

# Active Backup for Business Admin Guide for Windows PCs and Physical Servers



# Table of Contents

|                                          |    |
|------------------------------------------|----|
| <b>Introduction</b>                      | 2  |
| About this guide                         | 2  |
| Intended audience                        | 2  |
| What is Active Backup for Business?      | 2  |
| <b>Features and Management Tools</b>     | 3  |
| Backup and recovery features             | 3  |
| Backup management                        | 4  |
| <b>Planning and preparation</b>          | 6  |
| Requirements                             | 6  |
| Considerations and limitations           | 7  |
| Backup tips                              | 8  |
| <b>Backup Configuration</b>              | 9  |
| Windows PC and server backup             | 9  |
| Create a backup task                     | 9  |
| Manage backup tasks                      | 12 |
| <b>Restoration Guide</b>                 | 14 |
| Recovery options                         | 14 |
| Restore an entire device                 | 14 |
| Recover individual files                 | 16 |
| Restore servers to virtual machines      | 18 |
| <b>Best Practices</b>                    | 20 |
| Maintain remote backup copies and relink | 20 |
| Mass deployment in Windows environments  | 21 |
| <b>Learn more</b>                        | 24 |
| Related articles                         | 24 |
| Software specs                           | 24 |
| Other resources                          | 24 |
| <b>Appendix</b>                          | 25 |
| Permissions and security                 | 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 Windows PCs or physical servers.

## 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.

The CBT technology adopted in Active Backup for Business uses **Microsoft Volume Shadow Copy Service (VSS)** to take snapshots for devices and identify changed blocks between snapshots. To enable incremental backup, make sure that **VSS** on each protected device is turned on.

### 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** to virtual machines for physical servers.

## **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 Agent**

The **Active Backup for Business Agent** is a utility that is installed on your client device before backing up data in order to carry out backup tasks. Administrative privileges are required to install, update, or uninstall the agent.

This tool is available for download in the [Download Center](#). Refer to the [ABB Agent help article](#) for installation instructions, details on mass deployment, and other information.

## **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.

## **Active Backup for Business Recovery Media Creator**

Synology **Active Backup for Business Recovery Media Creator** is a desktop tool that can be used with ABB. This tool is designed for administrators to automatically create recovery media for bare-metal or volume-level restores. Administrators can use this tool as long as 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.

For devices that don't fit the requirements for automatic recovery media creation, administrators can manually create recovery media instead.

For both automatic and manual recovery media creation, follow the instructions in the [Recovery Media Creation Guide](#) to learn how to create recovery media for your device.

# 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"><li>• DSM 7.0 and above (ABB 2.2.0 and above)</li><li>• DSM 6.2 and above (ABB 2.1.0 and above)</li><li>• DSM 6.1.7 and above (ABB 2.0.4 and above)</li></ul> |
| 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          | <ul style="list-style-type: none"><li>• Windows 11 (all editions)</li><li>• Windows 10 Creators Update (all editions)</li><li>• Windows 10 (all editions)</li><li>• Windows 8.1 (all editions)</li><li>• Windows 7 SP1 (all editions)</li></ul> |

## Physical Server

- Windows 11 (all editions)
- 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

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 (PCs and physical servers)

- The backup client should use the **NTFS file system**.
- **Microsoft Volume Shadow Copy Service (VSS)** must be enabled in order to perform backups.
- Make sure to reserve an appropriate amount of disk capacity for VSS snapshot storage. For more information on VSS configuration, refer to [Volume Shadow Copy Service](#) by Microsoft.
- For external devices: Only external hard drives can be backed up. The backup of other external devices, such as floppy disks, thumb drives, and flash card readers is not supported.
- The backup of computers with 4Kn disks is not supported.
- The backup of virtual hard disks (VHDs) on Windows is not supported. To back up VHDs, you need to either back up the **entire device** or back up the **volume** where the VHD files are located.

### Network



- To establish a secure connection between the NAS and the client, make sure that DSM has a [valid certificate](#) for ABB.
- If you will use DDNS or an IP address to connect to the server from the agent, refer to our [suggested network configurations](#).

## Backup tips

- Avoid using any other backup software to prevent conflicts with Windows VSS functions.
- 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 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 preparing backup targets, creating and executing new backup tasks, and configuring options and settings.

## Windows PC and server backup

Active Backup for Business allows you to remotely conduct full backups of Windows PCs and servers with the help of the [Synology Active Backup for Business Agent](#).

### Before you start

1. Install the **Synology Active Backup for Business Agent** on the target device that you want to protect. Go to the Synology [Download Center](#) or **Active Backup for Business > PC or Physical Server > Add device** to download the 32-bit or 64-bit installer for the device.
2. Configure a **template** in **Active Backup for Business**. Go to **Settings > Template > Create** to make a new template, or select the default template and click **Edit**.

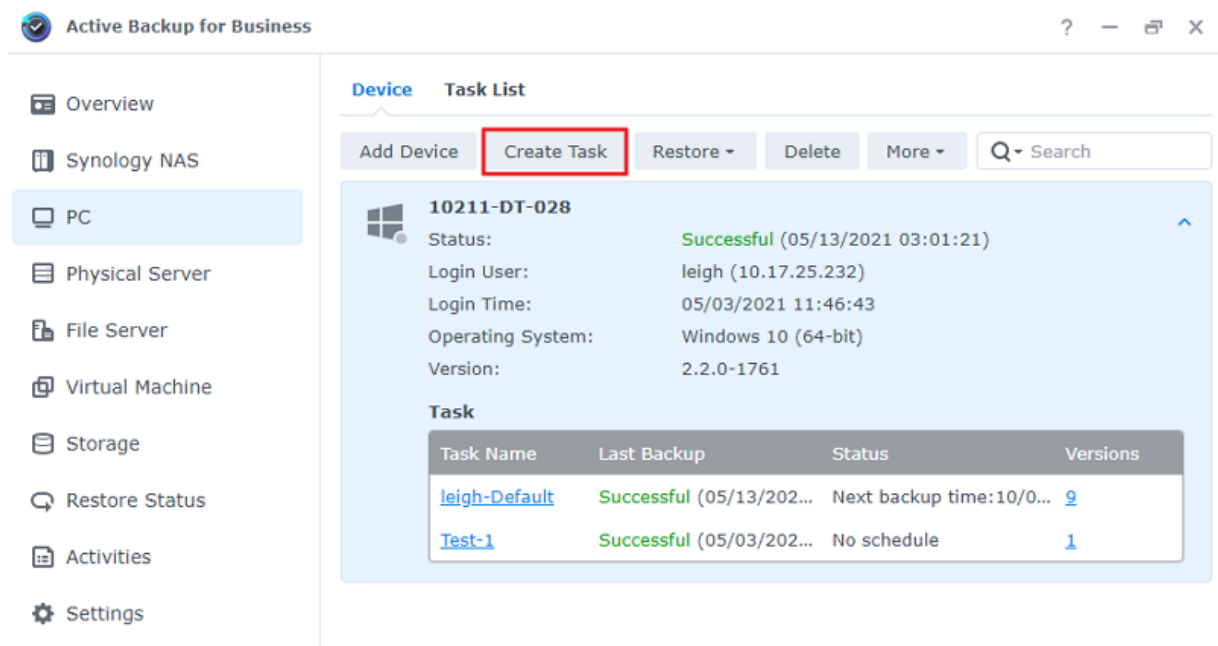
#### Notes:

- ABB uses TCP network port **5510**.
- Configuring backup settings in a **template** allows you to apply the same backup settings to multiple devices. The default backup template is always listed and cannot be removed.
- When creating a template, you can select the **backup type**, **backup schedule**, **compression settings**, **encryption settings**, and **version retention policy**.
- Only admins, users belonging to the administrators group, and users with privileges can access device backups using the **Active Backup for Business Portal** or restore full devices using recovery media. Privileges for performing PC restorations are **not** configurable. Privileges for performing physical server restorations can be configured in backup templates.

## Create a backup task

Once the **Active Backup for Business Agent** is installed on a PC or physical server and is connected to your Synology NAS, a backup task is created according to an applicable template. You can create more than one backup task for each device.

1. Go to **PC** or **Physical Server**, select the device and click **Create Task** to enter the **Agent Backup Creation Wizard**.



2. Follow the steps in the wizard to name the task, select a target device (if not yet selected), and choose a backup destination.

## Select a source type

You can select:

- **Entire device:** Back up full PCs or servers, including settings and applications.
- **System volume:** Protect partitions with Windows system data.
- **Customized volume:** Manually select backup targets. Note that external devices other than external hard drives are not supported.

## 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.

## Task settings

- You can enable data transfer compression, data transfer encryption, and application-aware backup.
- Compression and encryption can be enabled for the backup destination.

- For **physical server** backups, you 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 you can confirm that the backup can be successfully restored.
- You can customize pre/post scripts when performing **physical server** backups.

**Note:**

**Application-aware backup** uses **Microsoft Volume Shadow Copy Service (VSS)** to ensure that backed up data is consistent. Make sure that **VSS** is enabled on the target device if you want to use this feature.

## 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.
- **Backup by event**, available for PC backups, runs the task depending on your selection: when the screen is locked, when you sign out, or when the system starts up. You can also specify a minimum time interval between backups.

If you don't want tasks to run while your IT infrastructure is under heavy use, select **Configure Backup Windows** and set time slots for when the backup task can run each week.

## Select a retention policy

- You can choose to store all versions of your backup, limit the number of stored versions, or only keep 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 > PC or Physical Server > 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 the daily retention rule at the same time. Advanced

retention policy employs a **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                    | <input type="text" value="1"/> days    |
| <input checked="" type="checkbox"/> Keep the latest version of the day for   | <input type="text" value="7"/> days    |
| <input checked="" type="checkbox"/> Keep the latest version of the week for  | <input type="text" value="4"/> weeks   |
| <input checked="" type="checkbox"/> Keep the latest version of the month for | <input type="text" value="12"/> months |
| <input checked="" type="checkbox"/> Keep the latest version of the year for  | <input type="text" value="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 | <input type="text" value="10"/> versions |
|-----------------------------------|------------------------------------------|

CancelOK

## Manage backup tasks

All existing tasks are displayed under **Active Backup for Business > PC or Physical server > Task List**.

### Edit or delete backup tasks

To edit tasks individually or several tasks simultaneously, go to **PC or Physical Server > Task List**, select one or several tasks (Ctrl + left click), and click **Edit**.

- The **Backup destination** cannot be changed.
- **Task settings** and **Source type** can be changed both individually and simultaneously.
- The **Task name** can only be changed individually.

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.




Deleting tasks does not remove **Active Backup for Business Agent** from the client devices, which will continue to be displayed under **PC or Physical Server**. Templates are preserved under **Settings > Template**.

### 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                                                        |                     |                     |               | X                                                                                   |                                                                                     |
|-----------------------------------------------------------------------------------|---------------------|---------------------|---------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|                                                                                   | Time of creation    | End Time            | Backup Status |                                                                                     |                                                                                     |
|  | 05/13/2021 03:00:02 | 05/13/2021 03:01:21 | Successful    |  |  |

## Update the agent

If your Synology NAS is connected to the internet, go to **Active Backup for Business > PC or Physical Server**. Select the target device that needs to be updated and click **More > Update Agent**.

If your Synology NAS is **not** connected to the internet, but is on a private network:

1. Download the **Active Backup for Business Agent** installer from the [Download Center](#), and upload it to any folder on your Synology NAS using **File Station**. Make a note of the location of the installer.
2. [Sign in to DSM with root permissions](#) on your device.
3. Execute the following command to install the agent on your target devices:

```
cp /[volume_where_you_uploaded_the_installer]/[name_of_the_folder_where_you_uploaded_installer]/[installer_name**] /**[volume_where_you_installed_Active_Backup_for_Business]/@tmp/
```

For example, if the location of the installer is /volume1/Files/Synology Active Backup for Business Agent-2.0.4-0621-x64.msi and Active Backup for Business is installed on volume1, then the command should be:

```
cp /[volume1]/[Files]/[Synology Active Backup for Business Agent-2.0.4- 0621-x64.msi**] /**[volume1]/@tmp/
```

4. After completing the setup, the agent will be successfully updated.

# Restoration Guide

Active Backup for Business offers several methods to restore your Windows device backups. Which method is best for your case depends on whether you only want to recover files or restore an entire device to a previous state.

While **PC** backup tasks only allow for physical or file-level recoveries, **Physical Server** backup tasks allow you to use virtual recovery options.

## Recovery options

Two methods are available for both **PC** and **Physical Server** task restoration:

- **Entire device restore:** Create a bootable ISO image or USB drive and boot your device into the **Active Backup for Business Recovery Wizard**. You can later restore your full device (bare-metal restoration) or a specific volume over the network via your Synology NAS if necessary.
- **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.

**Physical Server** backup tasks can also be restored to a virtual machine via VMware vSphere, Microsoft Hyper-V, or Synology VMM via the following methods:

- **Instant Restore:** Restart your server as a virtual machine in VMware, Hyper-V, or Synology VMM directly from a compressed and deduplicated backup image to resume services efficiently.
- **Full Virtual Machine Restore:** Convert your backup image into a virtual machine before booting your server into VMware or Hyper-V for better virtual disk input-output performance.

## Restore an entire device

Returning full devices or volumes to a previous state requires you to create **recovery media** and boot your device using the recovery media.

Since this guide only provides a brief summary of how to create recovery media, we recommend that you refer to the [Recovery Media Creation Guide](#) for further details and instructions.

### Create recovery media

To restore full Windows devices or volumes, you must first create external recovery media. With Active Backup for Business, you can create a bootable USB drive or ISO image (for CD creation).

These can be booted into the **Active Backup for Business Recovery Wizard** to restore your device from your Synology NAS.

**Note:**

Recovery media must be created separately for each device configuration. If two devices have different language or region settings, run different windows versions, or contain different drivers, you must create two separate recovery media for each device.

## Available creation methods

There are two methods for creating a bootable recovery drive or disc with Active Backup for Business:

- **Automatic:** If you want to restore a 64-bit system, you can create recovery media automatically in Windows using the **Active Backup for Business Recovery Media Creator**. You must do this on a system with the same language and region settings, Windows versions, and drivers as those on the device that you want to restore.
- **Manual:** Manual recovery media creation is available for 32-bit systems, as well as for devices that do not meet the conditions for creating automatic recovery media.

## Windows Preinstallation Environment

When creating recovery media, a customized installation of the **Windows Preinstallation Environment (Windows PE)** will be set up on your recovery drive. Windows PE is a lightweight Windows operating system that can be easily booted from portable drives and used to repair or troubleshoot systems.

**Windows PE** is included with the **ABB Recovery Media Creator**, but needs to be downloaded together with **Deployment Tools** as part of the **Windows Assessment and Deployment Kit (Windows ADK)** for manual recovery media creation.

## Bare-metal restore with recovery media

Once you have successfully created recovery media for the device that you want to restore, you can use your recovery drive to boot the device into the **Active Backup for Business Recovery Wizard**.

For step-by-step instructions on how to restore your full Windows device or volume using the wizard, refer to the following article and video:

- [Synology Active Backup for Business Recovery Wizard Help article](#)
- [How to Back up and Restore Your Windows Devices Using Active Backup for Business | Synology](#)

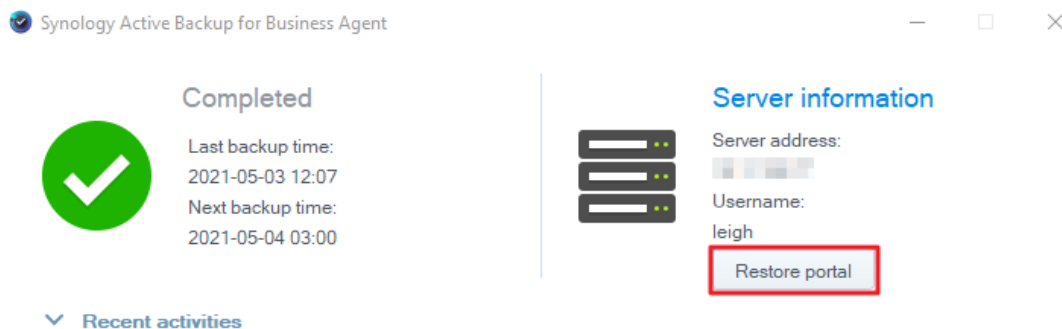
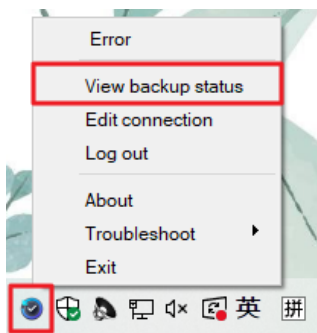


# Recover individual files

Individual file or folder restore is done through the **Active Backup for Business Portal**. There are two ways to access the portal, either directly from the DSM account that administrates Active Backup for Business, or from the **Active Backup for Business Agent** on the endpoint device that you want to restore.

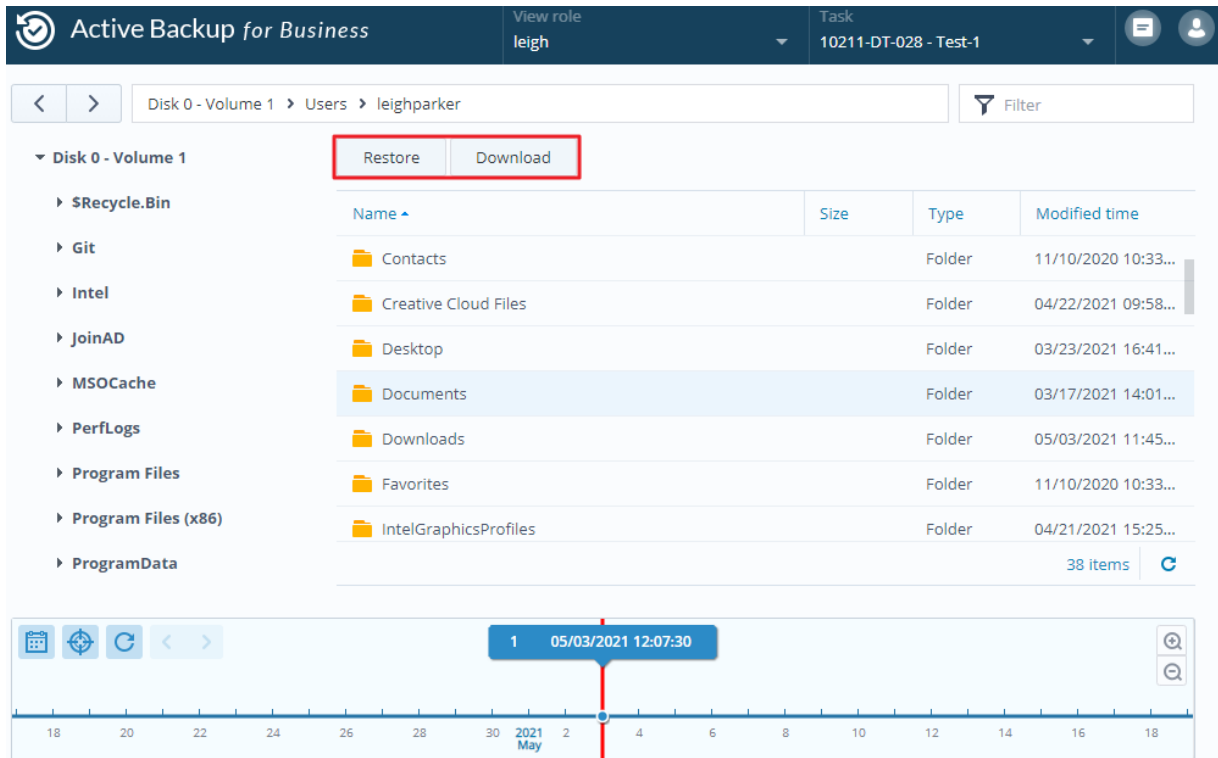
## Restore files or folders from an endpoint device

1. To access the portal, right-click on **Active Backup for Business Agent** in the Windows system tray, select **View backup status**, and then click **Restore Portal**.



2. Sign in with your DSM account.
3. In the upper right corner under **View role** and **Task**, make sure that the correct user and device are selected.
4. Use the slider at the bottom of the page to select a backup version to restore folders or files from, then click through the folder structure in file explorer to select the directory or file.
5. Choose if you want to **Restore** or **Download** the data. If you select **Restore**, your backup agent will download the files or folders and restore them to their original location on your device. If you select **Download**, the selected files will be downloaded via your browser to your

chosen download location.



## Restore files or folders from DSM

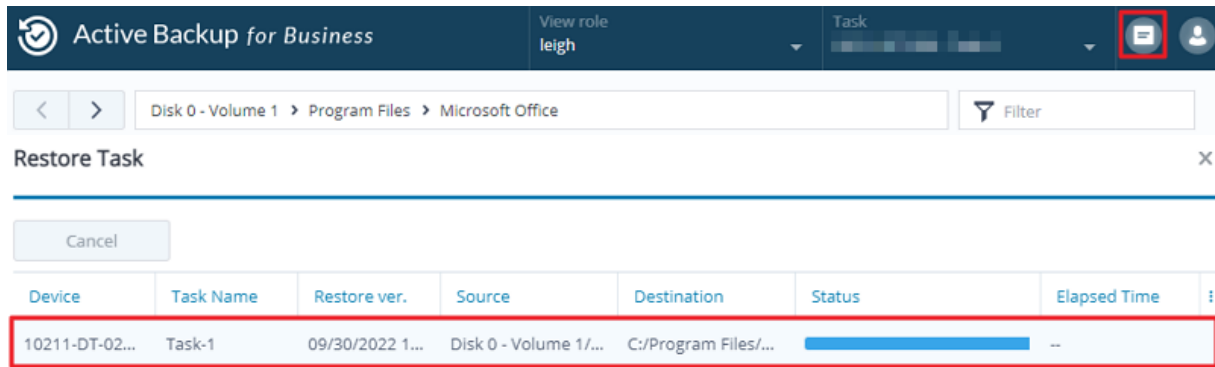
Administrators and accounts administrating Active Backup for Business can access the **Restore Portal** from any device. Use the following steps to restore files to the original backup source device or download them via your browser.

1. In DSM, go to the **Main Menu** and select **Active Backup for Business Portal**.
2. Under **View role** at the top of the page, select a user with the appropriate restoration privileges.
3. Under **Task**, select the source device from which you want to restore files.
4. Select the folders or files that you want to restore.
5. 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.



6. Choose if you want to **Restore** or **Download** the data. If you select **Restore**, your backup agent will download the files or folders and restore them to the specified location on your device. You can also choose if you want files with the same name to be skipped during the restoration by ticking the related checkbox. If you select **Download**, then the selected files will be downloaded via your browser to your chosen download location.

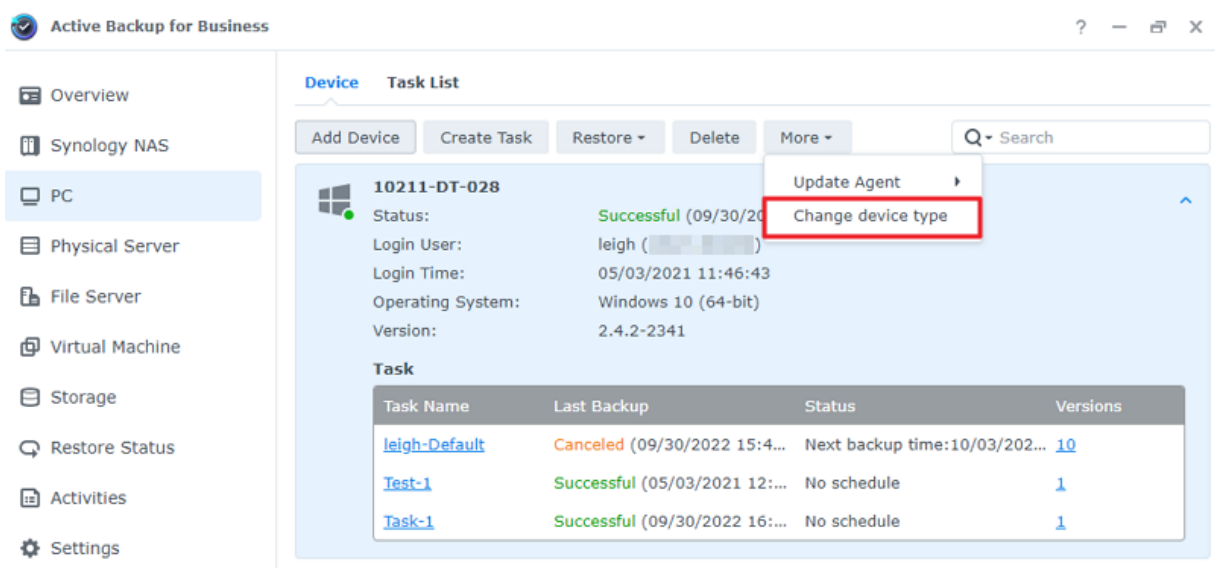
You can view the progress of the restoration by clicking the **Restore Task** icon in the upper right-hand corner.



## Restore servers to virtual machines

You can back up your **PC** as either a **PC** or a **physical server** in Active Backup for Business. Servers can be restored as virtual machines in **Virtual Machine Manager (VMM)**, **VMware vSphere**, or **Microsoft Hyper-V**. Use the following steps to restore your PC or server as a virtual machine using VMM.

1. If you backed up your computer as a **PC**, go to **Active Backup for Business > PC > Device** and click **More > Change device type** to change it into a physical server.



2. If the backup is already a physical server, go to **Physical Server**, select your device and click **Restore**.
3. Choose **Instant Restore to Synology Virtual Machine Manager (VMM)**, **Restore to VMware vSphere**, or **Restore to Microsoft Hyper-V**.
4. If you selected **Restore to VMware vSphere** or **Restore to Microsoft Hyper-V**, select **Instant Restore** or **Full Virtual Machine Restore**.
5. Select the desired restore point and follow the instructions in the wizard to complete the setup.

6. Upon completion, you should see the imported virtual machine on the **Virtual Machine** page in **Virtual Machine Manager**.

# Best Practices

The following sections provide recommendations on how you can protect your backup data against loss, ensure backup task continuity, and deploy the backup agent to many devices at once while keeping your Synology NAS 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 an entire infrastructure.

Natural disaster, theft, or network unavailability can prevent you from retrieving your data and 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.

It is 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 referred to as the [3-2-1 backup rule](#). Synology NAS includes software that allows you to easily 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 the 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 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.

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.

## Mass deployment in Windows environments

Active Backup for Business can be safely deployed to all Windows devices in an office. However, when implementing mass deployment, you may encounter the following challenges:

- **Installation:** Making sure that the correct version of **Active Backup for Business Agent** is installed on all of the source devices.
- **Setup:** Configuring all instances of the agent to back up to the same Synology NAS without making your sensitive account details available publicly.

### Mass deployment options

There are two methods for performing mass deployment when using **Active Backup for Business Agent**: Using a customized installer with a dedicated DSM account, and using a generic installer with domain accounts.

The method you should use depends on whether your Synology NAS is integrated with either LDAP or Active Directory Services, which will manage backups. It also depends on whether or not you want to grant end users full privileges for performing restorations.

### Customized installer using a dedicated DSM account (recommended)

We recommend you to set up a separate new DSM user account with limited permissions, exclusively for the group deployment of Active Backup for Business.

To set up the **Active Backup for Business Agent** on many computers without supplying login details via email or other means, you can pre-populate the Windows installer (.msi) file for the agent with the login details of a custom DSM account that you have created, or you can supply these details as part of a script.

Once you have successfully deployed the agent to all of the devices that you want to protect, you can then change the login details of your custom DSM account to secure your setup. By doing this, you can make sure that no one else can use the usernames or passwords visible in the installer file/script to access backup data on your NAS.

#### To create a custom DSM account:

1. Sign in to your DSM admin or administrators group account. Go to the **Package Center** and install **Active Backup for Business**.
2. Go to **Control Panel > User** and click **Create**. In the **User Creation Wizard**, under **User information**, enter a suitable username and a temporary password. This temporary password

will be distributed with the Microsoft installer and must not be used elsewhere. Click **Next** when done.

3. On the **Assign application permissions** page, tick **Allow** next to **Active Backup for Business** to grant this user access permissions to the package. Then, continue through the wizard to complete the setup.
4. You can now use this user account to deploy the agent to the devices that you want to protect.

## Generic installer using domain accounts

This method can be summarized in the following steps:

1. Create separate DSM accounts for each Microsoft Active Directory or LDAP end user.
2. Download a generic ABB Agent Microsoft installer file (.msi).
3. Use an **Active Directory Group Policy Object** or a **script** to distribute the installer to many PCs.
4. Let end users enter their own domain login details to conclude the setup.

### Notes:

- For a safe mass deployment of ABB, you must download and use the latest version of the **Active Backup for Business Agent**. In versions 2.0.3-0472 and below, DSM account login details cannot be changed remotely, which could present a security risk.
- If available, **Windows Active Directory** can also be used to install the **Active Backup for Business Agent** on a number of computers.
- Other methods to edit and distribute the agent to remote devices include using scripts and asking users to manually install the agent.
- Using a **Group Policy Object** in **Windows Server Manager** allows you to prepopulate the Windows installer for the agent with DSM login details.

## Prepare the Active Backup for Business Agent for mass deployment

Instead of entering the server address, username, and password and performing installation on each device, the **Active Backup for Business Agent installer** (.msi) can be pre-populated with the information in advance and installed on multiple devices at once.

Before deploying the installer to multiple computers, you can edit several properties. If you don't do this, you will have to enter them during installation on each client. Editing the installer is recommended if all clients are to share the same settings. These clients will share the same Synology NAS as the backup destination.

1. Download the .msi installer for the latest version of the **Active Backup for Business Agent** from the [Download Center](#).
2. Install **Microsoft Orca editor** or use your preferred MSI editor to edit the .msi installer file.
3. Follow the instructions in the [ABB mass deployment tutorial](#) to finish preparing the agent and to execute mass deployment with Group Policy.



# 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?](#)
- [How do I back up and relink Active Backup for Business data to a destination Synology NAS?](#)
- [How to set up Active Backup for Business Agent for mass deployment](#)
- [How do I back up and restore only Microsoft SQL Server using Active Backup for Business?](#)
- [How do I back up a full personal computer or server using Active Backup for Business?](#)
- [How do I back up Active Backup for Business data to another Synology NAS/Server/USB flash drive/cloud service?](#)
- [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](#).

# Appendix

## Permissions and security

### Active Backup for Business access and privileges

| ABB item           | Access and privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup storage     | <ul style="list-style-type: none"><li>• ABB stores data in shared folders on the DSM account where it is installed.</li><li>• Access from other accounts can be disabled.</li><li>• Backup folders can be encrypted to keep data secure.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Authentication     | <ul style="list-style-type: none"><li>• ABB uses the username and password of the DSM account where it is installed.</li><li>• Login details must be entered in the <b>Active Backup for Business Agent</b> on each source device separately.</li><li>• Changes to the DSM account password can only be configured on the server side.</li><li>• Changes to the DSM account password do not require the <b>Active Backup for Business Agent</b> on source devices to be reconfigured.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                             |
| Restore privileges | <p><b>PC backup:</b></p> <ul style="list-style-type: none"><li>• Privileges to perform restores cannot be configured.</li><li>• The DSM admin account, DSM admin group users, and the DSM account where ABB is installed can restore files, folders, and full devices or volumes using ABB in DSM, as well as files and folders using the <b>Active Backup for Business Portal</b>.</li></ul> <p><b>Physical Server backup:</b></p> <ul style="list-style-type: none"><li>• Privileges to perform restores can be configured or disabled for all types of DSM users and end users.</li><li>• DSM users can be assigned permissions to restore files, folders, and full devices or volumes using ABB in DSM.</li><li>• Both DSM users and end users can be assigned permissions to restore files and folders from Synology NAS using the <b>Active Backup for Business Portal</b>.</li></ul> |

|                 |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| Backup settings | Backup settings can only be configured on the server side by accounts that have access to Active Backup for Business in DSM. |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|

## Active Backup for Business Agent access and privileges

| ABB Agent item | Access and privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Install agent  | End users can install or remove the agent if they have sufficient domain privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Authentication | End users can edit the following login details during regular installation: <ul style="list-style-type: none"> <li>• Username of DSM account</li> <li>• Password of DSM account</li> <li>• IP address of Synology NAS</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Security       | <ul style="list-style-type: none"> <li>• End users can always view the following details: <ul style="list-style-type: none"> <li>◦ Username of DSM account</li> <li>◦ IP address of Synology NAS</li> </ul> </li> <li>• End users cannot change login details after installation.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Management     | <ul style="list-style-type: none"> <li>• End users cannot edit backup settings.</li> <li>• End users can change the server IP address at any time.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Recovery       | <p><b>PC backup:</b></p> <ul style="list-style-type: none"> <li>• Privileges for performing restorations cannot be configured.</li> <li>• The DSM admin account, DSM admin group users, and the DSM account where ABB is installed can restore files, folders, and full devices or volumes using ABB in DSM, as well as files and folders using the <b>Active Backup for Business Portal</b>.</li> </ul> <p><b>Physical Server backup:</b></p> <ul style="list-style-type: none"> <li>• Restore privileges can be configured or disabled for all types of DSM users and end users.</li> <li>• DSM users can be assigned permissions to restore files, folders, and full devices or volumes using ABB in DSM.</li> <li>• Both DSM users and end users can be assigned permissions to restore files and folders from Synology NAS using the <b>Active Backup for Business Portal</b>.</li> </ul> |