

Active Backup for Business Admin Guide for Virtual Machines

Based on Active Backup for Business 2.5.0



Table of Contents

Introduction	2
About this guide	2
Intended audience	2
What is Active Backup for Business?	2
Features and Management Tools	3
Backup and recovery features	3
Backup management	4
Planning and Preparation	5
Requirements	5
Considerations and limitations	6
Backup tips	7
Backup Configuration	9
VMware and Hyper-V backup	9
Create a backup task	10
Manage backup tasks	14
Restoration Guide	15
Recovery options	15
Instantly restore your virtual machine	16
Fully Restore your Virtual Machine	18
Instant Restore to Synology Virtual Machine Manager (VMM)	19
Guest OS Files (Windows / Linux) Restore	20
Best Practices	23
Maintain remote backup copies and relink	23
Learn more	25
Related articles	25
Software specs	25
Other resources	25

Introduction

About this guide

This guide will help you become familiarized with Active Backup for Business, walk you through the initial setup of a backup task, and provide information on recovery.

Intended audience

This guide is intended for anyone who wants to start using Active Backup for Business to back up their Microsoft Hyper-V or VMware vSphere virtual machines.

What is Active Backup for Business?

Synology's all-in-one commercial data protection solution, **Active Backup for Business (ABB)**, is based on the award-winning DSM operating system. ABB centralizes data protection across a variety of IT environments, including virtual machines, physical servers, file servers, and personal computers. Administrators can deploy their preferred protection plan single-handedly through ABB's centralized admin console.

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

Why should you use Active Backup for Business?

- Your one-stop-backup solution – Ensuring that everything in your backup environment is compatible can be a challenge, especially with so many factors to consider. ABB simplifies things by providing an all-in-one solution right on your Synology NAS.
- Smart storage – ABB is designed with cross-platform, device, and version deduplication to help reduce backup time and improve storage efficiency. ([See applicable models](#)).
- Unrestricted expand-ability – Increasing your number of devices and data? No problem. With ABB, you can protect an unlimited number of devices and data, license-free.
- Centralized management – Remove the burden on IT workers of managing backup tasks and devices across several platforms by using ABB's intuitive, web-based portal.
- Integrated support – When something goes wrong, whether it's hardware or software-related, Synology Technical Support is ready to help, reducing the time and effort needed when looking for help from different providers.

Features and Management Tools

Backup and recovery features

Application-aware backup

Application-aware backup is a backup feature that 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.

Incremental backup

Incremental backup is a backup feature that reduces the amount of data transferred for each backup, as well as the amount of duplicated data stored on your backup destinations. This is done by tracking changes and only backing up modified or new data in between full backups. This maximizes the number of available backup versions, minimizes the amount of storage used for backup retention, and also saves time and bandwidth on the source device.

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.

See [How to enable CBT manually for a virtual machine](#) for detailed setup instructions.

Data deduplication

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

For more detailed information on data deduplication techniques and how deduplication is calculated for ABB, refer to the [Data Deduplication White Paper](#).

Built-in hypervisor

Integration of ABB with Synology's built-in hypervisor, **Synology Virtual Machine Manager (VMM)**, powers two distinctive features of Active Backup for Business that enable efficient recovery after a server crash: **Backup Verification** and **Instant Restore**.

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, so you can confirm that the backed up data can be successfully restored in case of sudden disaster.

Instant Restore

Instant Restore allows you to instantly restore servers and virtual machines backed up to ABB as virtual machines in Synology VMM. You can use this feature to implement rapid recoveries while continuing to use services in case of system crashes.

Backup management

Active Backup for Business Portal

The **Active Backup for Business Portal** is ABB's affiliated restoration portal. 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 the Active Backup for Business package. Refer to the [ABB Portal help article](#) to learn more about how to navigate the portal, perform restores, and for other settings.

Planning and Preparation

Requirements

See the [full specifications for Active Backup for Business](#) for detailed information.

NAS system requirements

See [How to select a suitable NAS for running Active Backup for Business?](#) for recommendations.

Item	Requirements
Operating system	<ul style="list-style-type: none">• 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
Virtual machines	<ul style="list-style-type: none">• 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 2022• Windows Server Hyper-V 2019• Windows Server Hyper-V 2016

For a full list of requirements for backups and restorations, refer to the [Requirements and Limitations](#).

Considerations and limitations

NAS

- To maximize backup performance, avoid running too many packages at once in DSM.
- To perform a backup task, there should be at least 8 GB of free space both on the backup destination and on the volume where the package is installed.

Backup client (virtual machines)

VMware

- Make sure that **Secure Shell (SSH)** service is enabled on the virtual machine.
- To perform incremental backups, make sure that **Changed Block Tracking (CBT)** is enabled on the virtual machine.
- To perform **application-aware backups**, make sure that **VMware Tools** is properly installed on the virtual machine.
- To run a Pre-Freeze or Post-Thaw script on a backup task, make sure that **VMware Tools** is properly installed on the virtual machine.

Hyper-V

- Make sure that WinRM is enabled on the Hyper-V host.
- Allow SMB connections through the firewall on the Hyper-V host.
- If your Hyper-V host does not belong to a domain and you are using an account other than the built-in administrator account, make sure that **User Account Control (UAC)** is **disabled**.

Network

- If the hypervisor is behind a NAT, make sure that port forwarding rules are configured on it.
- If the hypervisor is behind a firewall, make sure that backup services are allowed by the firewall rules.
- To perform operations successfully and enable communication between your Synology NAS and virtual machines, make sure that the following TCP ports are **opened**:

Type	TCP Port Number	Details
------	-----------------	---------

VMware	<ul style="list-style-type: none"> vCenter servers ESXi hosts 	443	Default port used for connections to VMware infrastructure
	<ul style="list-style-type: none"> ESXi hosts 	902	Port used for transferring and moving data
Hyper-V	<ul style="list-style-type: none"> Hyper-V hosts 	445 (SMB port)	Port used for receiving and transferring data from Hyper-V to Synology NAS
	<ul style="list-style-type: none"> SCVMM Failover clusters Hyper-V hosts 	5986	Port used for in-flight encryption when transferring and moving data
	<ul style="list-style-type: none"> SCVMM Failover clusters Hyper-V hosts 	5985	Port used for transferring and moving data

Backup tips

- **For VMware vSphere:** Make sure that the account you use to add VMware vSphere hypervisor has either full administrative permissions (recommended) or [these specific permissions](#).
- **For Hyper-V:** Make sure that your virtual machine's system volume has at least 512 MB of free space.
- Antivirus software may interfere with API commands, which could result in backup failure. If a backup fails, check the activity log of the hypervisor host's antivirus software for any errors.
- To have new virtual machines automatically be added to the backup task, enable **Auto Discovery** and select the folders, hosts, or datacenters where you want to enable it.
- Make sure that the [device that you want to back up is supported](#) on your version of ABB.
- Set up a **Retention Policy** for your backup tasks to delete older backup versions so your backups don't take up too much space.
- Configure a **backup schedule** to maintain regular backups of your data.

- Allow users access to the **Active Backup for Business Portal** so they can browse backups and recover individual files or entire folders as needed.
- Add a second layer of protection to your data by implementing the [3-2-1 backup rule](#) (3 backups: 2 on different storage mediums and 1 offsite) using **Hyper Backup** or **Snapshot Replication**.

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** or **Microsoft Hyper-V**. If your device is not shown, use the following steps to add the vCenter Server, vSphere Hypervisor (ESX / ESXi), or Hyper-V servers to your device.

1. Click **Manage Hypervisor > Add**.
2. Fill in the server address and account information.

Notes:

- There must be at least 8 GB of free space on both the backup destination and on the volume where the package is installed.
- 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 to change the account names and passwords.
- **Delete:** Delete servers that are no longer needed. If there are protected virtual machines in current backup tasks, you need to delete those tasks before you can delete the servers.

Create a backup task

Use one of the following methods 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**" is automatically created when you install 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 on the VMware vSphere or Microsoft Hyper-V tab, the selected virtual machine will automatically be displayed in the wizard.

Task settings

- You can enable compression and encryption for the backup destination. These settings cannot be changed after the first backup task is created. If you want to use different settings for future tasks, you will have to create a task for a new destination.
- The **Maximum quantity of concurrent backup device(s)** depends on the RAM capacity.
- You can enable **Changed Block Tracking, application-aware backup**, data transfer compression, and data transfer encryption.
- Since taking snapshots may require additional space on the host datastore, insufficient space on the datastore may cause the suspension of virtual machines and thus data loss. With **source datastore usage detection** enabled, backup tasks will only fail if the host datastore's storage space is below the specified percentage.
- You can select **Backup Verification** to implement scheduled trial runs of the restoration in **Virtual Machine Manager**. The entire process will be recorded as a video for reference, so

that you can confirm that the backup can be successfully restored.

- In **Advanced settings**, you can configure the script and other information for each virtual machine.
 1. Select one or multiple virtual machines for which you want to specify the script or credentials.
 2. 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.
 3. In **VMware vSphere**: Click **Credential** to specify the username and password for virtual machines.
 4. 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. See [How to enable CBT manually for a virtual machine](#) for detailed instructions.
 - **Data transfer compression** cannot be enabled on vSphere 5.1 or below.

Schedule backup tasks

- **Manual backup** requires you to start each backup task manually.
- **Scheduled backups** can be set to run on an hourly, daily, or weekly basis.
- **Configure Backup Windows** allows you to specify time slots for when the backup task is allowed to run. This is useful if you don't want tasks to run when your IT infrastructure is being heavily used.

Select a retention policy

- You can choose to store all versions of your 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 **Long-Term Retention Policy (GFS)**.

Set Rules
✕

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

<input checked="" type="checkbox"/>	Keep all versions for	1	days
<input checked="" type="checkbox"/>	Keep the latest version of the day for	7	days
<input checked="" type="checkbox"/>	Keep the latest version of the week for	4	weeks
<input checked="" type="checkbox"/>	Keep the latest version of the month for	12	months
<input checked="" type="checkbox"/>	Keep the latest version of the year for	3	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

10

versions

Cancel
OK

Configure privilege settings

Select the users or groups to whom you want to grant privileges for performing **Guest OS Files (Windows / Linux) Restore** and browsing backup versions of the task. To ensure that only eligible users will be able to restore backed-up files and versions, you can configure privilege settings both during and after the creation of the backup task.

Notes:

- Only users belonging to the **administrators** group are allowed to perform **Instant Restore** and **Full Virtual Machine Restore**. Other users who are enabled in this step can only perform **Guest Files (Windows / Linux) Restore** via the **Active Backup for Business Portal**.

Apply settings

1. Confirm your backup settings and click **Apply**. 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 later on, go to the **Task List**, select the task, 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

To edit tasks individually or several tasks simultaneously, go to **Active Backup for Business > Virtual Machine > Task List**, select one or several tasks (Ctrl + left click), and click **Edit**.




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, select your task and click **Details**.

Versions

To view information about 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					X
	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:** 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 limited I/O performance.
- **Full Virtual Machine Restore:** Restore an entire virtual machine from a backup file to its 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 following table for a comparison of different recovery methods:

Item	Full Restore	Instant Restore to VMware	Instant Restore to Hyper-V	Instant Restore to VMM
RTO	Long RTO	Short RTO	Short RTO	Short RTO
I/O performance	Full disk	Limited disk	Limited disk	Full disk (NAS)
Service location	VMware or Hyper-V	VMware	Hyper-V	NAS
Backup data storage location	VMware or Hyper-V	NAS	NAS	NAS

Post-restoration requirements	No further action required if 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 are automatically stored on your Synology NAS. Make sure that there is enough space on your Synology NAS for this.
- For **Instant Restore to VMware vSphere**: To finalize the process, you must migrate the instantly restored virtual machine back to the production site. You can either migrate or clone the virtual machine to the hypervisor where you want it to run. We recommend that you first shut down the virtual machine in case any data inconsistencies result from the cloning process. Migration of VMs requires an eligible vCenter or Storage vMotion license. Refer to [Migrate VM](#) 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 the following methods.

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. 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, we recommend you 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 following methods to launch the restore wizard to restore virtual machines to their 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 its 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 [Virtual Machine Manager product specifications](#) for more information on the limitations, features, and other details.

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](#).

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 specific files instead of a whole virtual machine. Guest OS files can be restored via the **Active Backup for Business Portal**, which is automatically installed with **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

Restore Wizard [X]

Select Restore Platform

Restore to VMware vSphere

Restore to Microsoft Hyper-V

Instant Restore to Synology Virtual Machine Manager (VMM) i

Synology Virtual Machine Manager is not installed or run.

Note: For guest OS files (Windows/Linux) restoration, please go to [Active Backup for Business Portal](#).

Back Next

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

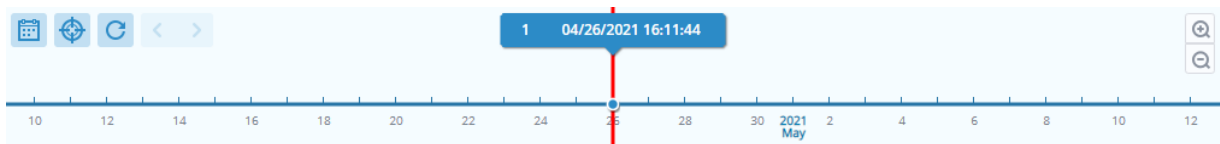
- Go to **Active Backup for Business > Virtual Machine > Microsoft Hyper-V**, select the virtual machine that you want to restore, and click **Restore** to launch the restore wizard. Select a

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 provide your Guest OS (Windows / Linux) login details in the pop-up window. 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**.

You can view the progress of the restoration by clicking the **Restore Task** icon in the upper right-hand corner.

A screenshot of the Active Backup for Business interface. The top navigation bar includes the logo, 'Active Backup for Business', 'View role admin', and 'Task'. A red box highlights a notification icon in the top right. Below the navigation bar is a breadcrumb '123 > ccc' and a 'Filter' button. The main content area is titled 'Restore Task' and contains a table with the following data:

Device	Task Name	Restore ver.	Source	Destination	Status	Elapsed Time
HQ_SUP_WIN...	vSphere-Task-1	2021-01-04 1...	/volume1/test/@A...	C:/Users/CBS/Do...	<div style="width: 100%; height: 10px; background-color: #007bff;"></div>	00:00:00:09

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 by creating remote backup copies and relinking.

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 an entire infrastructure.

Natural disaster, theft, or network issues can prevent you from retrieving your data or slow down the recovery process. Therefore, we strongly recommend you to keep remote copies of all of your backups on a different device and in a different location.

Keep in mind that you should always maintain three copies of your data (the original copy, a backup, and a copy of that backup in a different location). This is referred to as the [3-2-1 backup strategy](#). To make things easy, Synology NAS has everything you need to implement 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 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.
- **Hyper Backup:** This option allows you to back up your ABB data and settings to other locations, such as 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 can 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.

For detailed instructions on how to back up and relink your Active Backup for Business data using **Snapshot Replication** and **Hyper Backup**, refer to the following tutorial:

- [How do I back up and relink Active Backup for Business data to a destination Synology NAS?](#)

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 has the necessary packages installed.

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, white papers and more for Active Backup for Business in [Synology Documentation](#).