

Administrator's Guide for

# Active Backup for Business

## Virtual Machines



Based on

**Active Backup for Business 2.2.0**



# Table of Contents

<b>Introduction</b>	<b>01</b>
Active Backup for Business	
<b>Technical Overview</b>	<b>05</b>
Application-aware backup	
Forever-incremental backup	
Data deduplication	
Native hypervisor	
<b>Backup Configuration</b>	<b>08</b>
VMware and Hyper-V Backup	
Create a backup task	
Manage Backup Tasks	
<b>Restoration Guide</b>	<b>14</b>
Recovery Options	
Instantly Restore your Virtual Machine	
Fully Restore your Virtual Machine	
Instant Restore to Synology Virtual Machine Manager (VMM)	
Guest OS Files (Windows / Linux) Restore	
<b>Best Practices</b>	<b>22</b>
Maintain remote backup copies and relink	
<b>Learn more</b>	<b>24</b>
Related articles	
Software specs	
Other resources	



# Introduction

## Active Backup for Business

Active Backup for Business (ABB) is a centrally managed, comprehensive office backup solution for Synology NAS.

ABB allows administrators to create different backup templates and automatically apply them to groups of Windows and Linux PCs, servers, and file servers, as well as virtual machines running on Microsoft Hyper-V and VMware vSphere platforms.

Advanced features of ABB include: forever incremental backup, agentless backup, Instant Restore physical and virtual devices to virtual machines, and a powerful deduplication mechanism that helps cut back on storage use. These features come with each installation of ABB, which is free for Synology NAS users.

ABB also offers users a wide range of backup options and restoration tools, as well as a number of optional technical and safety features.

Users who wish to make full use of the possibilities in ABB will benefit from the information in this Administrator's Guide.

## Requirements

Full specifications for Active Backup for Business can be found [here](#).

### NAS System requirements

Item	Requirements
Operating system	DSM 7.0 and above (ABB 2.2.0 and above) DSM 6.2 and above (ABB 2.1.0 and above) DSM 6.1.7 and above (ABB 2.0.4 and above)
CPU architecture	64-bit x86 (x64)
System memory	4 GB RAM recommended for ideal backup performance
File system	Btrfs

## Supported systems

Backup type	System / version
PC	Windows 10 Creators Update (all editions), Windows 10 (all editions), Windows 8.1 (all editions), Windows 7 SP1 (all editions)
Physical Server	<p><b>Windows:</b> Windows 10 Creators Update (all editions), Windows 10 (all editions), Windows 8.1 (all editions), Windows 7 SP1 (all editions), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2</p> <p><b>Linux:</b> CentOS (versions 6.10, 7.8, and 8.1), RHEL (versions 6.10, 7.8, and 8.1), Ubuntu (versions 16.04, 18.04, and 20.04), Fedora (versions 30, 31, and 32), Debian (versions 8.0 to 10)</p>
Virtual Machine	VMware free ESXi, VMware vSphere Essentials, VMware vSphere Essentials Plus, VMware vSphere Standard, VMware vSphere Advanced, VMware vSphere Enterprise, VMware vSphere Enterprise Plus (versions 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0); Windows Server Hyper-V 2019, Windows Server Hyper-V 2016
File Server	SMB protocol; rsync 3.0 and above

For a full list of requirements for backups and restorations, refer to the [Requirements and Limitations](#) section of the Active Backup for Business Help page.

## Backup types

The following sections provide information on the types of backups that you can perform using ABB.

### PC Backups

- Back up full Windows devices with features that help keep workstations, laptops, and personal devices protected, including a **Backup by event** option that backs up computers when users lock their screen, sign out, or start up their device.
- Create recovery media for bare-metal restorations or restore individual files and folders via the Active Backup for Business Portal.
- Backup restorations can only be performed by the **admin** account, users belonging to the **administrators** group, or the account owner that is logged into **Active Backup for Business Agent**. Privileges to perform restorations are not configurable.
- **Active Backup for Business Agent** can perform **Application-aware backup** on Windows PC's with the help of Microsoft's **Volume Shadow Copy Service (VSS)**.

### Physical Server Backups

- Back up Windows and Linux devices with scheduled and manual backup options.
- Create recovery media for bare-metal restorations, restore individual files and folders using the **Active Backup for Business Portal**, or instantly restore your physical device to a virtual machine in **Synology Virtual Machine Manager**, **Hyper-V**, or **VMware**.
- Privileges to perform restorations can be assigned by the **admin** account (if enabled), as well as by all other DSM users or groups.
- Active Backup for Business Agent can perform **Application-aware backup** on Windows servers with the help of Microsoft's **Volume Shadow Copy Service (VSS)**.

### File Server Backups

- Back up files and folders from Windows and Linux devices using SMB and rsync file transfer protocols.
- Select a backup mode as needed:
  - **Multi-versioned:** Each time the task runs, a new version with the changes made on the source will be copied entirely to a new folder on the destination
  - **Mirroring:** Each time the task runs, any 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.
- Set up and fully control backups from one central console.
- No need to install a backup agent or enter sensitive DSM login details on source devices.

### Virtual Machine Backups

- Safely back up virtual machines directly from VMware and Hyper-V.
- Enable **Application-aware backup** on Virtual Machines to ensure data consistency with the help of Microsoft's Volume Shadow Copy Service (VSS).
- Fully restore your entire virtual machines to VMware or Hyper-V.
- Use **Instant Restore** to restore your virtual machine to Synology's native hypervisor, **Synology Virtual Machine Manager**, as well as directly to **VMware** or **Hyper-V**.
- Perform a **Guest OS Files (Windows / Linux) Restore** via **Active Backup for Business Portal** to restore specific files on your virtual machine instead of an entire virtual machine.

## Backup tools

### Active Backup for Business Agent

**Active Backup for Business Agent** must be installed on the client device before backing up your data in order to carry out backup tasks and store the back up data. Administrative privileges are required to install, update, or uninstall Synology Active Backup for Business Agent.

This tool is available for download in the [Download Center](#). Refer to [this article](#) for installation details and other information.

### Active Backup for Business Portal

The **Active Backup for Business Portal** is the affiliated restore portal dedicated to restoration use. This portal allows administrators and end-users appointed by an administrator to access, browse, download, and restore backed-up data.

This tool is automatically installed during the installation of Active Backup for Business. Refer to [this article](#) to learn more about how to navigate the portal, perform restores, and other settings.

### Active Backup for Business Recovery Media Creator

Synology **Active Backup for Business Recovery Media Creator** is a desktop tool that can be used with Active Backup for Business. This tool is designed for administrators to create recovery media for bare-metal or volume-level restores. Administrators can use this tool if the device intended to create the recovery media is running a 64-bit version of Windows and has the same language and region settings, as well as the same Windows versions and drivers as the device intended to be restored.

Follow the instructions in the [Active Backup for Business Recovery Media Guide](#) to learn how to create recovery media for your device.

# Technical Overview

## Application-aware backup

Enabling **application-aware backup** helps to ensure that your application data is consistent. Backups with application-aware backup enabled make it easier for application data to be restored in the future by creating a snapshot of the application data when the backup is performed.

This feature uses VMware Tools and Microsoft's **Volume Shadow Copy Service (VSS)** to make sure that the backed up data of virtual machines remain consistent and to prevent data inconsistencies from occurring when backing up actively used data.

## Forever-incremental backup

Synology recommends that users enable **Forever-incremental backup** to maximize the number of available backup versions and minimize the storage used for backup retention. When this policy is enabled, a full backup is only executed the first time that a task is performed. After that point, Active Backup for Business tracks changes and backs up only modified or new data.

**Forever-incremental backup** significantly reduces the amount of data transferred for each backup, as well as the amount of duplicated data stored to your backup destinations. This saves time and bandwidth on the source device. ABB relies on technologies native to Microsoft Windows, Microsoft Hyper-V, and VMware vSphere to perform incremental backup.

**Full backup** (bandwidth and storage intensive) is available if you cannot or do not wish to enable change-tracking technologies, or if you prefer to store full sets of data each time a backup is performed.

To enable **Forever-incremental backup**, you must first enable the following, depending on what type of device you are using:

- For PC's or physical servers: **Microsoft Volume Shadow Copy Service (VSS)**
- For VMware virtual machines: **vSphere Changed Block Tracking (CBT)**
- For Hyper-V virtual machines: **Hyper-V Resilient Change Tracking (RCT)**

## Personal computer and physical server

The CBT technology adopted in Active Backup for Business uses VSS to take snapshots for devices and identify changed blocks between snapshots. Make sure that Microsoft Volume Shadow Copy Service (VSS) on each protected device has been turned on to ensure that CBT is functioning properly. After the first full backup, CBT technology allows each device to transfer only changed blocks to your NAS, helping save bandwidth and speeding up the backup process.

## Virtual machine

**Changed Block Tracking (CBT)** and **Resilient Change Tracking (RCT)** are VMware vSphere's and Microsoft Hyper-V's native technology that track the blocks of a virtual machine disk that have been changed since a certain point in time. With VMware vSphere CBT and Microsoft Hyper-V RCT enabled, the amount of data transferred after the first full backup will be greatly reduced, speeding up the backup process.

To enable CBT for a virtual machine, refer to the instructions [this article](#).

## Data deduplication

Active Backup for Business detects and removes any data that are identical between different files, versions, or devices when storing backups to Synology NAS. Built-in deduplication technology can help to cut back on storage use, especially when the devices share similar operating systems, software applications, or files.

To best benefit from ABB deduplication technology, you should back up similar computers or virtual machines to the same Active Backup for Business host.

## Native hypervisor

The integration of ABB with Synology's native hypervisor, **Synology Virtual Machine Manager (VMM)**, powers two distinctive features of Active Backup for Business that make for a more efficient recovery after a server crash: **Backup Verification** and **Instant Restore** to virtual machines for physical or virtual servers.

If you want to use **Backup Verification** or **Instant Restore**, you must be using the **Physical Server** or **Virtual Machine** backup functionality in ABB. To switch devices from **PC backup** to **Physical Server** or **Virtual Machine backup** mode in ABB, go to **PC**, select a device, and then click **More > Change device type**.



## **Backup Verification**

If **Backup Verification** is enabled, a scheduled trial run of the restoration will be performed in VMM for a configured number of seconds. This process will be recorded into a video for your reference, allowing you to confirm that the backup can be successfully restored in case of sudden failure.

## **Instant Restore**

**Instant Restore** allows users to instantly run servers and virtual machines backed up with ABB as virtual machines in Synology VMM. Users can use this feature to implement rapid recoveries while continuing to use services in case of system crashes.

# Backup Configuration

The following sections provide instructions on creating and executing new backup tasks, and configuring essential options and settings.

## VMware and Hyper-V Backup

Active Backup for Business allows you to create backup tasks that can be used to process one or more of your virtual machines. You can either configure a backup task and run it immediately, or save the task and run it later.

Before you start, make sure that your virtual machines show up in **Active Backup for Business > Virtual Machine > VMware vSphere / Microsoft Hyper-V**. If your device is not shown, follow the steps below to add the vCenter Server, vSphere Hypervisor (ESX / ESXi), or Hyper-V servers to your device.

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

### Notes:

- The storage space of the backup destination and the volume where the package is installed has to be at least 8GB to perform backup tasks.
- When using Active Backup for Business to back up Hyper-V, a data mover will be installed on the Hyper-V host. Therefore, the host system's volume must have at least 512MB of free storage.
- If your NAS cannot be accessed by the Hyper-V server directly, click **Connection from Hyper-V to Synology NAS** to configure your network settings.

You can also edit or delete the vCenter Server, vSphere Hypervisor (ESX / ESXi), or Hyper-V server in **Manage Hypervisor**:

- **Edit:** Select existing servers and change the account names and passwords if needed.
- **Delete:** Delete servers when they are no longer needed. If there are protected virtual machines in current backup tasks, you will need to first delete those tasks in order to delete the servers.

## Create a backup task

Users can use any of the methods below to launch the Backup Wizard.

### VMware vSphere

- Go to **Active Backup for Business > Virtual Machine > VMware vSphere** and select one or several virtual machines (Ctrl + left click). Click **Create Task** to launch the backup wizard.
- Go to **Active Backup for Business > Virtual Machine > Task List**, and click **Create > vSphere task** to launch the backup wizard.

### Microsoft Hyper-V

- Go to **Active Backup for Business > Virtual Machine > Microsoft Hyper-V**, and select one or several virtual machines (Ctrl + left click). Click **Create Task** to launch the backup wizard.
- Go to **Active Backup for Business > Virtual Machine > Task List**, and click **Create > Hyper-V task** to launch the backup wizard.

## Select a backup destination

1. Make sure that your backup destination is using a **Btrfs file system**. A shared folder named **"ActiveBackupforBusiness"** will have been automatically created when you installed Active Backup for Business on your NAS.
2. Select a shared folder in the Btrfs file system as the backup destination.

### Notes:

- If you have already selected a virtual machine in the VMware vSphere or Microsoft Hyper-V tab, the selected virtual machine will be automatically displayed in the wizard.

## Task settings

- Compression and encryption can be enabled for the backup destination. These settings cannot be changed after the first backup task is created. If you wish to use different settings for future tasks, you should create a task in a new destination.
- The **Maximum quantity of concurrent backup device(s)** can be configured, but the maximum number of devices that can be backed up concurrently varies depending on RAM capacity.
- Users can enable **Changed Block Tracking, application-aware backup**, data transfer compression, and data transfer encryption.
- Taking snapshots may require additional space on the host datastore, and insufficient space may cause the virtual machine to automatically suspend and lose data. By enabling **source datastore usage detection**, backup tasks will only fail when the host datastore's storage space is below the specified percentage.

- When performing virtual machine backups, users can select **Backup Verification** to implement scheduled trial runs of the restoration, which will be performed in **Virtual Machine Manager**. The entire process will be recorded as a video for reference, so that users can confirm that the backup is able to be successfully restored. The duration of the video can be specified, which will begin recording once Virtual Machine Manager starts running the backup image.
- In **Advanced settings**, users can set up the script and other information for individual virtual machines.
  - Select one or multiple virtual machines for which you want to specify the script or credential settings.
  - Click **Script** to browse the script executed in the guest OS and specify the script processing mode.
    - **Successful script execution required to continue:** The virtual machine backup process will stop if the script fails to be executed.
    - **Ignore script execution failure and continue VM backup:** The virtual machine backup process will continue even if the script fails to be executed.
- In **VMware vSphere**: Click **Set credentials** to specify the username and password for virtual machines.
- In **Microsoft Hyper-V**: Click **VM Information** to configure the credentials, operating system, and IP address for the virtual machine.

**Notes:**

- Active Backup for Business 2.2.0 and above versions support the concurrent backup of up to 50 personal computers, physical servers, and virtual machines. The actual number varies by RAM capacity:
  - Less than 8 GB: 10
  - Between 8 GB and 32 GB: 30
  - More than 32 GB: 50
- **Application-aware backup** uses **Microsoft Volume Shadow Copy Service (VSS)** or **VMware Tools** to make sure that the backed up data of Linux and Windows virtual machines is consistent. For VMware, make sure that you have the latest version of VMware Tools. For Hyper-V, your virtual machine must support VSS and it must be enabled on the target device.
- Setting up the script and enabling the virtual machine script execution requires the credentials of your virtual machine. An error message will be displayed if the credentials are missing.
- **Synology Virtual Machine Manager** must be installed to enable **Backup Verification**.
- For VMware vSphere:
  - **VMware Tools** must be installed to execute a pre-post script.
  - If you are using a free version of an ESXi hypervisor, **CBT** must be manually enabled. Refer to [this article](#) for more information on how to manually enable **CBT**.
  - **Data transfer compression** cannot be enabled on vSphere 5.1 and below.

## Schedule backup tasks

If **Manual backup** is selected, users must start each backup task themselves.

**Scheduled backups** can be set to run on an hourly, daily, or weekly basis.

If you do not want tasks to run when your IT infrastructure is being heavily used, you can select **Configure Backup Windows** and specify time slots for when the backup task is allowed to run.

## Select a retention policy

Users can choose to store all versions of their backup, limit the number of stored versions, or keep only certain versions according to a schedule.

You can choose to set rules for keeping backup versions, such as to retain the latest version of each day, week, month, or year. You can edit the retention policy at **Active Backup for Business > Virtual Machine > Task List > select the task > Edit > Retention > Advanced retention policy > Set Rules**.

Selecting the **Keep only the latest ... versions** option will store a set number of versions regardless of the time intervals set. If more than one backup version exists within a certain 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 a backup task that will run every hour, only the version backed up at 23:00 will be kept.

A version can meet more than one retention rule at a time. For example, a version can be retained by the weekly retention rule and daily retention rule at the same time. Advanced retention policy employs the GFS, or Grandfather-Father-Son retention mechanism.

### Set Rules ✕

Apply the following rules to keep backup versions. One version can meet multiple rules at the same time. [Learn more](#)

- Keep all versions for  days
- Keep the latest version of the day for  days
- Keep the latest version of the week for  weeks
- Keep the latest version of the month for  months
- Keep the latest version of the year for  years

The system will ensure a certain number of latest versions are kept before applying the retention rules above.

Number of latest versions to keep  versions

Cancel OK

## Configure privilege settings

Check the users/groups to whom you wish to grant privileges for performing **Guest OS Files (Windows / Linux) Restores**, for the tasks, or browsing backup versions of the task. To make sure that only eligible users will be able to restore backed-up files and versions of the backup task, privilege settings can be configured both during or after the creation of the backup task.

### Notes:

- Only users belonging to the administrators group are allowed to perform **Instant Restores** and **Full Virtual Machine Restores**. Any other users who are assigned privileges can only perform **Guest Files (Windows / Linux) Restores** via **Active Backup for Business Portal**.

## Apply settings

After configuring the backup settings, a backup summary will be displayed. Once you have confirmed your settings, do the following to finalize your backup:

1. Click **Done** and a pop-up window will appear.
2. Click **Yes** if you would like to run the backup immediately. If you want to run the task afterwards, go to the **Task List**, select the task you have just created, and click **Back up**.

## Manage Backup Tasks

All existing tasks are displayed under **Active Backup for Business > Virtual Machine > Task List**.

### Edit or delete backup tasks

Users can edit tasks individually or several tasks simultaneously by going to **Active Backup for Business > Virtual Machine > Task List**, selecting one or several tasks (Ctrl + left click), and clicking **Edit**. Users can then configure task settings, create a backup schedule, set up a retention policy, and grant privileges.

To delete backup tasks, select one or more tasks in the corresponding task list. Once you confirm the action, all backed up data will be removed along with the backup task.

### Details

To view information on the **Status** and **Logs** for your task, such as the source, execution time, duration, and log time of the backups, and more, select your task and click **Details**.

## Versions

To view information about the backed up versions, such as the status and time of creation, select your task and click **Version**. You can also click the folder icon to browse your backed-up data and the live video of the backup if **Backup Verification** is enabled.

Backup Version Information					✕	
	Time of creation	End Time	Backup Status	Verify backup Status		
🔒	04/26/2021 15:47:41	04/26/2021 16:11:44	Successful		📁	🗑️



# Restoration Guide

Active Backup for Business offers several methods to restore backups of your virtual machines. Which method is best for your case depends on a number of factors, which will be referenced in this section.

## Recovery Options

The following methods are available for virtual machine restoration:

- **Granular (file or folder-level) restore:** Choose a backup version, select files or folders for recovery in the **Active Backup for Business Portal** and automatically restore them to their original location, or download the data to a different device or location. You can also assign end users restore or download permissions via **Control Panel** in DSM.
- **Instant Restore:** Quickly restart a virtual machine directly from a compressed and deduplicated backup file to minimize the downtime of the virtual machine. Instant Restore to VMware or Hyper-V can restart a virtual machine within seconds, but has a limited I/O performance.
- **Full Virtual Machine Restore:** Restore an entire virtual machine from a backup file to the latest state or a previous point in time if the primary virtual machine fails. This method requires more time and resources, but has full I/O disk performance.
- **Instant Restore to Synology Virtual Machine Manager:** Instantly restart a virtual machine from a backup file in Synology VMM.



Refer to the table below for a comparison of the different types of recovery methods.

Full Restore	Instant Restore to VMware	Instant Restore to Hyper-V	Instant Restore to VMM
Long RTO	Short RTO	Short RTO	Short RTO
Full disk I/O performance	Limited disk I/O performance	Limited disk I/O performance	Full disk I/O performance (NAS)
Services and backup data are run and stored on the VMware/Hyper-V	Services are run on VMware, and backup data is stored on NAS	Services are run on Hyper-V, and backup data is stored on NAS	Services and backup data are run and stored on NAS
No further action required if it's restoring to the production site	Need to migrate back to the production site to finalize	Need to export and import back to the production site to finalize	Need to migrate back to the production site to finalize

**Notes:**

- All changes made during **Instant Restore** will be automatically stored on your Synology NAS. Make sure that there is enough space on your Synology NAS.
- For **Instant Restore to VMware vSphere**: to finalize the **Instant Restore to VMware** process, you must migrate the instantly restored virtual machine back to the production site. You can either migrate the virtual machine or clone it to the hypervisor on which you wish it to run. We recommend that you first shut down the virtual machine in case data inconsistency occurs during the cloning process. Migration of VMs requires an eligible vCenter / Storage vMotion license. Refer to the **Migrate VM** section in [this article](#) for further information.

## Instantly Restore your Virtual Machine

### Launch the Instant Restore Wizard

With **Instant Restore to VMware** and **Instant Restore to Hyper-V** you can launch the restore wizard to restore a virtual machine to its most recent state or to any available restore point through any of the methods below.

#### VMware vSphere

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

**Notes:**

- Make sure that the hypervisor is authorized to access and mount the backup destination (shared folder).

### Microsoft Hyper-V

- Go to **Active Backup for Business > Virtual Machine > Microsoft Hyper-V**, select the virtual machine you want to restore, click **Restore** to launch the restore wizard, and select **Restore to Microsoft Hyper-V** and **Instant Restore**.
- 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 select **Restore to Microsoft Hyper-V** and **Instant Restore**.

#### Notes:

- Make sure that the hypervisor is authorized to access and mount the iSCSI target on your Synology NAS. When performing **Instant Restore to Hyper-V**, a backup image will be cloned to a temporary iSCSI target on your Synology NAS, and then the hypervisor will mount the iSCSI target.
- **iSCSI Initiator Service** must be enabled on the source server for the system to perform **Instant Restore to Hyper-V**.

## Select virtual machines and restore points

Select the virtual machines that you want to restore and choose their restore points.

### Select restore mode

- **Restore to the original location:** Restore the selected virtual machine to its original location, while keeping its original name and settings and minimizing the chance of input errors by users. This option instantly unregisters and replaces the original virtual machine on the production site.
- **Restore to a new location, or with different settings:** Customize the destination and settings for the restored virtual machine.

### 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 the virtual machine. Changes made during **Instant Restore** will be stored on your Synology NAS.

For **Instant Restore to VMware**, you can also select the datastore when executing virtual machine migration.

## Apply and Restore

A summary of the restoration will be shown. Once you have confirmed the information to be restored, click **Done**. You will then be automatically directed to **Restore Status** to monitor the restoration progress.

For **Instant Restore to VMware**, click the **Migrate VM** button to finalize the process.

Enable **Power on VM automatically after restoration** to immediately run the restored virtual machine. If you are performing Instant Restore for testing purposes, it is recommended to keep this option **disabled**, and to manually disconnect the initial virtual machine from the production network to avoid any conflicts.

## Fully Restore your Virtual Machine

### Launch the Full VM Restore Wizard

Use one of the methods below to launch the restore wizard to restore virtual machines to the most recent state or to any available restore point through full VM restore.

#### VMware vSphere

- Go to **Active Backup for Business > Virtual Machine > VMware vSphere**, select the virtual machine that you want to restore, and click **Restore** to launch the restore wizard. Click **Restore to VMware vSphere**, and click **Next**. Then, select **Full Virtual Machine Restore**.
- Go to **Active Backup for Business > Virtual Machine > Task List**, select the backup task that you want to restore, and click **Restore** to launch the restore wizard. Click **Restore to VMware vSphere**, and click **Next**. Then, select **Full Virtual Machine Restore**.

#### Microsoft Hyper-V

- Go to **Active Backup for Business > Virtual Machine > Microsoft Hyper-V**, select the virtual machine that you want to restore, and click **Restore** to launch the restore wizard. Click **Restore to Microsoft Hyper-V**, and click **Next**. Then, select **Full Virtual Machine Restore**.
- Go to **Active Backup for Business > Virtual Machine > Task List**, select the backup task you want to restore, and click **Restore** to launch the restore wizard. Click **Restore to Microsoft Hyper-V**, and click **Next**. Then, select **Full Virtual Machine Restore**.

### Select virtual machines and restore point

Select the virtual machines that you want to restore and a restore point for each.

## Select restore mode

- **Restore to the original location:** Restore the selected virtual machine 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 virtual machine at the production site.
- **Restore to a new location, or with different settings:** This option allows you to customize the destination and settings of the restored virtual machine.

## Configure restore settings

If you choose **Restore to the original location**, this step will be skipped.

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

## Apply and Restore

A summary of the restoration will be shown. Once you have confirmed the information to be restored, click **Done**. You will then be automatically directed to **Restore Status** to monitor the restoration progress.

Enable **Power on VM automatically after restoration** to immediately run the restored virtual machine. If you are performing Full VM Restore for testing purposes, it is recommended to keep this option **disabled**, and to manually disconnect the initial virtual machine from the production network and connect it to an isolated non-production network to avoid any 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 provides you with the prerequisites and instructions for instantly restoring your backed up device via Synology VMM.

Refer to the [Synology Virtual Machine Manager product specifications](#) for more information on the limitations, features, and other details of Synology VMM.

## Launch Synology VMM Wizard

### VMware vSphere

- Go to **Active Backup for Business > Virtual Machine > VMware vSphere** and select the virtual machine that 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)**.

### Microsoft Hyper-V

- Go to **Active Backup for Business > Virtual Machine > Microsoft Hyper-V** and select the virtual machine that 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)**.

## Select virtual machine and restore point

Select the virtual machine that you want to instantly restore via Synology Virtual Machine Manager (VMM) and select a restore point.

### Notes:

- Only one virtual machine in each backup task can be instantly restored on Synology VMM at a time. You cannot select multiple virtual machines and run them at the same time.

## Configure virtual machine settings

Once you have selected a virtual machine and restore point, you will need to configure its settings in the Synology VMM wizard. Refer to [this article](#) for more details.

## Apply and restore

After you have configured the settings, click **Done**. The backed up virtual machine will be imported to Synology VMM and you can power on the virtual machine in the Synology VMM console.

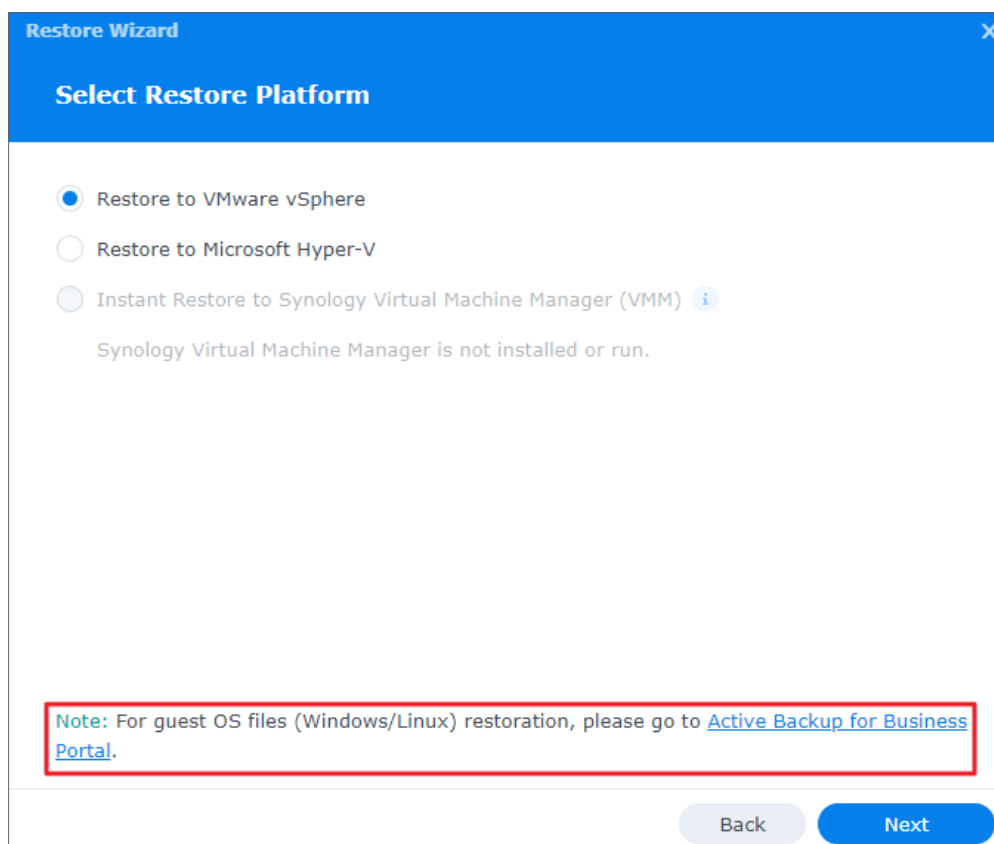
## Guest OS Files (Windows / Linux) Restore

**Guest OS files restore** allows users to restore only files instead of the whole virtual machine. Guest OS files can be restored via **Active Backup for Business Portal**, which is automatically installed when you install **Active Backup for Business**.

### Notes:

- **VMware Tools** is required to be installed to restore guest OS files.
- Supported file systems for Windows / Linux:
  - **Windows:** NTFS, FAT32
  - **Linux:** NTFS, FAT32, EXT3, EXT4

### Launch a guest file restore portal



### VMware vSphere

- Go to **Active Backup for Business > Virtual Machine > VMware vSphere**, select the virtual machine that you want to restore, and click **Restore** to launch the restore wizard. Select a restore point, and on the next page, click on the link to **Active Backup for Business Portal**.
- Go to **Active Backup for Business > Virtual Machine > Task List**, select the backup task you want to restore, and click **Restore** to launch the restore wizard. Select a restore point, and on the next page, click on the link to **Active Backup for Business Portal**.

### Microsoft Hyper-V

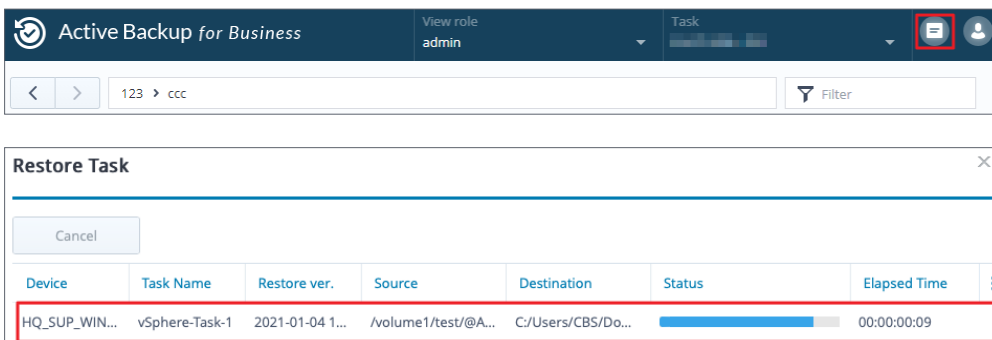
- Go to **Active Backup for Business > Virtual Machine > Microsoft Hyper-V**, select the virtual machine that you want to restore, and click **Restore** to launch the restore wizard. Select a restore point, and on the next page, click on the link to **Active Backup for Business Portal**.
- Go to **Active Backup for Business > Virtual Machine > Task List**, select the backup task you want to restore, and click **Restore** to launch the restore wizard. Select a restore point, and on the next page, click on the link to **Active Backup for Business Portal**.

### Recover individual files

1. In **Active Backup for Business Portal**, under **View role** at the top of the page, make sure that you're using an account with the appropriate privileges.
2. Under **Task**, confirm the source device to which or from which you want to restore files.
3. Select the folders or files that you want to restore.
4. Use the slider at the bottom of the page to select a backup version from which you wish to restore folders or files, then click through the folder structure in the file explorer to select the directory or file.



5. Click **Restore**, and in the pop-up window, you will need to provide your Guest OS (Windows / Linux) login details. In the **For duplicate data** field, you can select whether you want to Overwrite or Skip files that have the same name in the target directory. Click **Next**.
6. Choose the destination to which you want to restore your files, then click **Apply**.
7. You can view the progress of the restoration by clicking the **Restore Task** icon in the upper right-hand corner.



You can also download the files via your local browser by selecting the files and clicking **Download**.



# Best Practices

The following sections provide recommendations for how you can protect your backup data against loss, ensure backup task continuity, and deploy our backup agent to many devices at once while keeping your Synology NAS and DSM secure.

## Maintain remote backup copies and relink

Active Backup for Business safely stores backup data from all of your devices on your Synology NAS. However, issues that occur on one device can affect a whole infrastructure.

Natural disaster, theft, or network unavailability can prevent you from retrieving your data or slow down the recovery process. Therefore, it is strongly recommended that you keep remote copies of all of your backups on a different device and in a different location.

It is also important to always maintain three copies of all of your data (the original copy, a backup, and a copy of that backup in a different location). This is also referred to as the 3-2-1 backup strategy. Synology NAS includes software that allows you to execute this strategy.

### Create remote copies

The following two DSM applications can be used to copy your Active Backup for Business data and configurations from Synology NAS to other devices, or to the public cloud.

- **Snapshot Replication:** This option is recommended if you have access to a secondary Synology NAS. You can replicate your ABB data and settings to another Synology NAS and quickly restart all of your ABB tasks on that device directly from the replica.
- **Hyper Backup:** This option allows you to back up your ABB data and settings to more locations, including portable drives, file servers, and public cloud storage. However, recovery requires you to first restore the backup to a functioning Synology NAS before relinking and restarting ABB tasks.



## Relink

- After creating a replication or backup task, it is important to make sure that you know how to successfully restore or relink your existing Active Backup for Business tasks and backup data, whether they exist on a secondary NAS, in public clouds, or other storage media.
- [This tutorial](#) provides detailed instructions on how to back up and relink your Active Backup for Business data using **Snapshot Replication** and **Hyper Backup**. To do this, make sure that your Synology NAS has 64-bit processors, is running DSM 6.1.7 or above, is running Active Backup for Business 2.0.4 or above, and have the necessary packages installed on your Synology NAS. See the **Environment** section in the tutorial for more details.

# Learn more

## Related articles

- [Frequently asked questions about Active Backup for Business](#)
- [How do I select a suitable NAS for running Active Backup for Business?](#)
- [What VMware vSphere permissions are required for Active Backup for Business to back up and restore virtual machines?](#)
- [How do I migrate an instantly restored virtual machine to its original virtualization platform?](#)
- [How can I restore entire device backups from Active Backup for Business in Virtual Machine Manager?](#)
- [How many devices can I back up concurrently with Active Backup for Business?](#)

## Software specs

Refer to the Active Backup for Business [software specifications](#) to learn more about the package's features, components, and limitations.

## Other resources

For more step-by-step tutorials and visual information, feel free to also check out [Synology's YouTube channel](#). There, you can find related videos by searching for "Active Backup for Business".

You can also find admin guides, brochures, technical specifications, user guides, whitepapers and more for Active Backup for Business in [Synology Documentation](#).



**SYNOLOGY  
INC.**

9F, No. 1, Yuandong Rd.  
Banqiao Dist., New Taipei City 220545  
Taiwan  
Tel: +886 2 2955 1814

**SYNOLOGY  
AMERICA CORP.**

3535 Factoria Blvd SE, Suite #200,  
Bellevue, WA 98006  
USA  
Tel: +1 425 818 1587

**SYNOLOGY  
UK LTD.**

Unit 5 Danbury Court, Linford Wood,  
Milton Keynes, MK14 6PL  
United Kingdom  
Tel.: +44 (0)1908048029

**SYNOLOGY  
FRANCE**

102 Terrasse Boieldieu (TOUR W)  
92800 Puteaux  
France  
Tel: +33 147 176288

**SYNOLOGY  
GMBH**

Grafenberger Allee 295  
40237 Düsseldorf  
Deutschland  
Tel: +49 211 9666 9666

**SYNOLOGY  
SHANGHAI**

200070, Room 201,  
No. 511 Tianmu W. Rd.,  
Jingan Dist., Shanghai,  
China

**SYNOLOGY  
JAPAN CO., LTD.**

4F, No. 3-1-2, Higashikanda,  
Chiyoda-ku, Tokyo, 101-0031  
Japan

**Synology®**



[synology.com](https://synology.com)

Synology may make changes to specifications and product descriptions at any time, without notice. Copyright © 2020 Synology Inc. All rights reserved. ® Synology and other names of Synology Products are proprietary marks or registered trademarks of Synology Inc. Other products and company names mentioned herein are trademarks of their respective holders.