

Administrator's Guide for

Active Backup for Business

Windows PCs and Physical Servers



Based on

Active Backup for Business 2.2.0



Table of Contents

Introduction	01
Active Backup for Business	
Technical Overview	05
Application-aware backup	
Forever-incremental backup	
Data deduplication	
Native hypervisor	
Backup Configuration	08
Windows PC and Server Backup	
Create a backup task	
Manage backup tasks	
Restoration Guide	13
Recovery options	
Restore an entire device	
Recover individual files	
Restore servers to virtual machines	
Best Practices	18
Maintain remote backup copies and relink	
Mass deployment in Windows environments	
Learn more	22
Related articles	
Software specs	
Other resources	
Appendix	23
Permissions and security	



Introduction

Active Backup for Business

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

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

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

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

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

Requirements

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

NAS System requirements

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

Supported systems

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

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

Backup types

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

PC Backups

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

Physical Server Backups

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

File Server Backups

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

Virtual Machine Backups

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

Backup tools

Active Backup for Business Agent

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

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

Active Backup for Business Portal

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

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

Active Backup for Business Recovery Media Creator

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

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

Technical Overview

Application-aware backup

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

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

Forever-incremental backup

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

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

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

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

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

Personal computer and physical server

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

Virtual machine

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

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

Data deduplication

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

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

Native hypervisor

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

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

Backup Verification

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

Instant Restore

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

Backup Configuration

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

Windows PC and Server Backup

Active Backup for Business allows you to remotely conduct full backups of Microsoft Windows servers and PCs, including system volumes and configurations, with the help of **Synology Active Backup for Business Agent**.

Before you start

1. Install **Synology Active Backup for Business Agent** on the target device that you wish 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**.

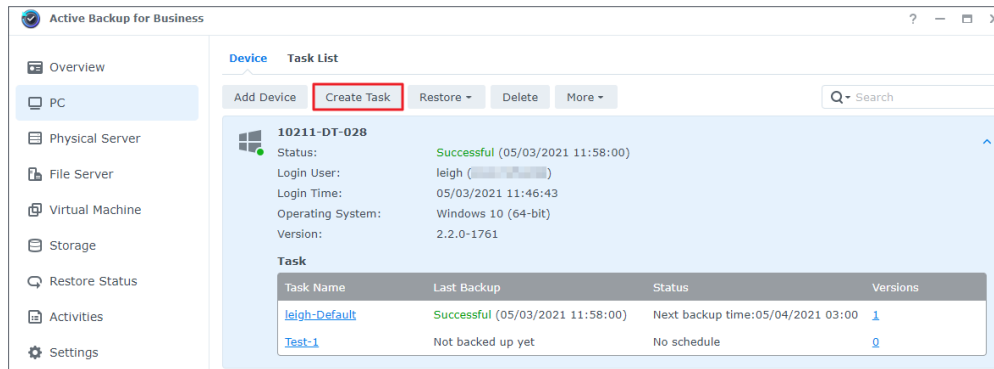
Notes:

- Active Backup for Business 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 backup versions of PCs using **Active Backup for Business Portal** or restore full PCs using recovery media. Privileges for performing **PC** restorations are not configurable.
- Admins, users belonging to the **administrators** group, and users with privileges can access physical server backups using the **Active Backup for Business Portal** or restore full devices using recovery media. Privileges for performing **physical server** restorations can be configured in backup templates.

Create a backup task

Once **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. More than one backup task can be created for each device.

1. To create a new task, 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

Users 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"** will have been automatically created when you installed Active Backup for Business on your NAS.
2. Select a shared folder in the Btrfs file system as the backup destination.

Task settings

- Users can enable data transfer compression, data transfer encryption, and **application-aware backup**.
- Compression and encryption can be enabled for the backup destination.
- When performing **physical server** backups, users can select **Backup Verification** to implement scheduled trial runs of the restoration, which will be performed in **Virtual Machine Manager**. The entire process will be recorded as a video for reference, so that users can confirm that the backup is able to be successfully restored.
- Users can customize pre/post scripts when performing **physical server** backups.

Notes:

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

Schedule backup tasks

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

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

Backup by event, available for PC backups, runs the task depending on your selection: whenever the screen is locked, when a user signs out, or when the system is started up. You can also specify a minimum time interval between backups.

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

Select a retention policy

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

You can choose to set rules for keeping backup versions, such as to retain the latest version of each day, week, month, or year. You can edit the retention policy at **Active Backup for Business > 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.

Backup Configuration

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

Set Rules ✕

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

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

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

Number of latest versions to keep versions

Cancel OK

Manage backup tasks

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

Edit or delete backup tasks

Users can edit tasks individually or several tasks simultaneously by going to **PC or Physical Server > Task List**, selecting one or several tasks (Ctrl + left click) and clicking **Edit**. The **Backup destination** cannot be changed. **Task settings** and **Source type** can be changed both individually and simultaneously, and 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				
	Time of creation	End Time	Backup Status	Verify backup Status
	04/26/2021 15:47:41	04/26/2021 16:11:44	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. Refer to [this article](#) for detailed instructions.
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 if 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 also 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 by using 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 into 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.

Notes:

- Recovery media must be created separately for each device configuration. Therefore, if two devices have different language or region settings, run different windows versions, or contain different drivers, you will have to 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 **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 wish to restore, you can use your recovery drive to boot the device into **Active Backup for Business Recovery Wizard**.

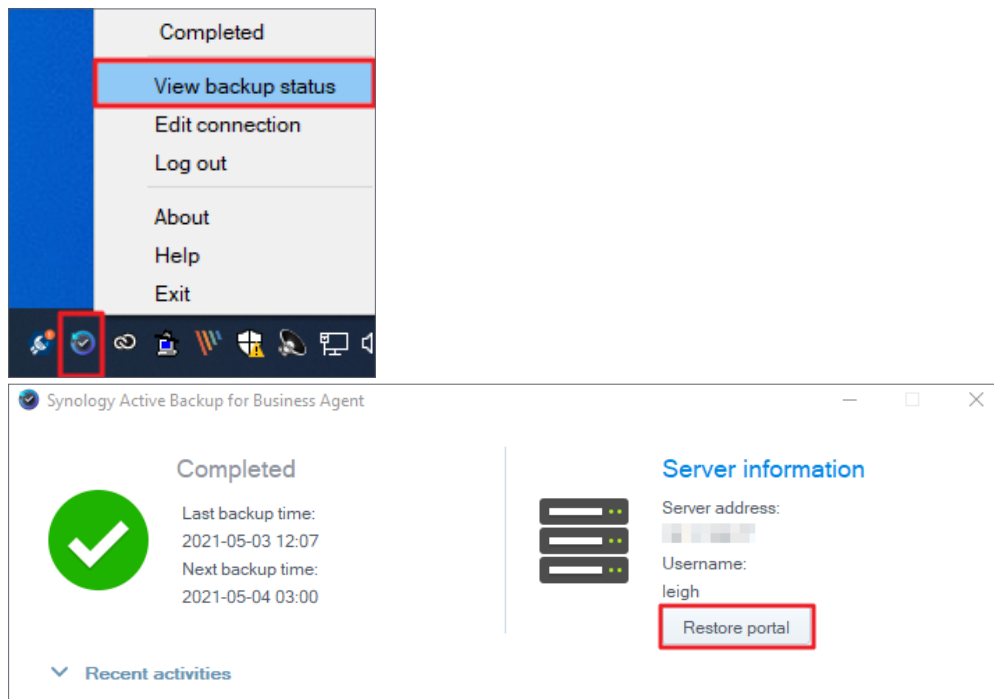
Step-by-step instructions on how to restore your full Windows device or volume using the wizard can be found in both [this article](#) and [this video](#).

Recover individual files

The restoring of individual files or folders 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 **Active Backup for Business Agent** on the endpoint device that you want to restore.

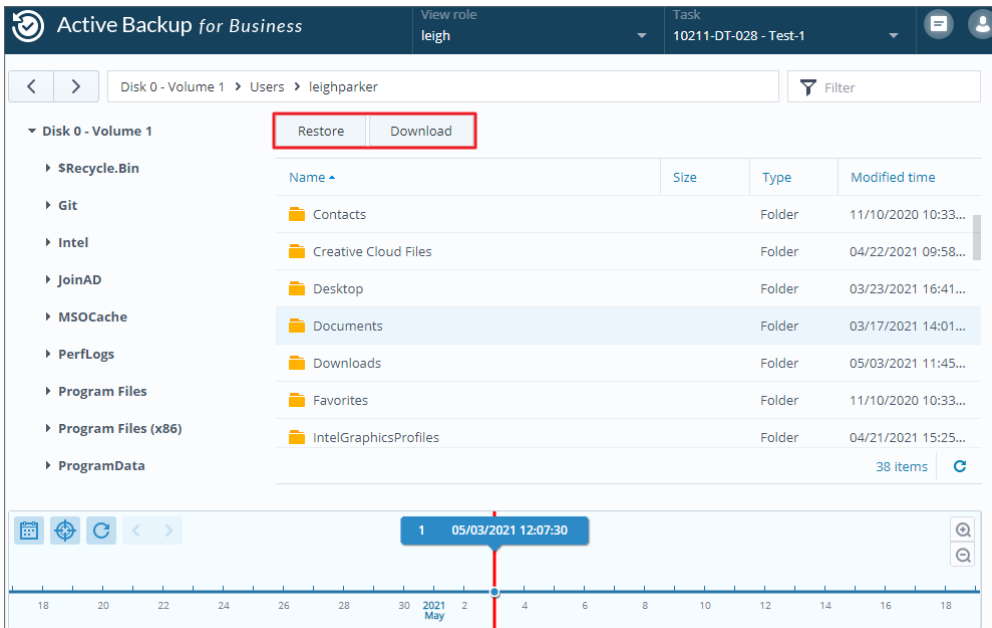
Restore files or folders from an endpoint device

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 details.
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 from which you wish to restore folders or files, then click through the folder structure in file explorer to select the directory or file.

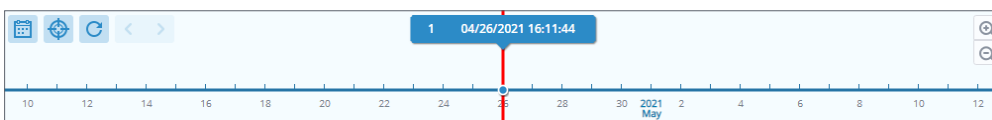
- Choose if you want to **Restore** or **Download** the data. If you select **Restore**, your backup agent will download the files or folders and restore them to their original location on your device. If you select **Download**, the selected files will be downloaded via your browser to your chosen download location.



Restore files or folders from DSM

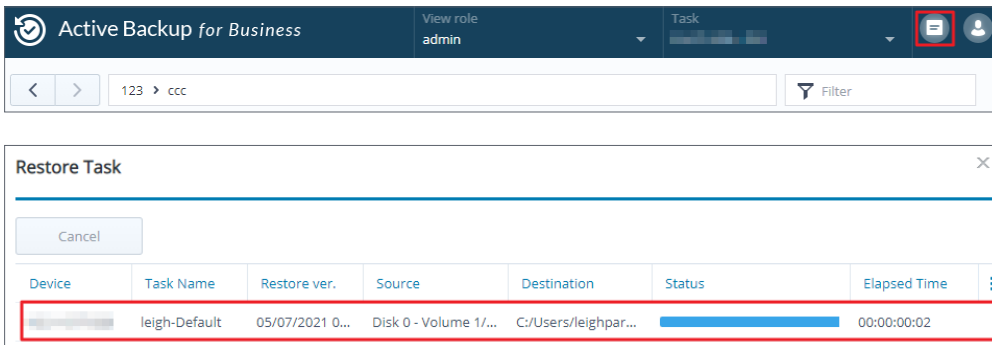
Administrators and accounts administrating Active Backup for Business can access the **Restore Portal** from any device. Follow the steps below to restore files to the original backup source device, or to download them via browser.

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



- 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 whether you want files with the same name to be skipped during the restoration by ticking the related checkbox. If you select **Download**, the selected files will be downloaded via your browser to your chosen download location.

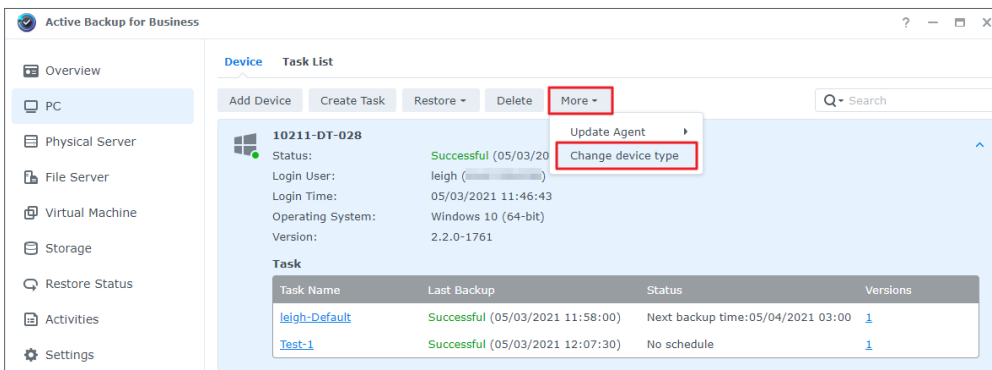
You can view the progress of the restoration by clicking the **Restore Task** icon in the upper right-hand corner.



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**. Follow the steps below 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 for how you can protect your backup data against loss, ensure backup task continuity, and deploy our backup agent to many devices at once while keeping your Synology NAS and DSM secure.

Maintain remote backup copies and relink

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

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

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

Create remote copies

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

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

Relink

After creating a replication or backup task, it is important to make sure that you know how to successfully restore or relink your existing Active Backup for Business tasks and backup data, whether they exist on a secondary NAS, in public clouds, or other storage media.

This tutorial provides detailed instructions on how to back up and relink your Active Backup for Business data using **Snapshot Replication** and **Hyper Backup**. To do this, make sure that your Synology NAS has 64-bit processors, is running DSM 6.1.7 or above, is running Active Backup for Business 2.0.4 or above, and have the necessary packages installed on your Synology NAS. See the **Environment** section in the tutorial for more details.

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**: Customized installer using a dedicated DSM account, and Generic installer using domain accounts.

The method you should use depends on if 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 that you set up a separate new DSM user account with limited permissions, exclusively for the group deployment of Active Backup for Business.

To set up 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 can use the usernames or passwords visible in the installer file/script to access backups on your NAS.

To create a custom DSM account:

1. Sign in to your DSM admin or administrators group account. Go to **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 safe mass deployment of ABB, you must download and use the latest version of 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 **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 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 on multiple computers, you can edit several properties. If not, 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. Also, these clients will share the same Synology NAS as the backup destination.

1. Download the .msi installer for the latest version of Active Backup for Business 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 [this article](#) 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 customize Active Backup for Business Agent installer 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 Windows PC 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"> • ABB stores data in shared folders in the DSM account on which it is installed. • Access via other accounts can be disabled. • Backup folders can be encrypted to keep data secure.
Authentication	<ul style="list-style-type: none"> • ABB uses the username and password of the DSM account on which it is installed. • Login details must be entered in Active Backup for Business Agent on each source device separately. • Changes to the DSM account password can only be configured on the server side. • Changes to the DSM account password do not require Active Backup for Business Agent on source devices to be reconfigured.
Restore privileges	<p>PC backup: Privileges to perform restores cannot be configured. The DSM admin account, DSM admin group users, and the DSM account on which ABB is installed can restore files, folders, and full devices or volumes using ABB in DSM, as well as files and folders using Active Backup for Business Portal.</p> <p>Physical Server backup: Privileges to perform restores can be configured or disabled for all types of DSM users and end users. DSM users can be assigned permissions to restore files, folders, and full devices or volumes using ABB in DSM. Both DSM users and end users can be assigned permissions to restore files and folders from Synology NAS using Active Backup for Business Portal.</p>
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	<ul style="list-style-type: none"> • End users can edit the following login details during regular installation: <ul style="list-style-type: none"> • Username of DSM account • Password of DSM account • IP address of Synology NAS
Security	<ul style="list-style-type: none"> • End users can always view the following details: <ul style="list-style-type: none"> • Username of DSM account • IP address of Synology NAS • End users cannot change login details after installation.
Management	<ul style="list-style-type: none"> • End users cannot edit backup settings. • End users can change the server IP address at any time.
Recovery	<p>PC backup: Privileges for performing restorations cannot be configured. The DSM admin account, DSM admin group users, and the DSM account on which ABB is installed can restore files, folders, and full devices or volumes using ABB in DSM, as well as files and folders using Active Backup for Business Portal.</p> <p>Physical Server backup: Restore privileges can be configured or disabled for all types of DSM users and end users. DSM users can be assigned permission to restore files, folders, and full devices or volumes using ABB in DSM. Both DSM users and end users can be assigned permission to restore files and folders from Synology NAS using Active Backup for Business Portal.</p>



**SYNOLOGY
INC.**

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

**SYNOLOGY
AMERICA CORP.**

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

**SYNOLOGY
UK LTD.**

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

**SYNOLOGY
FRANCE**

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

**SYNOLOGY
GMBH**

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

**SYNOLOGY
SHANGHAI**

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

**SYNOLOGY
JAPAN CO., LTD.**

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

Synology®



synology.com

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