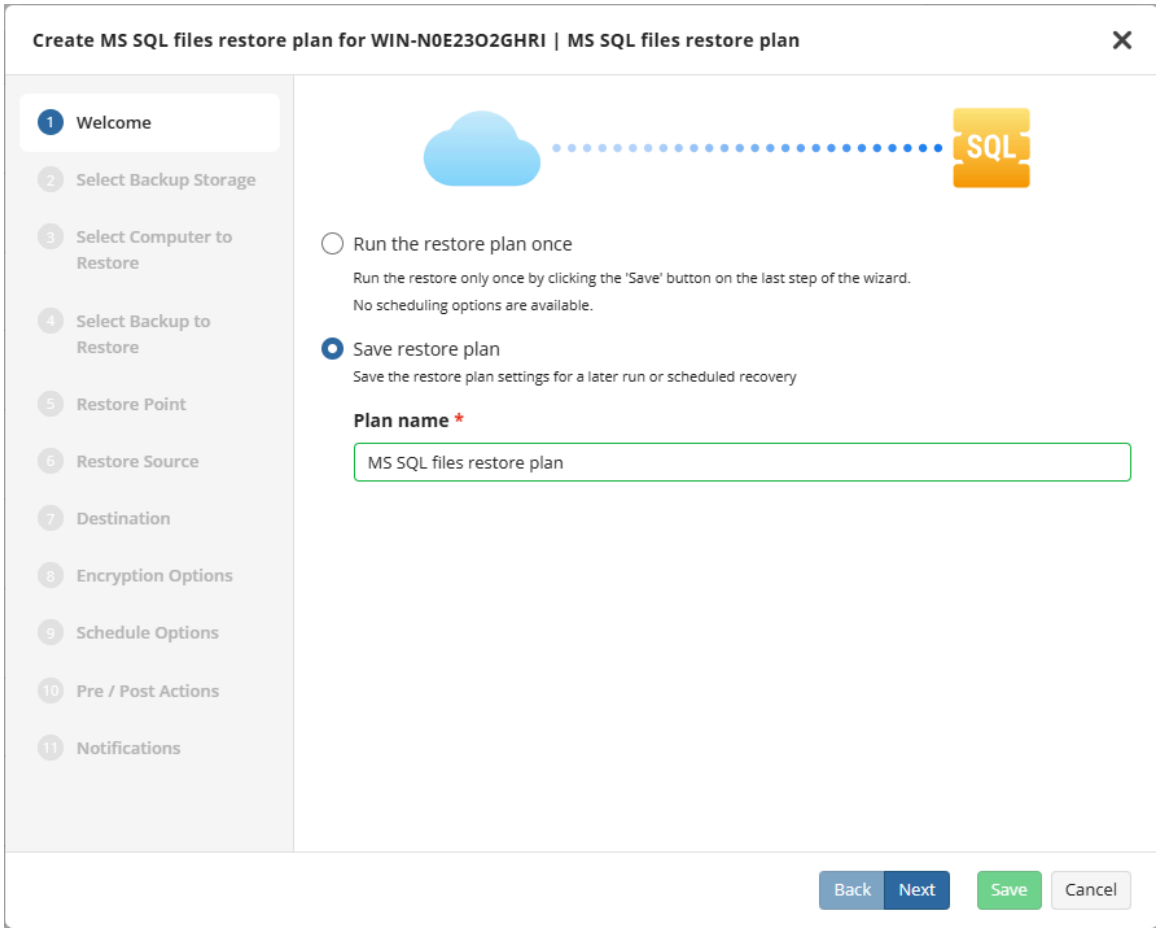
Click on the computer name or select "Show Plans" from the three-dot drop-down menu.



Step 3. In the side panel, navigate to the “Restore Plans” section. Click on the “Add New Plan” button and select “MS SQL Files Restore Plan” from the drop-down menu.



Step 4. The first step when creating a new MS SQL restore plan is to decide whether to run it a single time immediately after plan creation, or give it a name and save it for later.

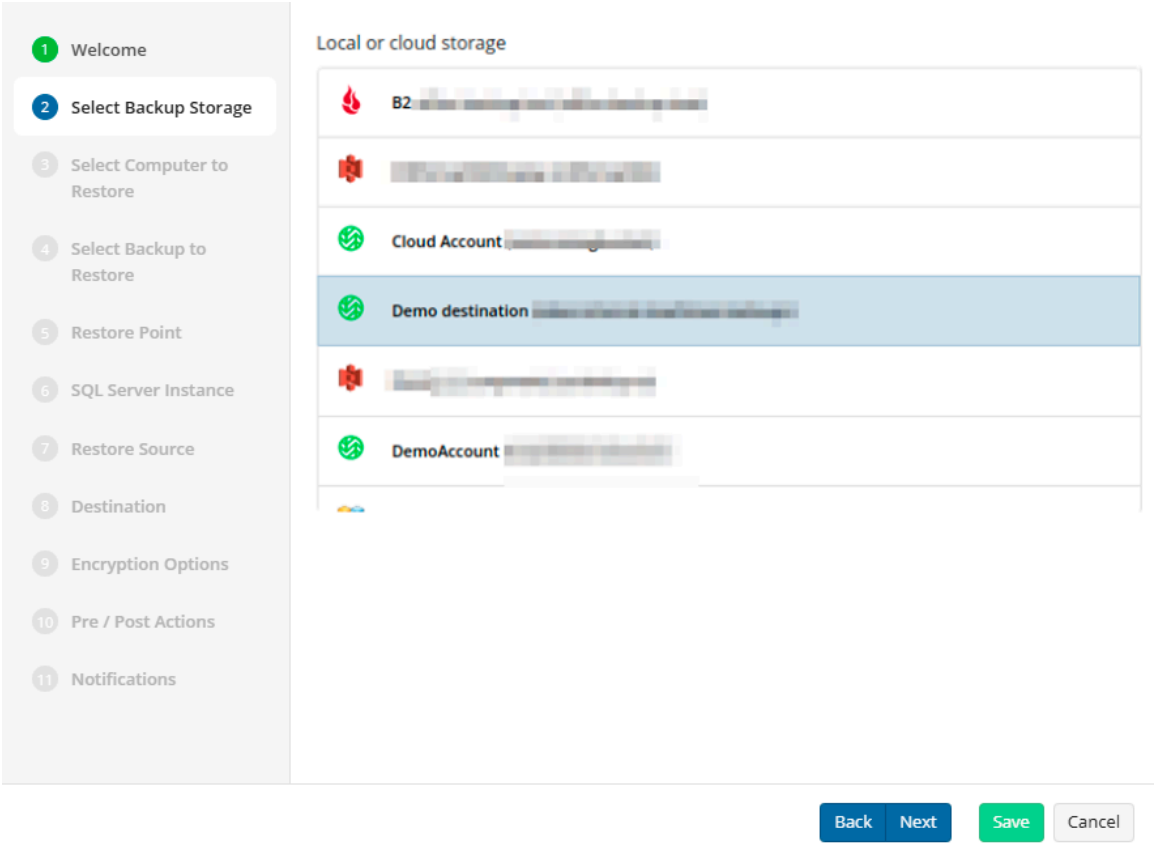


"Run restore once" will execute the restore immediately upon completing the wizard.

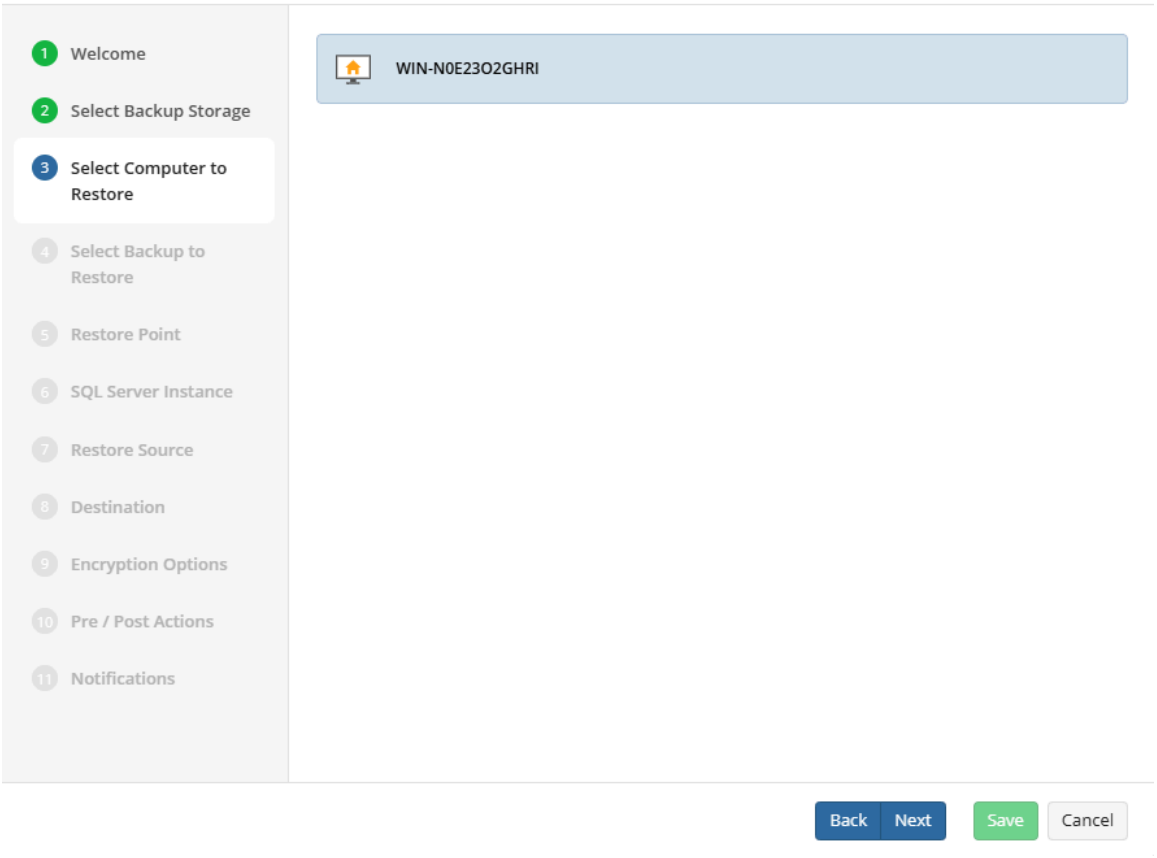
"Save restore plan" will allow you to schedule the plan to run at a later time and also schedule repeating restorations if needed.

It is recommended to use a descriptive name which will distinguish the plan from others.

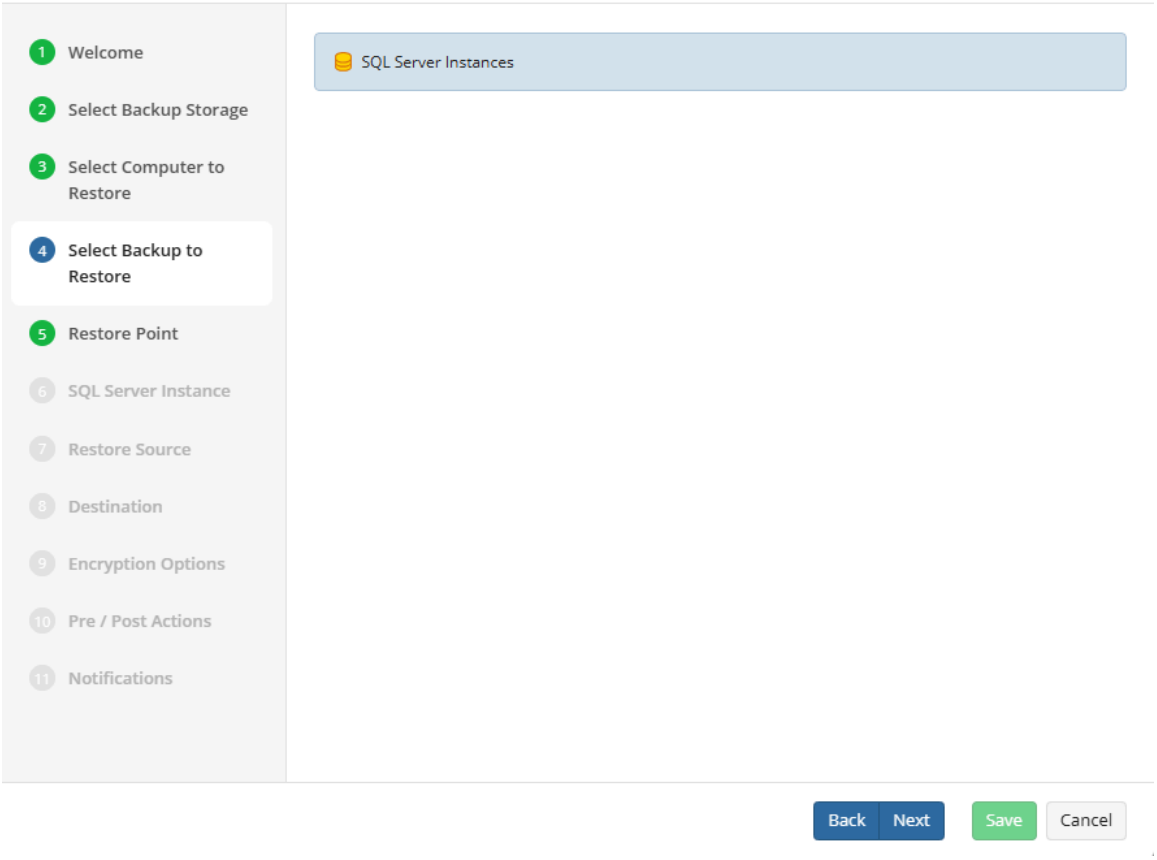
Step 5. Next, select the storage which contains the desired data.



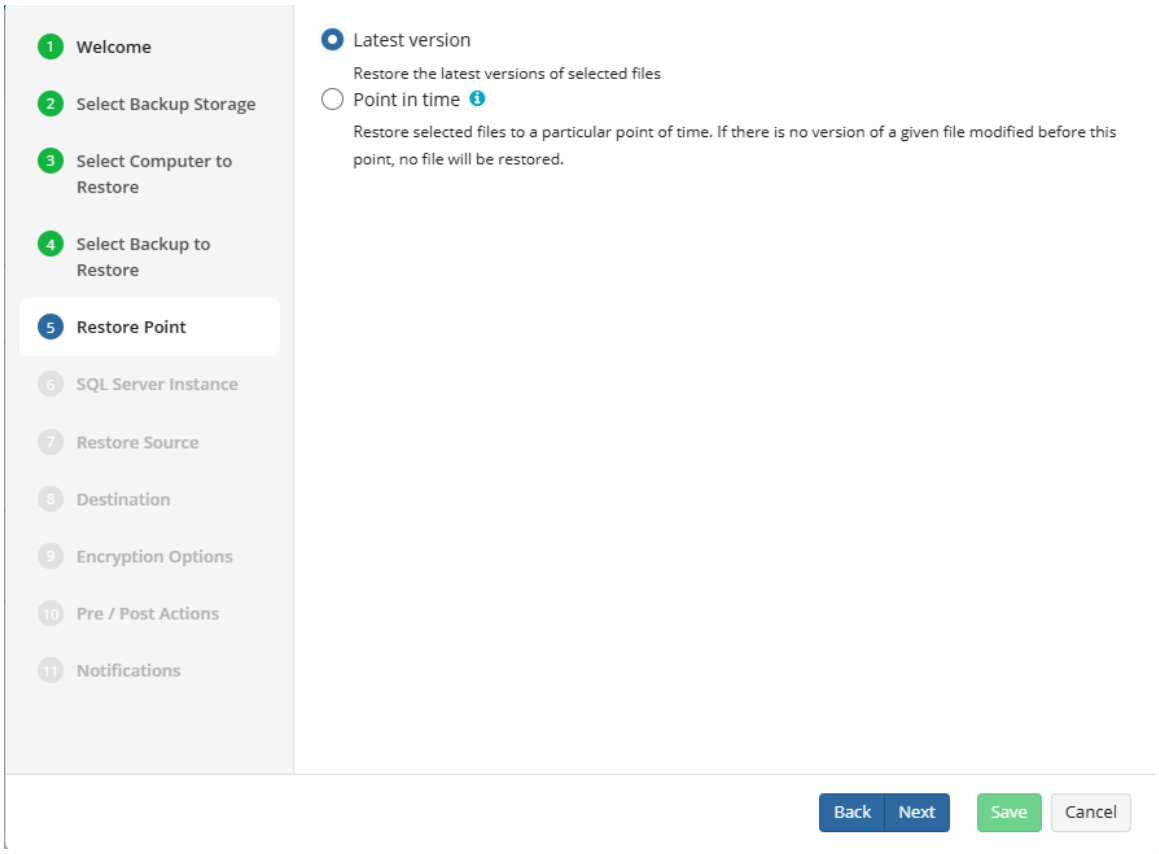
Step 6. With the Backup Storage selected, the next step is to select the computer associated with the backup which you would like to restore.



Step 7. Next, you will be presented with a list of available backup types for the selected host. Select the “SQL Server Instances” option to continue.

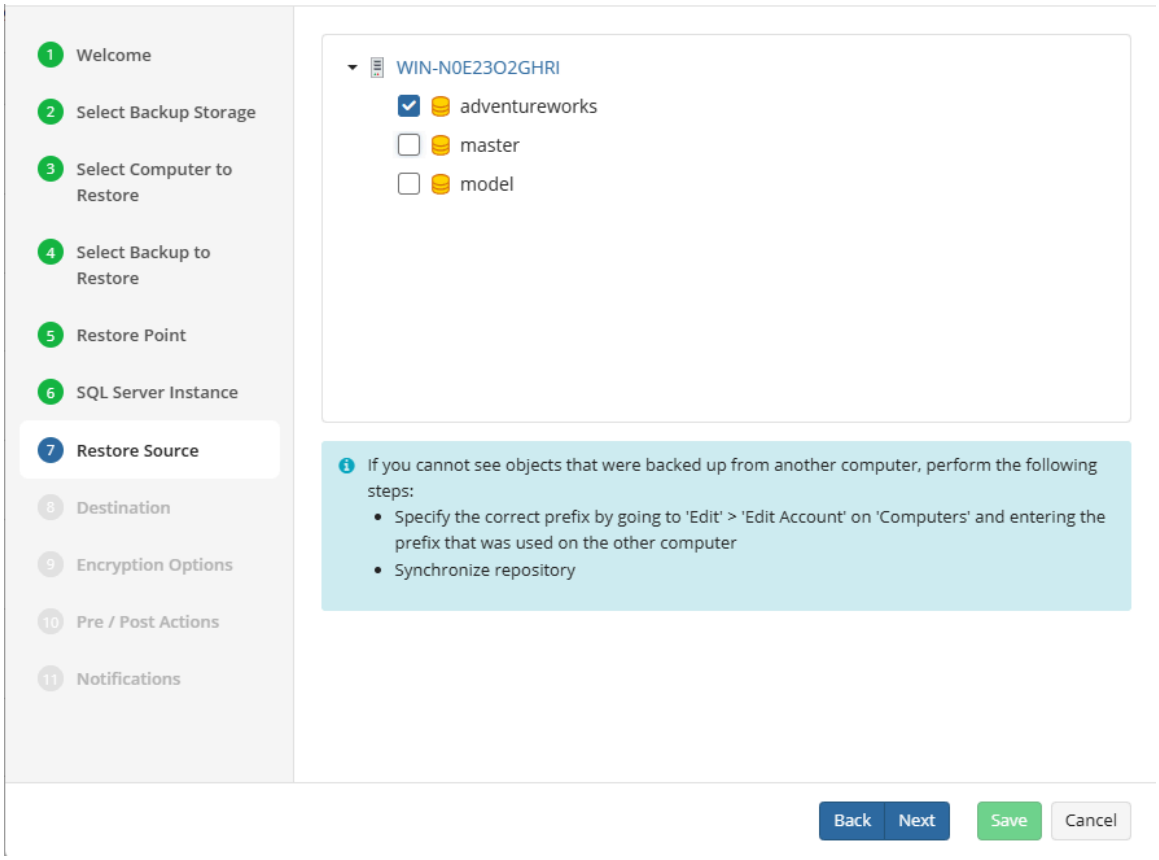


Step 8. The next step is to select the desired point in time to restore to.

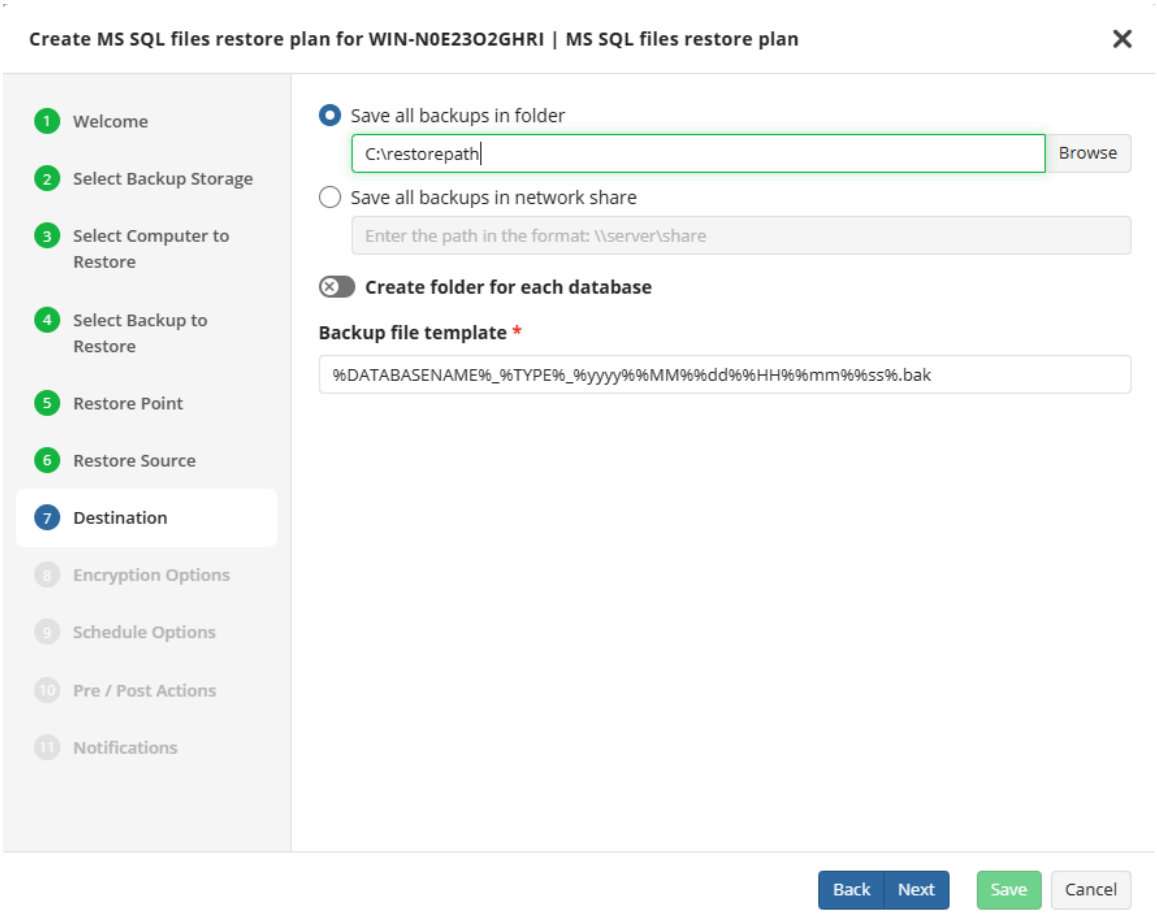


If there is no exact match for the point in time selected, the application will automatically select the closest previous restore point.

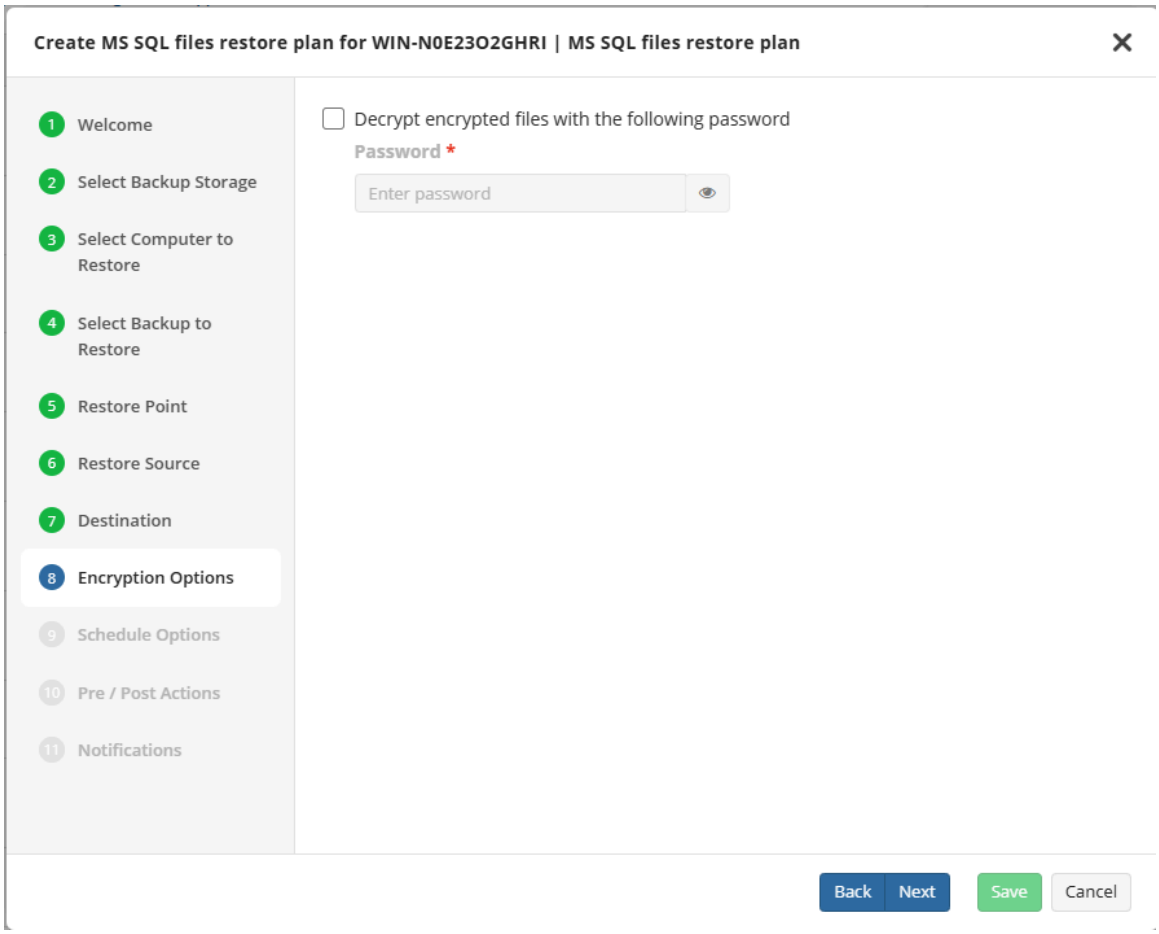
Step 9. Next, select which database to restore.



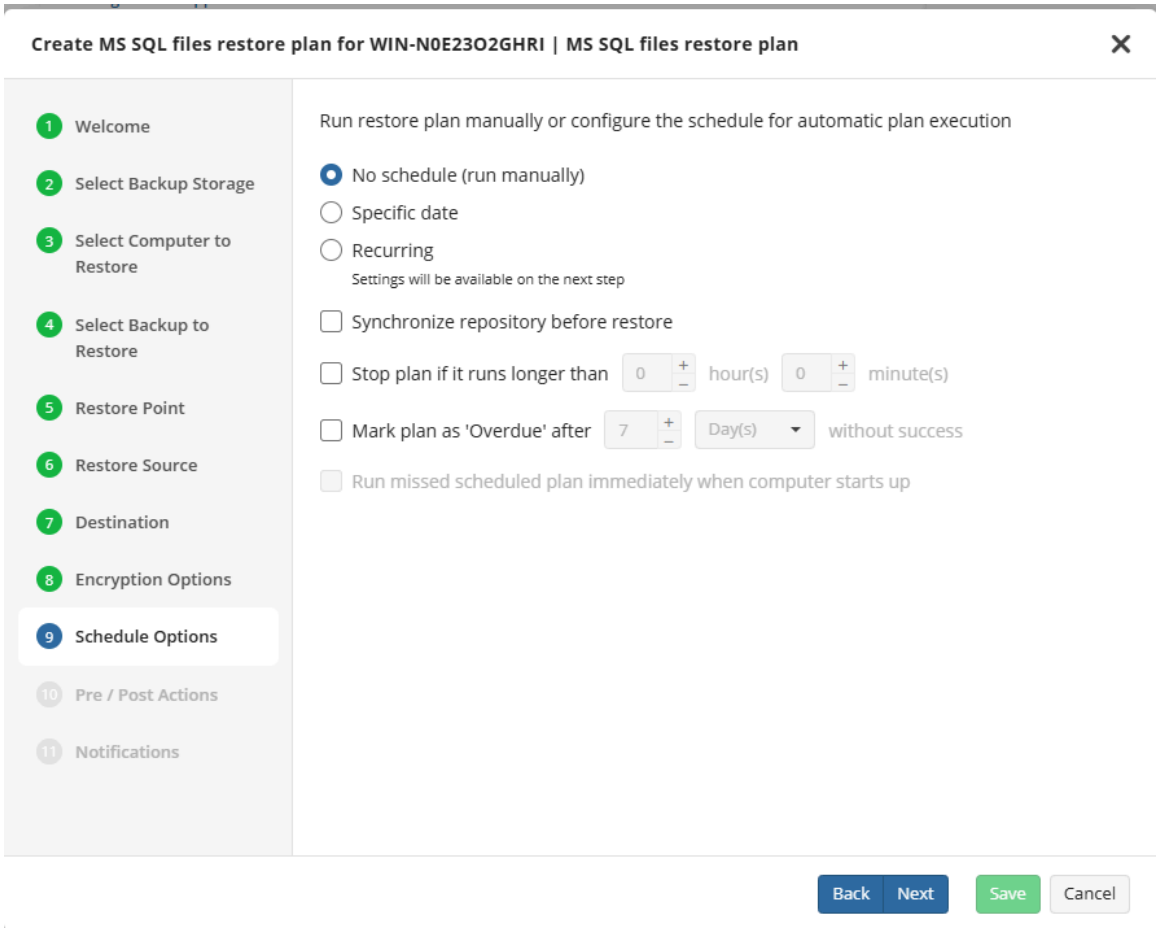
Step 10. The next step asks you to provide the paths the database files will be restored to, and you will be given options to overwrite an existing database or restore the database with a new name.



Step 11. If the backed up data was encrypted, the next step will be to enter the password for decryption. If the password is incorrect or missing, the restore plan will fail and you will need to edit the plan to input the correct password.

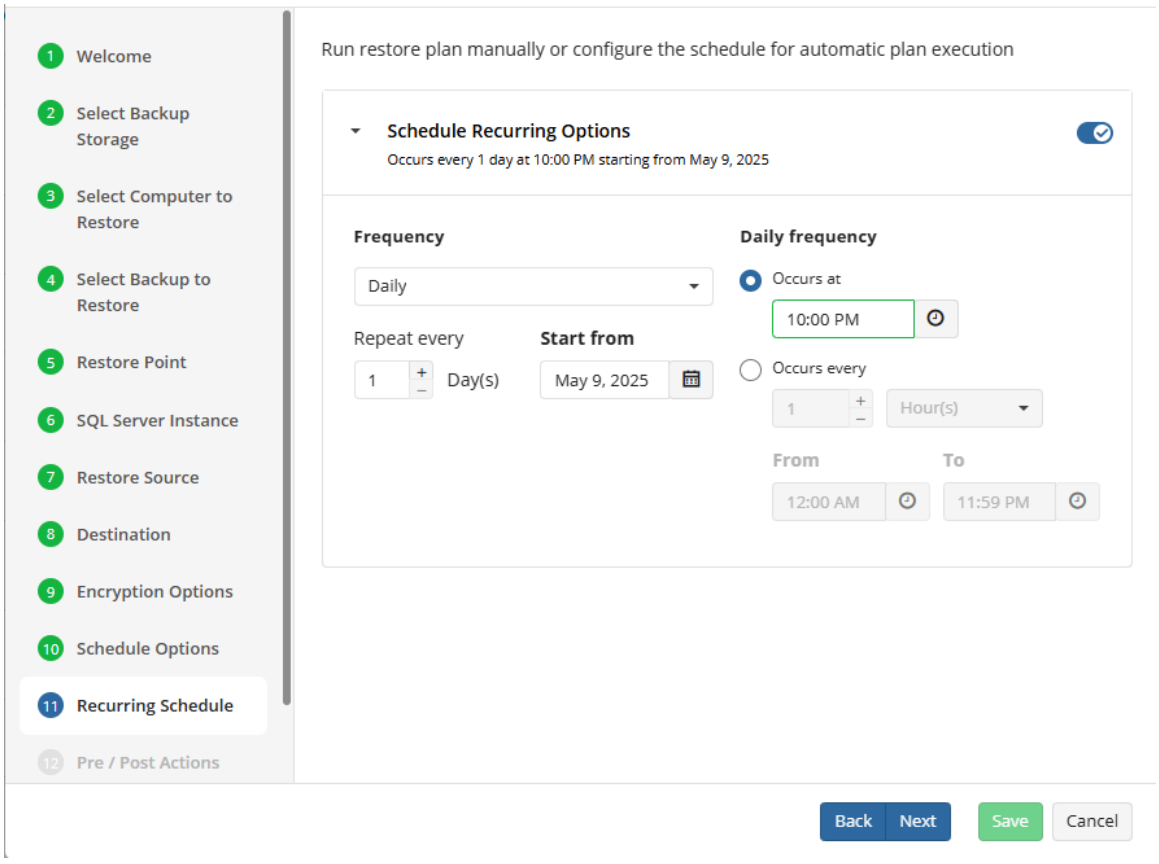


Step 12. Next, if you opted to save the restore plan, the next step is to specify how the plan should be triggered.

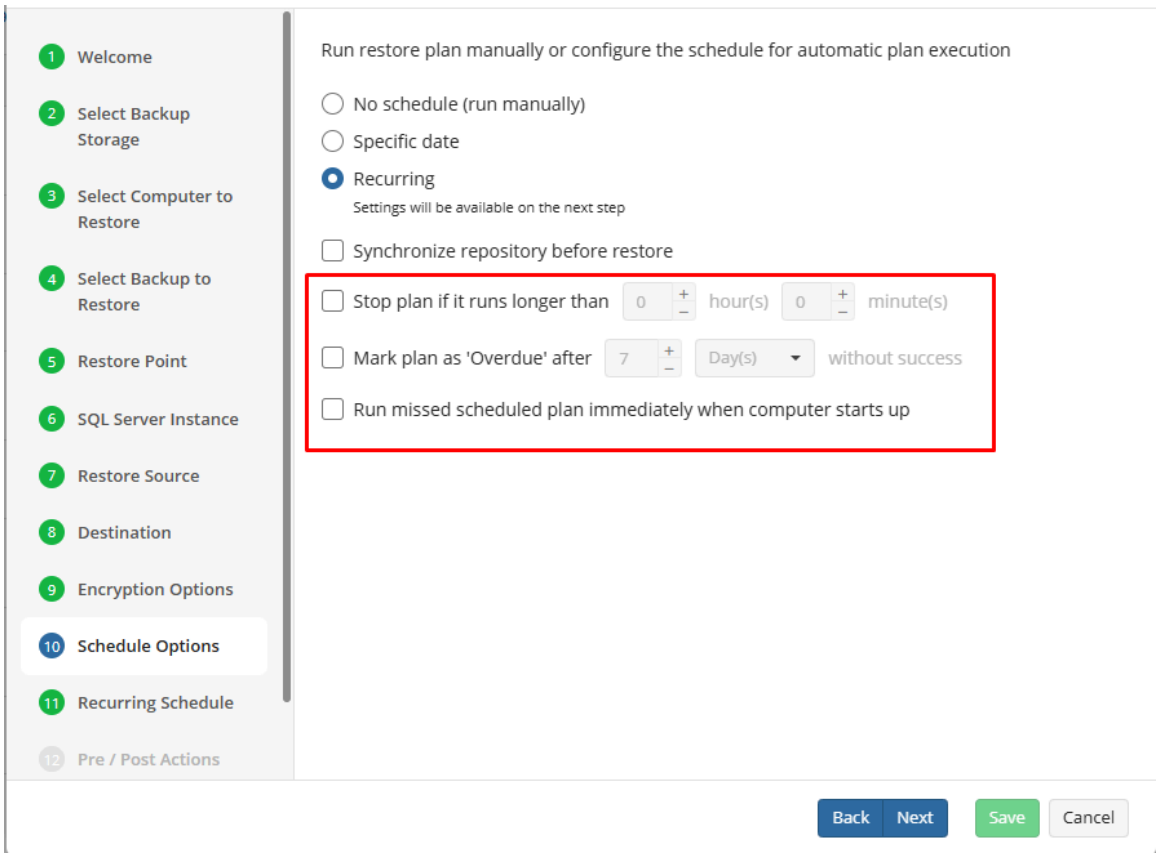


- **No schedule (run manually):** Use this option only when you wish to execute the Restore manually.
- **Specific date:** Use this to schedule a one-time Restore at the specified date and time.
- **Recurring:** Using this option enables you to schedule recurring Restorations based on the criteria in the following step.

Step 13. With “Recurring” selected on the previous step, you are then prompted to define the time and frequency the plan should execute.



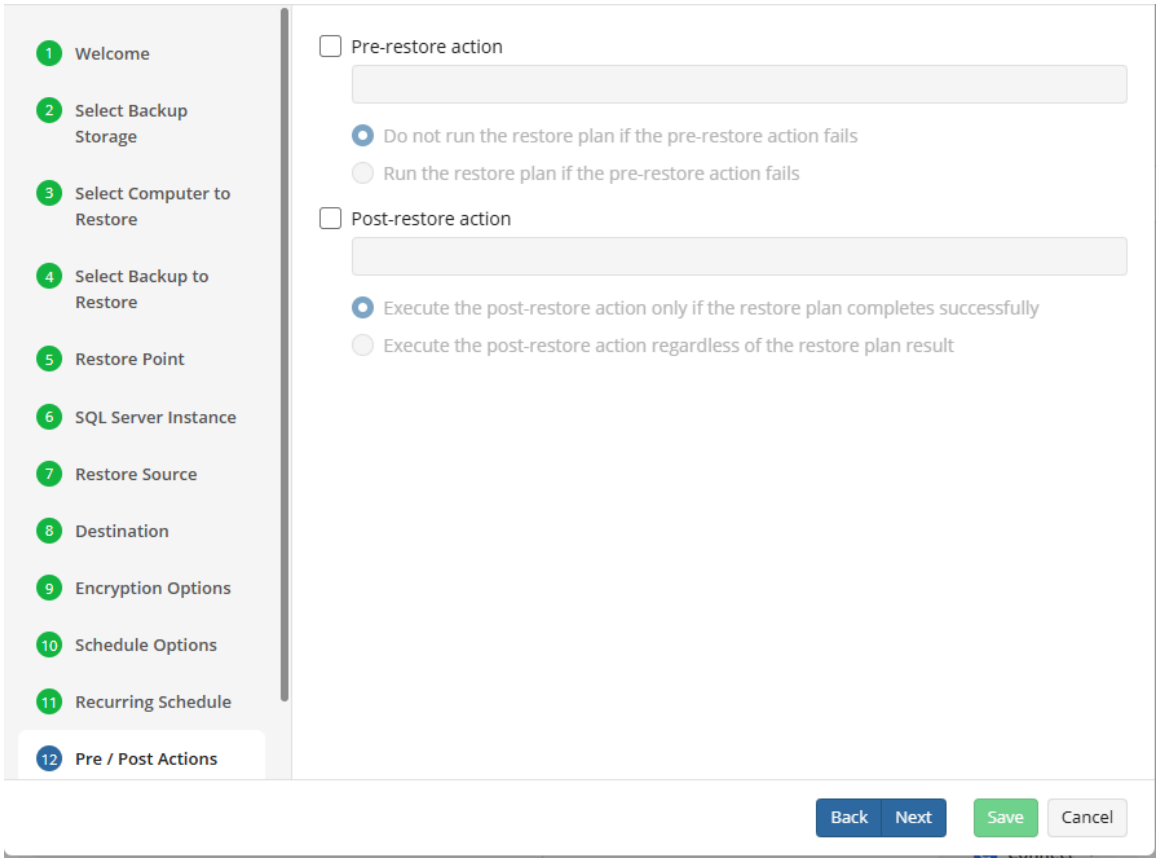
In addition to scheduling the restore, other options are available regarding notification and management of long running or missed plans.



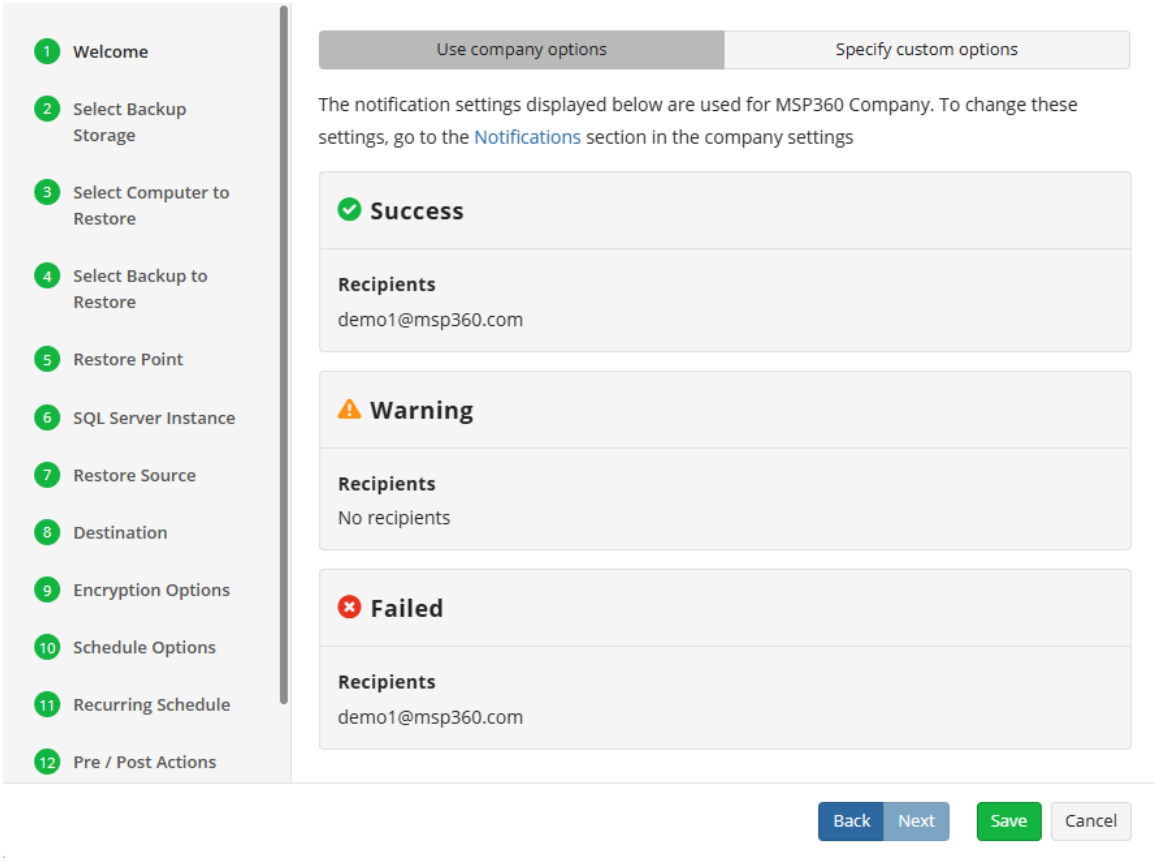
Do not use the "**Stop the plan if it runs for:**" option if you have a slow or unstable internet connection.

Enabling the "**Run missed scheduled restore immediately when computer starts up"** option will ensure that the restore plan will begin automatically after the computer starts up if it was unable to run at the scheduled time. This is only recommended for desktops and laptops. For servers, it is recommended that you run the restore plan manually when all maintenance works are completed to avoid adversely affecting server performance and internet bandwidth during working hours.

Step 14. The **Pre/Post Actions** page allows the execution of custom scripts before and/or after the running of a backup task.



Step 15. The final step is to review the Notifications and Logging. The default settings applied at the Company level are selected by default, however you are also able to specify custom options per plan.

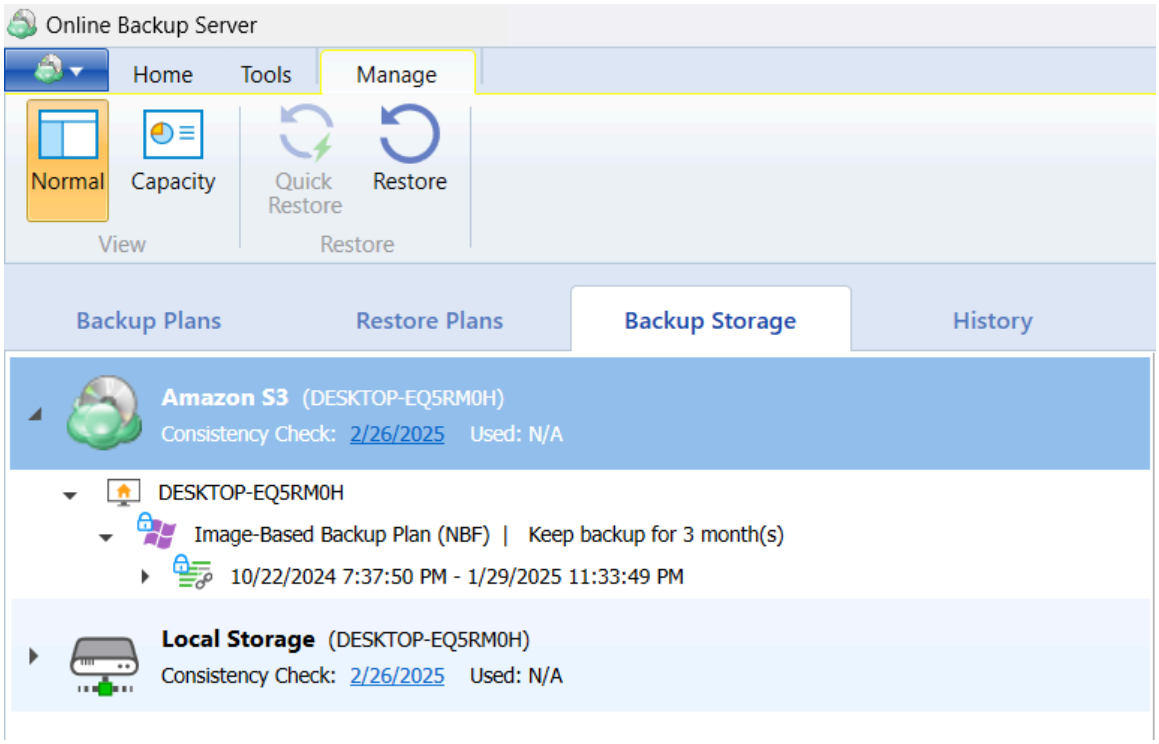


Step 16. Click on Save when you are happy with your selections. If the plan is set to run only a single time and has no set schedule, it will automatically start. Otherwise, if it is set to run only once and is scheduled, it will display in the list of plans until the scheduled time. If it is only set to run once, then when it completes successfully it will remove itself from the list of plans. Only Restore Plans which are saved will remain in the list for future use.

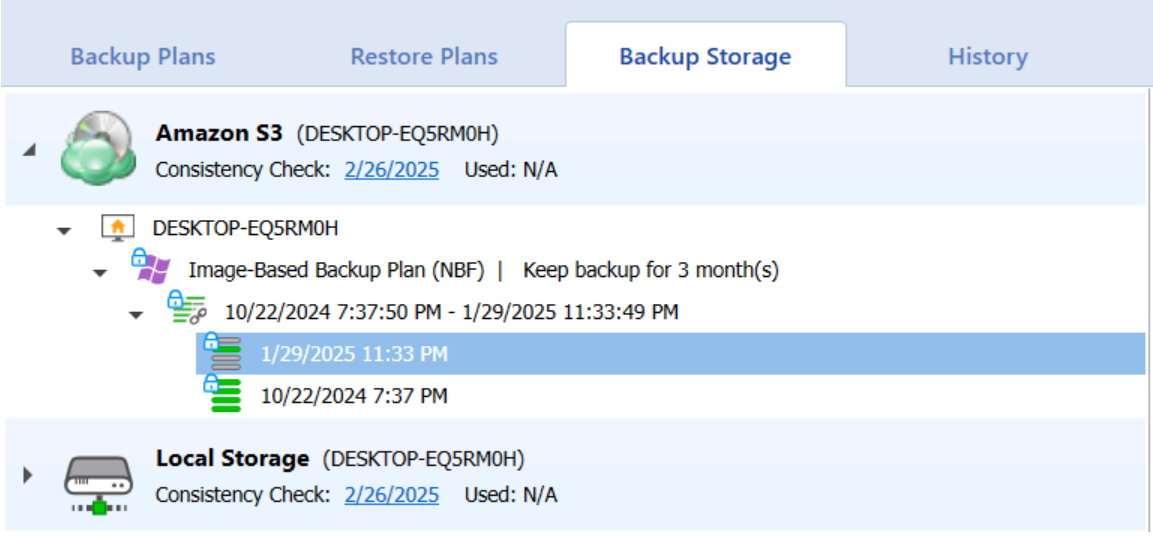
Item-Level Restore

Restore Items from an Image, File, or VM Backup using the Agent

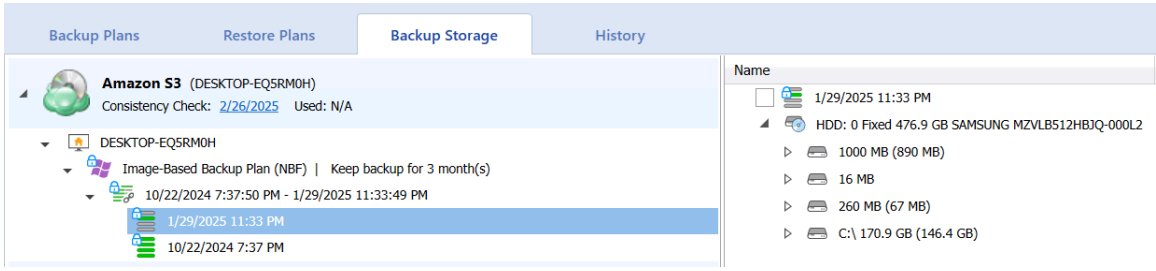
Step 1. Launch the Managed Backup, then navigate to Backup Storage tab. Select your storage account, then open the list of plans for the computer and select “Image Based”.



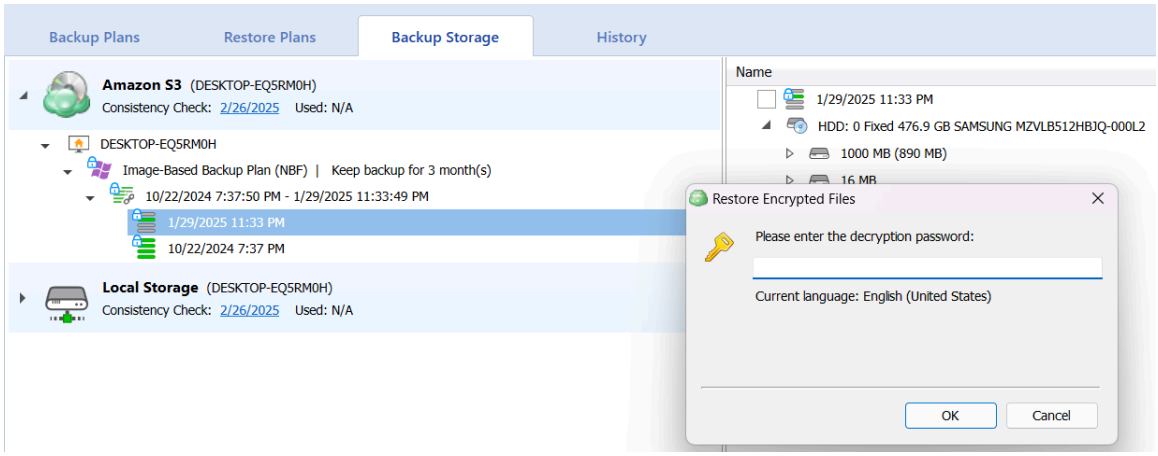
Step 2. Select the generation and restore point (date) you want to restore a file or folder from.



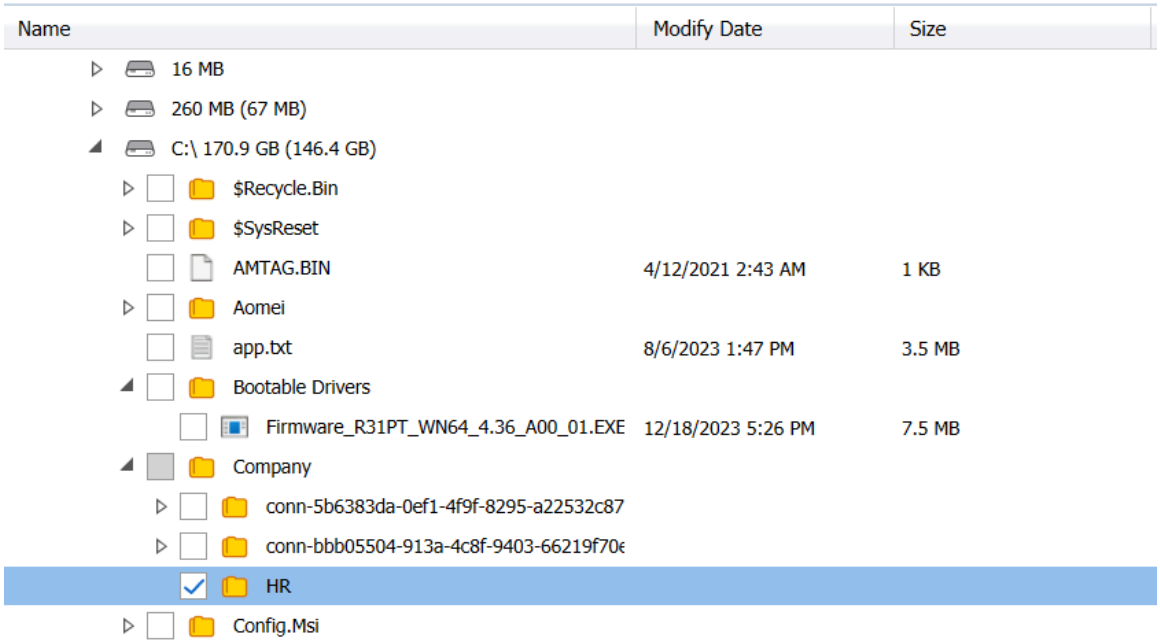
Step 3. A list of volumes that are included in the system image backup will be displayed.



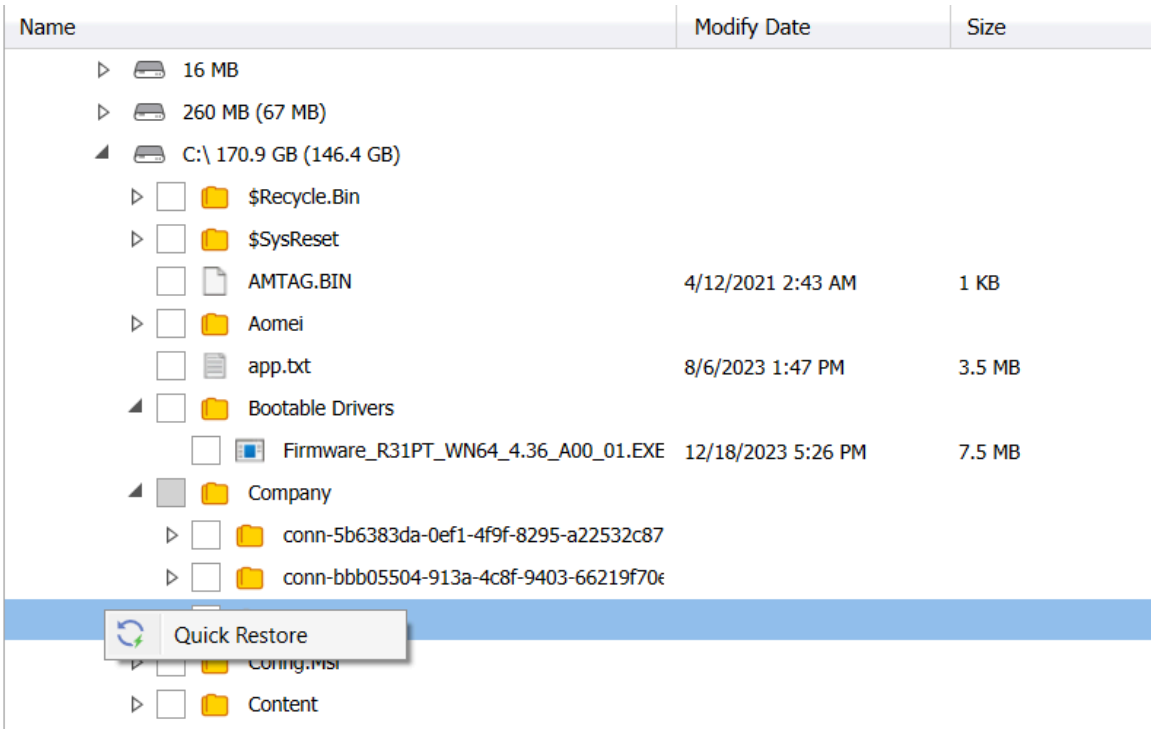
Step 4. Expand the volumes and find the individual files that you would like to restore from the Image-Based backup. If your backup was encrypted, you need to enter the password to view the available folders and files.



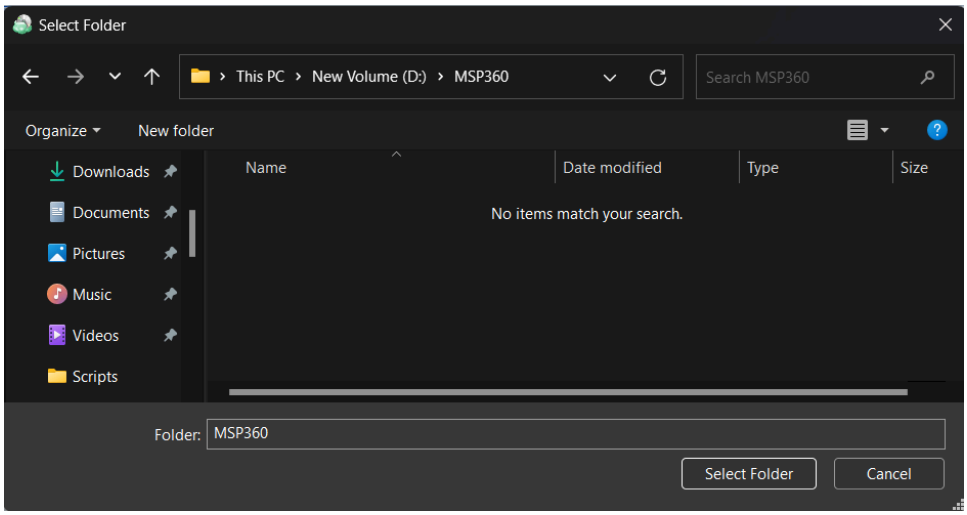
After entering the right password, you can expand the folders and select a file or folder you would like to restore.



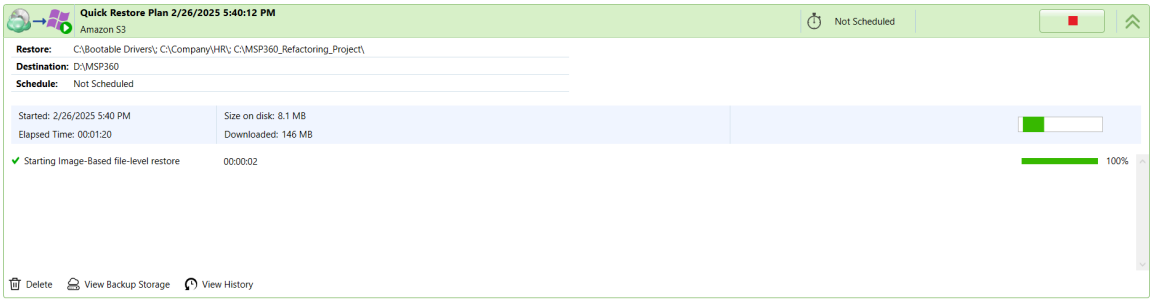
Step 5. You can select multiple files or folders, then right-click to proceed with “Quick Restore”.



Step 6. Select the location where you want to restore the files to and click OK.



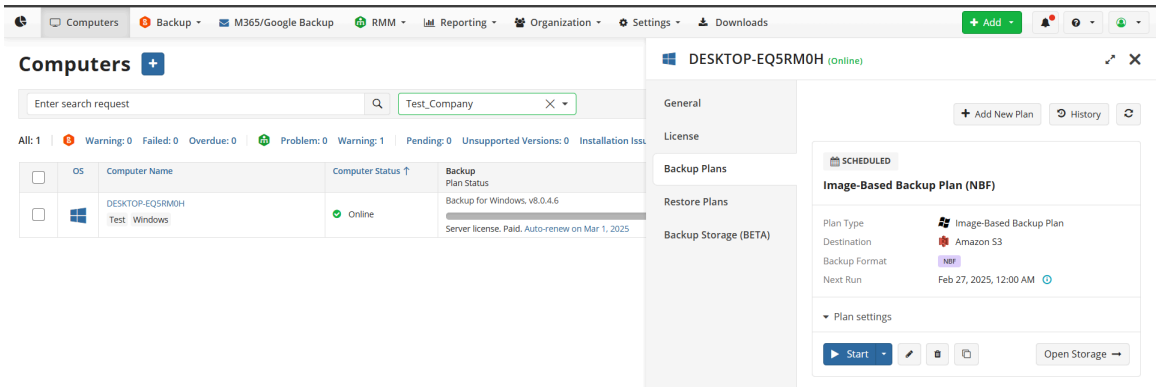
Step 7. You will be automatically redirected to the Restore Plans tab where you will see the progress of your Quick Restore job.



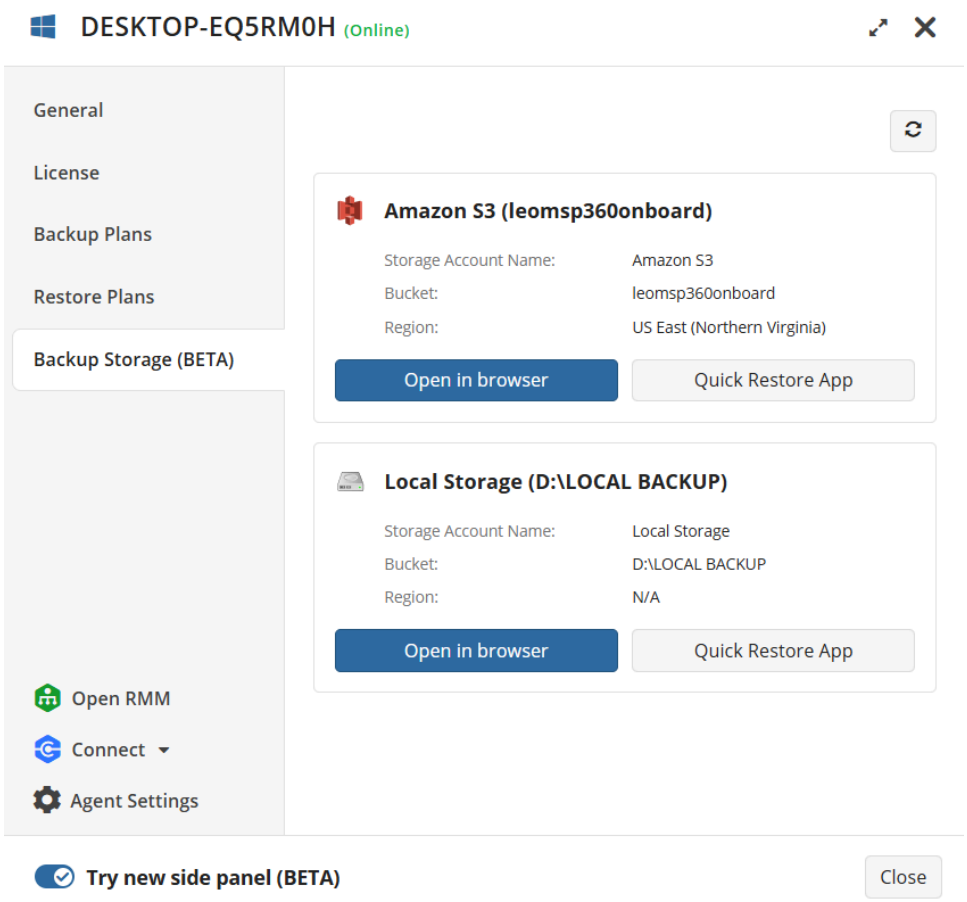
If the plan fails, it will remain in the Restore Plans tab displaying the cause and the error code. If the Quick Restore job completes successfully, the restore plan will automatically disappear and you can view the restored data.

Restore Items using the Quick Restore App

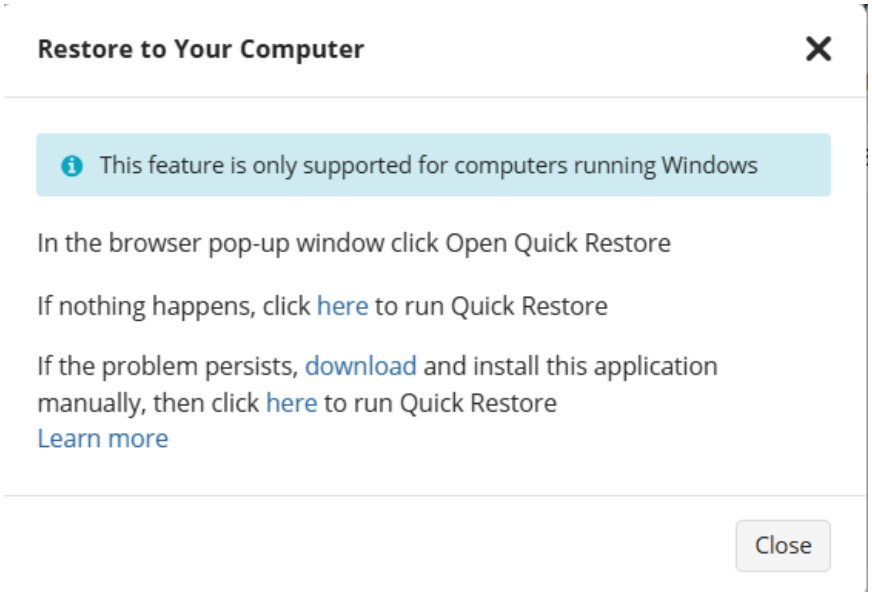
Step 1. Navigate to the MBS Portal and select the “Computers” page on the main menu. Locate the computer which backup dataset you wish to restore from and click on the name of the computer or the backup status bar.



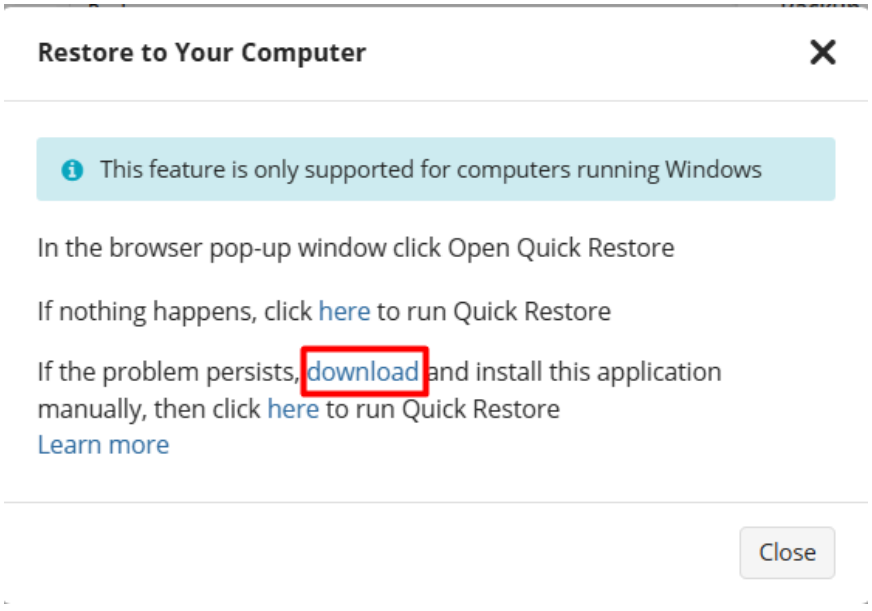
Step 2. Select the “Backup Storage (BETA)” tab and then click on the "Quick Restore App” button for the storage account you want to restore from.

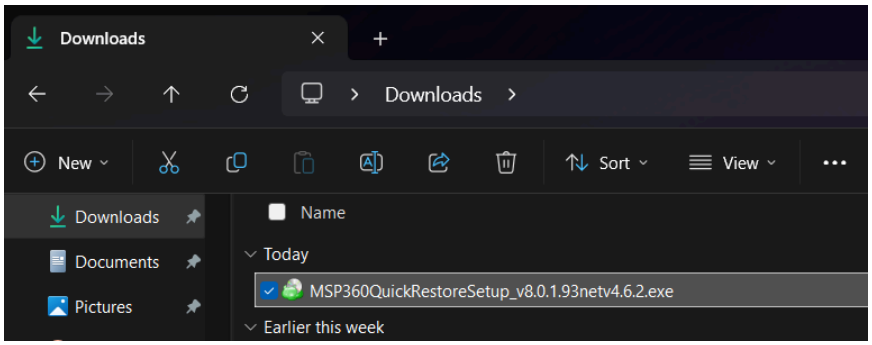


Step 3. You should see a pop-up dialog suggesting to run or download the Quick Restore app.

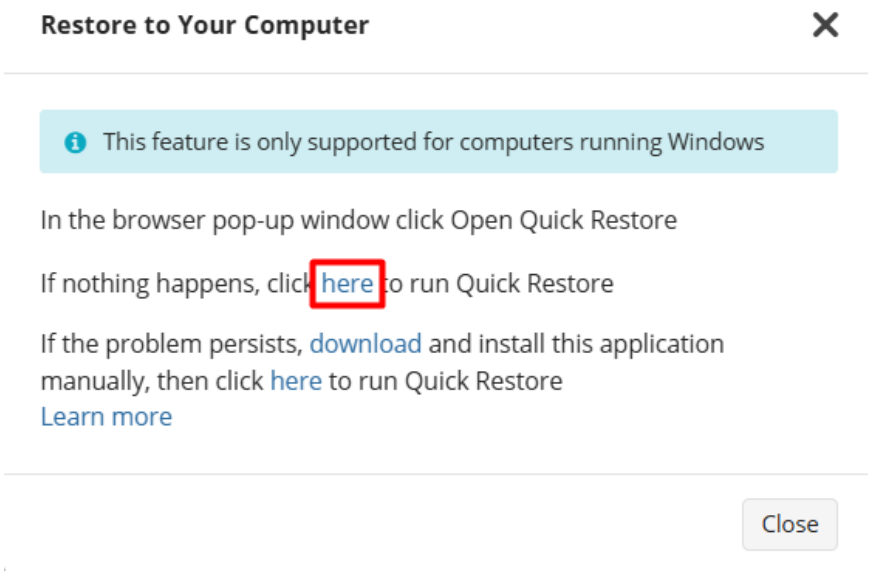


If this is the first time you are launching the Quick Restore, please make sure to download and run the installer file first:

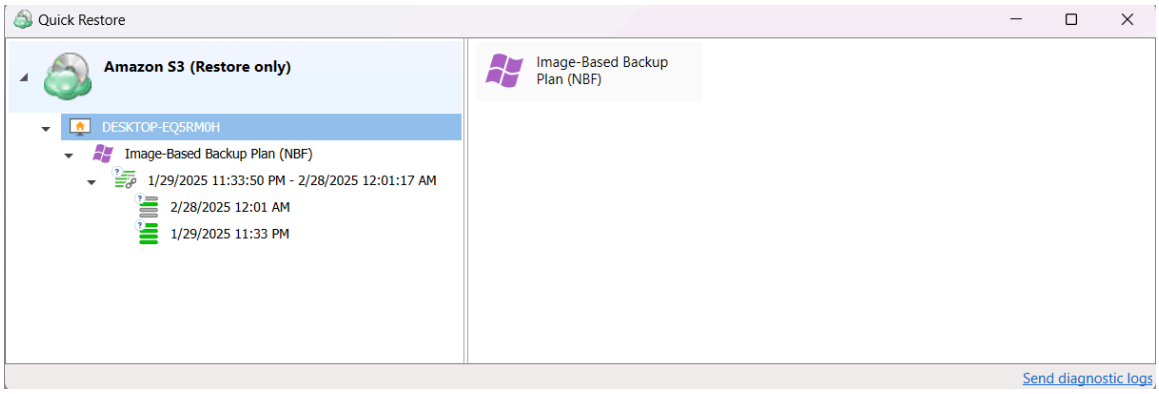




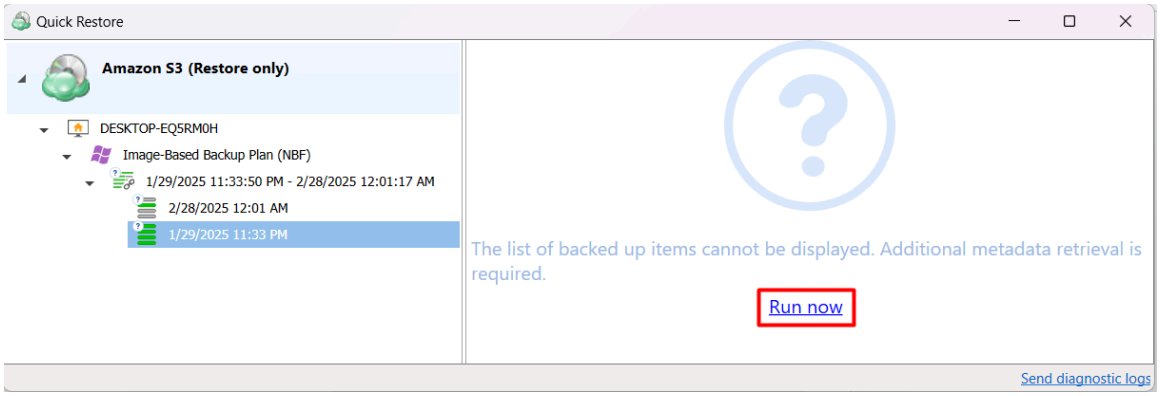
Once the Quick Restore is installed, you should be able to launch it by clicking on the “here”:



Step 4. Using the Quick Restore application, you can select the backup plan and restore point.

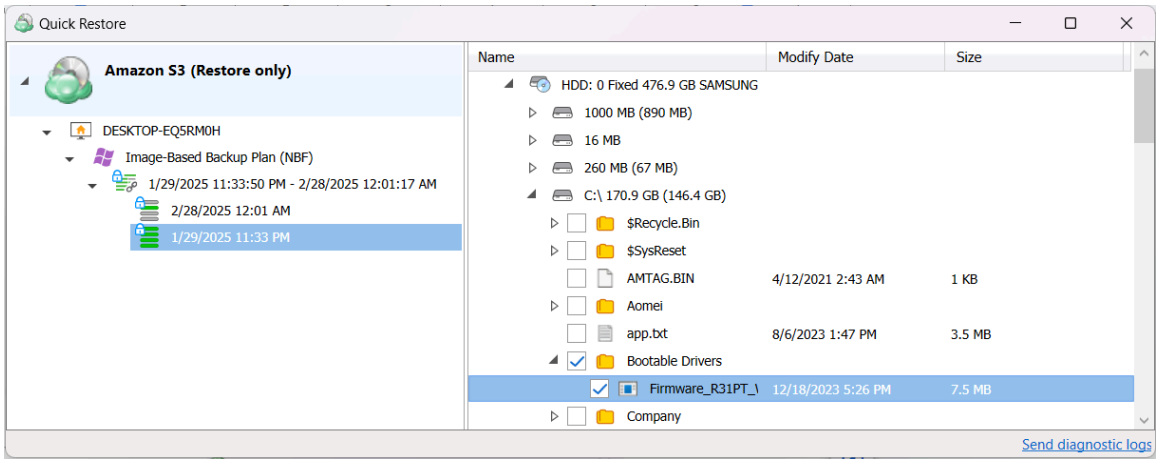


Step 5. Additional metadata retrieval might be required. Please click on “Run now”.

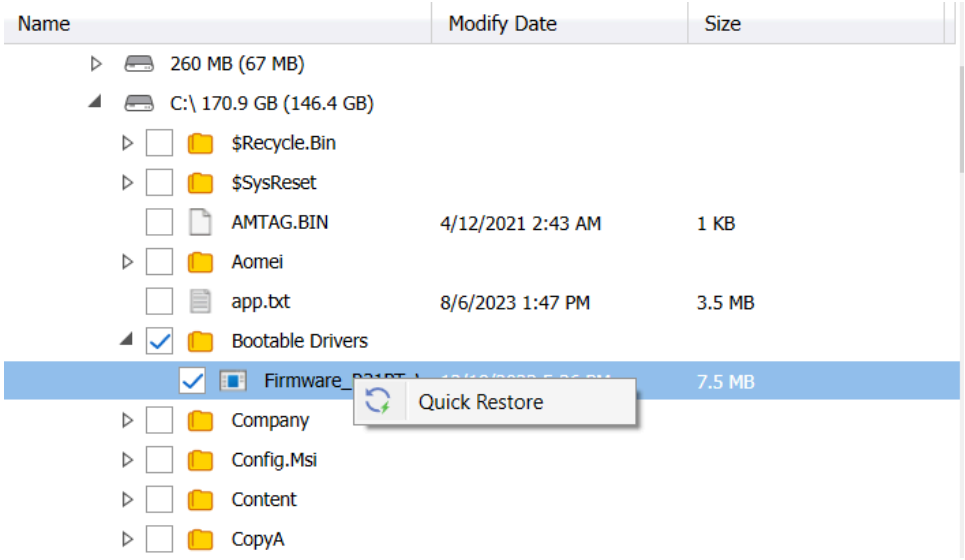


If your backup was encrypted, you need to enter the password to view the available folders and files:

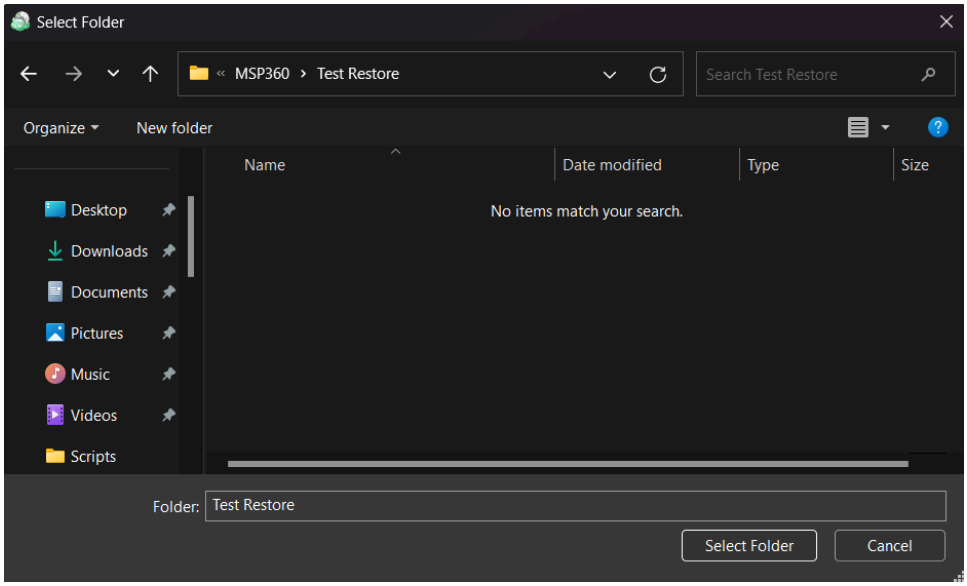
After entering the right password, you can and select file(s) or folder(s) you would like to restore:



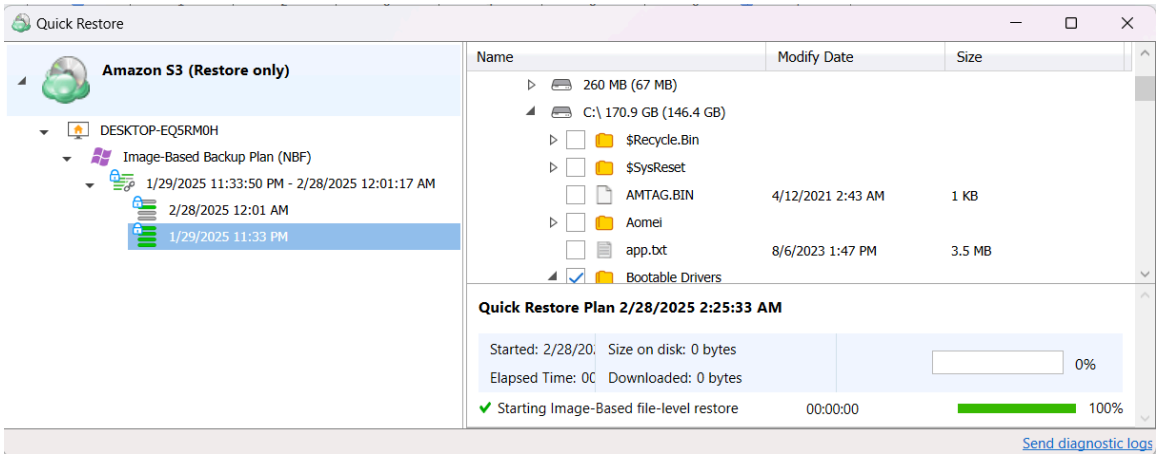
Step 6. Right-click on a file or folder and proceed with “Quick Restore”.



Step 7. Select the destination folder for your restore job.



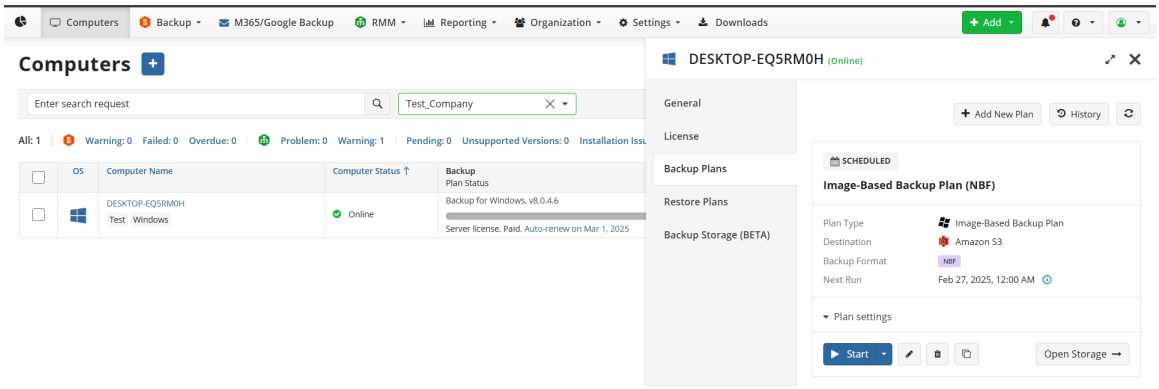
Step 8. The progress bar will appear once the restore process has started:



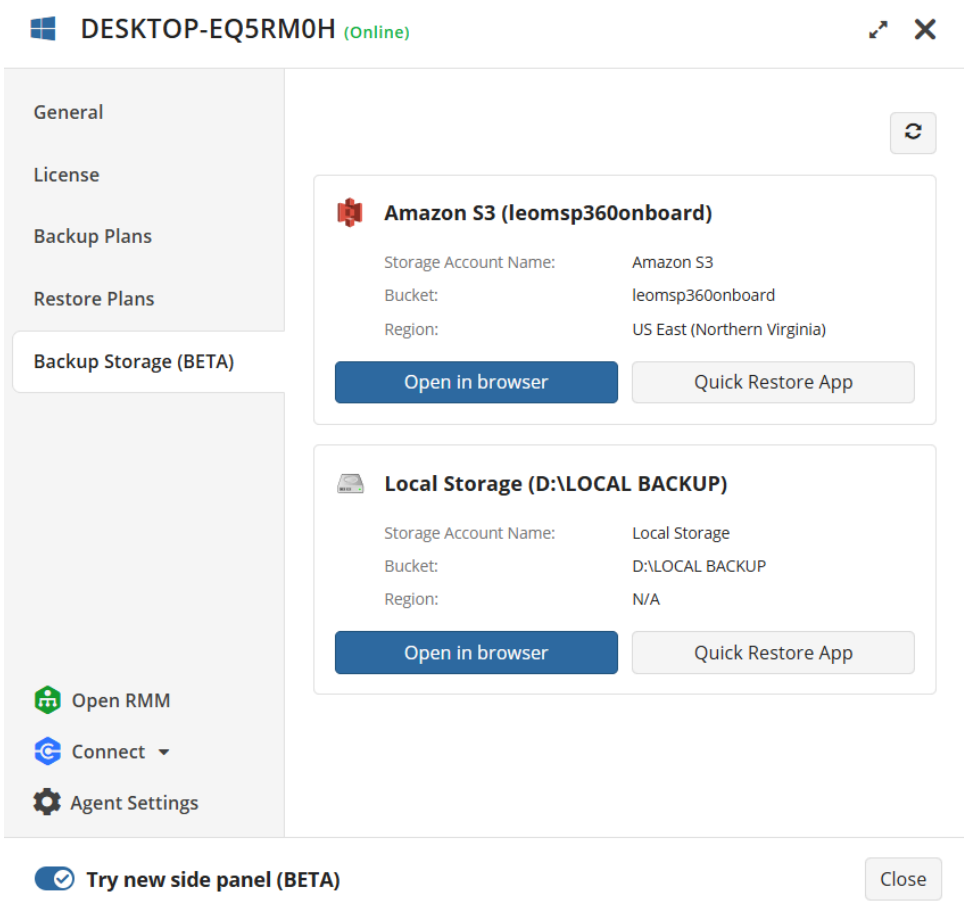
Once the Quick Restore plan is complete, you should see restored files in the destination folder.

Restore Items using the MBS Backup Storage Browser (BETA)

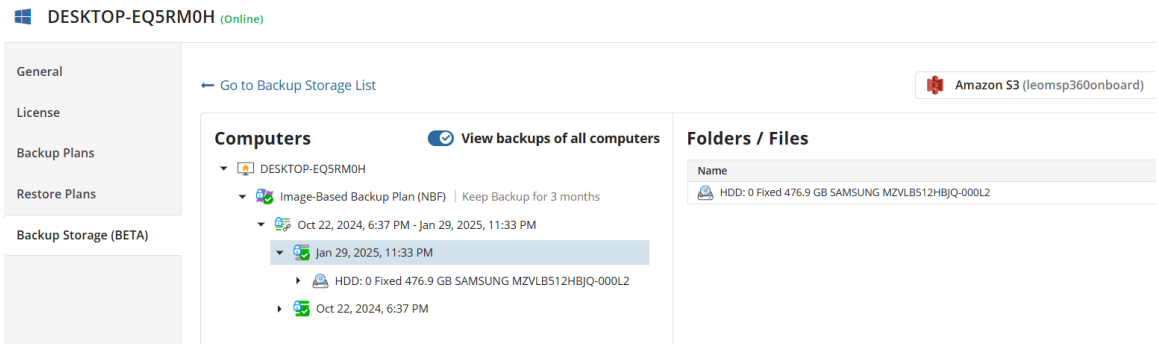
Step 1. Navigate to the MBS Portal and select the “Computers” page on the main menu. Locate the computer which backup dataset you wish to restore from and click on the name of the computer or the backup status bar.



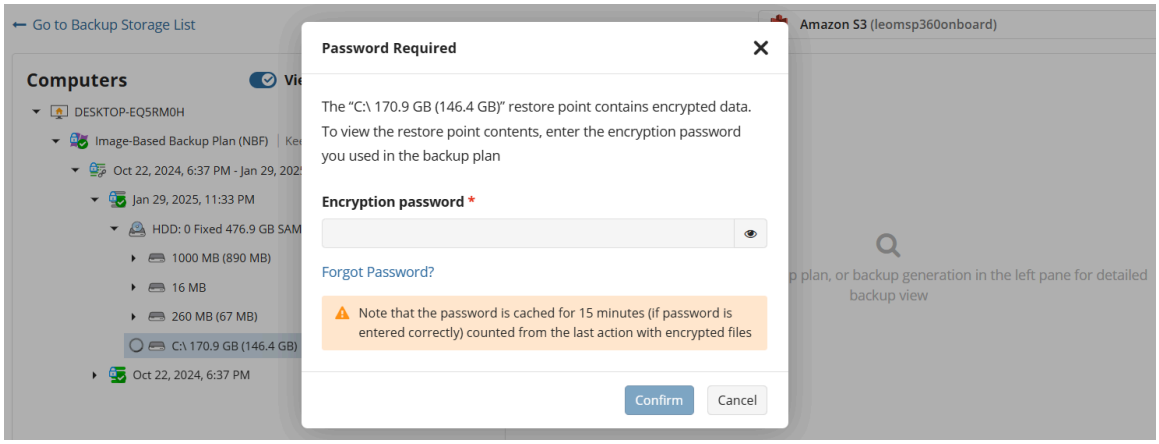
Step 2. Select the “Backup Storage (BETA)” tab and then click on the “Open in browser” button for the storage account you want to restore from.



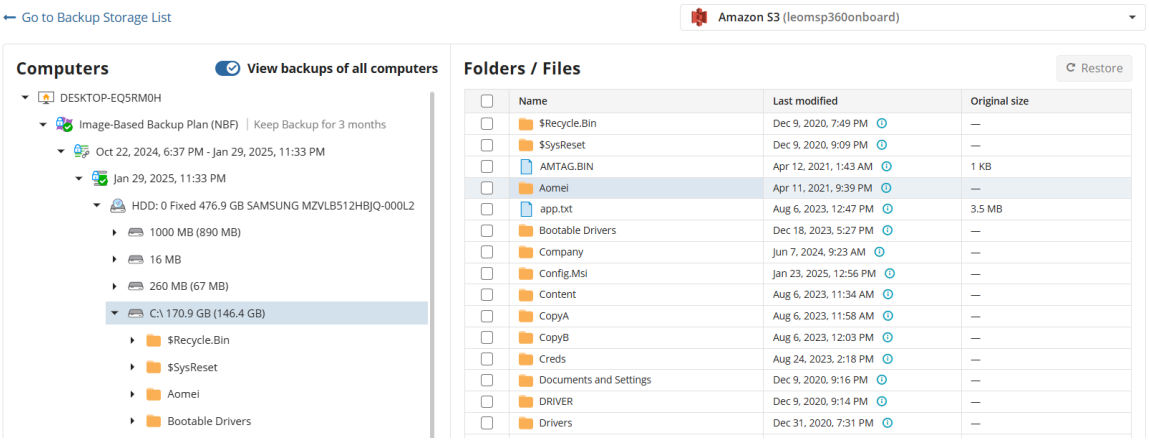
Step 3. Expand the volumes and find the individual files that you would like to restore from the Image-Based backup.



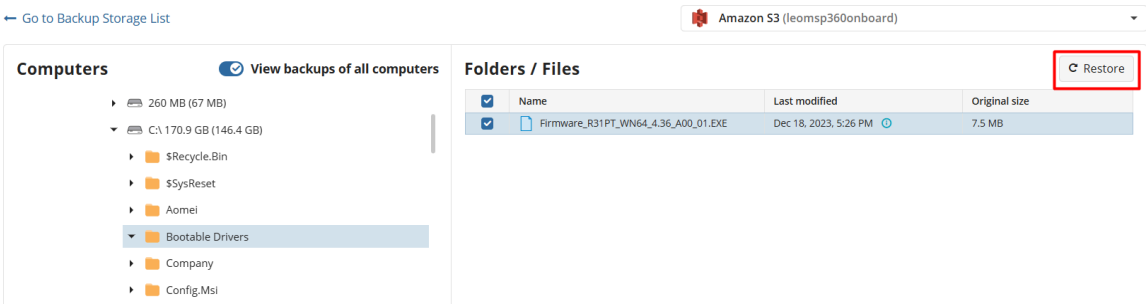
Step 4. If your backup was encrypted, you need to enter the password to view the available folders and files.



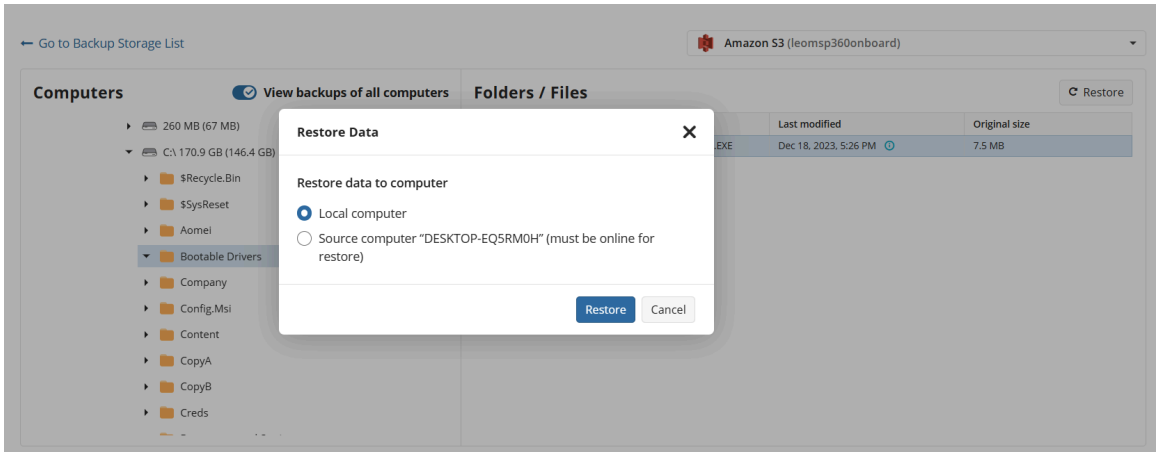
After entering the right password, you can select file(s) or folder(s) you would like to restore.



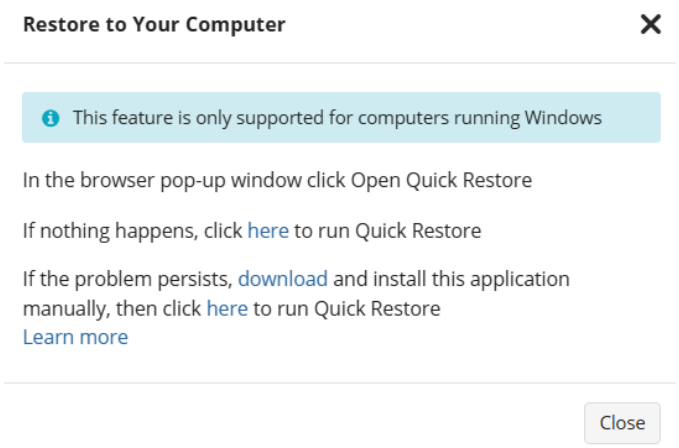
Step 5. Proceed by clicking the “Restore” button in the top right corner of the window.



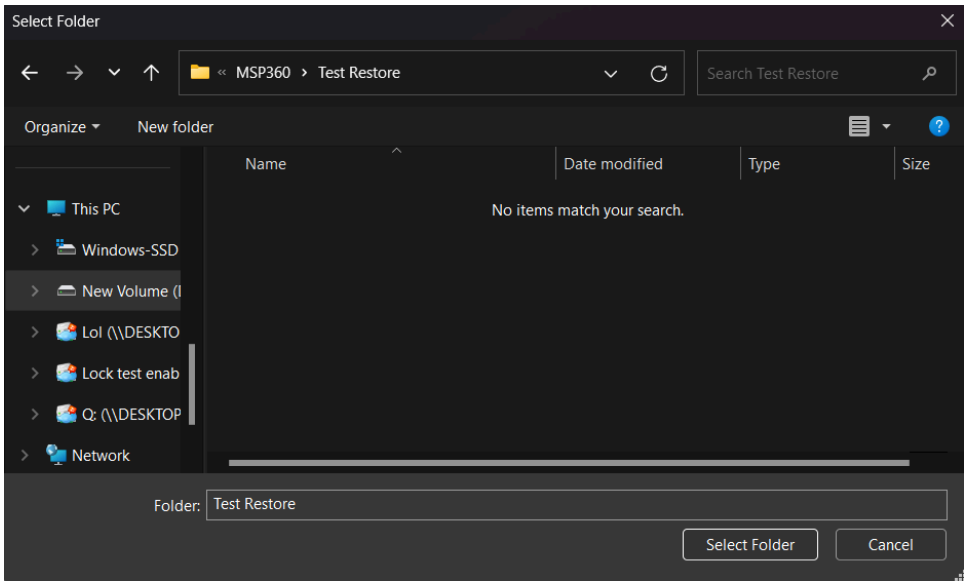
Step 6. Select the target computer and destination folder for the restore.



- **Local Computer:** If you select the “Local computer” (where you are logged into the Managed Backup Service portal) option, the portal will open the "Quick Restore” application.

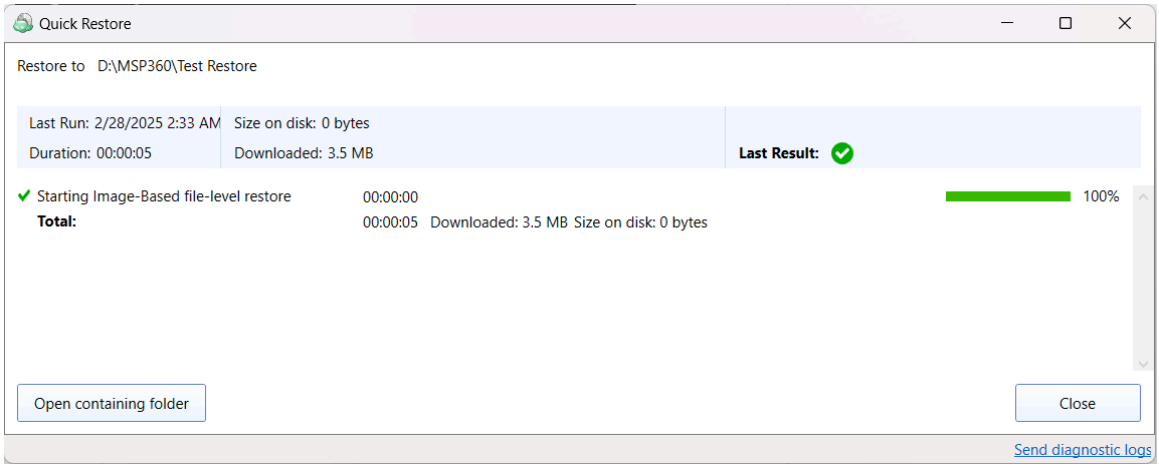


After launching the Quick Restore, the application will prompt you to select the destination folder:

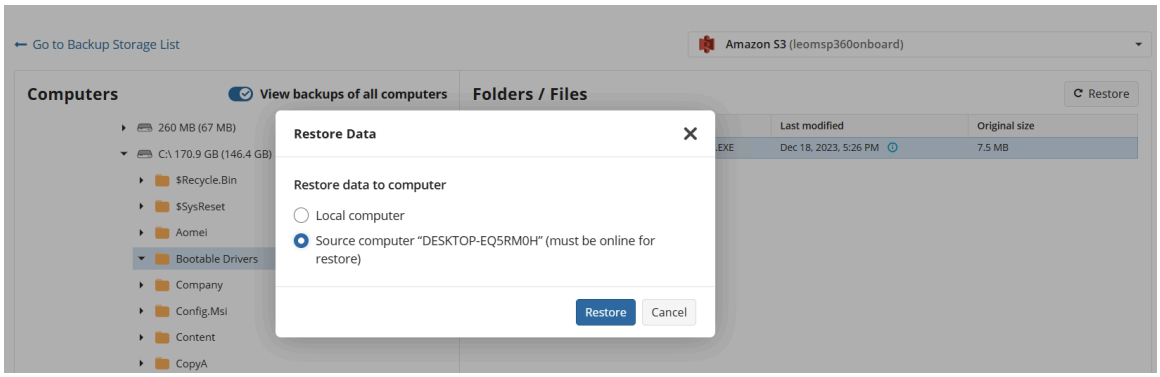


If the data was encrypted, you will need to enter the password:

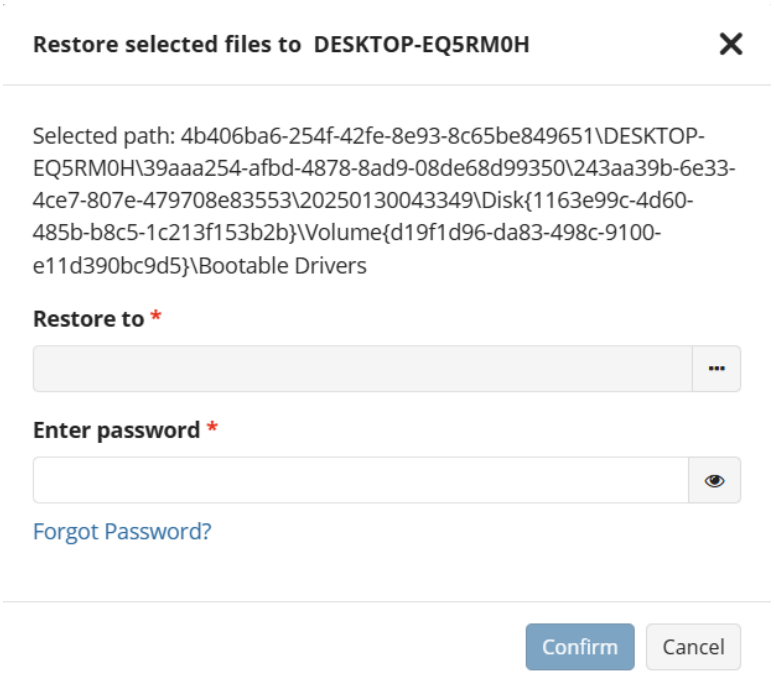
A progress bar will appear. Once the Quick Restore job is complete, you can navigate to the destination folder by clicking on the “Open containing folder”:



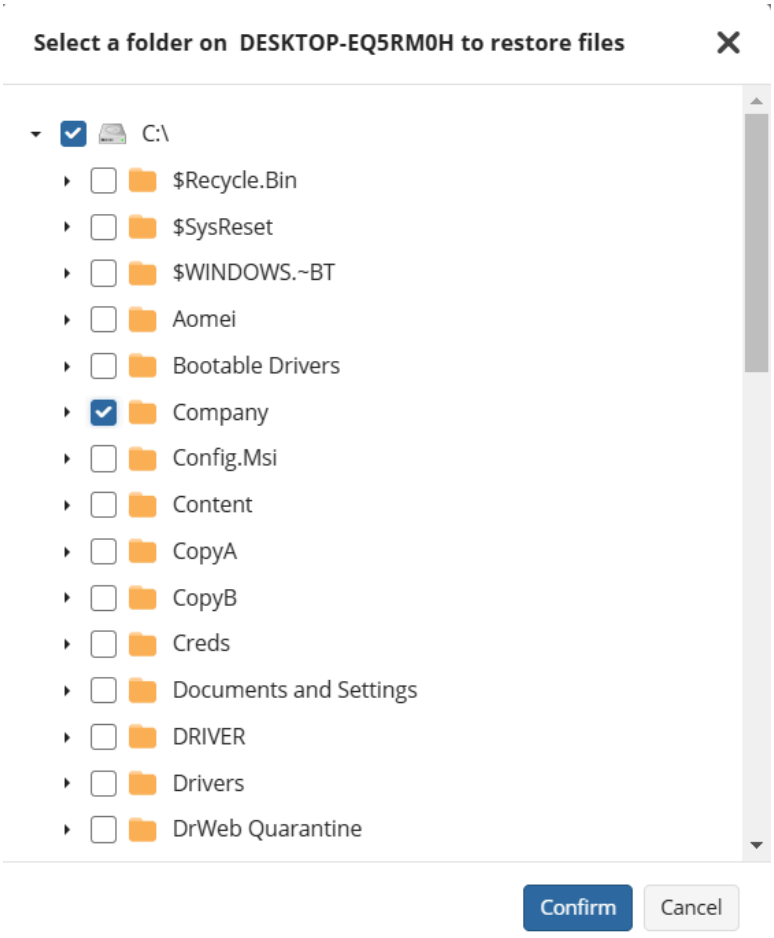
- **Source computer.** You can select the “Source computer” option if the machine is online to perform the restore job.



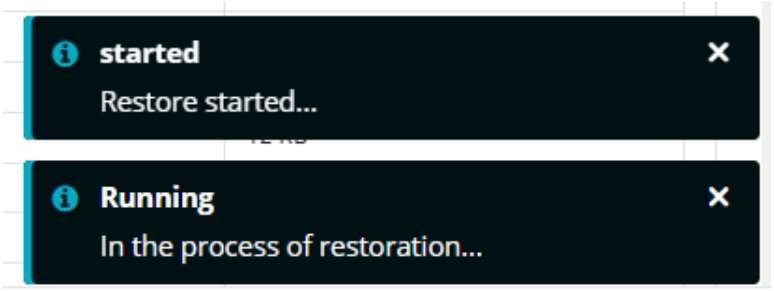
You will need to specify the destination path in the “Restore to” field and provide the encryption password.



You can open the file tree view by clicking on the options next to the “Restore to” field:



Once you click on “Confirm” the restore operation will begin. You should see the related notification messages in the right bottom corner of the Managed Backup Service portal.



Disaster Recovery

How to Create a Bootable USB Device / ISO image - Agent

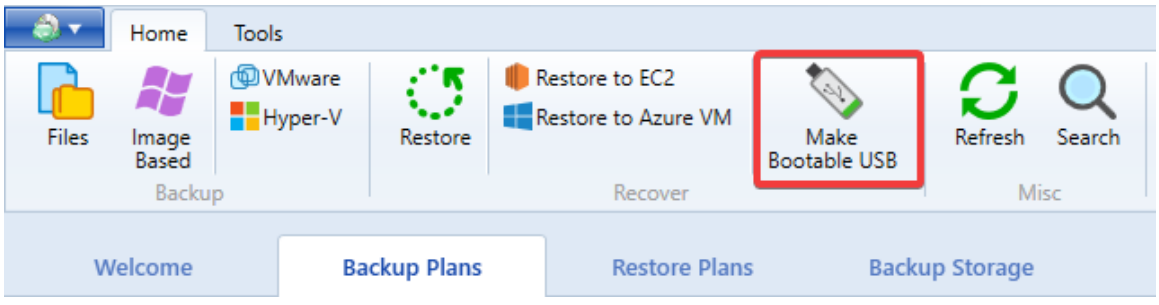
Step 1. Plug the USB device that you want to use as a bootable device into your computer.

> Please note that all information stored on this USB device will be permanently deleted, we strongly recommend that you backup all the data from the USB device in order to avoid losing any important data.

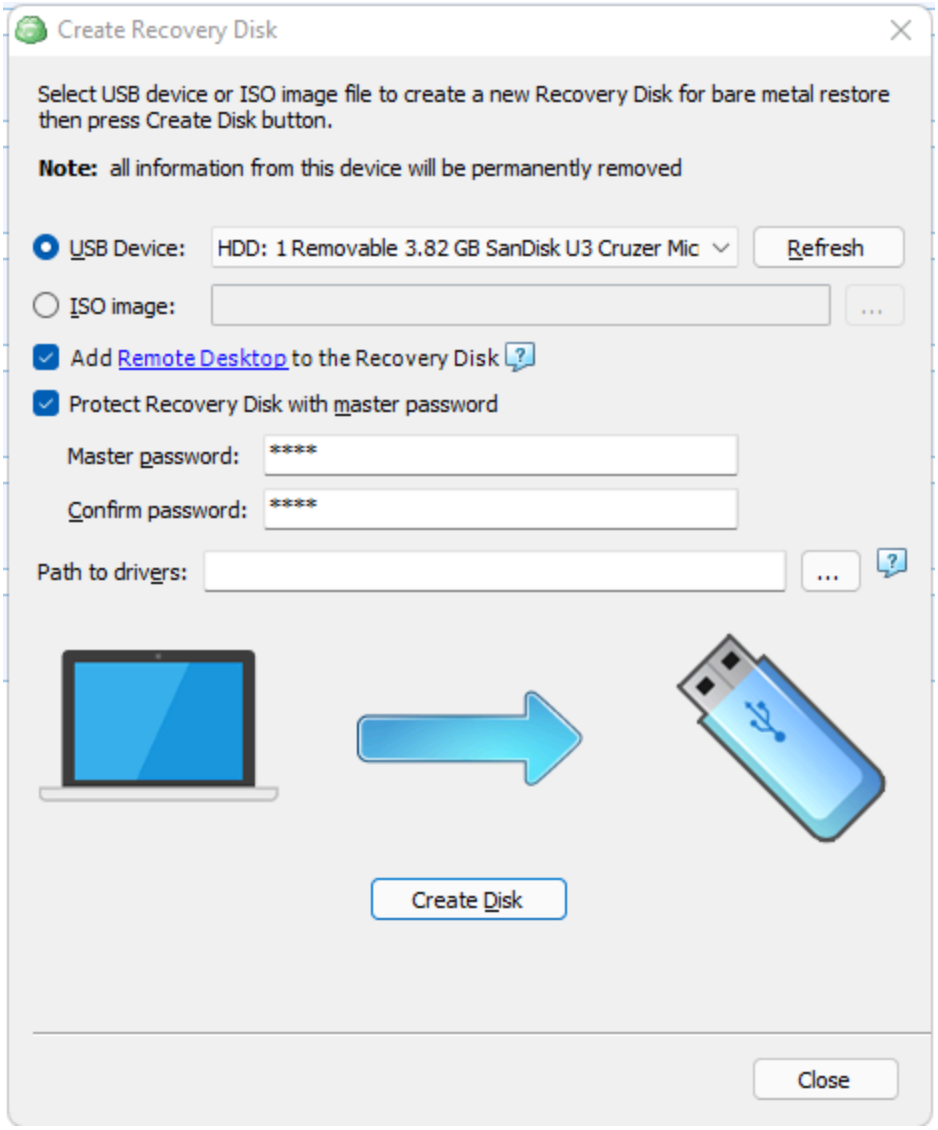
> A USB Drive with a minimum capacity of 1 GB is required.

> To create a Bootable ISO image on the USB device, the following two components from the Windows ADK (Windows 10 requires ADK version 10.1.18362.1) must be installed:
>
> - Deployment Tools (https://go.microsoft.com/fwlink/?linkid=2086042)
> - Windows Preinstallation Environment (Windows PE) (https://go.microsoft.com/fwlink/?linkid=2087112)
>
> The first setup (adksetup.exe) will generate suggestions for other components to be included, only the Deployment Tools are required.

Step 2. Launch Online Backup and click the “Make Bootable USB” button on the toolbar.



Step 3. In the dialog box, select your USB device from the drop-down list and choose a Master Password to protect your Recovery Disk. Then click the Create Disk button.



- **USB Device:** Select the removable USB device you want to use, click refresh if it does not automatically appear when plugging in.
- **ISO Image:** Specify the path in which you would like to save the bootable ISO image to be used later when making other bootable media
- **Add Remote Desktop to the Recovery Disk:** Selecting this will include the MSP360 Remote Desktop client on recovery disk
- **Protect Recovery Disk with master password:** Protect the recovery media with a master password

- **Path to drivers:** In the event that custom drivers are needed, specify the path to the folder here and they will be included in the recovery media.

> If no specific drivers are needed, the recovery media may be used for any computer. Otherwise, if specific drivers, such as RAID controllers, are included, you must create separate bootable recovery media for each hardware profile.

Step 4. Once the process has completed, click the Close button. If creating a bootable USB device, it will contain a new folder named "Boot". Otherwise, the ISO will be created in the specified folder.

How to Create a Bootable USB Device / ISO image - MBS

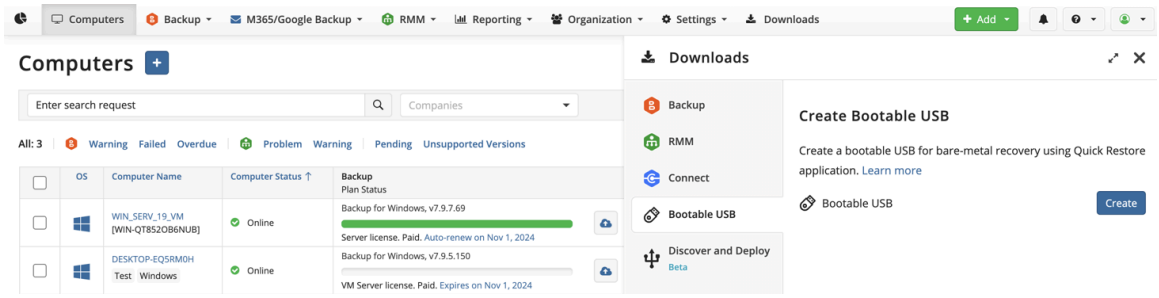
Step 1. Plug the USB device that you want to use as a bootable device into your computer.

> Please note that all information stored on this USB device will be permanently deleted, we strongly recommend that you backup all the data from the USB device in order to avoid losing any important data.

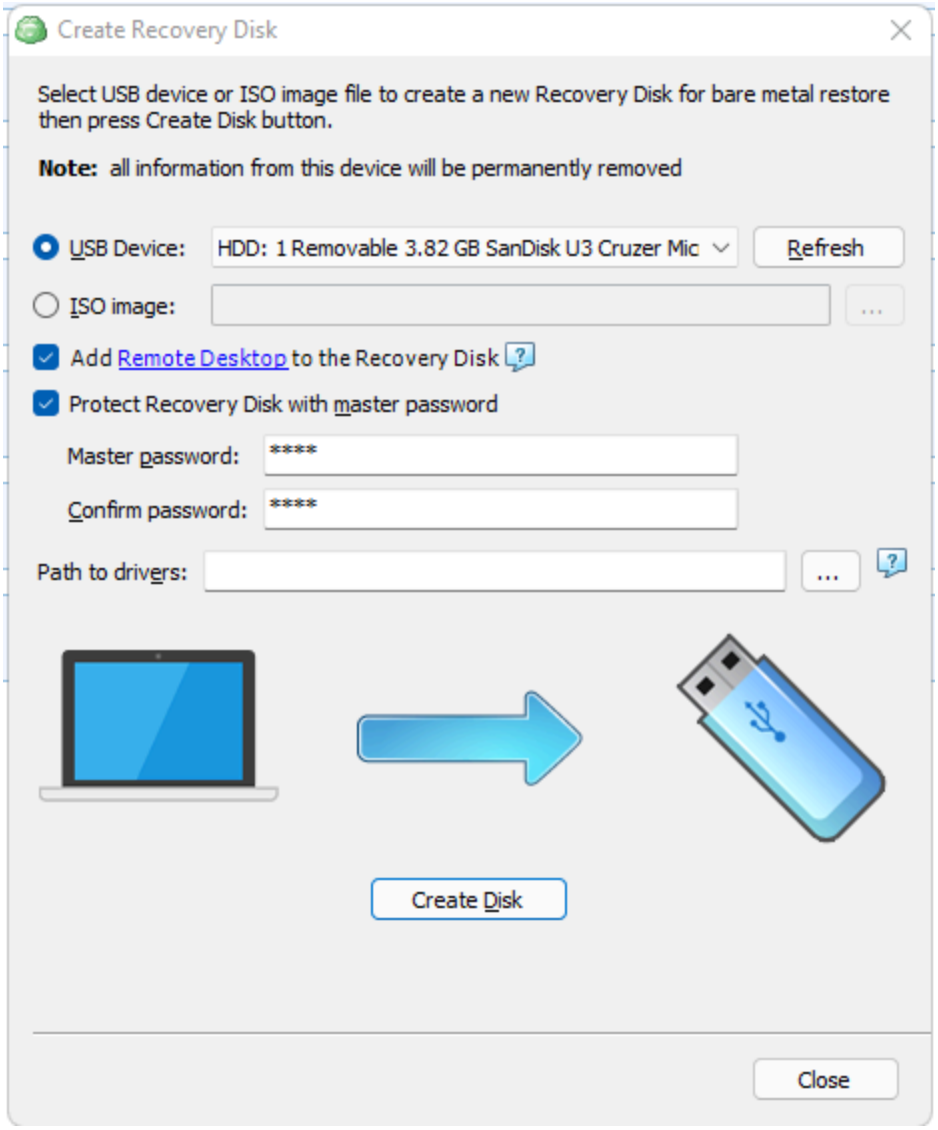
> A USB Drive with a minimum capacity of 1 GB is required.

> To create a Bootable ISO image on the USB device, the following two components from the Windows ADK (Windows 10 requires ADK version 10.1.18362.1) must be installed:
>
> - Deployment Tools (https://go.microsoft.com/fwlink/?linkid=2086042)
> - Windows Preinstallation Environment (Windows PE) (https://go.microsoft.com/fwlink/?linkid=2087112)
>
> The first setup (adksetup.exe) will generate suggestions for other components to be included, only the Deployment Tools are required.

Step 2. From MBS, navigate to the Downloads menu and then go to the Bootable USB tab.



Step 3. In the dialog box, select your USB device from the drop-down list and choose a Master Password to protect your Recovery Disk. Then click the Create Disk button.



- **USB Device:** Select the removable USB device you want to use, click refresh if it does not automatically appear when plugging in.
- **ISO Image:** Specify the path in which you would like to save the bootable ISO image to be used later when making other bootable media
- **Add Remote Desktop to the Recovery Disk:** Selecting this will include the MSP360 Remote Desktop client on recovery disk
- **Protect Recovery Disk with master password:** Protect the recovery media with a master password

- **Path to drivers:** In the event that custom drivers are needed, specify the path to the folder here and they will be included in the recovery media.

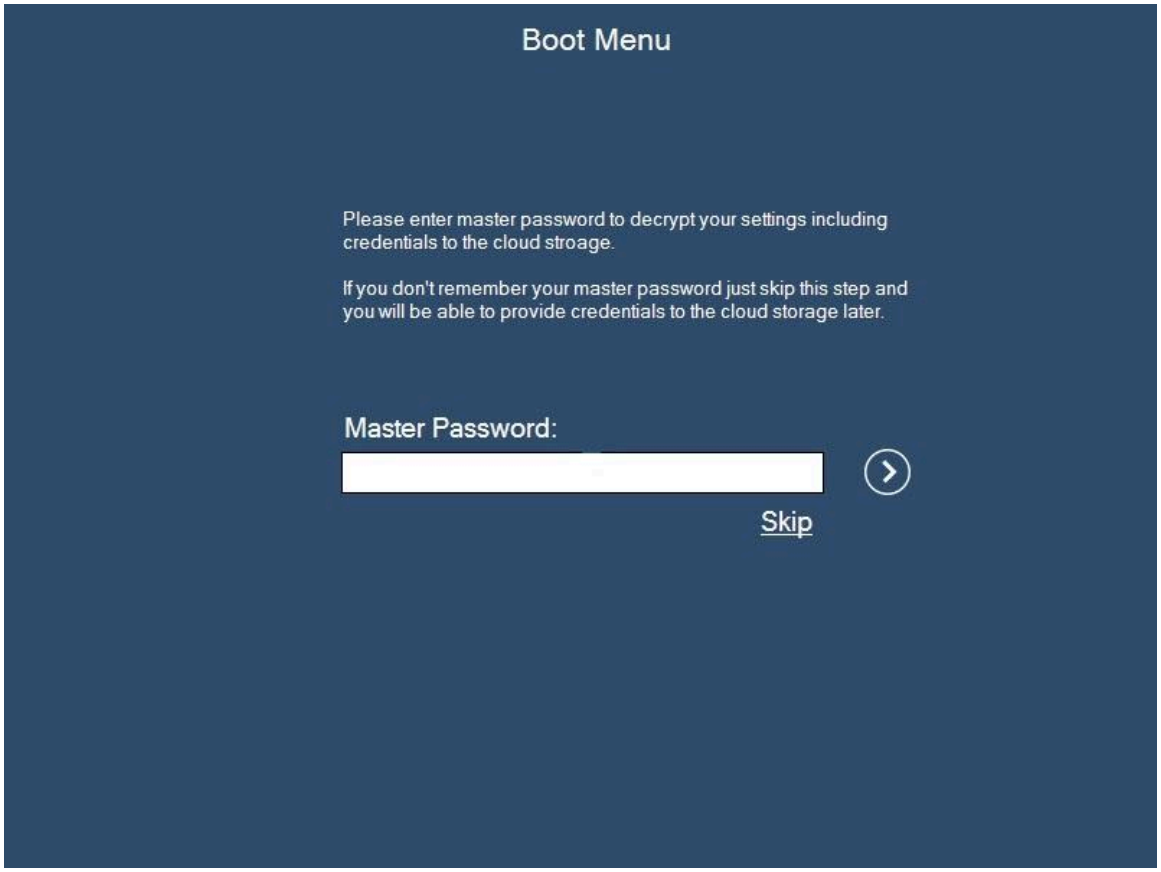
> If no specific drivers are needed, the recovery media may be used for any computer. Otherwise, if specific drivers, such as RAID controllers, are included, you must create separate bootable recovery media for each hardware profile.

Step 4. Once the process has completed, click the Close button. If creating a bootable USB device, it will contain a new folder named "Boot". Otherwise, the ISO will be created in the specified folder.

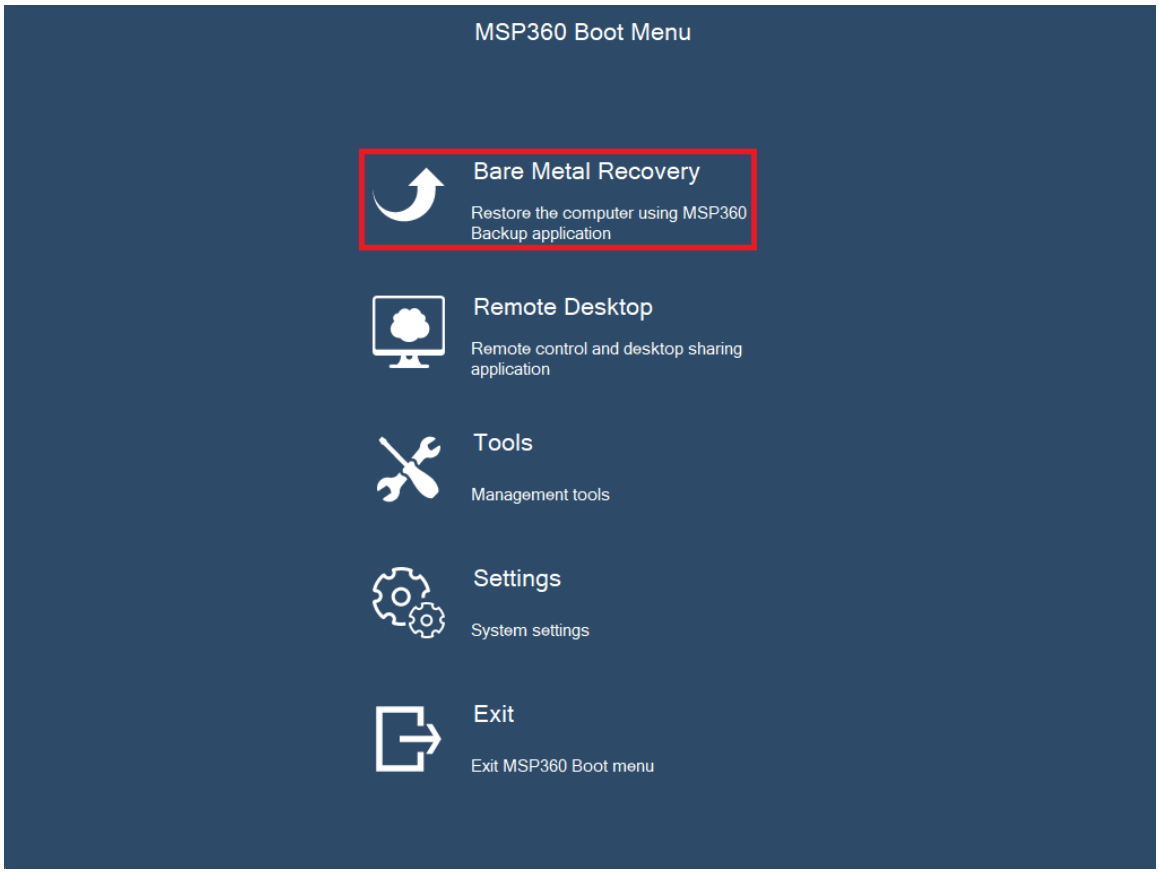
Bare-metal restore from USB/ISO image

Step 1. Plug the bootable USB device into the computer, or mount the ISO file as a drive, and then restart the computer.

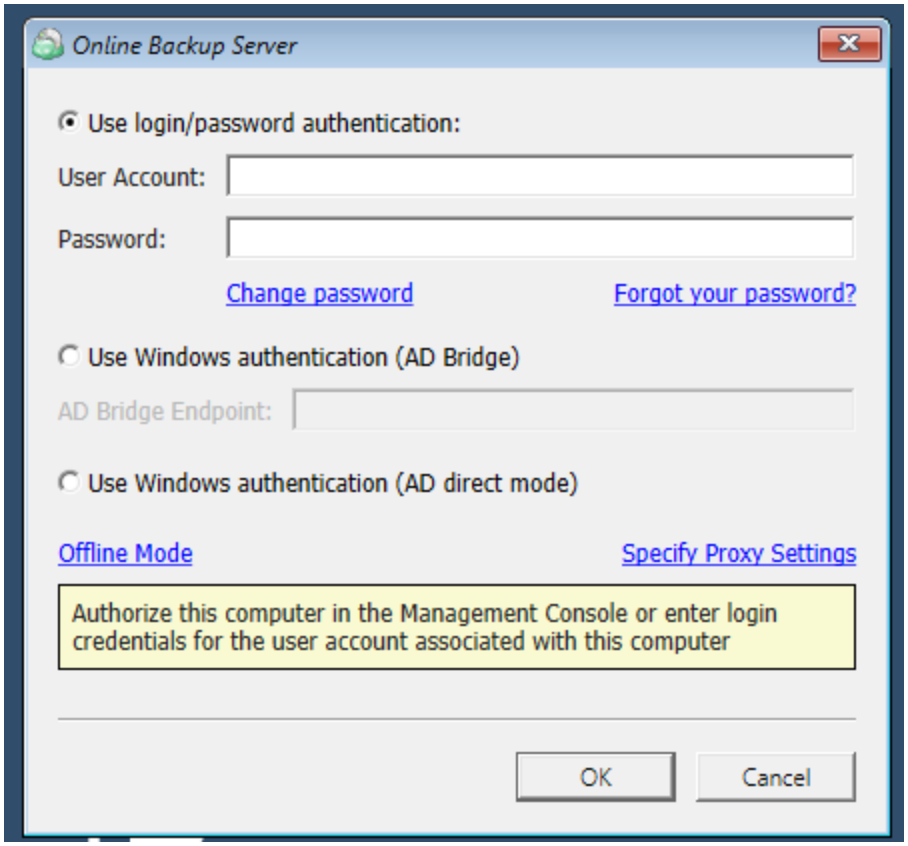
Step 2. You will see the “Boot Menu” welcome screen where you will be prompted to enter the Master Password that you specified during the creation of the bootable device (if you did not specify a password then skip this step).



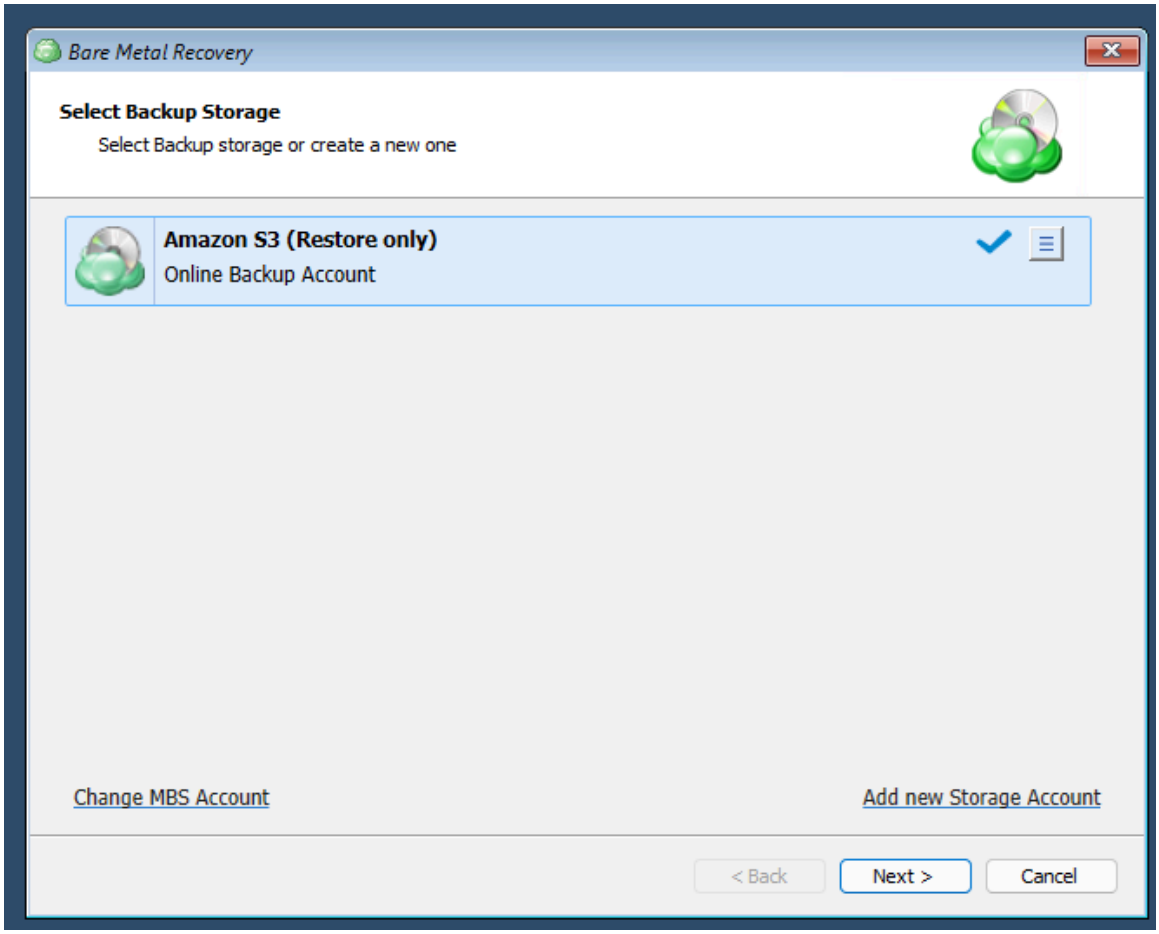
Step 3. Click the Bare Metal Recovery button.



Step 4. The Bare Metal Recovery wizard will start and prompt you for the Backup User credentials associated with the computer you would like to restore. You can check the name of the Backup User from the “Company & User Account” column on the “Computers” page in your MBS Console. If you need to reset the password for it, you can do so from “Users” in the “Organization” menu in the MBS Console.

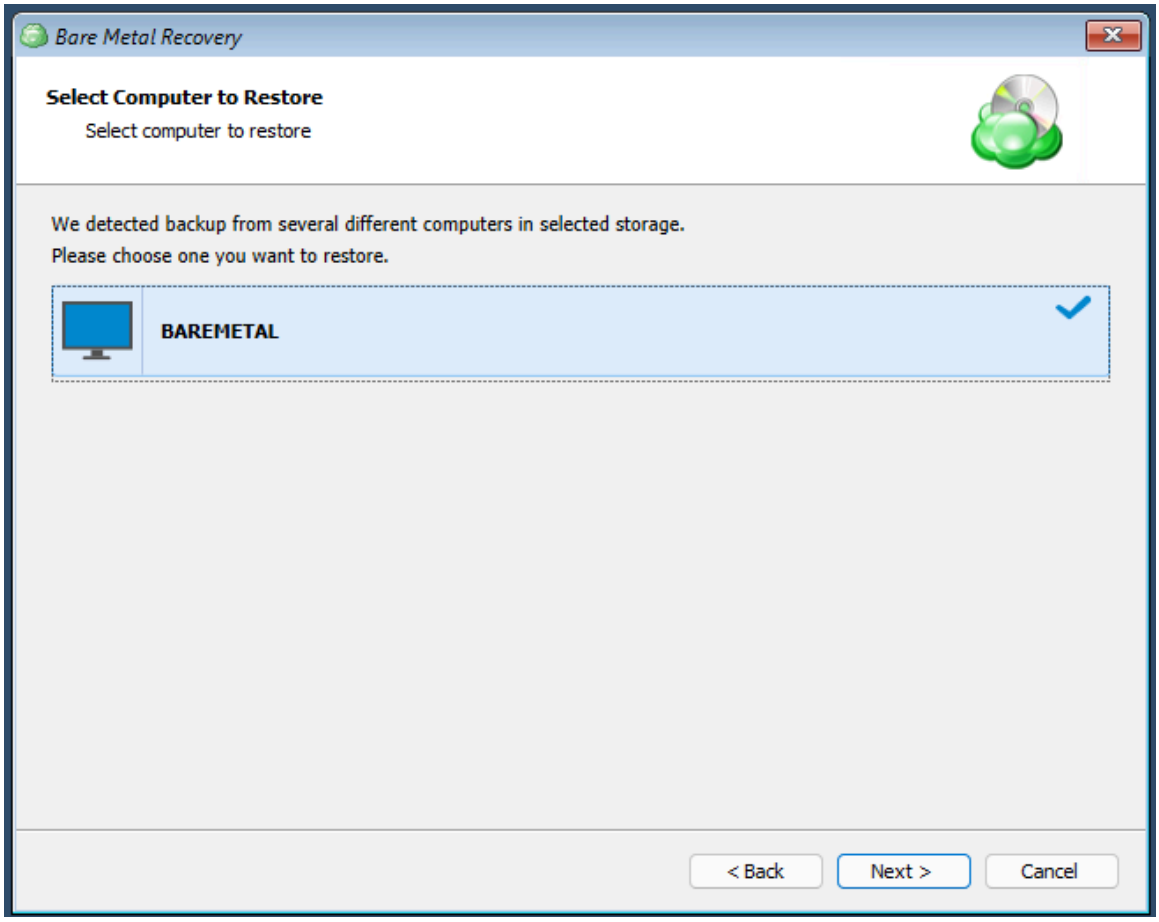


Step 5. Once the credentials are authorized, you will be able to select the storage which contains the backup data.

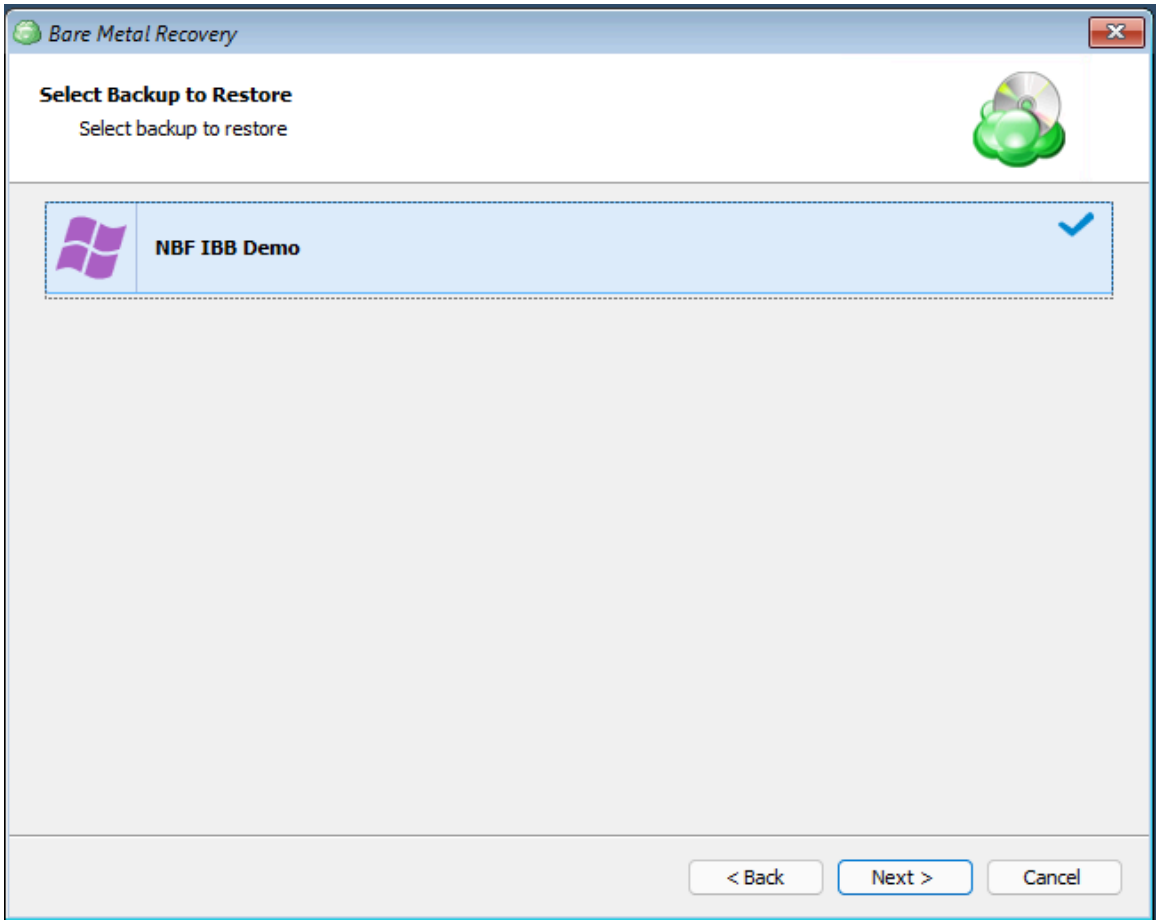


- **Change MBS Account:** Use this to change to a different backup user account if needed for the restoration.

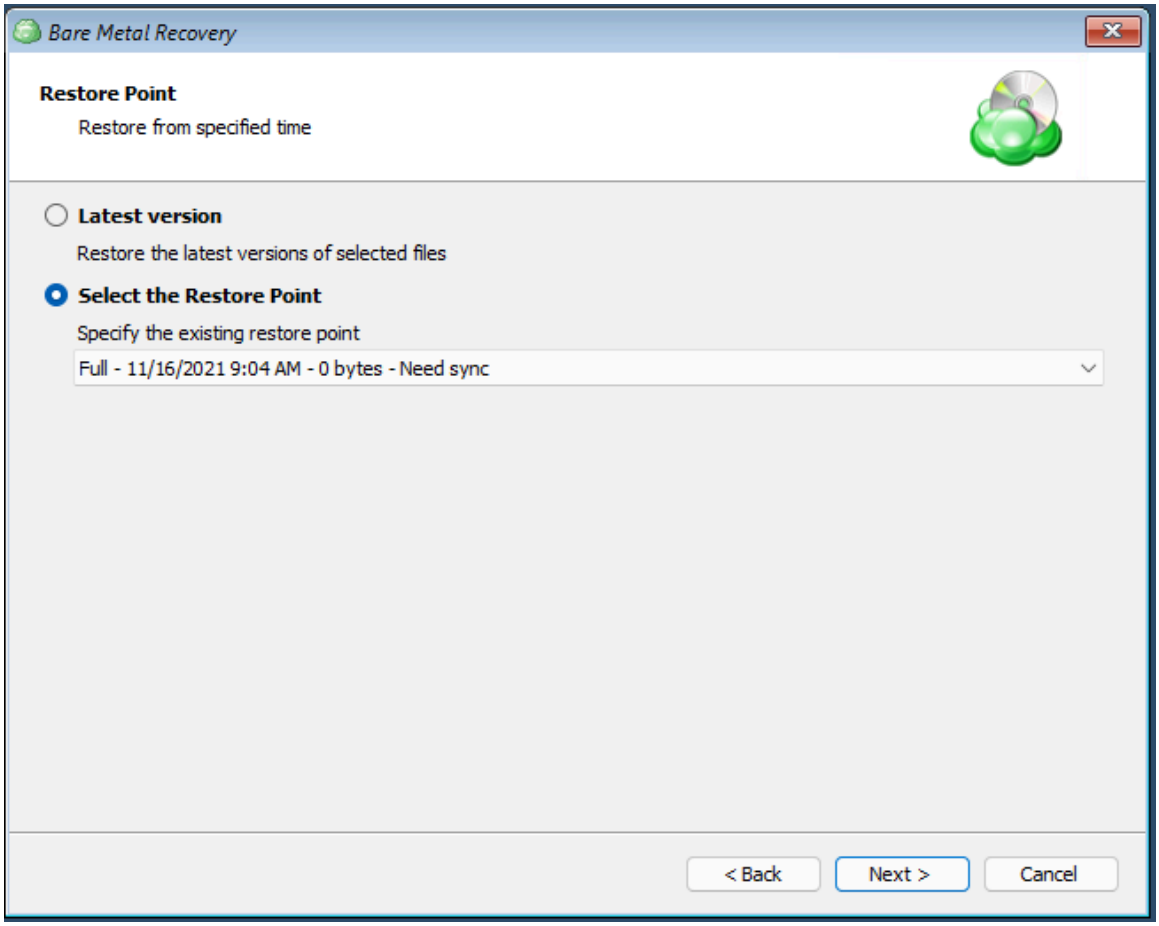
Step 6. The next screen will list all computers for which backups were found created by the user in the selected storage. Select the appropriate source and click Next.



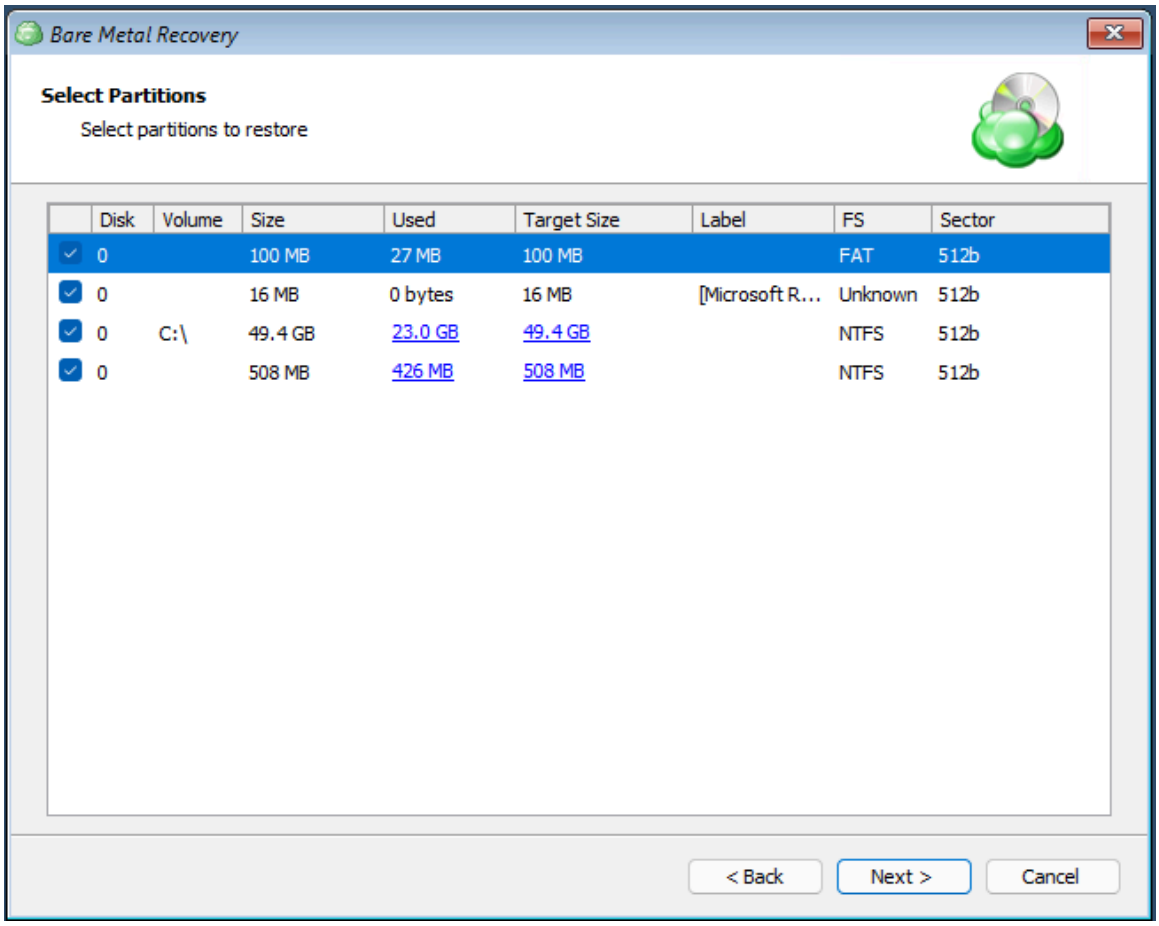
Step 7. Next you will be given a list of available backups which can be restored. Select the appropriate one and click Next.



Step 8. With the backup selected, you will now be prompted to select which restore point should be used. Select either Latest Version, or another from the drop down list, then click Next.

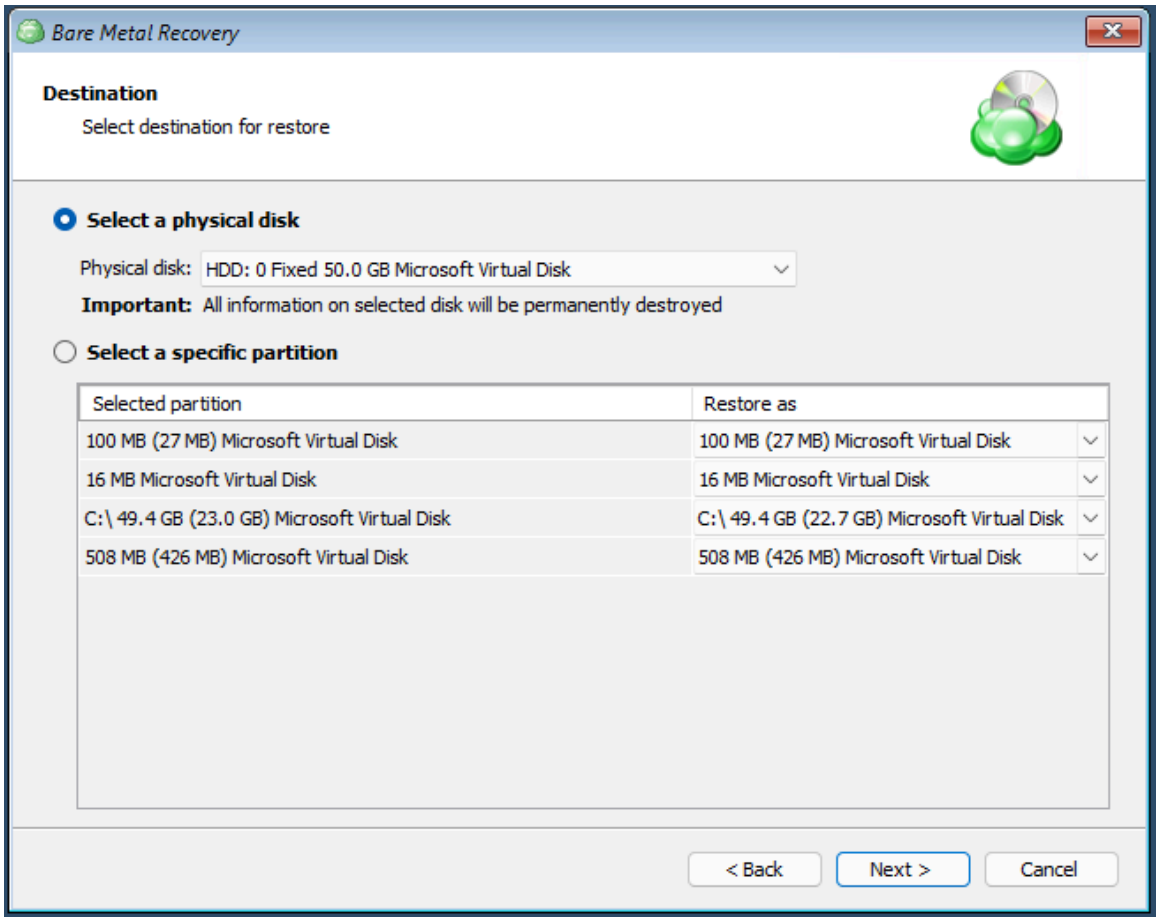


Step 9. Next, select the partitions you wish to restore.



Select all the required partitions including boot one. Make sure that you have selected all the partitions prior to the C: drive.

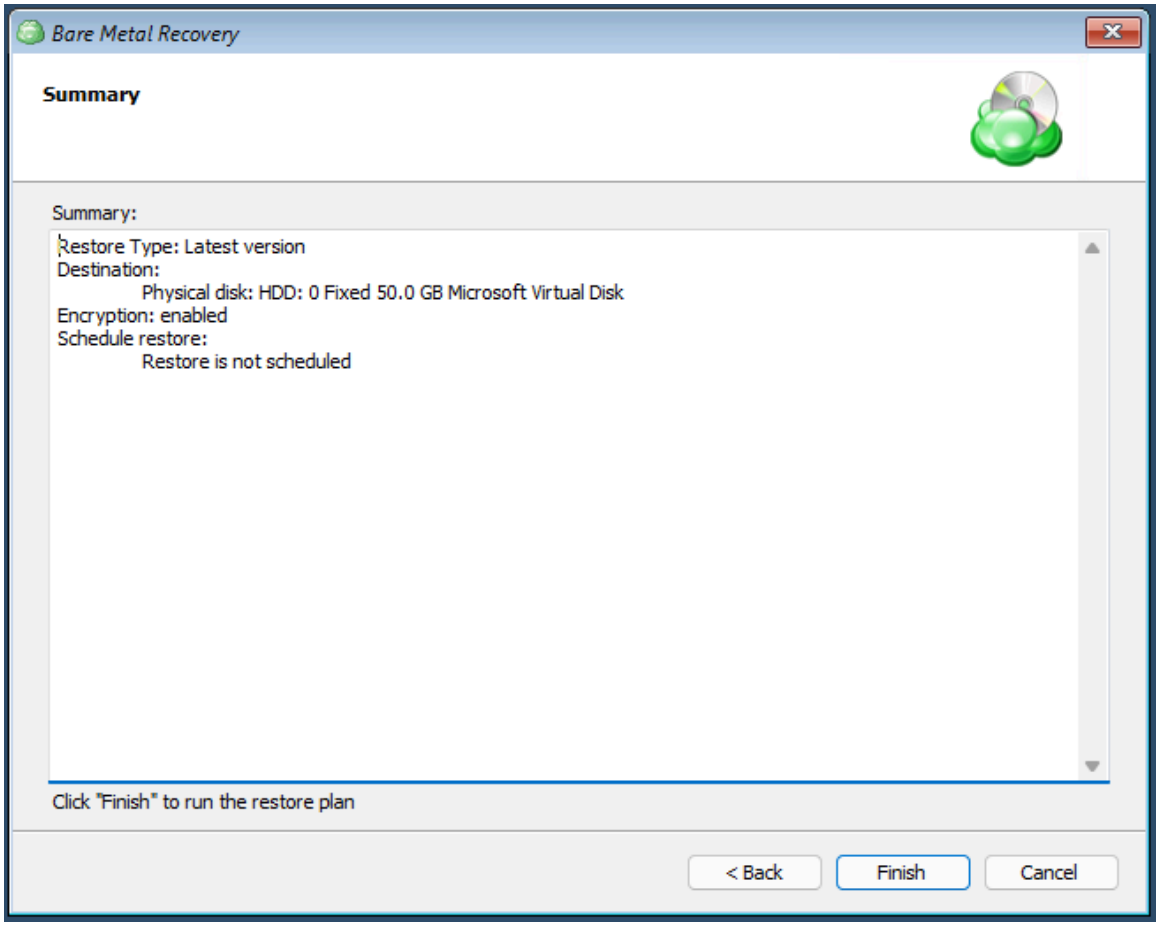
Step 10. Select the local destination disks or partitions, then click Next.



If you are restoring an image to a **new or empty disk**, select a physical disk as the destination for the restore.

If you want to restore **specific corrupted partitions**, then select these specific partitions as the destination for the restore.

Step 11. The last step of the wizard is a summary of the selected actions. Click Finish to run the restore plan.



Addendum: If you want to take advantage of the available management tools to perform any specific backup management actions such as logs or modifying the registry then click on the System Tools button on the Backup Boot Menu screen.

Here you will be given a list of useful tools and utilities, including an alternative recovery interface similar to the Online Backup application.