



Active Backup for Business Administrator's Guide

Based on Active Backup for Business 2.0.4

Table of Contents

Chapter 1: Introduction

Chapter 2: Getting Started with Active Backup for Business

Synology NAS Requirements and Limitations.....	4
Supported Backup Sources.....	4
Install Active Backup for Business.....	6

Chapter 3: Backup

Overview.....	7
Create Backup Tasks.....	10
Manage Backup Tasks.....	28
Backup Settings.....	34
Create a Second Backup.....	34

Chapter 4: Recovery

Virtual Machine.....	36
Physical Server.....	43
Personal Computer.....	43
File Server.....	44

Chapter 5: Report

View Statistics of Backup Tasks.....	45
View Restore Status.....	50
Generate Reports.....	52

Introduction

Active Backup for Business is an all-in-one business data protection solution, centralizing protection over diverse IT environment that consists of virtualized environments, physical servers, file servers, and personal computers based on the award-winning DSM operating system. Admins can deploy desired protection single-handedly through the centralized admin console.

Getting Started with Active Backup for Business

Synology NAS Requirements and Limitations

To install Active Backup for Business, a NAS device running DSM 6.1.7 or above is required and only x64 Synology NAS servers and Btrfs file system is supported. For backup performance, it is recommended to have at least 4G of RAM and not to set up the shared folder quota due to deduplication mechanism.

Supported Backup Sources

Personal computer requirements and limitations

Active Backup for Business supports backing up end-point devices running on Windows platform.

Supported Windows edition:

- Windows 10 Creators Update (all editions)
- Windows 10 (all editions)
- Windows 8.1 (all editions)
- Windows 7 SP1 (all editions)

Note: On dynamic disks, only simple volumes are supported for backup, while other types of volumes are not.

Physical server requirements and limitations

For backing up physical server, Active Backup for Business supports Windows operating system.

Supported Windows edition:

- Windows 10 Creators Update (all editions)
- Windows 10 (all editions)
- Windows 8.1 (all editions)
- Windows 7 SP1 (all editions)
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Note: On dynamic disks, only simple volumes are supported for backup, while other types of volumes are not.

File Server requirements and limitations

For backing up file server, Active Backup for Business supports the servers running with SMB (Windows) and rsync 3.0 or above (Linux) protocol. You may back up data to your Synology NAS using Active Backup for Business.

Note: On dynamic disks, only simple volumes are supported for backup, while other types of volumes are not.

Virtual Machine requirements and limitations

This section provides you with important information on deployment limitations and supported virtual machine (VM) environments.

- **Virtual Infrastructure**

For virtual machine backup, Active Backup for Business supports the following versions of the VMware vSphere platform.

- Supported VMware vSphere versions: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7
- Supported VMware editions:
 - VMware free ESXi
 - VMware vSphere Essentials, VMware vSphere Essentials Plus
 - VMware vSphere Standard, VMware vSphere Advanced
 - VMware vSphere Enterprise, VMware vSphere Enterprise Plus

Note:

- For VMware free ESXi, users will need to enable the SSH port to perform virtual machine backup.
- Your Synology NAS is required to have a public IP or a private IP that can be accessed via VMware vSphere ESXi/ESX.
- Full administrative permissions (recommended) or limited permissions are required.

- **TCP Ports**

To perform operation successfully and enable communication between Synology NAS and VMware Servers, the following TCP ports are required.

TCP Port	Where	Notes
443	vCenter Server, ESXi Host	Default port used for connections to VMware infrastructure (vCenter server and ESXi host). Must be opened on vCenter Servers and ESXi hosts.
902	ESXi Host	Port used for data transfer and moving. Must be opened on ESXi hosts.

- **Virtual Machines**

- **Operating System**

- All operating systems supported by VMware and any application.
- Application-aware backup for Microsoft Windows 2003 SP1 or later except Nano Server due to the absence of the VSS framework.

Note: If you want to run the backed up device on Synology Virtual Machine Manager, only specific operating systems can be supported. Please refer to [this article](#) for more information regarding the supported operating system on Synology VMM.

- **Virtual Hardware**

- All types and versions of virtual hardware are supported, including 62 TB VMDK.
- Raw Device Mapping (RDM) disks in physical mode, independent disks, disks connected via in-guest iSCSI initiator or disks engaged in SCSI bus sharing are not supported since VMware does not support snapshot of such VMs, and are skipped from processing automatically. If you want to back up data on such disks, please install the Active Backup for Business agent on your guest operating system and use physical server backup instead.

- **Software**

- VMware Tools: VMware Tools are required for application-aware backup and guest OS file-level restore (Windows / Linux).
- All latest OS service packs and patches are required for application-aware backup.
- File Level Restore: If the guest OS is Windows, supported file systems are NTFS and FAT32; if the guest OS is Linux, supported file systems include NTFS, FAT32, EXT3, and EXT4.

- **Limitations**

- Encrypted virtual machines, a feature introduced in VMware vSphere 6.5, are not supported for now.
- Fault tolerant machines, a feature introduced in VMware vSphere 6.0, are not supported for now.

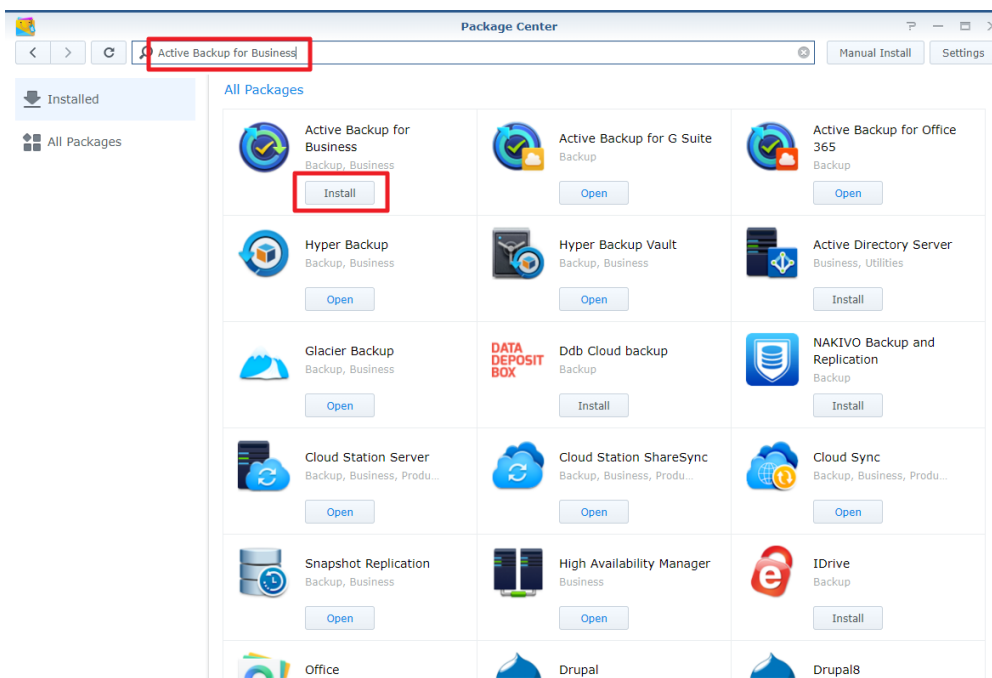
Install Active Backup for Business

Before installing the Active Backup for Business package on your DiskStation, please check the following:

- Your Internet connection is normal.
- The volume of your DiskStation is normal.
- The DiskStation Manager (DSM) of your DiskStation is updated to the latest version.
- You are the DSM **admin** (or a user belonging to the **administrators** group) for your DiskStation

To install Active Backup for Business:

- 1 Log in to DiskStation Manager (DSM) as **admin** or a user belonging to the **administrators** group.
- 2 Go to **Package Center**, and search for Active Backup for Business. Click **Install** and follow onscreen instructions to complete the installation process.



To install Active Backup for Business Agent:

Before protecting and backing up data stored on personal computers and physical servers, this Active Backup for Business Agent is required to be installed on the target device to carry out backup tasks. You can do any of the following to install Active Backup for Business Agent:

- Go to **Download Center**, and enter your product's model name. ActiveBackup for Business Agent for 32 bits and 64 bits devices are available under **Desktop Utilities** category. Please download the compatible installer for your device.
- Go to **Active Backup for Business** on DSM > **Physical Server** or **PC** > **Add device**. The download links for 32 bits and 64 bits installers will be displayed. Please download the compatible installer for your device.

Backup

Overview

This section gives you an overview of how Active Backup for Business performs backup, some of the technologies adopted, and how to create a backup task step by step.

Backup methods

Active Backup for Business provides two methods for creating backup chains:

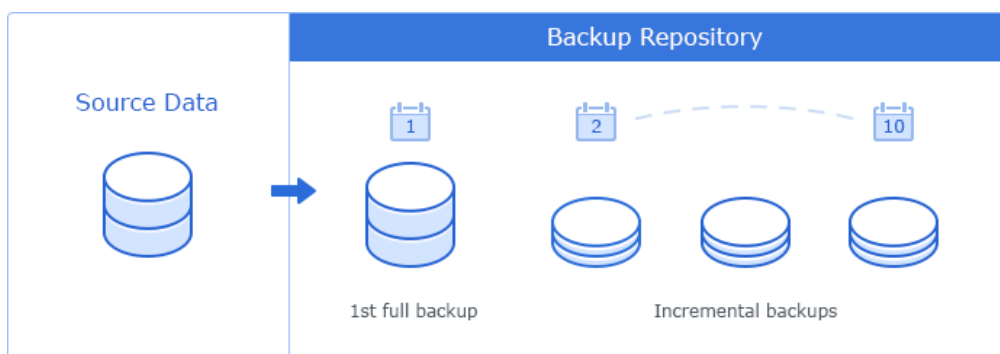
- **Full backup**

A full backup task creates a complete copy of the source data set. Since Synology Active Backup for Business leverages VMware native techniques to perform incremental backup, users whose CBT is disabled or those who do not want to perform incremental backup will have to choose full backup. However, due to the large volume of data to be transferred, full backup is a highly time-consuming process. It also imposes considerable workload on the network each time a backup task is run and may interrupt routine operations of your production site. Besides, continuously arriving full backups will also occupy a great amount of storage in Synology NAS.

- **Forever incremental backup**

There are many different types of incremental backup, such as reverse incremental, forever forward incremental, and regular incremental.

Synology Active Backup for Business uses the forever-incremental scheme, which is similar to regular incremental backup but only executes a full backup once, rather than periodically. After the initial full backup, the software will only copy increments, which helps save storage space. A forever incremental backup chain is created following the way you can see in the diagram below.



Other legacy backup solutions can also perform forever-incremental backups but periodically require transforming those increments into full VM backups. Such approaches are time-consuming, resource intensive, and require additional storage space. To offset the drawback and to offer the benefit, Synology Active Backup for Business uses forever incremental backup along with exclusive data storage methods based on Synology's unique deduplication technology.

After a backup task is run, all transferred data will be divided into individual blocks and have a unique reference number. Duplicated blocks will be deleted, while new blocks will be saved in the backup repository. In addition, a recovery point is created with a set of references to data blocks in the repository, which are required to reconstruct the entire VM as of a particular point in time.

- Here is an example of how it works:

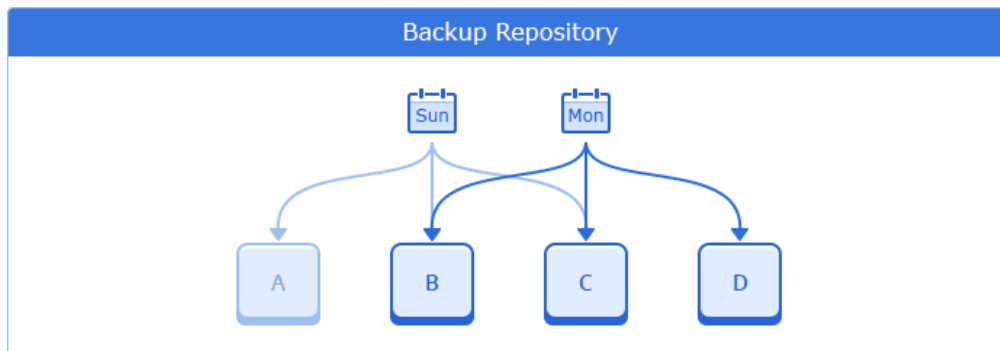
You run the first full backup of a VM on Sunday. For the sake of simplicity, let's say the VM consists of only 3 data blocks: A, B, and C.

So there will be 3 data blocks saved on your Synology NAS.

Then on Monday, you run an incremental backup, which finds out that block A was deleted, but a new block D was added.

So the blocks B and C, which remain the same, won't be saved on your NAS again, while the new block D will. At the end, there will be four blocks on your NAS: A, B, C, and D.

The Sunday version has a set of references to data blocks A, B, and C, while the Monday version has a set of references to data blocks B, C, and D.



There will be no need to perform synthetic backup since all recovery points consist of a set of references to data blocks, which helps achieve fast recovery time since the system doesn't need to process all the increments or run full backup. The benefit of creating a recovery point with referenced blocks along with forever incremental backup is to reduce storage usage and bring fast recovery time. Since this exclusive way of storing data is based on Synology's deduplication technology, please click [here](#) to learn more about the built-in feature.

Changed Block Tracking

- **Virtual machine**

Changed Block Tracking (CBT) is VMware's native technology that tracks the blocks of a virtual machine disk that have been changed since a certain point in time. This native feature is employed on VMware VMs with hardware version 7 and later. It is derived from the VMware Data Protection API which allows third-party backup applications to take advantage of CBT to perform incremental backups. Instead of performing the full backup, Synology Active Backup for Business VM backup queries CBT through VMware and gets a list of changed blocks since the last backup session.

With VMware CBT enabled, the amount of data transferred after the first full backup will be greatly reduced and therefore speed up the backup process.

In some situations, VMware vSphere CBT might be disabled, such as when VMs run an earlier version of virtual hardware, or when CBT is disabled at the ESX host level due to free license. If Synology Active Backup for Business VM backup cannot use VMware vSphere CBT, full backup will be performed automatically.

To enable CBT for a virtual machine, please refer to [this article](#) for more information.

- **Personal computer and physical server**

The CBT technology adopted in Active Backup for Business leverages VSS to take snapshots for devices and identify the changed block between snapshots. To ensure CBT is functioning well, please make sure Microsoft Volume Shadow Copy Service (VSS) on each protected device has been turned on. VSS belongs to Microsoft's built-in technology, and thus it can avoid performance interference while Active Backup for Business is performing the CBT technology. After the first full backup, the CBT technology allows each device to transfer only the changed block to your NAS. Therefore, it helps you to save the bandwidth resource and speeds up the process of backing up.

Storage Reduction

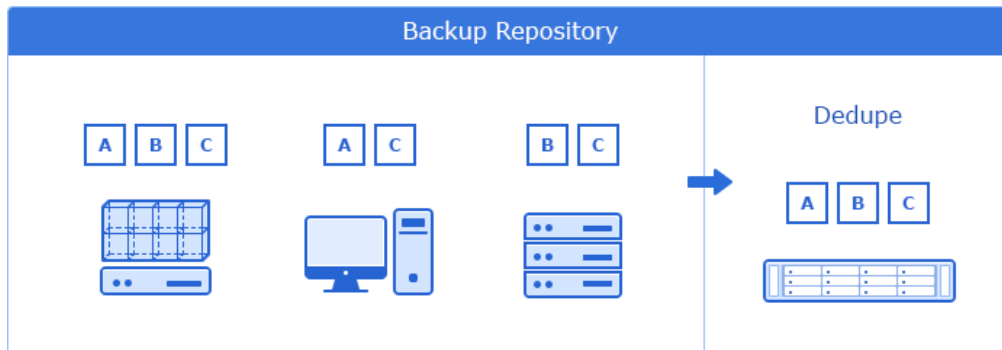
Active Backup for Business provides built-in deduplication technology to greatly enhance storage efficiency. In addition, storing full synthetic data, which leverages the Btrfs file system, helps reduce the usage of storage.

- **Built-in deduplication**

Data deduplication reduces the size of backup files and is automatically enabled. You can greatly save storage space when backing up several VMs that have a large amount of free space on their logical disks or VMs that have similar data blocks. Data deduplication also works across devices and platforms, so it can delete identical blocks on your PC / server / VM. With this feature enabled, storage efficiency can be significantly enhanced.

Here is an example of how it works:

You execute the first full backup of a VM running Windows Server 2016 from Hypervisor One, and at the same time, you also have a physical server running Windows Server 2016. When you create two backup tasks for these two different devices, only one copy of Windows Server 2016 will be written on Synology NAS since the other will be duplicated almost completely. Even you back up two Windows devices running different operating systems such as Windows 8 and 10, as long as there are identical blocks, they will still be deleted.



There are different deduplication mechanisms in the market. To ensure maximum storage and resource efficiency, Synology Active Backup for Business uses target inline deduplication with hash-based duplicate detection.

Inline deduplication scans the data and deletes the duplicated blocks before it is written to a backup repository. Since this technique clears repeated backup data, it helps to reduce the requirement of storage in a repository. To identify identical blocks, this technique uses cryptographic algorithms such as SHA-256 to calculate a hash for each block, which is the divided fixed length backup data. The blocks with same hashes are considered to be identical and therefore deleted.

Backup verification

To ensure the backup reliability, Synology Active Backup for Business integrates with Synology Virtual Machine Manager to verify the backups. Synology Virtual Machine Manager (VMM) will shoot a video when importing the backup image and running up the image. The duration of the video is decided by the user and the video will be played at 3x speed. Users will receive a preview of the video along with the notification email. Please note that Synology VMM 2.3 or above must be installed before you enable this feature, and the cluster of Synology VMM and the backup destination should be on the same volume to perform the backup verification. For further information on how to create a backup task with the live video verification, please refer to [here](#).

Create Backup Tasks

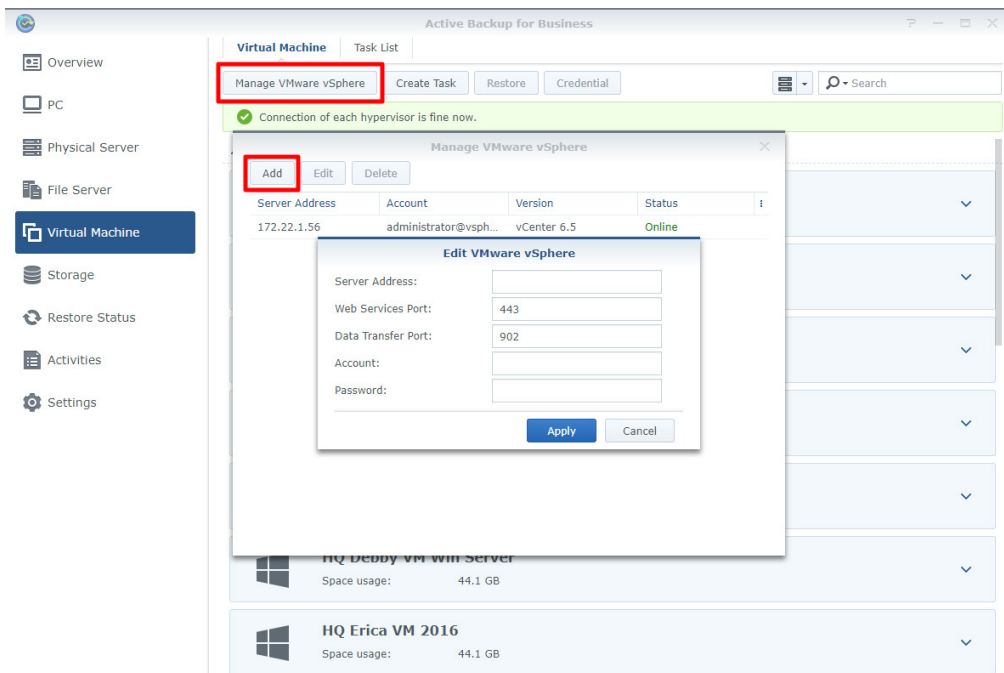
Virtual machine

To back up VMs, you must configure a backup task, which defines how, where, and when to back up VM data. One backup task can be used to process one VM or more. You can configure a backup task and start it immediately or save the task and run it later. This section will guide you through how to create backup tasks step by step.

• Before You Start

Before you start, please check if there are existing VMs. If not, please follow the following steps to add the vCenter Server or vSphere Hypervisor (ESX / ESXi) to have VMs available.

- 1 Click **Manage VMware vSphere** > **Add** to connect to VMware vSphere.
- 2 Fill in the server address and account information to connect to VMware vSphere.



Note: The storage space of the backup destination and the volume where the package is installed has to be at least 8G to perform backup tasks.

Apart from adding VMware vSphere, you can also edit / delete the vCenter Server or vSphere Hypervisor (ESX / ESXi) in **Manage VMware vSphere**:

- Edit: Select existing servers and change the account names and passwords.
- Delete: Delete servers that are not needed. If there are protected VMs in current backup tasks, you need to delete those tasks in order to delete the servers.

• Launch the Backup Wizard

You can do any of the following to launch the backup wizard:

- Go to **Active Backup for Business** > **Virtual Machine** > **Virtual Machine**, single select or shift / ctrl + left click to multi-select the virtual machines you want to back up, and click **Create Task** to launch the backup wizard.
- Go to **Active Backup for Business** > **Virtual Machine** > **Virtual Machine**, and click **Create Task** to open the backup wizard.
- Go to **Active Backup for Business** > **Virtual Machine** > **Task**, and click **Create** to launch the backup wizard.

- **Backup Wizard:**

To select backup destination and VMs:

After the backup wizard is opened, select a shared folder which is in the Btrfs file system as the backup destination, specify a name for the backup task, and select virtual machines for this backup task.

Note: For users who have already done the selection in the virtual machine tab, the selected VMs will be automatically displayed on the page.

To configure task settings:

- **Maximum quantity of concurrent backup device(s):** Configure the number of concurrent backed up devices. The maximum number of backed up virtual machines is 10.
- **Enable VMware Changed Block Tracking:** Enable VMware Changed Block Tracking (CBT) to only transfer blocks that have changed since the last backup and greatly reduce the transferred data size.
- **Enable Application-aware Backup:** Perform an application-aware backup to ensure application data is consistent. Please note that this feature leverages VMware Tools and Microsoft's Volume Shadow Copy Service (VSS) to ensure the consistency of the backed up data for Linux and Windows VMs. Therefore, the latest version of VMware Tools needs to be installed, and the Windows VMs supporting VSS is required.
- **Enable Data Transfer Compression:** Compress the source data to reduce the transferred data size and significantly reduce the used storage space.
- **Enable Data Transfer Encryption:** Encrypts the transferred data to enhance data security.
- **Enable source datastore usage detection:** Since taking snapshot may require additional space on the host datastore, insufficient space on the datastore may cause the virtual machine to suspend automatically and lose data. By enabling this feature, the backup job will fail when the host datastore is lower than the certain percentage you have set.
- **Enable backup verification:** Enable backup verification to enhance backup reliability. By using Synology Virtual Machine Manager (VMM) to boot up a backed up device and shoot a video, users can make sure that the backup file can be properly executed.
- **Take livevideo for ... sec.:** Specify the duration for your video, which will start shooting once Synology Virtual Machine Manager begins running the backup image. The video will be played at 3x speed.
- **Advanced settings:** Set up the script and credential for individual VMs.
 - Select single virtual machine or shift + left click to multi-select virtual machines to specify script / credentials setting for VMs.
 - Click **Script** to browse the script executed in the guest OS and specify the script processing mode.
 - **Required successful processing:** VM backup process will stop if the script failed to be executed.
 - **Ignore script execution failure and continue the VM backup:** VM backup process will continue even if the script failed to be executed.
 - Click credential to specify the username and password for individual VM.

Create a virtual machine backup task
✕

Task Settings

Configure settings for your task

Maximum quantity of concurrent backup device(s):

Enable VMware Changed Block Tracking i

Enable application-aware backup i

Enable data transfer compression i

Enable data transfer encryption

Enable source datastore usage detection

When free space is less than %, backup will fail.

Enable backup verification i

Take live video for sec. i

Advanced Settings

Back
Next
Cancel

Note:

- By setting up the script and enabling the VM script execution, the credential of VM is required. An error message will be displayed if the credential is missing.
- VMware Tool is required to be installed to execute pre-post script.
- For free ESXi, CBT is required to be manually enabled.
- Synology Virtual Machine Manager is required to be installed to enable backup verification
- Data transfer compression cannot be enabled for versions below vSphere 5.1 because of VMware limitations.

To set the backup schedule:

You may set up the backup schedule based on your backup policy.

- **Manual Backup:** Backup task will only be performed upon manually click Backup. No scheduled backup will be performed.
- **Scheduled Backup:** Set the backup task to be performed on an hourly, daily or weekly basis. Click on the drop-down menu to check the days of the week you wish the task to be carried out.

×Create a virtual machine backup task

Schedule Backup Task

Choose whether you would like to back up manually or configure a backup routine

Manual backup

Scheduled backup

Run on: Daily ▼

Repeat type: Hourly ▼

Start at: 00 ▼ : 00 ▼

BackNextCancel

To set the retention policy:

In this step, you can choose either one of the following retention policy to apply to the created task:

- **Keep all versions:** All the backed-up versions will be preserved.
- **Apply the following methods:**

Synology employs the Grandfather-Father-Son (GFS) retention policy. You can configure the time ranges of backup versions to be retained for the following time ranges respectively: daily, weekly, monthly, and yearly. If more than one backup version exists within a time range, only the latest one will be kept. For example, if you set a policy as **Keep the latest version of the day for** 1 day for the backup task which will be run every hour per day, only the version backed up at 23:00 will be kept.

You need to set at least one policy if you check **Apply the following methods**. Please note that every configured policy overlaps with each other. For example, if you would like to set the policy as keeping daily backup versions in the first three months, weekly backup versions in the second three months, and monthly backup versions in the third three months. Please tick the checkboxes and insert the numbers as the below picture displays.

Create a virtual machine backup task
✕

Select Retention Policy

Select a retention policy you prefer

Keep all versions

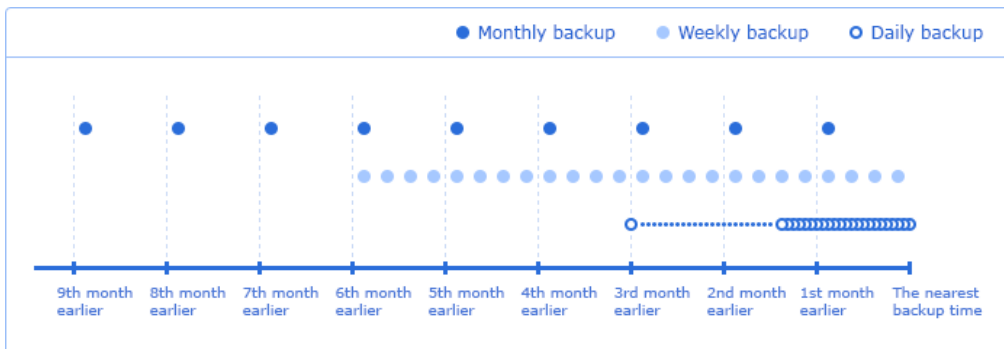
Apply the following methods

<input type="checkbox"/> Keep all the versions for		<input type="text" value=""/>	days
<input checked="" type="checkbox"/> Keep the latest version of the day for		<input type="text" value="90"/>	days
<input checked="" type="checkbox"/> Keep the latest version of the week for		<input type="text" value="24"/>	weeks
<input checked="" type="checkbox"/> Keep the latest version of the month for		<input type="text" value="9"/>	months
<input type="checkbox"/> Keep the latest version of the year for		<input type="text" value=""/>	years

Note: First day of the week is Sunday; first month of the year is January.

Back
Next
Cancel

The duration of 24 weeks includes the previous daily backup versions of 90 days, and the first weekly backup will be equal to the seventh daily backup. The duration of 9 months also includes the previous weekly backup versions of 24 weeks and daily backup versions of 90 days, and the first monthly backup will be equal to the fourth weekly backup.



To configure privilege settings:

Privilege settings are configurable when creating the backup task. To ensure only eligible users can have access to restore backed-up files and versions of the backup task, privilege settings can be configured during task creation. You can always edit the task to change the privilege settings.

Check the user/group that can browse and restore backed-up versions of the task.

Administrators group/users are default eligible to restore the backup task.

To apply settings and back up the task:

After configuring all the backup settings, a backup summary will be displayed. Please follow the instructions below to finalize the backup after confirming your settings:

- 1 Click **Apply** to create the backup task and a pop-up window will appear.
- 2 Click **Yes** if you would like to run the backup immediately, or you may click **Backup** on the task list if you want

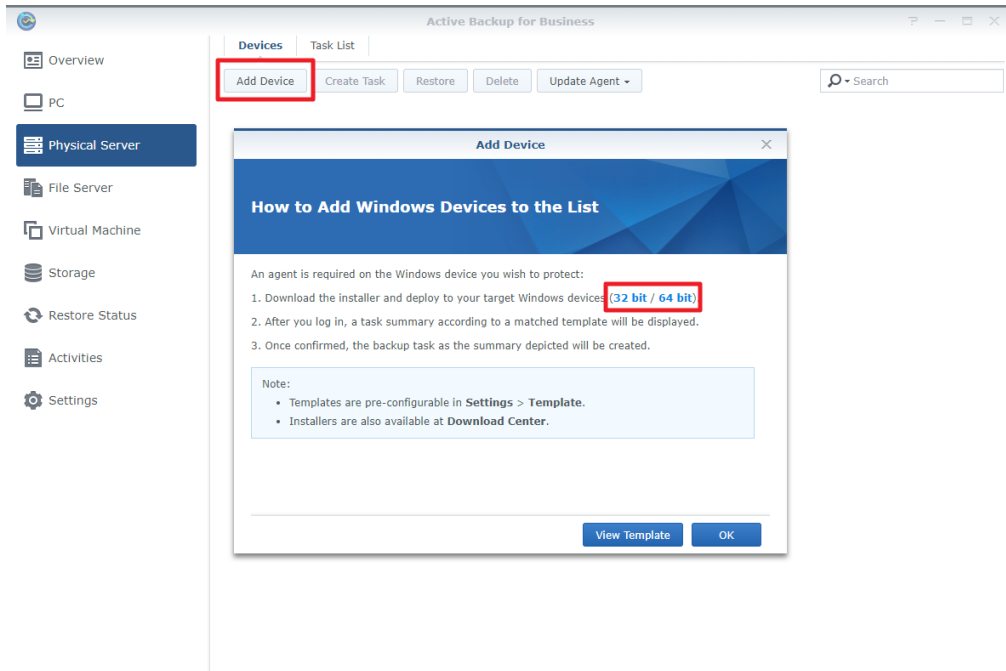
to run the task afterward.

Physical server

• Before You Start

Please note the following:

- Install Active Backup for Business Agent on the target device you wish to protect. You can either go to Synology [Download Center](#) or go to [Active Backup for Business > Physical Server > Add device](#) to download the 32-bit or 64-bit installer for the device.



- Configure a **Template** on Active Backup for Business. Go to **Settings > Template > Create** to create a template or select the default template and click **Edit** to edit the default template.
- Configuring backup settings of a template can help apply the same backup settings to multiple devices in mass deployment. To avoid gap between deployment and protection, a default template set to protect physical servers will be listed and cannot be removed. You can always edit the default template or add other templates.
- When creating a template, you can decide the backup type, backup schedules, compression, encryption settings, and the version retention policy. The restore permission of physical server backup is not adjustable. Only admin (user), administrators (group), and the logged-in account (user) owner can access the backup versions of devices.

• Back up Physical Server

To create a backup task:

Once the agent is installed on the physical server and the physical server is connected to the server, a backup task of the connected server will be created according to the matched **template**. It also supports creating more than one backup task to each device. To create a new task of a specific device: Go to **Physical Server**, you can either start from the device view, select the target device, and then click **Create** to enter the task creation wizard, or go to **Task List > Create**, and decide which device you wish to protect later in the task creation wizard.

- **Create backup task:**
 - **Task name:** Configure the name of the task. It is suggested to have a naming pattern for faster filter/search for the task.
- **Select target device:**

This step only appears if no device is selected before clicking **Create**. A list of physical servers that have been connected to the server will be shown in this step.

- **Backup destination:**

During package installation, a Btrfs shared folder - ActiveBackupforBusiness will be created automatically. Only Btrfs shared folder can be selected as the backup destination on the NAS.

- **Select source type:**

Three types of source are supported:

- **Bare metal:** The entire physical server including the device settings, applications and all the files will be backed up in this mode.
- **System volume:** Only the drivers will be backed up.
- **Customized volume:** Click **Select** then choose the target volume you wish to protect. USB (Flash Driver) is not supported.

Task settings: The source data can be compressed and encrypted according to the task settings. Click **Task Settings** and configure your preference.

The screenshot shows a window titled "Agent Backup Creation Wizard" with a close button (X) in the top right corner. The main heading is "Select Source Type" with the subtitle "Select a backup scope".

Source type:

- Bare-metal
- System volume
- Customized volume: ---

Task settings:

- Enable data transfer compression
- Enable data transfer encryption
- Enable application-aware backup
- Enable backup verification **i**

Take live video for sec. **i**

At the bottom, there are three buttons: "Back", "Next", and "Cancel".

- **Schedule backup task:**
 - **Manual Backup:** Manual Backup means one-time only backup. After creating a backup task, you can run the task by choosing to back up immediately in the last step or selecting the task then click **Run now** on the console.
 - **Scheduled Backup:** Define the desired backup schedule to be a daily or only on specific days' backup. The task can run once a day or once an hour according to the settings.

Agent Backup Creation Wizard ✕

Schedule Backup Task

Choose whether you would like to back up manually or configure a backup routine

Manual backup

Scheduled backup

Run on:

Repeat type:

Start at: :

- **Select retention policy:**

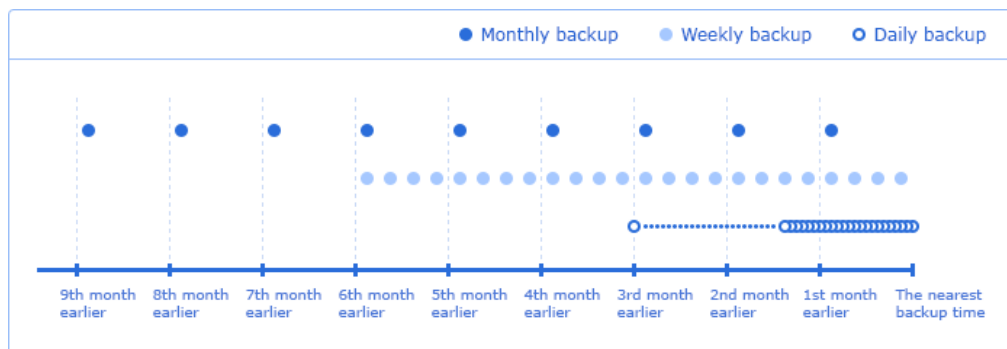
In this step, you can choose either one of the following retention policy to apply to the created task:

- **Keep all versions:** All the backed-up versions will be preserved.
- **Apply the following methods:**

Synology employs the Grandfather-Father-Son (GFS) retention policy. You can configure the time ranges of backup versions to be retained for the following time ranges respectively: daily, weekly, monthly, and yearly. If more than one backup version exists within a time range, only the latest one will be kept. For example, if you set a policy as **Keep the latest version of the day for** 1 day for the backup task which will be run every hour per day, only the version backed up at 23:00 will be kept.

You need to set at least one policy if you check **Apply the following methods**. Please note that every configured policy overlaps with each other. For example, if you would like to set the policy as keeping daily backup versions in the first three months, weekly backup versions in the second three months, and monthly backup versions in the third three months. Please tick the checkboxes and insert the numbers as the below picture displays.

The duration of 24 weeks includes the previous daily backup versions of 90 days, and the first weekly backup will be equal to the seventh daily backup. The duration of 9 months also includes the previous weekly backup versions of 24 weeks and daily backup versions of 90 days, and the first monthly backup will be equal to the fourth weekly backup.



- **Backup now:**

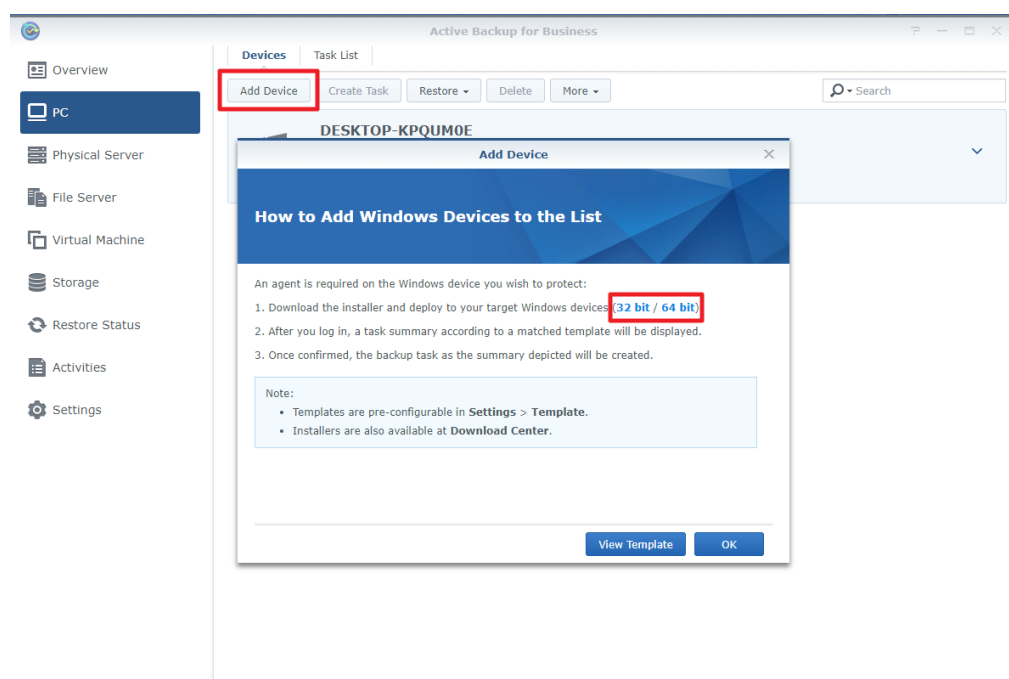
The wizard allows an immediate backup regardless of the schedule.

Personal computer

- **Before You Start**

Please note the following:

- Install Active Backup for Business Agent on the target device you wish to protect. You can either go to Synology [Download Center](#) or go to **Active Backup for Business > PC > Add device** to download the 32-bit or 64-bit installer for the device.



- Configure a **Template** on Active Backup for Business. Go to **Settings > Template > Create** to create a template or select the default template and click **Edit** to edit the default template.
- Configuring backup settings of a template can help apply the same backup settings to multiple devices in mass deployment. To avoid gap between deployment and protection, a default template set to protect personal computers will be listed and cannot be removed. You can always edit the default template or add other templates.
- When creating a template, you can decide the backup type, backup schedules, compression, encryption settings, and the version retention policy. The restore permission of PC backup is not adjustable. Only admin (user), administrators (group), and the logged-in account (user) owner can access the backup versions of devices.

- **Back up Personal Computer**

To create a backup task:

Once the agent is installed on the personal computer and the personal computer is connected to the server, a backup task of the connected server will be created according to the matched **template**. It also supports creating more than one backup task to each device. To create a new task of a specific device: Go to **PC**, you can either start from the device view, select the target device, and then click **Create** to enter the task creation wizard, or go to **Task List > Create**, and decide which device you wish to protect later in the task creation wizard.

- **Create backup task:**
 - **Task name:** Configure the name of the task. It is suggested to have a naming pattern for faster filter/search for the task.
- **Select target device:**

This step only appears if no device is selected before clicking **Create**. A list of personal computers that have been

connected to the server will be shown in this step.

- **Backup destination:**

During package installation, a Btrfs shared folder - ActiveBackupforBusiness will be created automatically. Only Btrfs shared folder can be selected as the backup destination on the NAS.

- **Select source type:**

Three types of source are supported:

- **Bare metal:** The entire physical server including the device settings, applications and all the files will be backed up in this mode.
- **System volume:** Only the drivers will be backed up.
- **Customized volume:** Click **Select** then choose the target volume you wish to protect. USB (Flash Driver) is not supported.

The screenshot shows a window titled "Agent Backup Creation Wizard" with a close button (X) in the top right corner. The main heading is "Select Source Type" with the subtitle "Select a backup scope".

Under "Source type:", there are three radio button options:

- Bare-metal
- System volume
- Customized volume: ---

Under "Task settings:", there are two checked checkboxes:

- Enable data transfer compression
- Enable data transfer encryption

At the bottom, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted in blue.

Task settings: The source data can be compressed and encrypted according to the task settings. Click **Task Settings** and configure your preference.

- **Schedule backup task:**
 - **Manual Backup:** Manual Backup means one-time only backup. After creating a backup task, you can run the task by choosing to back up immediately in the last step or selecting the task then click **Run now** on the console.
 - **Scheduled Backup:** Define the desired backup schedule to be a daily or only on specific days' backup. The task can run once a day or once an hour according to the settings.

The screenshot shows a dialog box titled "Agent Backup Creation Wizard" with a close button (X) in the top right corner. The main heading is "Schedule Backup Task" with the instruction "Choose whether you would like to back up manually or configure a backup routine". There are two radio button options: "Manual backup" (unselected) and "Scheduled backup" (selected). Below these are three configuration fields: "Run on:" with a dropdown menu set to "Daily", "Repeat type:" with a dropdown menu set to "Hourly", and "Start at:" with two dropdown menus for hours and minutes, both set to "00". At the bottom, there are three buttons: "Back", "Next" (highlighted in blue), and "Cancel".

- **Select retention policy:**

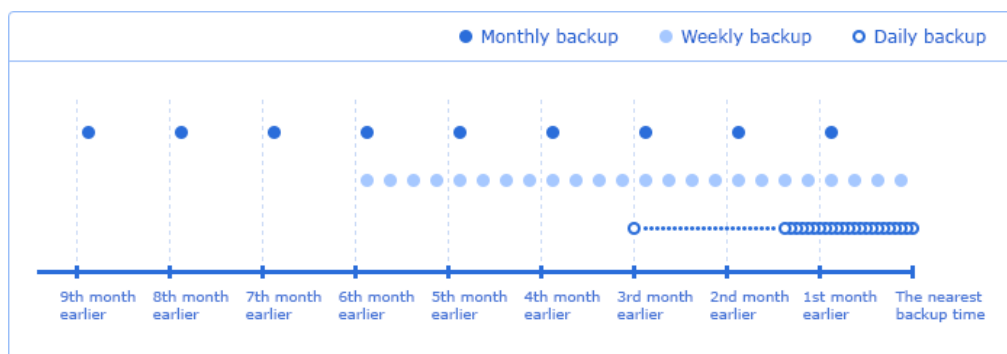
In this step, you can choose either one of the following retention policy to apply to the created task:

- **Keep all versions:** All the backed-up versions will be preserved.
- **Apply the following methods:**

Synology employs the Grandfather-Father-Son (GFS) retention policy. You can configure the time ranges of backup versions to be retained for the following time ranges respectively: daily, weekly, monthly, and yearly. If more than one backup version exists within a time range, only the latest one will be kept. For example, if you set a policy as **Keep the latest version of the day for** 1 day for the backup task which will be run every hour per day, only the version backed up at 23:00 will be kept.

You need to set at least one policy if you check **Apply the following methods**. Please note that every configured policy overlaps with each other. For example, if you would like to set the policy as keeping daily backup versions in the first three months, weekly backup versions in the second three months, and monthly backup versions in the third three months. Please tick the checkboxes and insert the numbers as the below picture displays.

The duration of 24 weeks includes the previous daily backup versions of 90 days, and the first weekly backup will be equal to the seventh daily backup. The duration of 9 months also includes the previous weekly backup versions of 24 weeks and daily backup versions of 90 days, and the first monthly backup will be equal to the fourth weekly backup.



- **Backup now:**

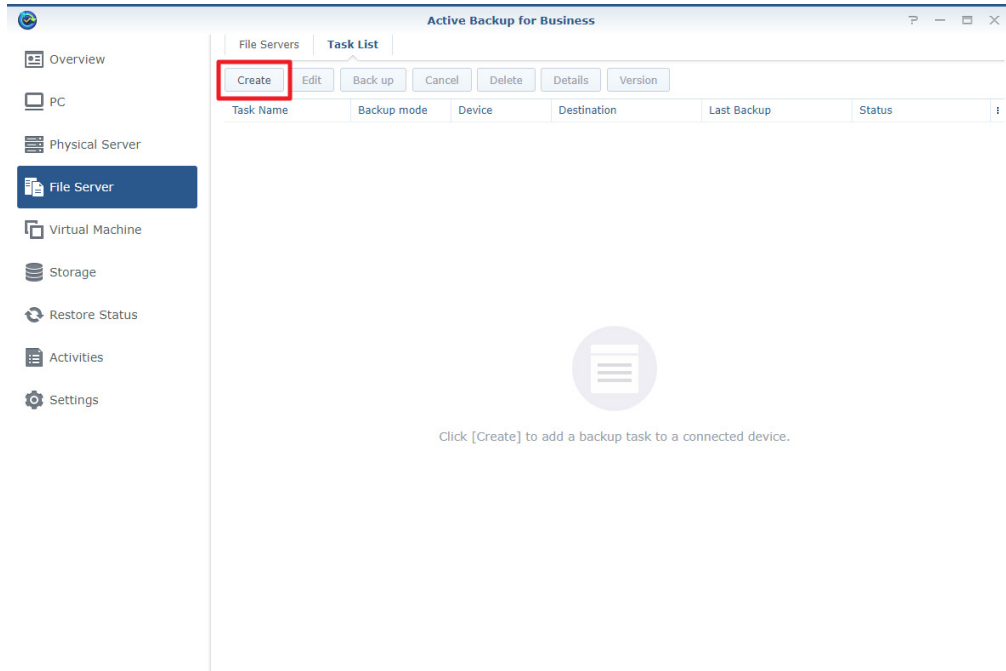
The wizard allows an immediate backup regardless of the schedule.

File server

In File Server, servers communicating with SMB or rsync can be protected. Depending on your source, you can create SMB backup or rsync backup tasks in the corresponding tabs.

To create a backup task:

1 Click **Create** to start the wizard.

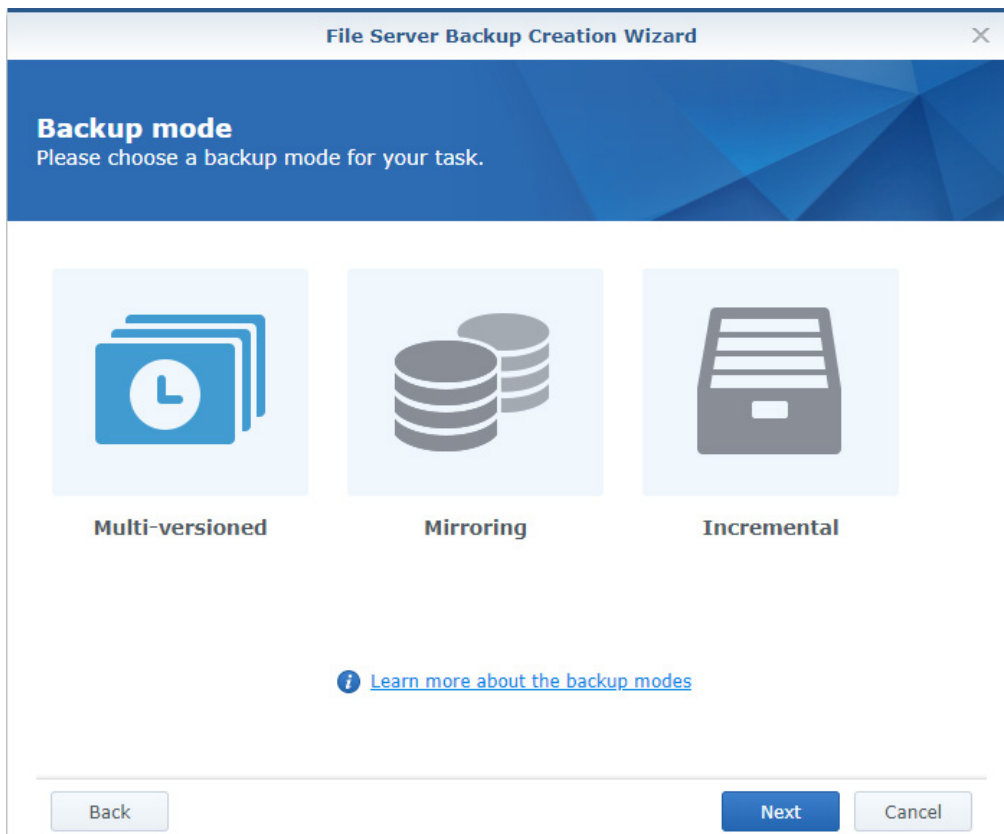


2 Select your backup mode:

- **Multi-versioned**: each time the task runs, a new version of the changes at the source will be copied in its entirety to a new folder at the destination.

Note: For Linux sources, block transfer can be configured at a later stage in the setup.

- **Mirroring**: each time the task runs, all changes made in the source folder will be copied to the destination and overwrite the existing file, making the destination folder a complete mirror copy of the source.
- **Incremental**: each time the task runs, newly added and modified source files will be copied to the destination, overwriting the previous version of the file.



Please see the table below to learn the variations of final backup files on DSM with three different types of backup modes.

Backup order / Source files	Multi-version mode	Mirroring mode	Incremental mode
1st Backup: A B	ver.1 A B	A B	A B
2nd Backup: A B C	ver.1 A B ver.2 A B C	A B C	A B C
3rd Backup: A B C D E	ver.1 A B ver.2 A B C ver.3 A C D E	A C D E	A B C D E
4th Backup: A B C D E	ver.1 A B ver.2 A B C ver.3 A C D ver.4 A E	A E	A B C D E

3 Do the following to configure your backup task:

- **For SMB backup:** enter your **Server address**, **Account**, and **Password**.
- **For rsync backup:** enter your **Server address**, **Port**, and **Account**, and select **Connection Mode** and **Auth Policy** from the drop-down menus.
 - **Connection Mode:** **rsync shell mode via SSH**, **rsync module mode via SSH**, **rsync module mode** (which offers data transmission without encryption).
 - **Auth Policy:** **by password** or **by SSH key**.

4 Click **Next** to continue.

5 Indicate what you want to transfer using the following four states:

- All subordinate folders and files in this folder will not be backed up.
- All subordinate folders and files in this folder will be backed up.
- Only the subordinate folders you have selected in this folder will be backed up.
- The files in this folder and the subordinate folders you have selected will be backed up.

6 Click **Next** to continue.

7 Enter your **Task name** and **Local path**, and set a **Schedule** for your backup task.

- If you are configuring **rsync backup**, you have the option of configuring **Bandwidth** as well as enabling **compression** and **block transfer**.

The screenshot shows the 'File Server Backup Creation Wizard' window. The title bar reads 'File Server Backup Creation Wizard'. The main heading is 'Task settings' with the instruction 'Please fill in the task related information.' Below this, there are several input fields and checkboxes: 'Task Name:' with an empty text box; 'Local path:' with an empty text box and a 'Browse' button; 'Enable Volume Shadow Copy' with an unchecked checkbox; 'Enable schedule' with a checked checkbox; 'Run on the following days:' with a dropdown menu set to 'Daily'; and 'First run time:' with two dropdown menus set to '00' and '00'. There is an 'Advanced Settings' button below the time fields. At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Cancel'.

8 If you selected **Multi-versioned** as your backup mode, you will have the option to set up a **Retention Policy** to manage backup versions by automatically deleting unwanted versions and potentially freeing up storage space.

- **Keep all versions:** All the backed-up versions will be preserved.
- **Apply the following methods:**

Synology employs the Grandfather-Father-Son (GFS) retention policy. You can configure the time ranges of backup versions to be retained for the following time ranges respectively: daily, weekly, monthly, and yearly. If more than one backup version exists within a time range, only the latest one will be kept. For example, if you set a policy as **Keep the latest version of the day for 1 day** for the backup task which will be run every hour per day, only the version backed up at 23:00 will be kept.

You need to set at least one policy if you check **Apply the following methods**. Please note that every configured policy overlaps with each other. For example, if you would like to set the policy as keeping daily backup versions in the first three months, weekly backup versions in the second three months, and monthly backup versions in the third three months. Please tick the checkboxes and insert the numbers as the below picture displays.

Agent Backup Creation Wizard
✕

Select Retention Policy

Select a retention policy you prefer

Keep all versions

Apply the following methods

Keep all versions for how many days: days

Keep the last one version of the day for how many days: days

Keep the last one version of the week for how many weeks: weeks

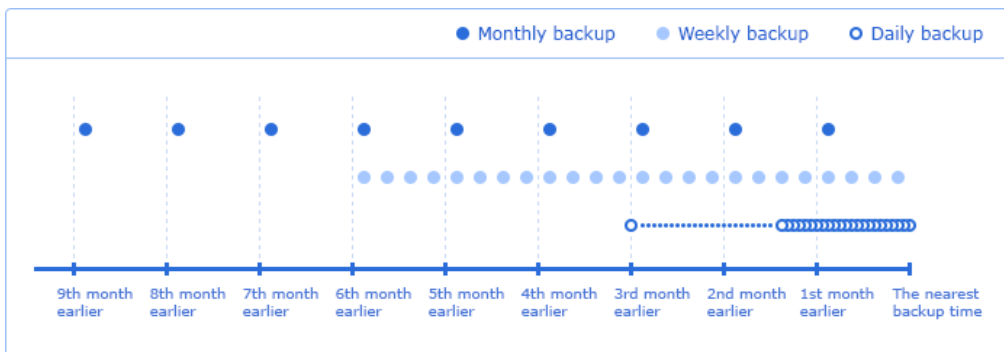
Keep the last one version of the month for how many months: months

Keep the last one version of the year for how many years: years

Note: First day of the week is Sunday; first month of the year is January.

Back
Next
Cancel

The duration of 24 weeks includes the previous daily backup versions of 90 days, and the first weekly backup will be equal to the seventh daily backup. The duration of 9 months also includes the previous weekly backup versions of 24 weeks and daily backup versions of 90 days, and the first monthly backup will be equal to the fourth weekly backup.



9 Check your task settings and click Apply to finish creating your backup task.

Note:

- Files will not be backed up by Active Backup for Business under the following circumstances:
 - The file/folder path is longer than 4096 characters.
 - The file/folder name is longer than 255 characters.
 - The file/folder name is ". " or ".. "
 - The file/folder name contains **@ActiveBackup** or **target.db**.
 - The file/folder under encrypted share, names longer than 135 characters.
- **SMB backup** does not support Microsoft accounts.
- **SMB backup** does not back up **junction points**.
- **SMB backup** supports Windows Volume Shadow Copy Service (VSS) to ensure data consistency. Windows VSS is supported on Windows Server 2012 and above. **By enabling VSS on the Windows server**, Active Backup for Server can create a volume shadow copy of VSS-aware server applications that store data on remote SMB file shares.
- Administrative shared folders (E.g. C\$, D\$) do not support Windows VSS by default.
- Authentication by SSH key will require a SSH key. Supported key types include rsa2, dsa, ecdsa, and ed25519, while rsa1 and SSH keys with a passphrase are not supported.

Manage Backup Tasks

This section demonstrates how to monitor backup status, examine detailed information about the backed up versions of each task, and delete/edit backup tasks.

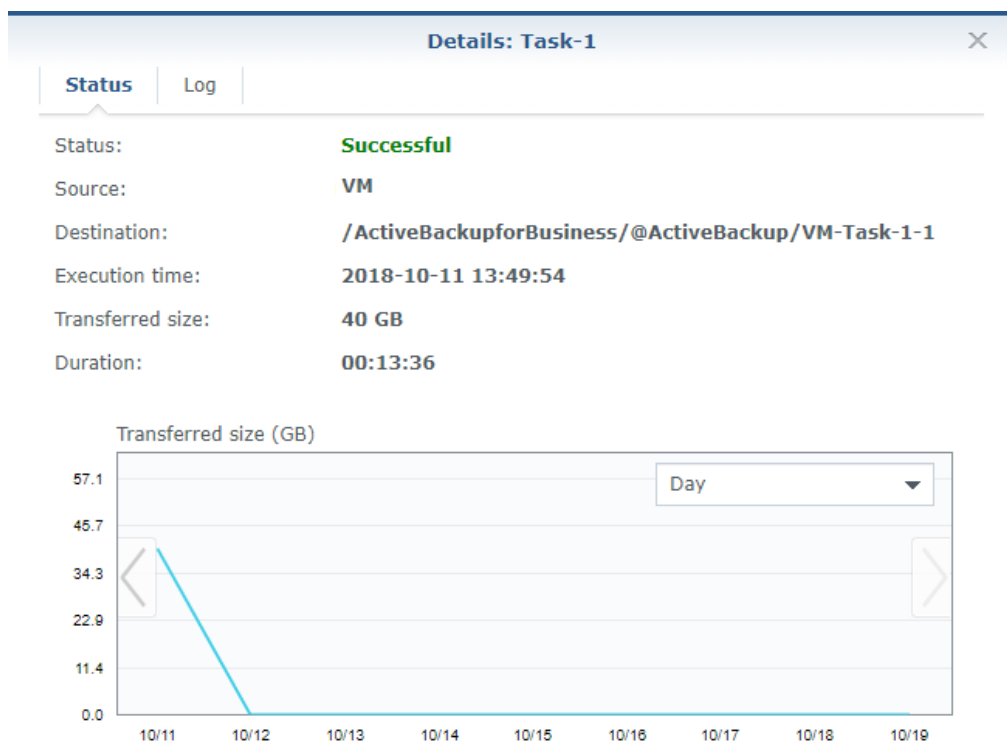
Virtual machine

This section demonstrates how to monitor backup status, examine detailed information about the backed up versions of each task, and delete / edit backup tasks.

- **Examine detailed information**

All existing tasks are displayed in **Active Backup for Business > Virtual Machine > Task**. Select the one you want to view more info about and click **Details**, which will include the following:

- **Status**
 - Status: complete, failed, or partially complete, suggesting the current status of the backup task.
 - Source: all backed-up VMs in the task.
 - Destination: backup destination of the stored data.
 - Execute time: last backup time of the task.
 - Transferred size: volume of data transferred from the source side. The displayed number may be different from the actual used storage space due to deduplication and compression.
 - Duration: elapsed time of the backup task.



- **Log**
 - Log type: the category that the log belongs to, information / warning / error.
 - Log description: the backup process of each task or encountered issues.
 - Log time: the time of each log.
 - Settings: You can click here to set up a log rotation policy.

X
Details: Task-1

Status | **Log**

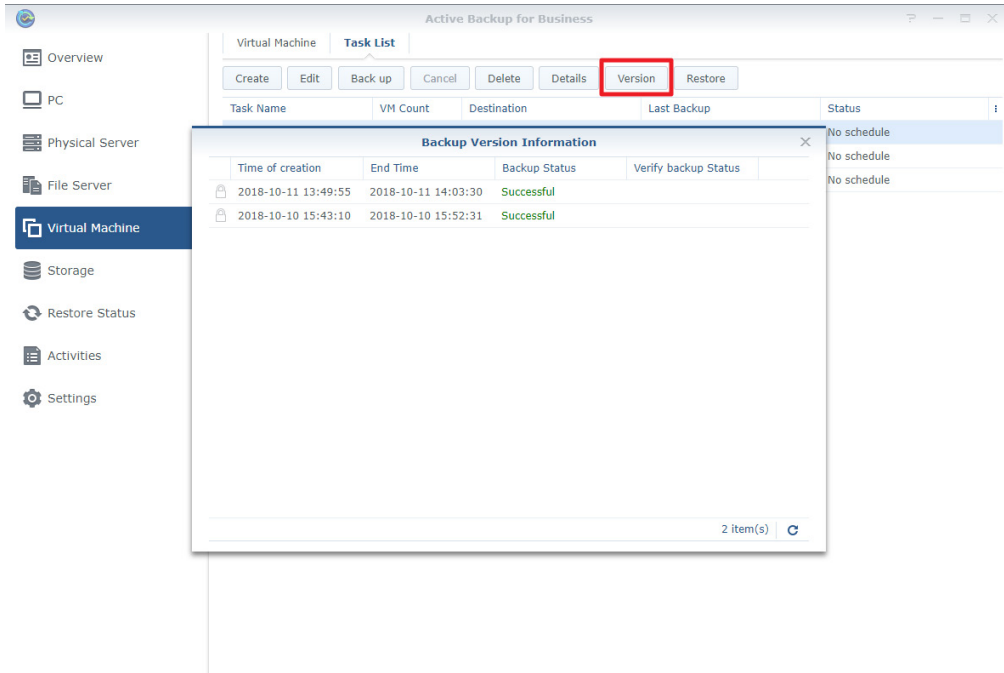
Log Type	Log Time	Log Description	⋮
Informati...	2018-10-11 14:0...	The backup task Task-1 was completed.	↗
Informati...	2018-10-11 14:0...	The VM VM was successfully backed up.	
Informati...	2018-10-11 13:4...	Starting to back up the VM VM.	
Informati...	2018-10-11 13:4...	The backup task Task-1 has started.	
Informati...	2018-10-10 16:5...	The restore task Task-1 was completed.	↗
Informati...	2018-10-10 16:5...	The VM VM was successfully restored.	
Informati...	2018-10-10 16:5...	Starting to restore the VM VM.	
Informati...	2018-10-10 16:5...	The restore task Task-1 has started.	
Informati...	2018-10-10 16:4...	The restore task Task-1 was completed.	↗
Informati...	2018-10-10 16:4...	The VM VM was successfully restored.	
Informati...	2018-10-10 16:4...	Starting to restore the VM VM.	
Informati...	2018-10-10 16:4...	The restore task Task-1 has started.	

30 item(s) | 🔄

- **Examine backed-up versions**

All existing tasks are displayed in **Active Backup for Business > Virtual Machine > Task**. Select the one you want to view more info about and click **Version**, which will include the following:

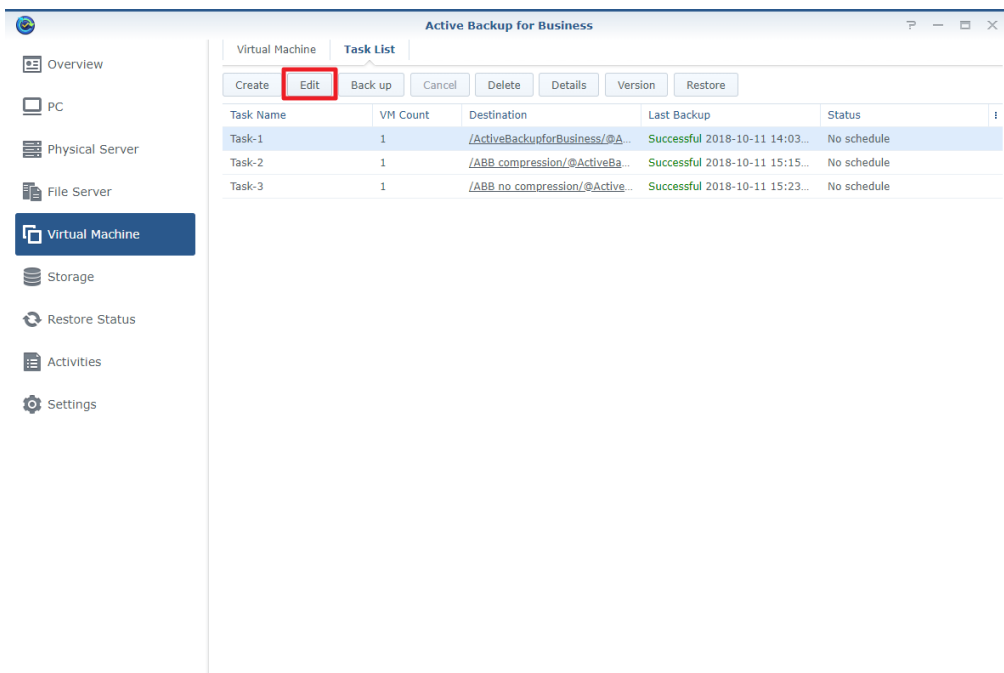
- Status: complete, failed, or partially complete.
- Date Created: the time when a backed-up version is created.
- You can also click the export icon to browse your backed-up data and the live video of the backup if the backup verification is enabled



- **Edit backup task settings**

All existing tasks are displayed in **Active Backup for Business > Virtual Machine > Task**. You can choose to edit a single task or multiple ones at the same time.

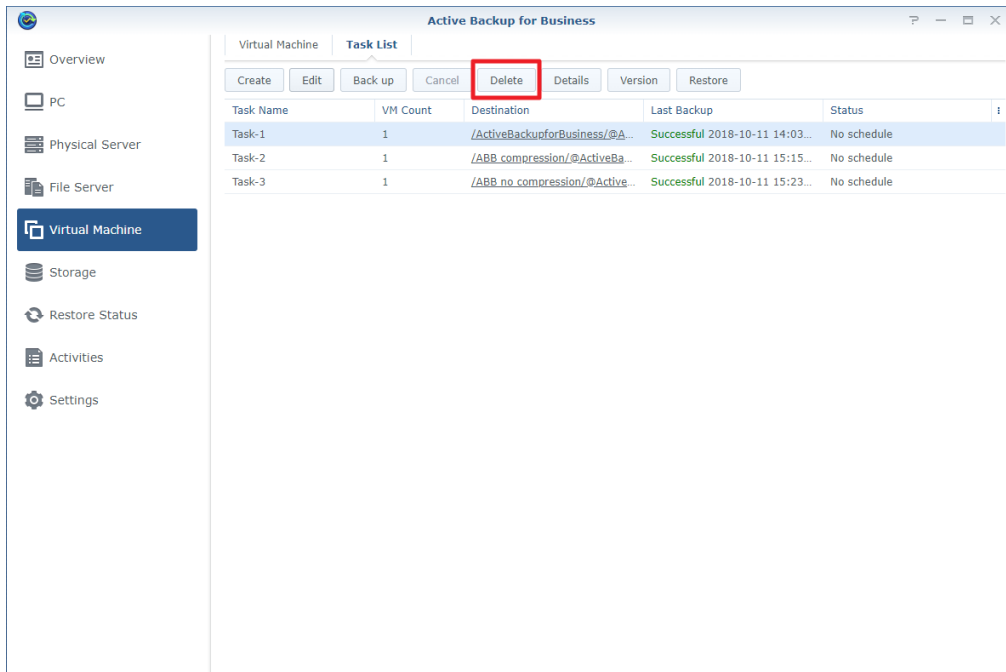
Single select the task you want to edit, and click **Edit**. You can then change the VMs you want to protect, configure task settings, make a backup schedule, set up a retention policy, and grant privileges.



- **Delete backup tasks**

All existing tasks are displayed in **Active Backup for Business > Virtual Machine > Task**. You can choose to delete a single task or multiple ones at the same time.

- Single select the task you want to edit, and click **Delete**. The task will be deleted from the panel, and all backed-up data in the task will be deleted as well.
- Shift / Ctrl + left click to multi-delete the backup tasks you want to delete, and click **Delete**. The task will be deleted from the panel, and all the backed-up data will be deleted as well.



Physical server

To edit one or more backup tasks:

It supports both editing tasks individually and in batch. Other than backup destination, most of the settings can be modified. However, in batch edit, the **task name** as well as the **destination** cannot be changed.

To avoid mistakenly changing the settings that varied across different tasks, the settings are set to remain as they are by default. Tick the checkbox of the section that you wish to change when batch editing is required.

To delete one or more backup tasks:

Go to **Task List** to select the task, and then click **Delete**. After confirming the action, the selected task will be removed while the data will remain in the backed up destination.

The device would still remain connected to the server even when it does not have any task. This device can always be found on the **Device List**, and you can create a task for the device at any time.

Note: If you tick the unchecked box before clicking **Apply**, the setting of the section would remain the same in every selected task.

Personal computer

To edit one or more backup tasks:

It supports both editing tasks individually and in batch. Other than backup destination, most of the settings can be modified. However, in batch edit, the **task name** as well as the **destination** cannot be changed.

To avoid mistakenly change the settings that varied across different tasks, the settings are set to remain as they are by default. Tick the checkbox of the section that you wish to change when batch editing is required.

Note: If you tick the unchecked the box before clicking **Apply**, the setting of the section would remain the same in every selected task.

To delete one or more backup tasks:

Go to **Task List** to select the task, and then click **Delete**. After confirming the action, the selected task will be removed while the data will remain in the backed up destination.

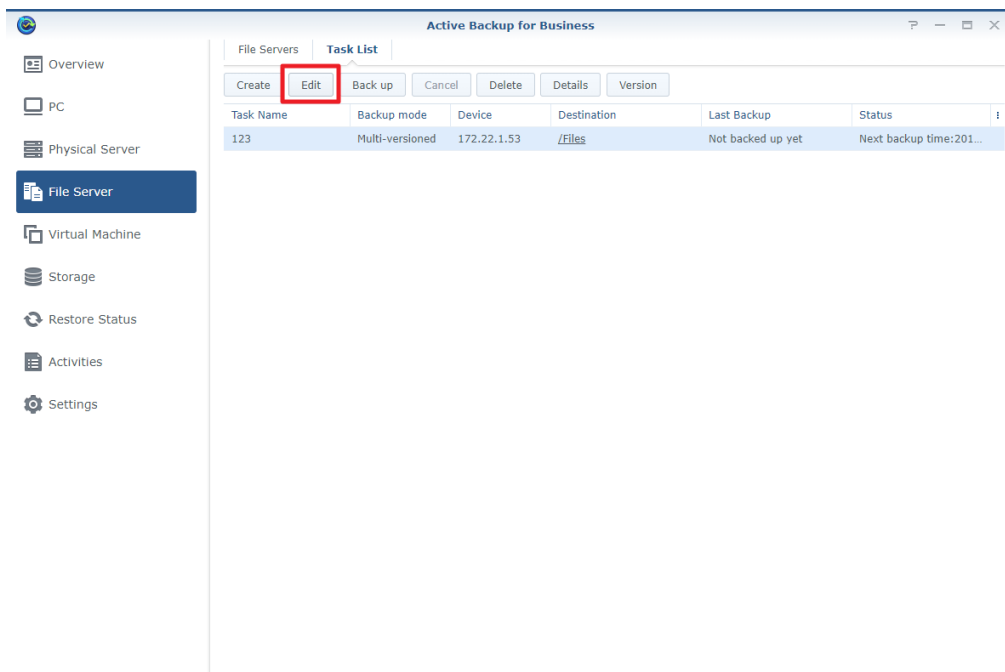
The device would still remain connected to the server even when it does not have any task. This device can always be found on the **Device List**, and you can create a task for the device at any time.

File Server

In **Task List**, you can see a list of all the backup tasks that have been created. You can also manage them with the buttons at the top of the tab.

To edit backup tasks:

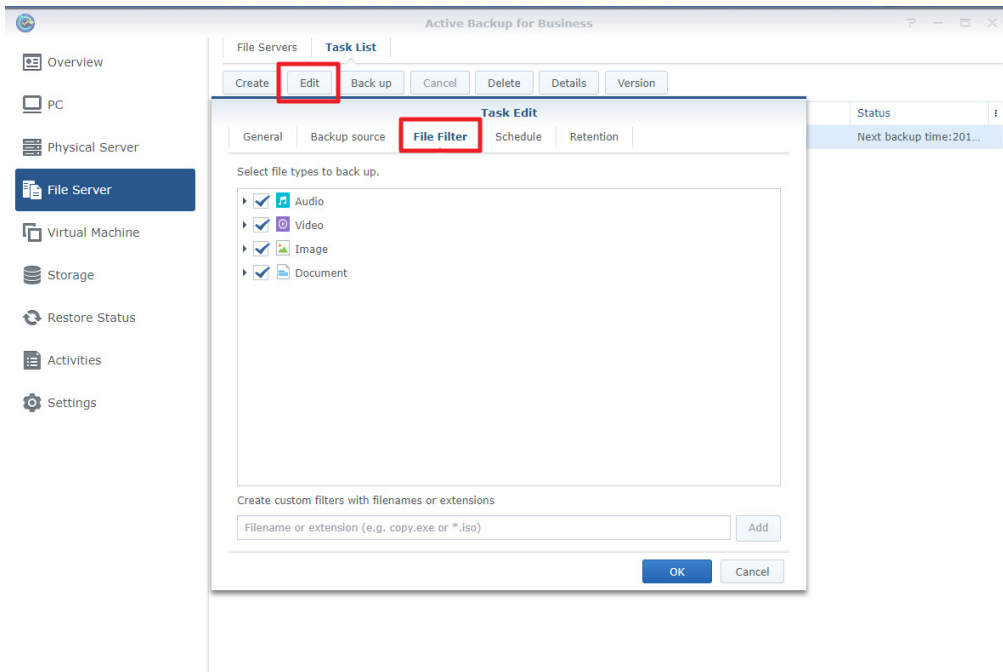
- 1 Select the backup task you want to edit and click **Edit**.



- 2 Here you can modify remote server information, connection mode and authentication method, adjust backup folder and file filter settings, enable and disable backup schedule, and configure other settings.
- 3 If you selected **Multi-versioned** as your backup mode, you can also edit backup rotation settings.

To manage file filters:

1 Select the backup task and click **Edit** > **File Filter**.



2 You can exclude specific files from backup jobs based on their file types, or create custom filters with the following methods:

- **Filenames:** Create custom filters with filenames. Files with designated filenames will be excluded from backup.
- **File extension:** Create custom filters with file extensions. Files with designated file extensions will be excluded from backup. You can specify file extensions by adding *.extension (e.g. *.iso).
- **Wildcard characters:** You can use wildcard characters (*) for more advanced filename filters.

Note:

- **File Filter** only filters out files and not folders.
- The wildcard represents zero or more non-space characters. Please see examples below:
 - **a*** can represent any word starting with **a**, such as **account**, **apple**.
 - ***e** can represent any word ending with **e**, such as **apple**, **table**.
 - ***12*** can represent any word that contains **12**, such as **2012**, **1220**, **341256**.

To run backup tasks:

You can set up a backup schedule during setup so your backup tasks will run regularly according to your schedule, or you can click **Back up** to run your task immediately.

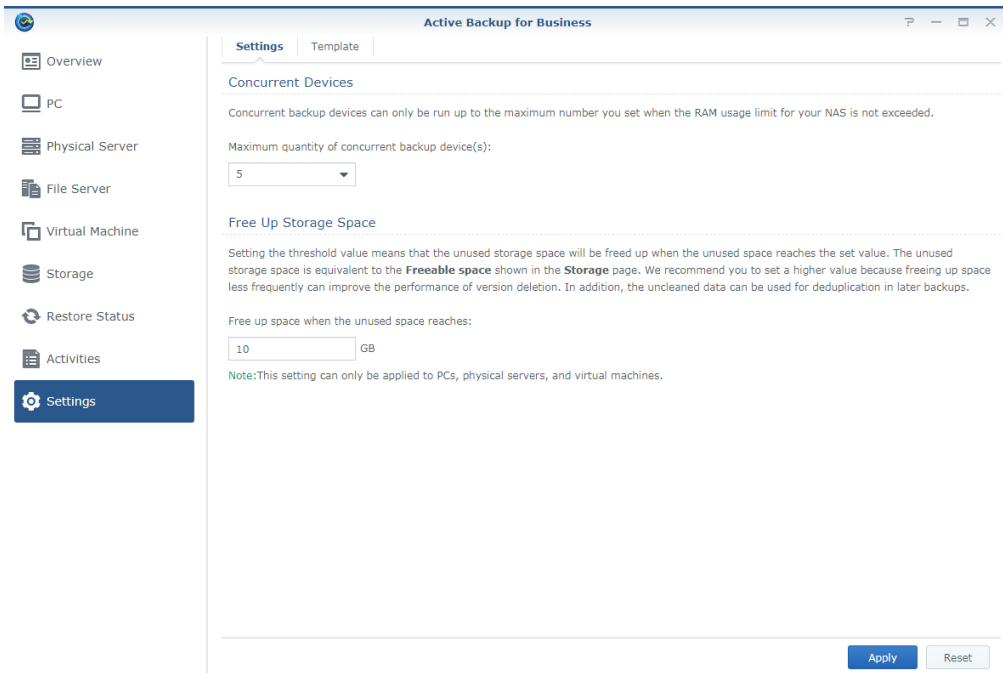
To delete backup tasks:

- 1 Select the backup task you want to delete.
- 2 Click **Delete**.

Backup Settings

In **Active Backup for Business > Settings**, you can set up a maximum number of concurrent backed up devices. Please note that concurrent backup devices can only be run up to the maximum number you set when the RAM usage limit for your NAS is not exceeded.

In **Active Backup for Business > Settings**, you can also set a threshold for releasing the unused storage space. When the unused space reaches the set value, the space will be freed up. The unused storage space is equivalent to the **Freeable space** shown in **Storage** page. You are recommended to set a higher value because freeing up space less frequently can improve the performance of version deletion. In addition, the uncleaned data can be used for deduplication in later backups.



Create a Second Backup

According to 3-2-1 backup strategy (create 3 copies of your data, 2 of which are on different storage mediums, and 1 of which should be kept in another location), you are recommended to create copies of the data of Active Backup for Business. When an IT disaster strikes, you can recover the data and task settings of Active Backup for Business and keep backing up or restoring your devices by relinking data.

To create copies of the data of Active Backup for Business:

You can choose either of the following packages on DSM to create copies of the data and task settings of Active Backup for Business.

- **Snapshot Replication:** Snapshot Replication helps you copy your data to another Synology NAS continuously by taking snapshots of your shared folders. When the recovery is needed, you can install Active Backup for Business and relink the data on another Synology NAS to continue backup and restoration tasks immediately. To learn more about Snapshot Replication, please refer to this [help article](#).
- **Hyper Backup:** Besides backing up shared folders to another Synology NAS, you have more choices of backup destinations via Hyper Backup, such as USB, file servers, and other cloud services. Please make sure that you select the "**@ActiveBackup**" folder in the **ActiveBackupforBusiness** shared folder when backing up Active Backup for Business via Hyper Backup. For more information about creating copies of the shared folder, please refer to this [help article](#).

Note: When creating copies of Active Backup for Business 2.0.4 with **Snapshot Replication**, you are strongly recommended to delete all the snapshots of the shared folder containing the earlier Active Backup for Business versions. Active Backup for Business has adopted a different dedup mechanism since version 2.0.4. If users use Snapshot Replication to take snapshot or perform replication of earlier versions, the replication efficiency might be influenced.

To retrieve the existing data and task settings of Active Backup for Business:

- 1 Please make sure there is a shared folder containing data and task settings of Active Backup for Business in the Synology NAS where you would like to recover Active Backup for Business.

Note: Only the shared folders containing the data backed up by Active Backup for Business 2.0.4 and later versions can be displayed and relinked.

- 2 In **Storage**, click **Relink**.

The below information of the shared folder which contains the data and task settings of Active Backup for Business will be displayed:

- The name of the shared folder.
- **Last backup time:** The last time when you backed up your data to this shared folder.
- **Source device:** The device which have been backed up.
- **Task name:** The name of the backup task contained in this shared folder.

- 3 Select the shared folder containing the data and task settings of Active Backup for Business you would like to recover and click **Relink**.

Recovery

Virtual Machine

This section provides an overview of the recovery options that Active Backup for Business provides for various disaster recovery scenarios.

Instant Restore to VMware

Instant Restore to VMware is a feature that can quickly restart a VM directly from a compressed and deduplicated backup file to minimize the downtime of VMs. This section guides you through the prerequisites for Instant Restore to VMware and how to perform it step by step.

- **Before You Start**

Instant Restore to VMware can quickly restart a VM directly from a compressed and deduplicated backup file to minimize downtime of VMs. Compared with the full VM restore that requires longer time and has a full I/O performance, Instant Restore to VMware can restart a VM within seconds but has a limited I/O performance.

Note:

- To finalize the whole Instant Restore to VMware process, you will need to migrate the VM restored instantly back to the production site. You can migrate the VM or clone it to the hypervisor where you want to run the VM. We recommend you to shut down the VM in case data inconsistency occurs during the cloning. Migration of VMs requires eligible vCenter / Storage vMotion license, please refer to the **Migrate VM** section in [here](#) for further information.
- Since all the changes made during Instant Restore to VMware will be automatically stored on Synology NAS, please make sure that there is enough space on your Synology NAS.

- **Launch the Instant Restore to VMware**

With Instant Restore to VMware, you can launch the restore wizard to restore a VM to its most recent state or to any available restore point by doing either of the following:

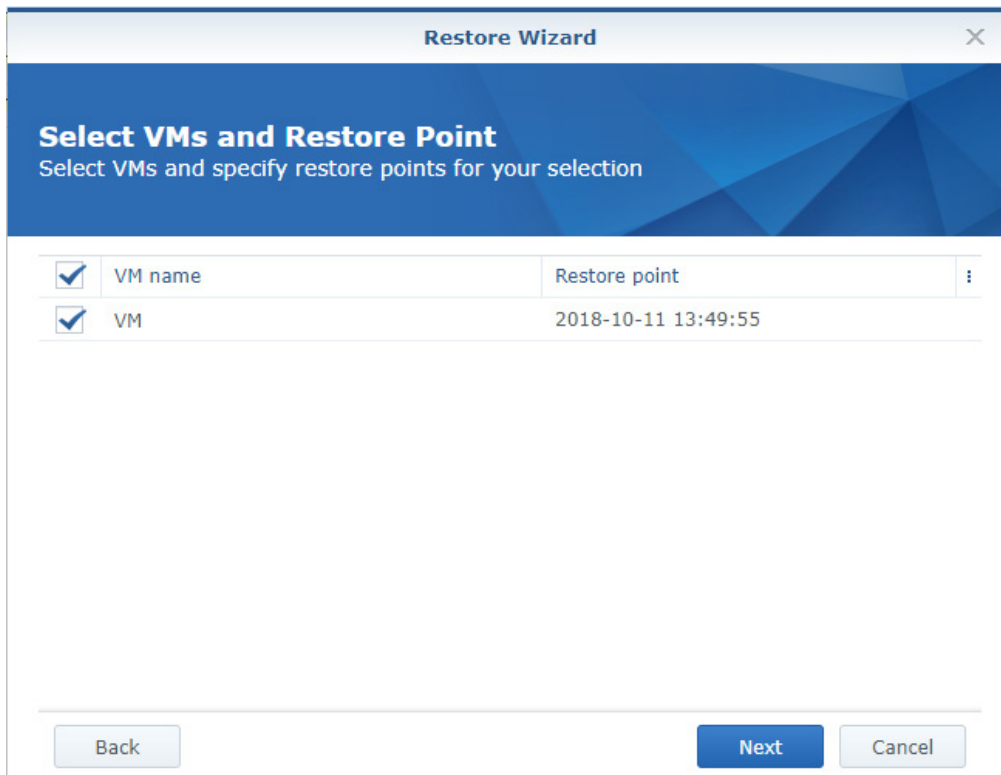
- Go to **Active Backup for Business > Virtual Machine > Virtual Machine**, single select the virtual machine you want to restore, click **Restore** to launch the restore wizard, and select **Instant Restore to VMware**.
- At **Active Backup for Business > Virtual Machine > Task**, select the backup task you want to restore and click **Restore** to launch the restore wizard and select **Instant Restore to VMware**.

Note: To perform Instant Restore to VMware, please make sure the hypervisor is authorized to access and mount the backup destination (shared folder).

- **Restore Wizard**

To select VMs and restore points:

Select the VMs you want to restore and choose a restore point for each of them.



To select the restore mode:

You can select either of the following modes according to your needs:

- **Restore to the original location:** This option restores the selected VM to its original location while keeping the original name and settings, minimizing the chance of input errors by users. This option will instantly unregister and replace the original VM in the production site.
- **Restore to a new location, or with different settings:** This option allows you to customize the destination and settings for the restored VM.

Restore Wizard

Select Restore Mode

Specify an ultimate destination for the instantly restored VM.

Restore to the original location

Instantly initiate restoring the selected VM to the original location, and under the original name and settings. This option minimizes the chance of user input error and immediately replaces the original VM in the production site.

Restore to a new location, or with different settings

Customize destination and settings for the instantly restored VM by selecting a hypervisor, resource pool, network, and folder. Changes made during Instant Restore to VMware will be stored on Synology NAS, and you may select the datastore when migrating VM.

Regenerate a new MAC address for restored VMs

Back Next Cancel

To configure restore settings:

- If you select **Restore to the original location**, you will be directed to the summary page of the restore wizard.
- If you select **Restore to a new location, or with different settings**, you will need to specify the name and select a folder, hypervisor, resource pool, and network to restore a VM. The changes made during Instant Restore to VMware will be stored on Synology NAS, and you can select the datastore when executing VM migration.

To apply settings and restore VMs:

In the summary step, please check the information of the VM intended to be restored and click **Apply** to restore it. You will then be automatically directed to **Restore Status** to monitor the restoration progress. To finalize the whole process of Instant Restore to VMware, please click the **Migrate VM** button.

Enable **Power on VM automatically after restoration** if you want to run the restored VM immediately. For testing purposes, we suggest you not to select this option. Instead, we recommend you to manually disconnect the initial VM from the production network to avoid possible conflicts.

Full VM Restore

Full VM Restore provides users to restore an entire VM from a backup file and to have full disk I/O performance. In this section, you will learn how to restore full VM step-by-step.

• Before You Start

Full VM Restore provides users to restore an entire VM from a backup file to the latest state or a previous point in time if the primary VM fails. It takes more time and resources to restore but has full disk I/O performance.

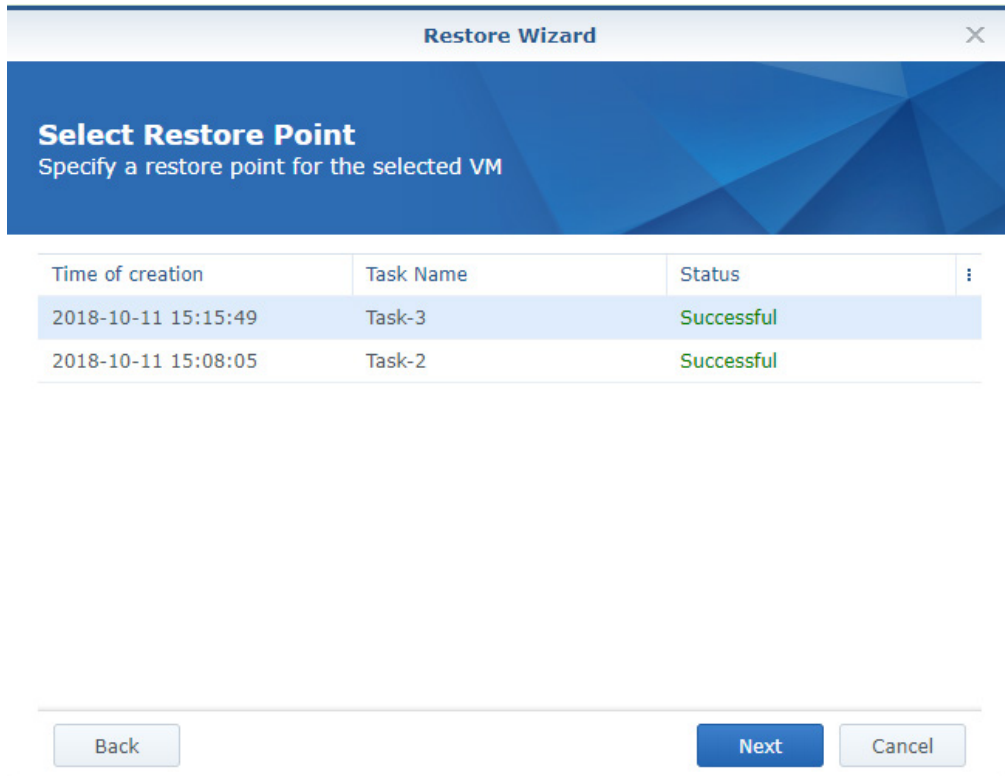
- **Launch the Full VM Restore Wizard**

Launch the restore wizard to restore VMs to the most recent state or to any available restore point through full VM restore, you can do one of the following:

- At **Active Backup for Business > Virtual Machine > Virtual Machine**, single select the virtual machine you want to restore and click **Restore** to launch the restore wizard and select full VM restore
- At **Active Backup for Business > Virtual Machine > Task**, select the backup task you want to restore and click **Restore** to launch the restore wizard and select full VM restore.

- **Restore Wizard: Select VMs and Restore Point**

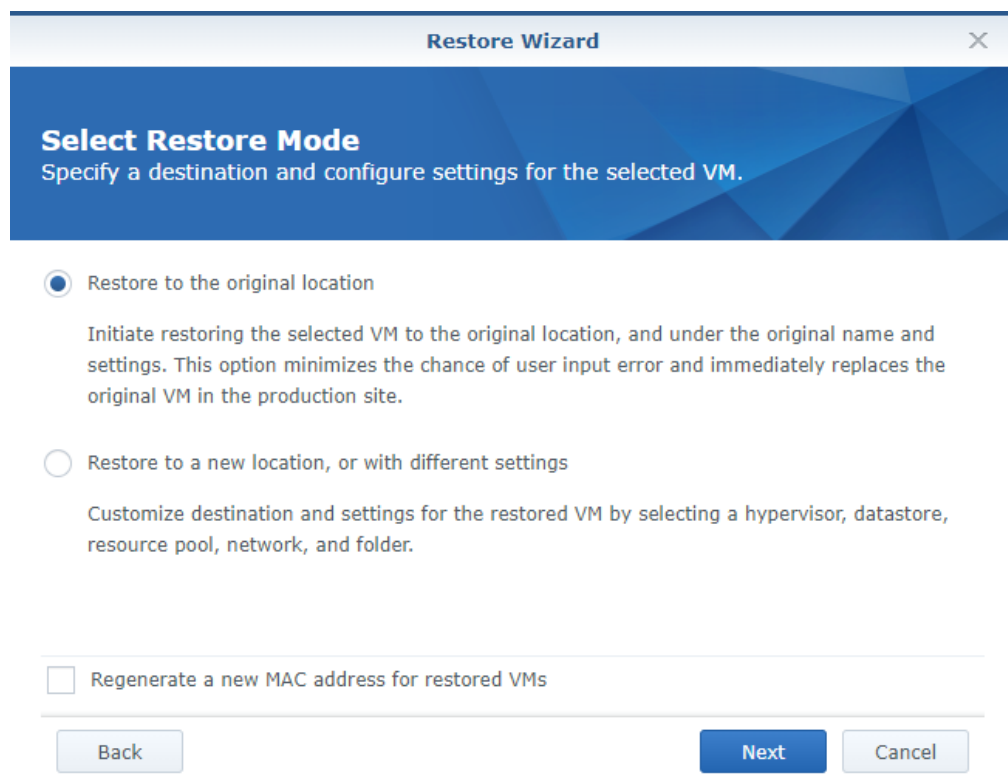
Select the VMs you want to restore and restore point for each selected one.



- **Restore Wizard: Select Restore Mode**

Select the restore mode you want to perform.

- **Restore to the original location:** Restore the selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error and will un-register and replace the original VM in the production site.
- **Restore to a new location, or with different settings:** Customize destination and settings for the restored VM.



- **Restore Wizard: Configure Restore Settings**

If you choose **Restore to the original location**, you will pass directly to the summary step of the wizard.

For users who choose **Restore to a new location, or with different settings**, please specify a name, and select a folder, hypervisor, resource pool, datastore, and network to run the restored VM.

- **Restore Wizard: Apply and Restore**

On the task summary page, please check the info of the restored VM and click **Apply** to start. You will then be directed to **Restore Status** to monitor the restoration progress.

Enable Power on VM automatically if you want to run the restored VM immediately. For testing purposes, it's recommended to keep this option disabled, manually disconnect the initial VM from the production network, and connect it to an isolated non-production network to avoid conflicts.

Instant Restore to Synology Virtual Machine Manager (VMM)

The integration of Active Backup for Business with Synology Virtual Machine Manager (VMM) provides users with an alternative solution for disaster recovery, browsing and restoring application data, and upgrading test environments. This section guides you through how to instantly restore the backed up device on Synology VMM and the prerequisites for executing such a task.

- **Before you start**

Instant Restore to Synology Virtual Machine Manager provides users with an alternative solution for disaster recovery, upgrade testing, and restoring application data by leveraging native export/import tools.

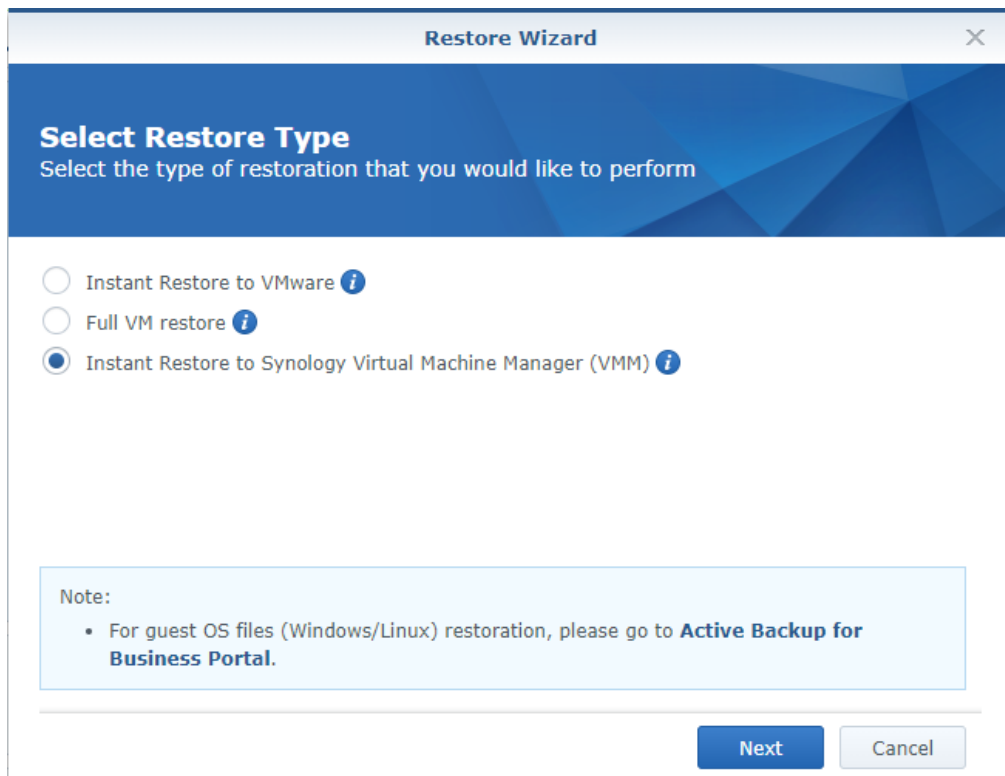
Limitations: VM backup in Synology VMM is only supported on DSM 6.2 and Synology VMM 2.3.4 or above. For

further information about the limitations of Synology VMM, please refer to [here](#).

- **Launch Synology VMM Wizard**

To instantly restore the backed up device on Synology VMM, you can do either of the following:

- Go to **Active Backup for Business > Virtual Machine > Virtual Machine** and select the VM you want to restore. Click **Restore** to launch the restore wizard and select **Instant Restore to Synology Virtual Machine Manager (VMM)**.
- Go to **Active Backup for Business > Virtual Machine > Task List** and select the backup task you want to restore. Click **Restore** to launch the restore wizard and select **Instant Restore to Synology Virtual Machine Manager (VMM)**.

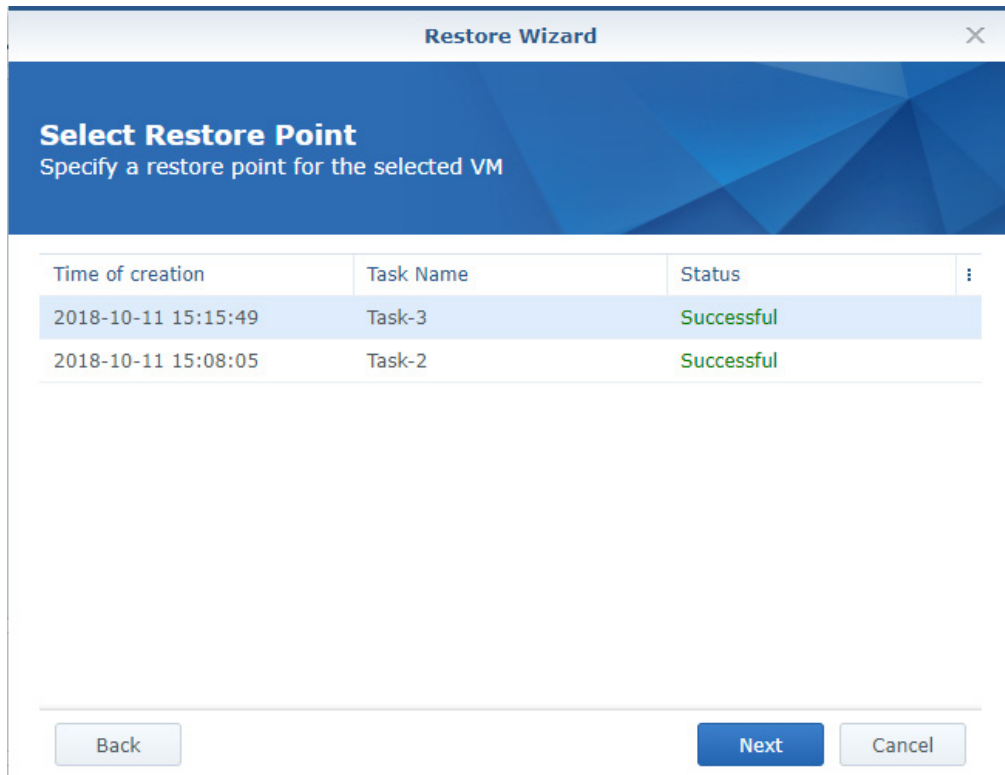


- **Restore Wizard:**

Follow the restore wizard to do the following:

To select a VM and restore point:

Select the VM you want to instantly restore on Synology VMM and select a restore point.



Note: Only one VM in each backup task can be instantly restored on Synology VMM. You cannot select multiple VMs and run them at the same time.

To configure VM settings:

After you have selected the VM you want to restore and the restore point, a Synology VMM wizard will be launched for configuring the settings of the selected VM. Please refer to [Synology Virtual Machine Manager](#) for more details.

To apply settings and restore VM:

After you have configured the settings, click **Apply**. The VM backup will be imported into Synology VMM and you can choose to power on the VM in the VMM console.

Guest Files (Windows / Linux) Restore

Guest files restore allows users to restore files only instead of the whole VM. In this section, you will learn about how to execute such restoration tasks step by step.

• Before You Start

Guest files restore allows you to only restore individual files or folders from Microsoft Windows and Linux VMs. Please note that VMware Tools are required to be installed to restore guest OS files. Supported file systems for Windows / Linux are listed below.

- Windows: NTFS, FAT32
- Linux: NTFS, FAT32, EXT3, EXT4

• Launch a guest file restore portal

- Go to **Active Backup for Business > Virtual Machine > Virtual Machine**, single-select the VM you want to restore, click **Restore** to launch the restore wizard, and open **Active Backup for Business Portal**.
- Go to **Active Backup for Business > Virtual Machine > Task List**, select the backup task you want to restore, click **Restore** to launch the restore wizard, and open **Active Backup for Business Portal**.

Note: Active Backup for Business Portal, which is mainly used for data restore, will be installed automatically when users install Active Backup for Business.

Physical Server

Physical Server backup supports various ways to restore the backed up data.

- **Instant Restore to VMware:** This method converts the Windows-based physical devices' format of backup images to a virtual machine in VMware, and it can restart a virtual machine in VMware directly from a compressed and deduplicated physical server backup file to minimize the downtime.
- **Full VM restore:** This method converts the Windows-based physical devices' format of backup images to a virtual machine in VMware, and it can be restored to the latest status or a previous point of time. This method takes more time and system resources but provides full disk I/O performance.
- **Instant Restore to Synology Virtual Machine Manager (VMM):** During urgent cases when tolerance for downtime is limited, mounting the backed-up image of your physical server on **Synology Virtual Machine Manager (VMM)** and power it on to continue your business could be your choice. To mount the backed-up image of your physical server on **Virtual Machine Manager, Virtual Machine Manager** requires to be installed on the same DSM.
- **Granular (file/folder level) restore:** Physical Server backup supports granular (file and folder-level) restore through **Active Backup for Business Portal**. Admins are able to delegate the restore permission during the task creation and the task editing. For more information, please refer to the help article: [Active Backup for Business Portal](#).
- **Bare metal restore:** Bare metal restore is available with a recovery media. To restore the entire device or the backed-up volume, please create a recovery media in advance. You can refer this [creation guide](#) to learn how to use **Active Backup for Business Recovery Media Creator** to create a media automatically or create a customized media. You can download Synology Active Backup Recovery Media Creator in [Download Center](#).

Note:

- Backup tasks of physical server can only be restored by admin, administrators group, and the assigned account. This setting is always adjustable on Active Backup for Business.
- Backing up physical servers with 4Kn disks is not supported on Active Backup for Business for now.

Personal Computer

- **Granular (file/folder level) restore:** Personal Computer backup supports granular (file and folder-level) restore through **Active Backup for Business Portal**. Admins are able to delegate the restore permission

to each end user through DSM **Control Panel**. For more information, please refer to the help article: [Active Backup for Business Portal](#).

- **Bare metal restore:** Bare metal restore is available with a recovery media. To restore the entire device or the backed-up volume, please create a recovery media in advance. You can refer this [creation guide](#) to learn how to use **Active Backup for Business Recovery Media Creator** to create a media automatically or create a customized media. You can download Synology Active Backup Recovery Media Creator in [Download Center](#).

File Server

File Server backup supports granular restore (file-level) to restore the backed up data.

To restore backup tasks:

- 1 Select the task you want to restore and click Restore.
- 2 Select a restoration method you prefer:
 - Custom location - overwrite
 - Custom location - skip
 - Original location - overwrite
 - Original location - skip
- 3 Select the folders or files you want restored and click Next.
- 4 If you want to restore to a custom location, please select the destination folder you want the data to be restored in and click Next.
- 5 Check your settings and click Restore to commence restoration.

Note: For information on how to back up and restore a Microsoft SQL or Exchange server, please refer to the following tutorials.

- For [Microsoft SQL servers](#)
- For [Microsoft Exchange servers](#)

Report

View Statistics of Backup Tasks

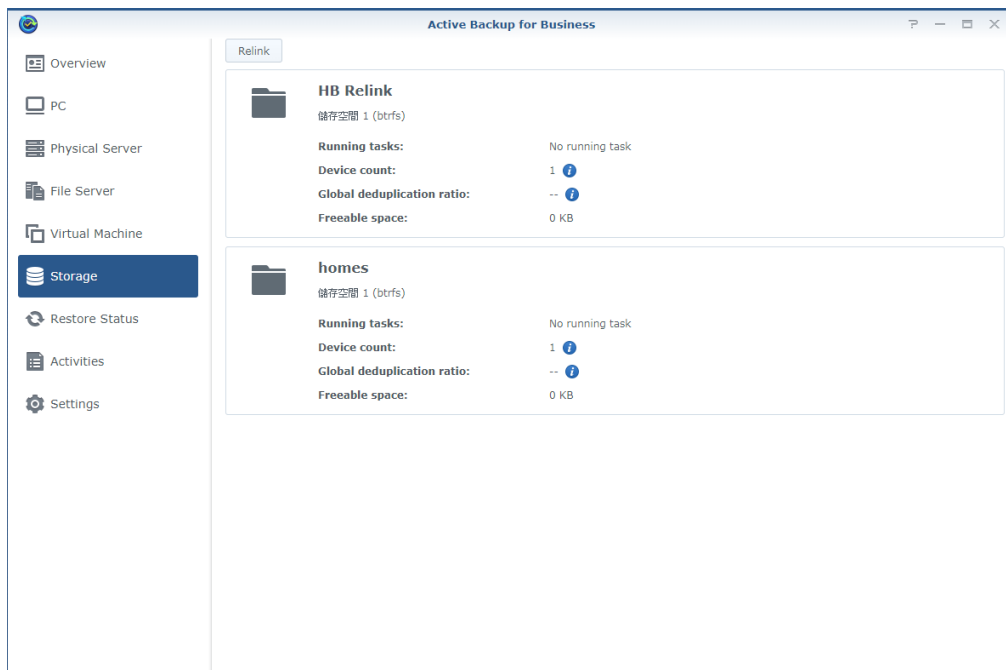
Storage status

In **Active Backup for Business** > **Storage**, you can monitor the status and storage usage of each shared folder when there is at least one backup task. You can also retrieve the existing data and task settings of Active Backup for Business by relinking the shared folders in this page, please refer to [this section](#) in Chapter 3 for more information.

To view the status and storage usage of each shared folder:

Click **Storage**. The following information of each shared folder will be displayed:


- **Running tasks:** Whether there is any running backup task.
- **Device count:** The number of backed-up devices in this shared folder.
- **Global deduplication ratio:** The number calculated from original source data size divided by actual stored data size. For example, the original source data is 100GB which is also written to the disk, and then only 80GB data are stored on Synology NAS after deduplication. Then the deduplication ratio will be $100\text{GB} / 80\text{GB} = 1.25\text{x}$. For the second backup with CBT, only changed data will be added instead of adding the whole data size again. If the transferred size of changed data is 10GB and 5GB data are stored on Synology NAS in the second backup, the deduplication ratio will be $(100+10) / (80+5) = 1.29\text{x}$.
- **Freeable space:** The storage space will be freed when the unused space reaches the value which was set in **Settings** > **Settings**.



Activities

For better and easier management among all the events on Active Backup for Business, Active Backup for Business provides administrators detailed event information in **Activities** tab, including activity logs, activity details, and adjustable daily, weekly, monthly, and annual reports.

To access logs in Activities tab, do any of the following:

- 1 Click **Activities** tab to access logs.
- 2 In **Overview** tab, click on a specific day on the calendar to access logs.
- 3 In **Overview** tab, click  on the top right corner of Logs section to access logs.

Please note that ongoing events will only be displayed on **Ongoing Activities** section in **Overview** tab as well as the task monitor.


- **Log**

All the events happened on this backup server are listed in this tab.

Below are the event details you can see in the log list:

- **Log Type:**

Logs are categorized into the following three types:

- **Information:** When a task has been carried out properly and successfully, it will be recorded as an information log.
- **Warning:** When a task was only partially successful or canceled, it will be recorded as a warning log. It usually happens to file server and VM backups.
- **Error:** When the task failed thoroughly, the log will be categorized as an error log. It is suggested to click on  for more information for you to troubleshoot. The common errors could be damaged source disk, insufficient space on the NAS, etc.

- **Log time:**

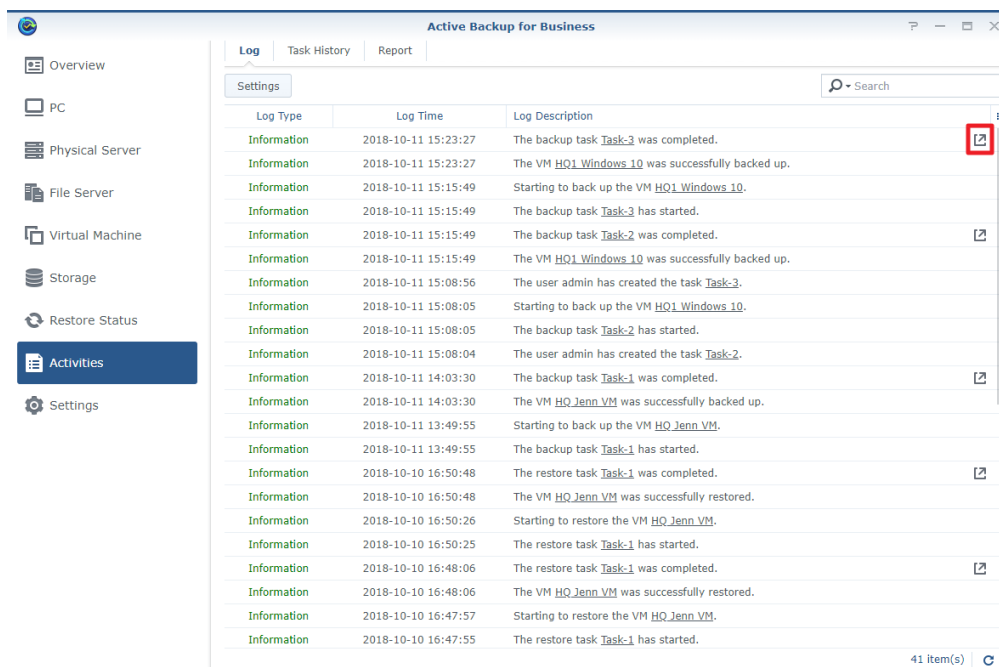
The time when a task finished, failed, or was canceled is recorded in **Log Time**.

- **Log Description:**

Each event is summarized in one short description for instant understanding on what has happened to a certain task. For further information, you can click on the name of the task in the description to view the task.

To go to the task history of the log:

Click the icon at the right side of the log, and the task history including the backup duration and transferred size will be displayed for your reference.



The screenshot shows the 'Active Backup for Business' interface. On the left is a navigation sidebar with 'Activities' selected. The main area displays a 'Log' table with the following columns: Log Type, Log Time, and Log Description. The table contains 20 rows of log entries, all marked as 'Information'. The first row is highlighted. To the right of the table, there is a search bar and a vertical list of icons. A red box highlights the information icon (a square with a lowercase 'i') next to the first log entry.

Log Type	Log Time	Log Description
Information	2018-10-11 15:23:27	The backup task Task-3 was completed.
Information	2018-10-11 15:23:27	The VM HQ1_Windows_10 was successfully backed up.
Information	2018-10-11 15:15:49	Starting to back up the VM HQ1_Windows_10 .
Information	2018-10-11 15:15:49	The backup task Task-3 has started.
Information	2018-10-11 15:15:49	The backup task Task-2 was completed.
Information	2018-10-11 15:15:49	The VM HQ1_Windows_10 was successfully backed up.
Information	2018-10-11 15:08:56	The user admin has created the task Task-3 .
Information	2018-10-11 15:08:05	Starting to back up the VM HQ1_Windows_10 .
Information	2018-10-11 15:08:05	The backup task Task-2 has started.
Information	2018-10-11 15:08:04	The user admin has created the task Task-2 .
Information	2018-10-11 14:03:30	The backup task Task-1 was completed.
Information	2018-10-11 14:03:30	The VM HQ_Jenn_VM was successfully backed up.
Information	2018-10-11 13:49:55	Starting to back up the VM HQ_Jenn_VM .
Information	2018-10-11 13:49:55	The backup task Task-1 has started.
Information	2018-10-10 16:50:48	The restore task Task-1 was completed.
Information	2018-10-10 16:50:48	The VM HQ_Jenn_VM was successfully restored.
Information	2018-10-10 16:50:26	Starting to restore the VM HQ_Jenn_VM .
Information	2018-10-10 16:50:25	The restore task Task-1 has started.
Information	2018-10-10 16:48:06	The restore task Task-1 was completed.
Information	2018-10-10 16:48:06	The VM HQ_Jenn_VM was successfully restored.
Information	2018-10-10 16:47:57	Starting to restore the VM HQ_Jenn_VM .
Information	2018-10-10 16:47:55	The restore task Task-1 has started.

To set retention rules for logs:

1 Click on **Settings**.

Log Type	Log Time	Log Description
Information	2018-10-11 15:23:27	The backup task Task-3 was completed.
Information	2018-10-11 15:23:27	The VM HQ1_Windows_10 was successfully backed up.
Information	2018-10-11 15:15:49	Starting to back up the VM HQ1_Windows_10 .
Information	2018-10-11 15:15:49	The backup task Task-3 has started.
Information	2018-10-11 15:15:49	The backup task Task-2 was completed.
Information	2018-10-11 15:15:49	The VM HQ1_Windows_10 was successfully backed up.
Information	2018-10-11 15:08:56	The user admin has created the task Task-3 .
Information	2018-10-11 15:08:05	Starting to back up the VM HQ1_Windows_10 .
Information	2018-10-11 15:08:05	The backup task Task-2 has started.
Information	2018-10-11 15:08:04	The user admin has created the task Task-2 .
Information	2018-10-11 14:03:30	The backup task Task-1 was completed.
Information	2018-10-11 14:03:30	The VM HQ_Jenn_VM was successfully backed up.
Information	2018-10-11 13:49:55	Starting to back up the VM HQ_Jenn_VM .
Information	2018-10-11 13:49:55	The backup task Task-1 has started.
Information	2018-10-10 16:50:48	The restore task Task-1 was completed.
Information	2018-10-10 16:50:48	The VM HQ_Jenn_VM was successfully restored.
Information	2018-10-10 16:50:26	Starting to restore the VM HQ_Jenn_VM .
Information	2018-10-10 16:50:25	The restore task Task-1 has started.
Information	2018-10-10 16:48:06	The restore task Task-1 was completed.
Information	2018-10-10 16:48:06	The VM HQ_Jenn_VM was successfully restored.
Information	2018-10-10 16:47:57	Starting to restore the VM HQ_Jenn_VM .
Information	2018-10-10 16:47:55	The restore task Task-1 has started.

2 You can permanently preserve these logs on the backup server when not checking the options, or you can do any of the following to set the retention rules for logs:

- Check the checkbox next to **The number of logs is greater than** and set the number to delete logs when logs on the server is more than a designated quantity: 1 million, 3 million, 5 million, or 10 million.
- Check the checkbox next to **The log was created earlier than** and set the time to clear the outdated logs which are no longer needs to be preserved

Log Settings

Log Delete Rules

Delete logs from the database when the following events occur:

- The number of logs is greater than **1,000,000 (1 million)**
- The log was created earlier than **1 month**

Delete all logs

OK **Cancel**

3 Click **OK** to apply your retention rules.

To delete all logs:

- 1 Click on Settings.
- 2 Click **Delete all logs**, and confirm the action if no log needs to be preserved on the server.

• **Task History**

You can view further information of each performed task in **Task History** tab.

To view detail information of a performed task, do any of the following:

- Click on the task you wish to view, and click **Information**.
- Double click the task you wish to view.

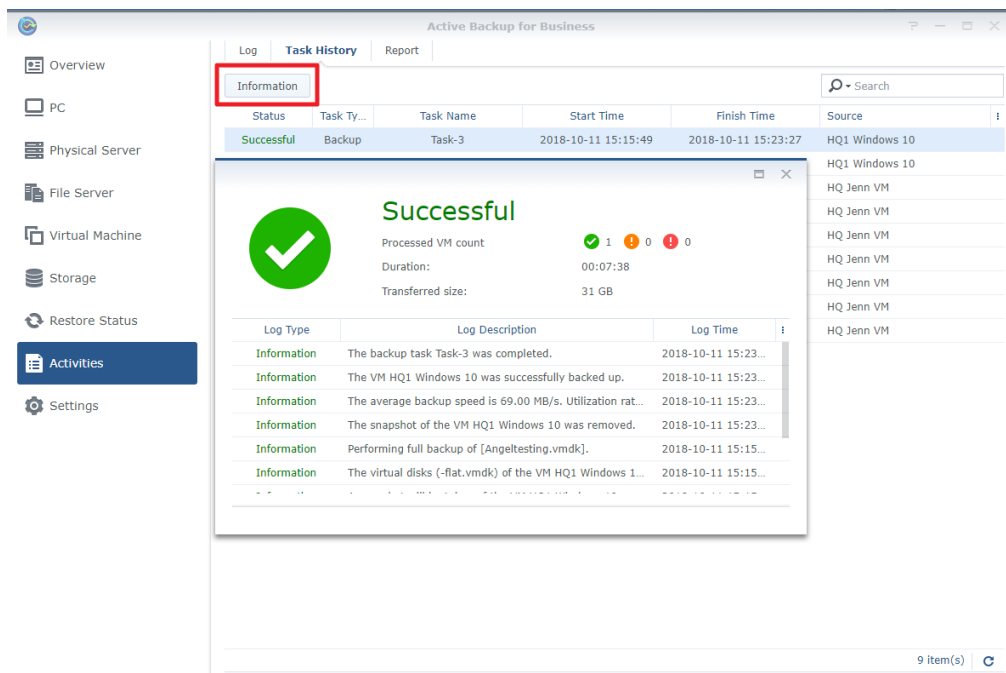
An information window will be launched for your reference.

In the information window, you can view the following details:

- **Duration:** the time which the task had taken.
- **Transferred size:** the size of the transferred data.
- **Log list:** all the events which had happened during a task. You can view the complete log description by hovering your mouse to a log.

For file server backup tasks, an additional indicator will display the counts of files that have been processed successfully, partially, or even unsuccessfully.

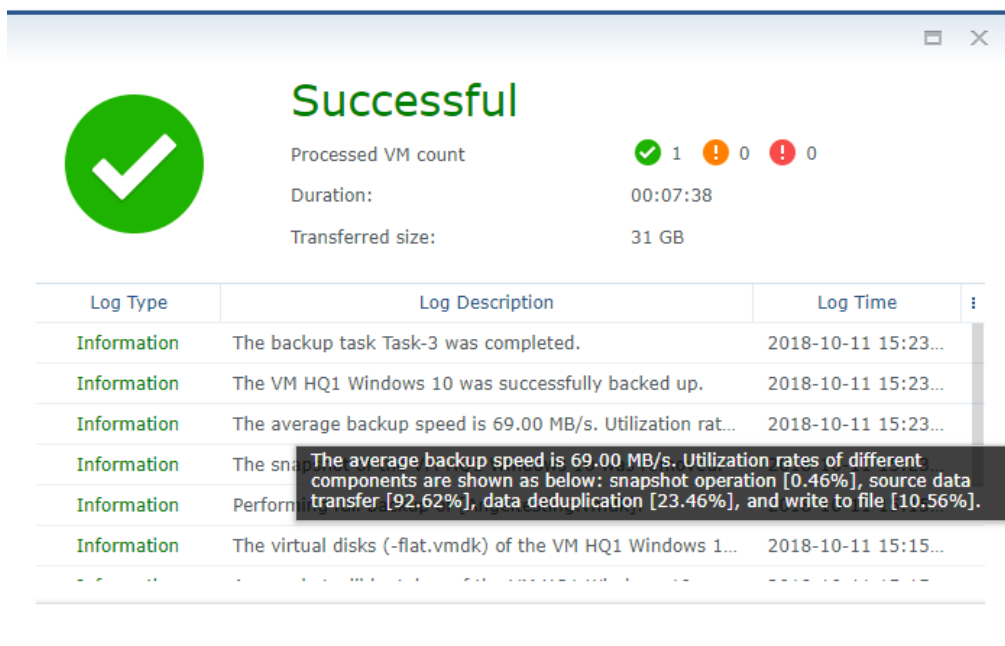
For VM backup tasks, an additional indicator will display the counts of VMs that have been processed successfully, partially, or even unsuccessfully.



To check the speed and utilization rates:

Summary of the backup performance including the backup speed and the utilization rates are recorded on the log list as well.

- 1 Find the log entry which recorded the backup speed and the utilization rates. It is recorded in the last log before the backup completion announcement.
- 2 Hover your mouse to the log to view complete log entry.
 - The average backup speed: transferred size per second.
 - Utilization rates:
 - **Taking snapshot**: the percentage time spent on taking snapshot of total duration.
 - **Source disk read**: the percentage time spent on reading the source disk of total duration.
 - **Data transfer**: the percentage time spent on transferring data of total duration.
 - **Data deduplication**: the percentage time spent on deduplicating data of total duration.
 - **Write to file**: the percentage time spent on writing to file of total duration.



The screenshot shows a window titled "Successful" with a green checkmark icon. It displays the following summary information:

- Processed VM count: 1 (green checkmark), 0 (yellow warning), 0 (red error)
- Duration: 00:07:38
- Transferred size: 31 GB

Below the summary is a log table with the following data:

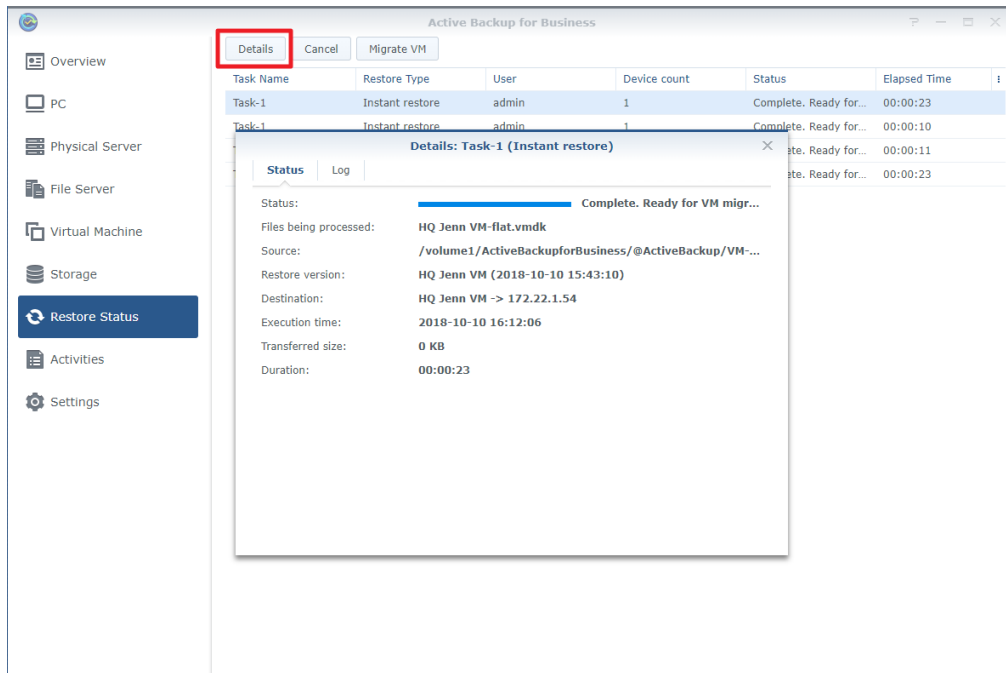
Log Type	Log Description	Log Time
Information	The backup task Task-3 was completed.	2018-10-11 15:23...
Information	The VM HQ1 Windows 10 was successfully backed up.	2018-10-11 15:23...
Information	The average backup speed is 69.00 MB/s. Utilization rat...	2018-10-11 15:23...
Information	The sn... The average backup speed is 69.00 MB/s. Utilization rates of different components are shown as below: snapshot operation [0.46%], source data transfer [92.62%], data deduplication [23.46%], and write to file [10.56%].	
Information	Perform...	
Information	The virtual disks (-flat.vmdk) of the VM HQ1 Windows 1...	2018-10-11 15:15...

View Restore Status

At **Active Backup for Business** > **Restore Status**, you can monitor the progress of restoration tasks, cancel restoration tasks, and migrate virtual machines.

Details of Restored Tasks

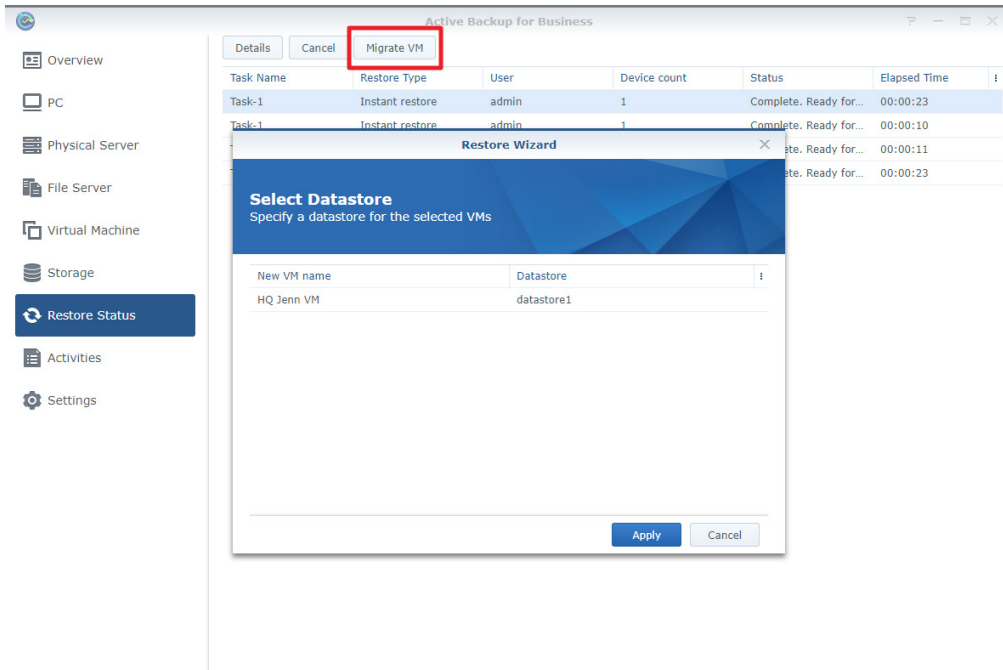
You can select any restoration task and click **Details** to get more task information.



- **Status / Files being processed:** the restoration progress of the task and the files that are being restored
- **Source:** where the data is restored from
- **Restore version:** the recovery point the task will be restored to
- **Destination:** where the devices will be running on
- **Execution time:** start time of the restoration
- **Transferred size:** size of the restored data
- **Duration:** how much time the restoration has taken

Migrate VM

You can select the restoration task and click **Migrate VM** to finalize **Instant Restore to VMware**.



After clicking **Migrate VM**, users will need to select the datastore where all changes made during **Instant Restore to VMware** should be restored to.

Please note that since VM migration leverages native VMware vCenter migration mechanisms, vMotion, and Storage vMotion, only eligible VMware vSphere license with support for vMotion and Storage vMotion can perform VM migration. If your VMware vSphere license does not provide support for vMotion and Storage vMotion, or you need to migrate VMs from one standalone ESX(i) host to another, VMware vCenter migration methods cannot be used and migration of VMs will be disabled.

Cancel Restoration Tasks

You can select any restoration task and click **Cancel** to stop restoration.

Please note that all changes made during **Instant Restore to VMware** will be discarded after you click **Cancel**. Users may only retain the last backed up version of each restored task.

Generate Reports

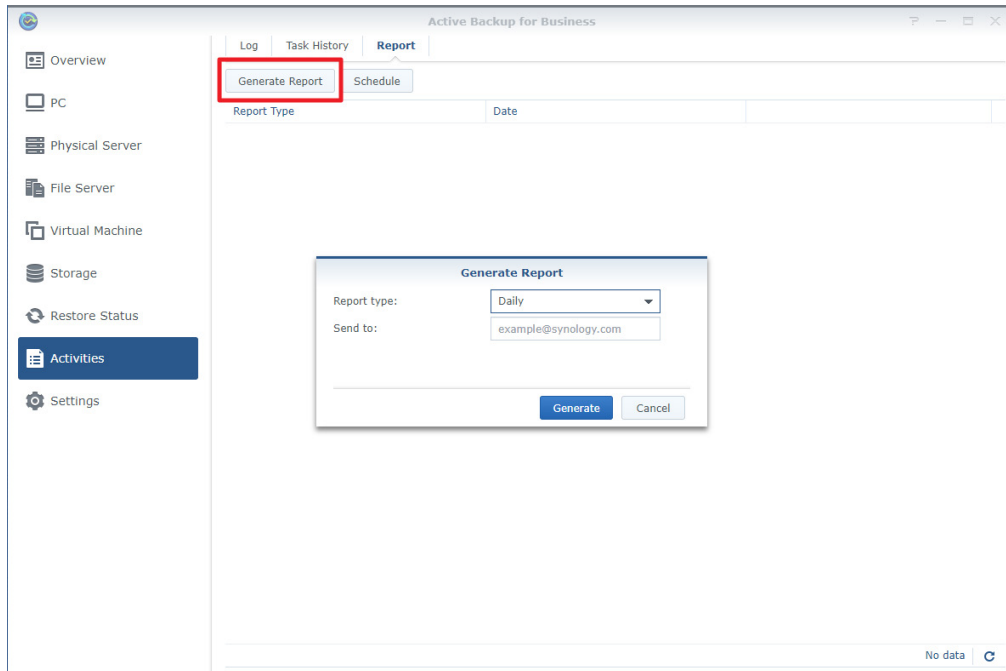
A detailed and adjustable report is supported on Active Backup for Business for IT admin's routine monitor on the backup performance. This report contains most of the information in **Overview** tab. IT admins can generate daily, weekly, monthly, and annual reports in **Report** by request or by a configurable schedule.

All the generated reports are listed in **Report** tab. You can always click **Open report** at the end of each generated report entry to view the report.

Note: It is not supported to generate a report which ends earlier than today.

To generate a report instantly:

1 Click **Generate Report**.



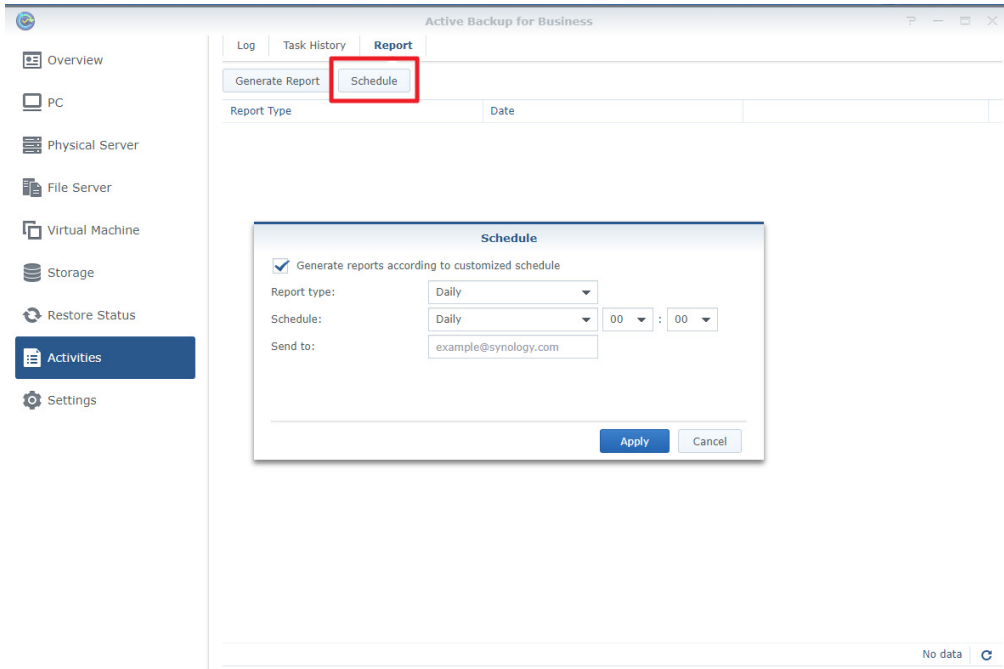
2 Select your report type to be **Daily**, **Weekly**, **Monthly**, or **Annual**.

- **Daily:** A daily report displays the data of the last 23 hours. For example, if a daily report is generated on July 22nd 16:30, then this report will display the data starting from July 21st 17:00.
- **Weekly:** A weekly report displays the data of the last 7 days. For example, if a weekly report is generated on July 22nd 16:30, this report will display the data since July 16th 00:00.
- **Monthly:** A monthly report displays the data of the last 31 days. For example, if a monthly report is generated on July 22nd 16:30, this report will display the data since June 22nd 00:00.
- **Annual:** An annual report displays the data of the last 12 months. For example, if an annual report is being generated on 2018 July 22nd 16:30, then this report will display the data since 2017 August 1st 00:00.

3 If you would like the report to be sent to your mailbox, fill in the blank with the mail address.

To generate a report by a schedule:

- 1 Click **Schedule**.
- 2 Check the checkbox next to **Generate reports according to customized schedule**.
- 3 Configure your scheduled report settings.
- 4 If you would like the report to be sent to your mailbox, fill in the blank with the mail address.



Note: Only one report is supported to be scheduled and mailed to a designated email address.