

# Acronis



## Acronis Cyber Backup 12.5

**EVALUATION GUIDE**

## Table of contents

<b>1</b>	<b>Introduction .....</b>	<b>3</b>
<b>2</b>	<b>What's new in Acronis Cyber Backup 12.5.....</b>	<b>3</b>
<b>3</b>	<b>Getting Acronis Cyber Backup 12.5 .....</b>	<b>4</b>
<b>4</b>	<b>Preparation and requirements .....</b>	<b>5</b>
4.1	Installation .....	5
4.1.1	Installing the management server .....	6
<b>5</b>	<b>Evaluation scenarios .....</b>	<b>9</b>
5.1	Backup console views .....	9
5.2	Backup of entire machine and granular file recovery .....	10
5.3	Application-aware backup and SQL database recovery .....	14
5.4	Virtual machine backup and recovery .....	18
5.5	Acronis Instant Restore.....	23
5.6	Using the Dashboard .....	25
5.7	Group management.....	27
5.8	Acronis Active Protection .....	31
5.9	Off-host replication of backups to cloud storage .....	33
5.10	Off-host validation of backups by calculating checksum and Instant Restore .....	37
5.11	Tape management .....	42
5.12	Reporting .....	45
<b>6</b>	<b>Disclaimer.....</b>	<b>47</b>

# 1 Introduction

We are happy to introduce Acronis Cyber Backup 12.5 – the solution that protects your entire business, backing up data on-premise, in remote systems, and in private and public clouds.

This document will help you evaluate Acronis Cyber Backup 12.5 and see how it can protect your business-critical systems from data loss and disasters.

## Intended audience

For testing Acronis Cyber Backup 12.5, it is expected that the reader:

- Knows basic principles, processes, and terminology of backup solutions.
- Possesses necessary experience and knowledge in installing and managing backup software.
- Is capable of using virtual machines (VM).

## Precautions

- Acronis Cyber Backup 12.5 is not designed to be installed along with any Acronis software, such as Acronis Backup, Acronis Backup Service, Acronis Backup Cloud, or Acronis True Image.
- Do not test Acronis Cyber Backup 12.5 on your production servers, desktops, or work laptops right away. Testing in a controlled environment will allow you to evaluate the software without taking any unnecessary risks.

## Evaluation

Acronis Cyber Backup 12.5 supports a wide range of data protection scenarios. Feel free to perform any scenario, test any available feature and option. In this document, you can find sample scenarios that will give you a quick overview of what the product is capable of.

## Support

If you face any issues during your evaluation, there are multiple ways for you to find help:

- Check out Acronis Cyber Backup 12.5 Online Help: <http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html>
- Find the solution in the Acronis Knowledge Base: <http://kb.acronis.com/>
- Contact Acronis Support: <https://www.acronis.com/support/>

## References

Latest updates and release notes: <https://www.acronis.com/support/updates/>

Datasheet: <https://www.acronis.com/resource-center/resource/acronis-backup-datasheet>

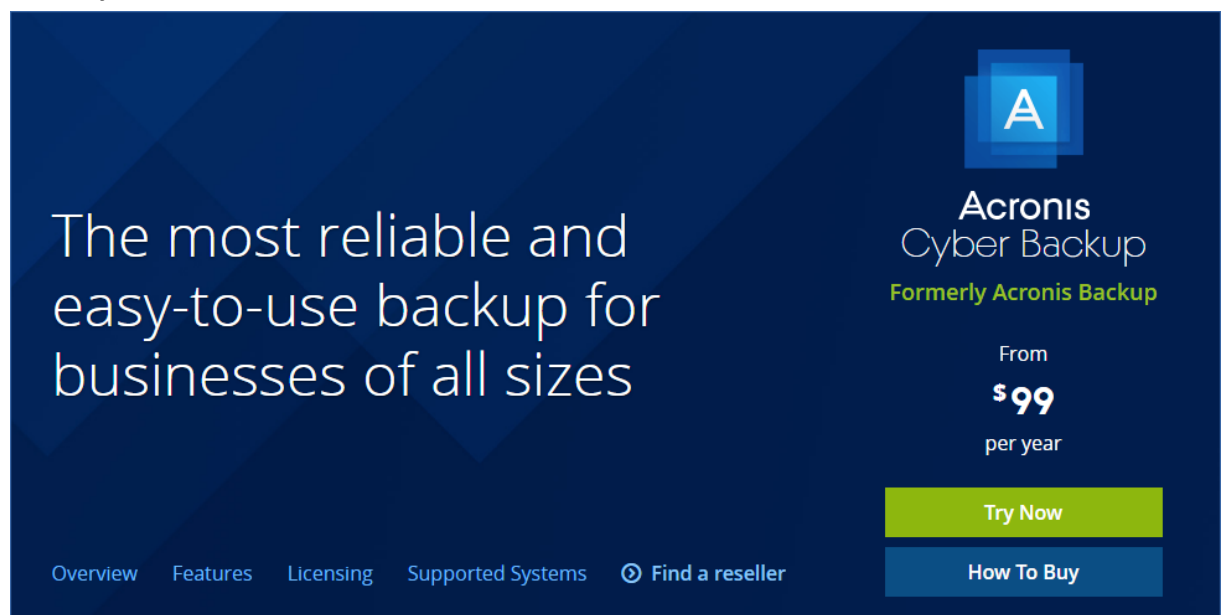
# 2 What's new in Acronis Cyber Backup 12.5

- Unique! **Acronis Active Protection** to proactively detect and protect systems from ransomware attacks.
- **Centralized backup policies, static and dynamic groupings, and the ability to manage, delegate, and establish roles for multiple administrators** — all to support larger environments and greater volumes of data.

- **Customizable dashboards and advanced reporting** for quick insights into your entire IT infrastructure.
- Unique! Backup of **XenServer, Linux KVM, Red Hat Enterprise Virtualization, and Oracle VM Server** for complete protection of any virtual environment.
- Support for **tape drives, autoloaders, and tape libraries** for off-site storage to ensure compliance with company regulations.
- **Off-host backup management operations**, including staging (moving), replication (copying), validation, and retention (cleanup) of backups.
- **Unified, web-based**, touch-friendly, centralized management console to reduce management complexity.
- Unique! Protection for **VMware vSphere ESX(i)** and **Microsoft Hyper-V hosts** and VMs for complete protection of any virtual workload.
- **VMware VM replication with WAN optimization** for faster disaster recovery.
- Unique! **Acronis Instant Restore** (Run Backup as a VM) and **vmFlashback** for VMware & Hyper-V to reduce recovery time objectives (RTOs).
- **SAN storage snapshots** support for VMware backups to reduce ESXi resource utilization.
- **Remote and automated** bootable media for significant reduction of the RTO of remote systems and data centers.

### 3 Getting Acronis Cyber Backup 12.5

1. Go to the Acronis Cyber Backup 12.5 web page: <https://www.acronis.com/business/backup>
2. Click **Try now**.



3. Do one of the following:
  - If you have an Acronis account, click **Log in here**, specify your user name and password, and then click **Login**.
  - If you do not have an Acronis account, fill in the registration form, and then click **Register**. You will receive an email message that contains your Acronis account user name and password.
4. As a result, you will see the web page where you can download the installation files.

## 4 Preparation and requirements

The evaluation implies that all Acronis Cyber Backup 12.5 components, including the management server, are installed locally in your environment (test lab). Therefore, there is no requirement for an Internet connection, although it is recommended.

### Management Server

To install Acronis Cyber Backup Management Server, we recommend a physical or virtual machine running Windows Server 2008 or later. Operating systems starting with Windows 7 are also supported.

- The machine must have minimum 4 GB of RAM and 5 GB of free space on the system volume.
- Other Acronis software must not be installed on this machine.
- You can use various virtualization software to run the virtual machine: VMware, Virtual PC, and so on. In Windows 8.x or 10 Enterprise, you can enable the Hyper-V role and use a Hyper-V virtual machine for testing.

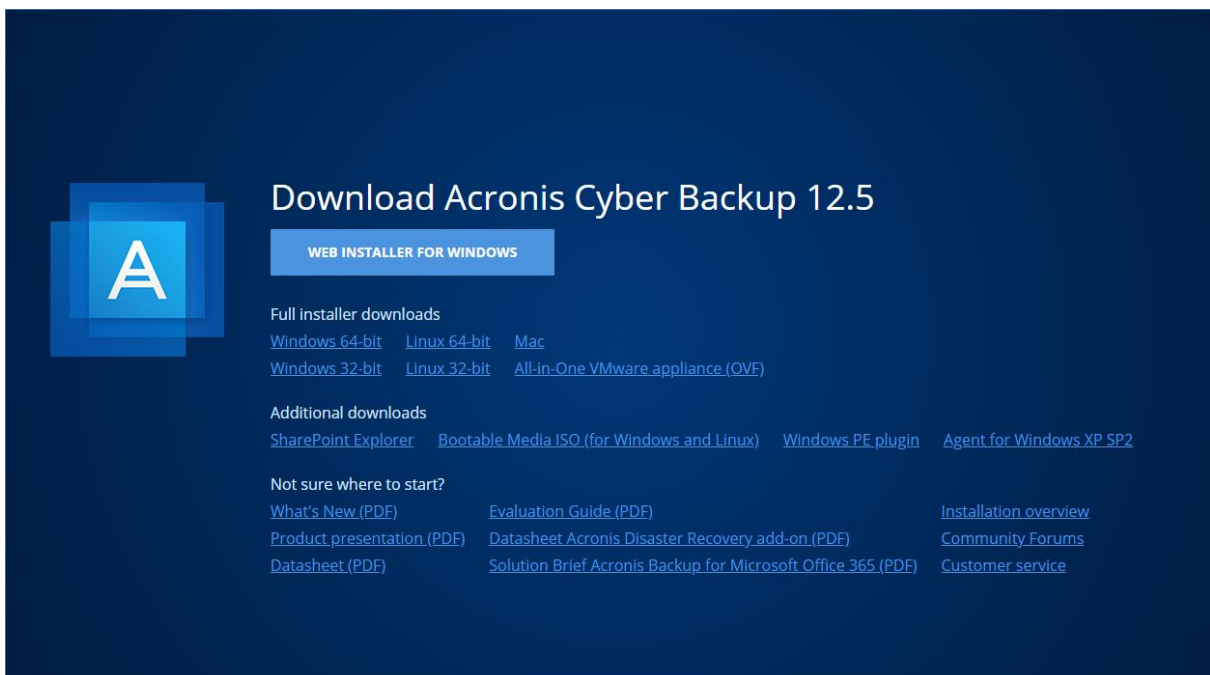
### Backup location

To store backups, we recommend a network shared folder with at least 30 GB of free space.

- Share this folder for read/write for **Everyone** by using Windows file sharing (the SMB protocol).
- Ensure that this folder can be accessed from the machines that you will back up.

## 4.1 Installation

Click **Web installer for Windows** or **Windows 64-bit** to download the setup program that contains the management server.



**Download Acronis Cyber Backup 12.5**

**WEB INSTALLER FOR WINDOWS**

**Full installer downloads**

[Windows 64-bit](#) [Linux 64-bit](#) [Mac](#)  
[Windows 32-bit](#) [Linux 32-bit](#) [All-in-One VMware appliance \(OVF\)](#)

**Additional downloads**

[SharePoint Explorer](#) [Bootable Media ISO \(for Windows and Linux\)](#) [Windows PE plugin](#) [Agent for Windows XP SP2](#)

**Not sure where to start?**

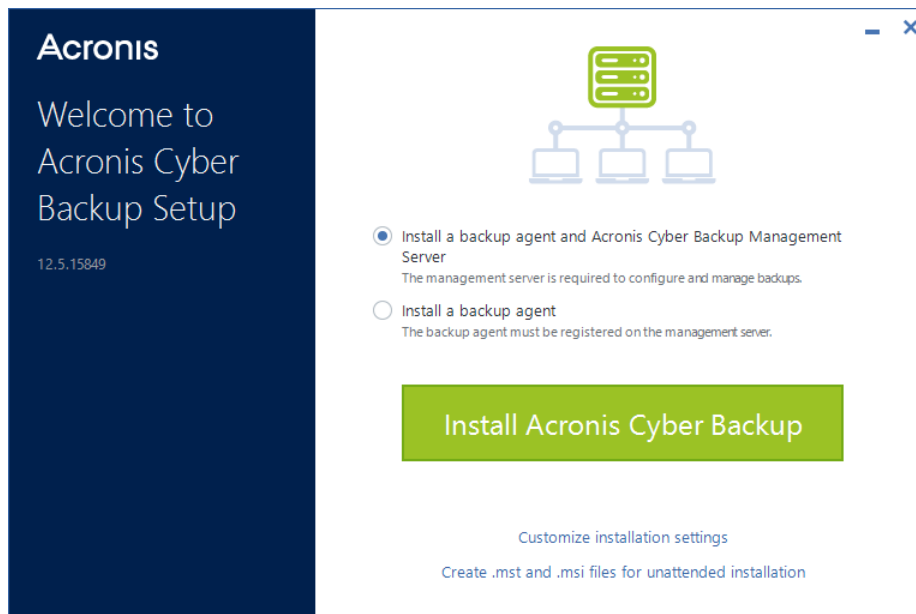
[What's New \(PDF\)](#) [Evaluation Guide \(PDF\)](#) [Installation overview](#)  
[Product presentation \(PDF\)](#) [Datasheet Acronis Disaster Recovery add-on \(PDF\)](#) [Community Forums](#)  
[Datasheet \(PDF\)](#) [Solution Brief Acronis Backup for Microsoft Office 365 \(PDF\)](#) [Customer service](#)

### 4.1.1 Installing the management server

*In this step, you will install the management server. Also, you will start the trial period for the software, so that you can use the fully functional product, without entering license keys.*

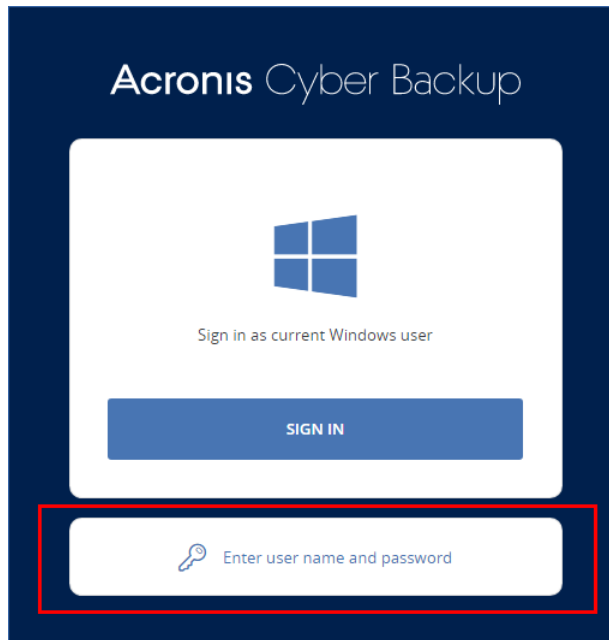
The management server is a central point for managing your backups. Backups are performed by agents, which need to be installed on each machine that you want to back up.

1. Log on as an administrator and start the Acronis Cyber Backup setup program.
2. [Optional] To change the language the setup program is displayed in, click **Setup language**.
3. Accept the terms of the license agreement and select whether the machine will participate in the 7.7 Customer Experience Program (CEP).
4. Leave the default setting **Install a backup agent and Acronis Cyber Backup Management Server**.



5. Click **Install Acronis Cyber Backup** to proceed with the installation.
6. After the installation completes, click **Close**. The backup console will open in your default web browser.

7. Click **Enter user name and password**.

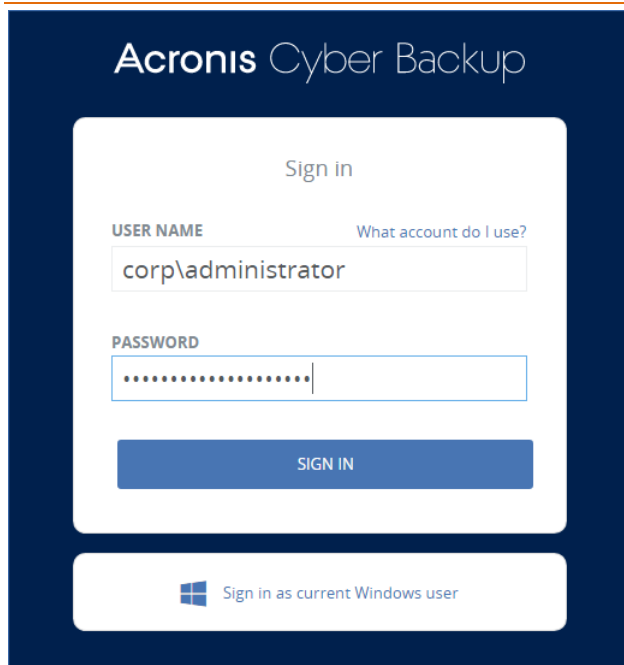


8. Enter the user name and password, and then click **Sign in**. Use a local or domain account with administrative privileges on the machine where the management server is installed.

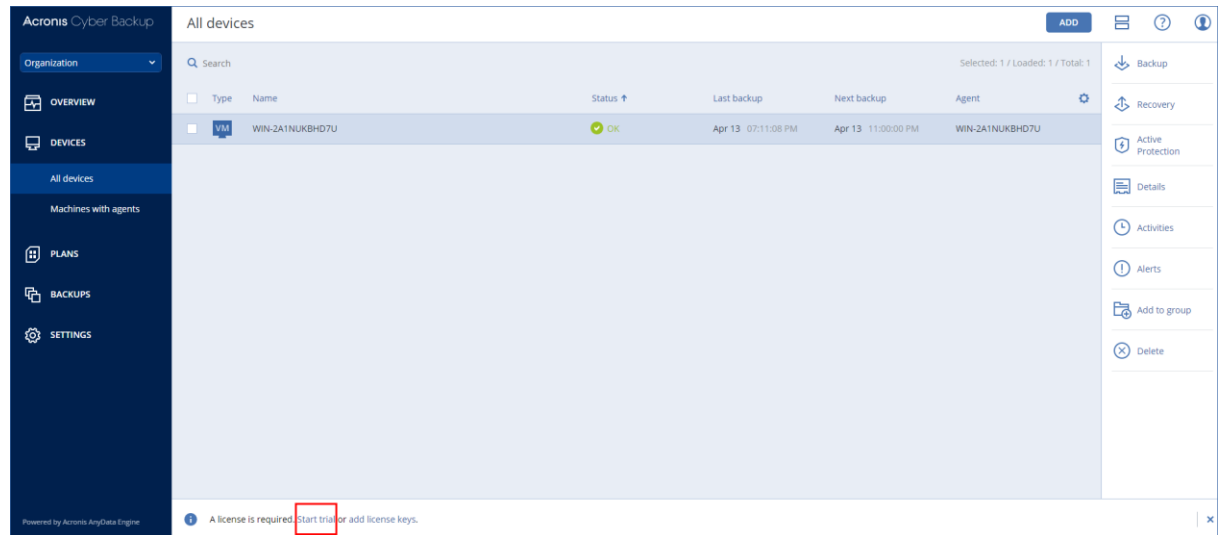
---

**Important** Please remember that you are logging in to the system deployed on your premises. Do not try to use your Acronis account to log in!

---



9. Click **Devices**, and then click **Start trial**.



10. Do one of the following:

- If the machine is connected to the Internet, specify your Acronis account, and then click **Sign in**.
- If the machine is not connected to the Internet, click **Start the trial without activation**.

×

Start trial

Please sign in to your Acronis account to get:

✓

Fully-functional product for the 30-day trial period

✓

Free 30-day cloud backup subscription

✓

Free technical support

Enter email and password for your Acronis account

john.smith@mail.com

.....

SIGN IN

Forgot password?

Create account

Done

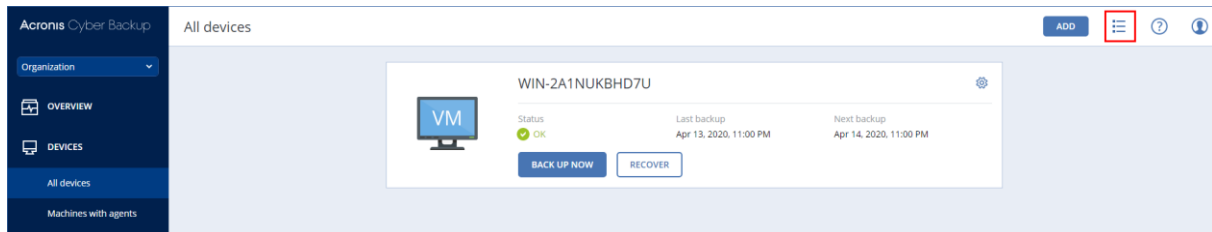


## 5 Evaluation scenarios

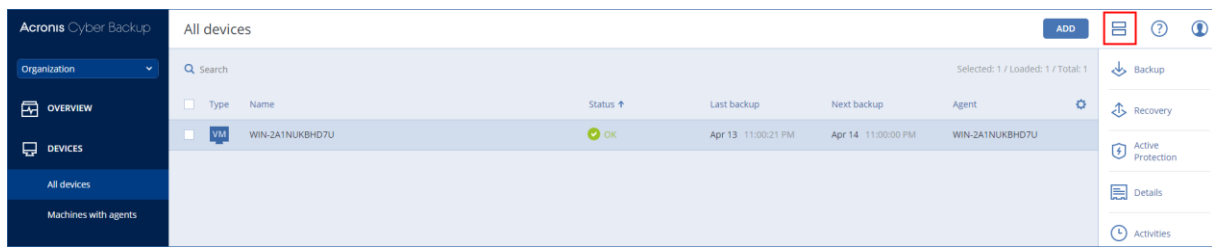
### 5.1 Backup console views

The backup console has two views: a tile view and a table view. To switch between the views, click the corresponding icon in the top right corner.

The tile view supports a small number of machines.



The table view is enabled automatically when the number of machines becomes large.



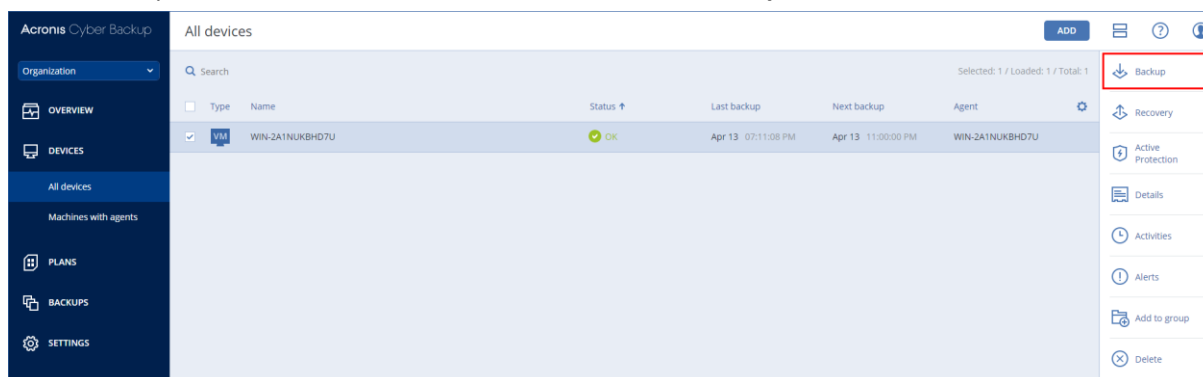
Both views provide access to the same features and operations. This document describes access to operations from the table view.

## 5.2 Backup of entire machine and granular file recovery

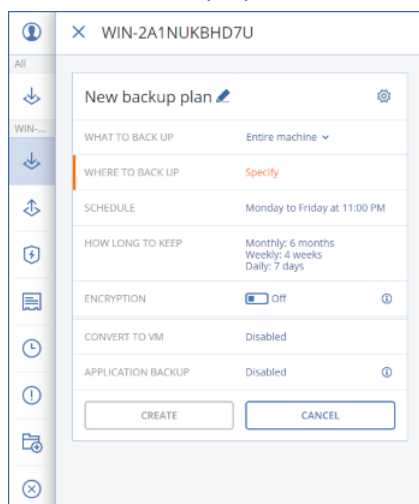
*In this scenario, you will back up the entire machine with the management server to a network share and recover a file from this backup. Using a similar procedure, you can recover volumes, disks, or the entire machine.*

### To back up the machine

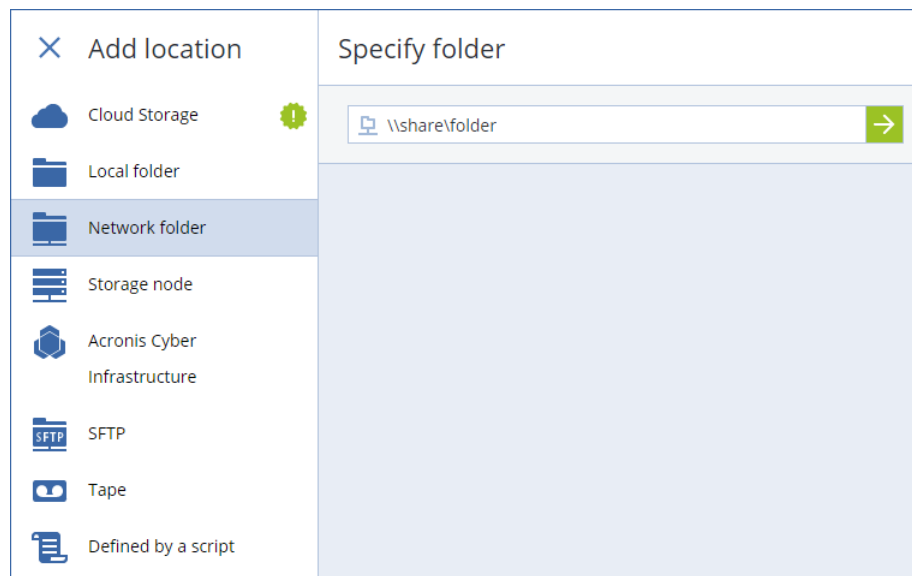
1. In the backup console, select the machine, and then click **Backup**.



The software displays a new backup plan template.

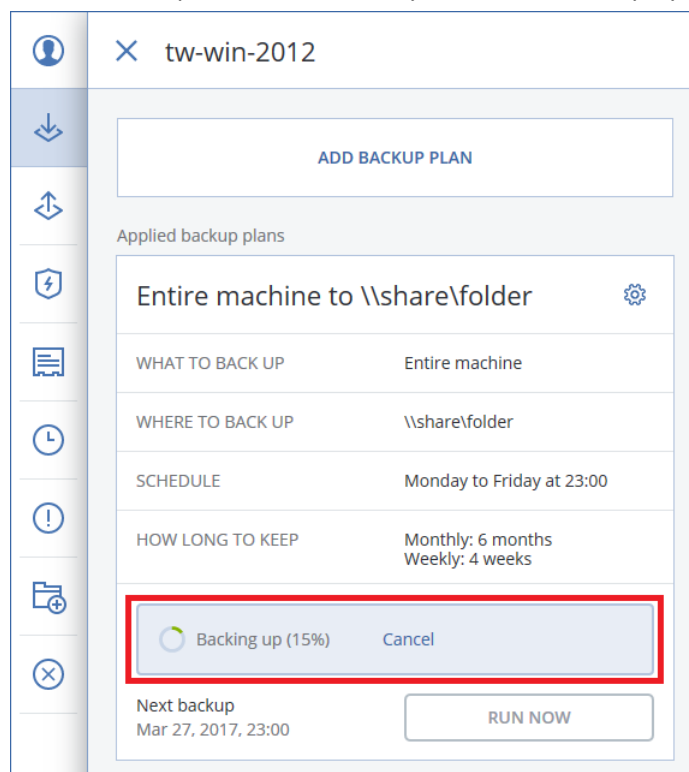


- Click **Where to backup > Network folder**, and then browse to the shared folder you created earlier or enter its path. If prompted, specify the user name and password for the shared folder. Click **Add**.



- On the backup plan panel, click **Create**.
- Click **Run now**.

The full backup starts immediately. The software displays the backup progress.



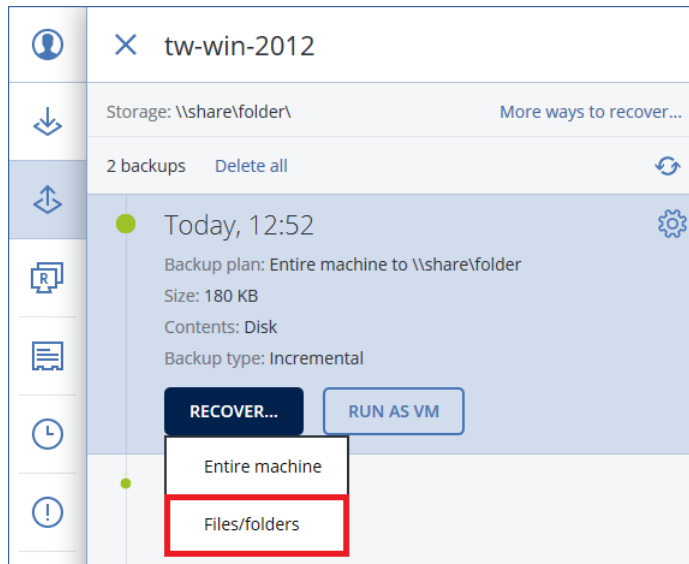
- Wait until the backup is complete.
  - Click the down arrow next to **Run now**, and then click **Incremental**.
- The incremental backup starts immediately.

To learn more about backup, refer to:

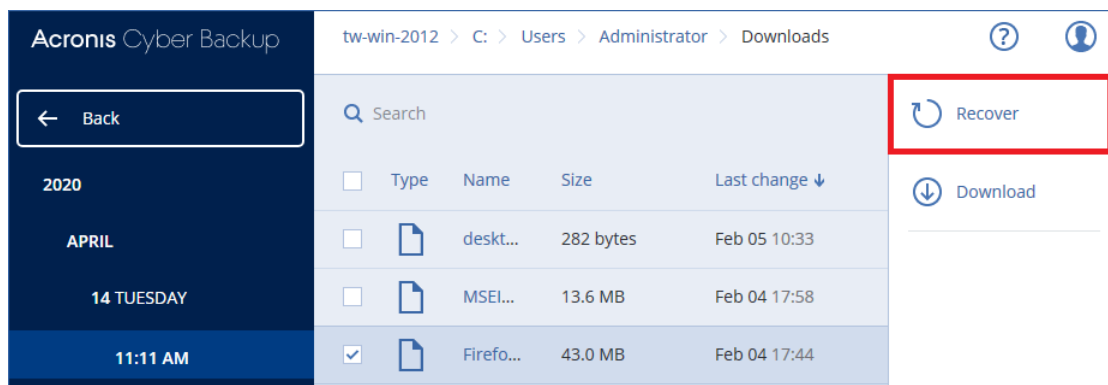
<http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html#38164.html>.

## To recover a file from a backup

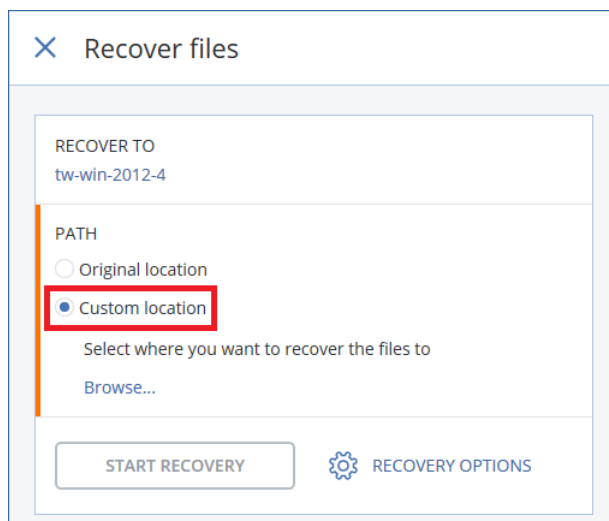
1. In the backup console, select your machine, and then click **Recovery**.
2. Select the recovery point, and then click **Recover > Files/folders**.



3. Browse to the required file or use search to locate it. You can use one or more wildcard characters (\* and ?).
4. Select the file that you want to recover.
5. Click **Recover**.



6. In **Path**, select **Custom location**.



7. Click **Browse**, and then specify a destination for the recovered files.
8. Click **Start recovery**.
9. Select one of the file overwriting options:
  - **Overwrite existing files**
  - **Overwrite an existing file if it is older**
  - **Do not overwrite existing files**
10. Click **Proceed** to start the recovery.

The recovery progress is shown on the **Activities** tab.

---

*To learn more about recovery, refer to:*

<http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html#36648.html>.

---

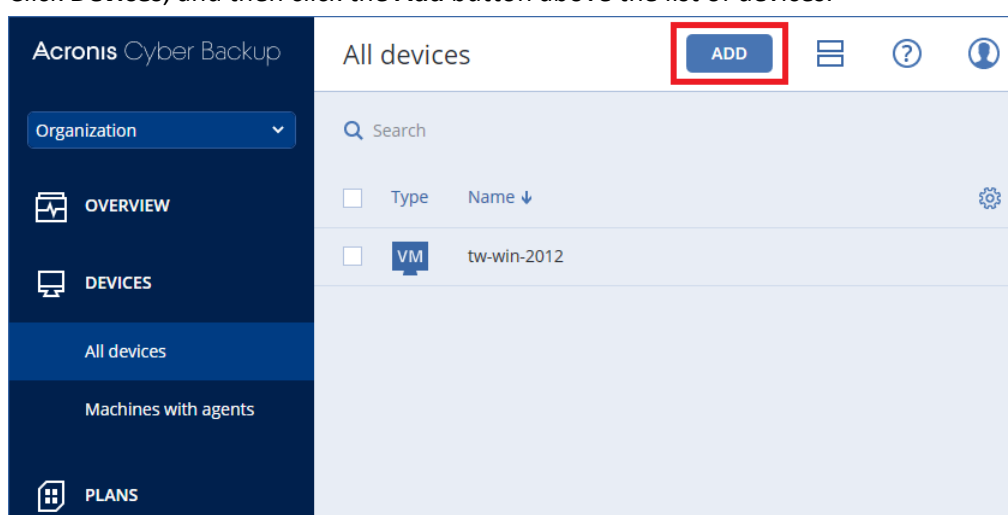
## 5.3 Application-aware backup and SQL database recovery

*In this scenario, you will install Agent for Windows and Agent for SQL, back up the entire machine with application-aware backup, and recover a database from this backup to a local folder.*

Application-aware backup is a disk-level backup that also collects the application metadata. This metadata enables browsing and recovery of the application data without recovering the entire disk or volume. The disk or volume can also be recovered as a whole.

### To install Agent for Windows and Agent for SQL

1. Ensure that the prerequisites for application-aware backups are met. Refer to: <http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html#36264.html>.
2. Click **Devices**, and then click the **Add** button above the list of devices.



3. Click **Microsoft SQL Server**.
4. Specify the host name or IP address of the machine where Microsoft SQL Server is installed and the credentials of an account with administrative privileges on that machine.

The screenshot shows a dialog box titled 'Add Microsoft SQL Server'. It contains a text input field for the host name, currently showing 'sql.company.com', and a 'Browse' button next to it. Below this is a text input field for the username, showing 'corp\admin', and a password field represented by dots. At the bottom of the dialog is a large blue 'ADD' button.

5. Click **Add**.  
The agents will be silently deployed to the selected machine. The machine will appear under **Devices** on the **Microsoft SQL** tab.

---

*If you have problems with the installation, refer to the preparatory steps described at: <http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html#36533.html>.*

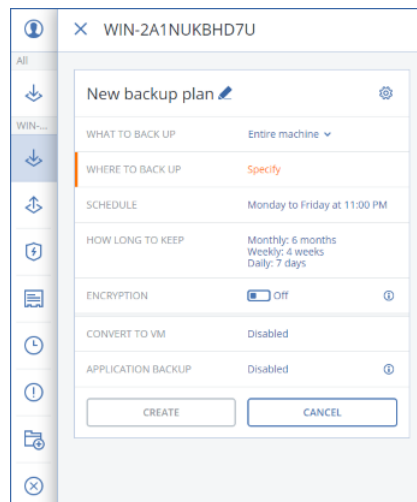
---

### To back up the machine

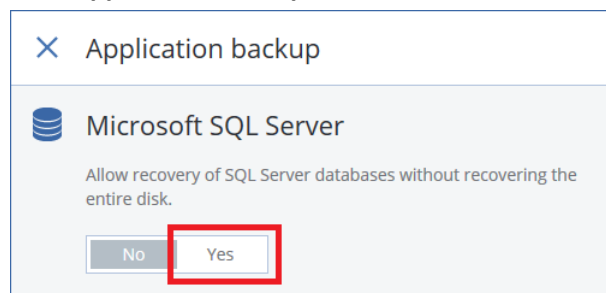
1. Click **All machines**, and then select the machine where Microsoft SQL Server is installed.

2. Click **Backup**.

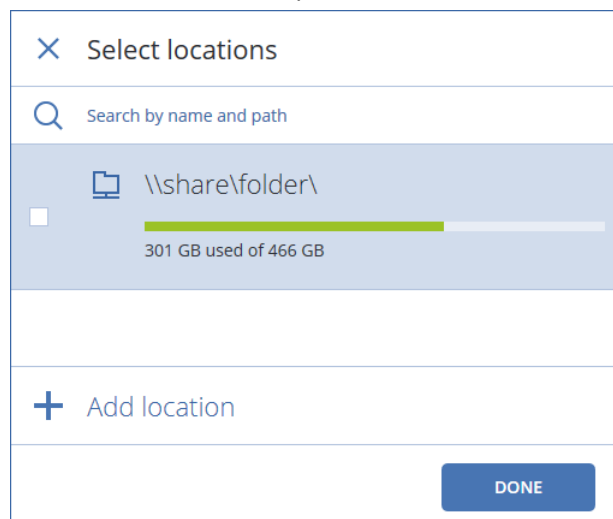
The software displays a new backup plan template.



3. Click **Application backup**, and then click **Yes** under **Microsoft SQL Server**.



4. If prompted, specify the credentials of a domain account with administrative privileges on the machine where Microsoft SQL Server is installed.
5. Click **Where to backup**, and then do one of the following:
  - Select the shared folder you created earlier, and then click **Done**.
  - To add a new backup location, click **Add location**.



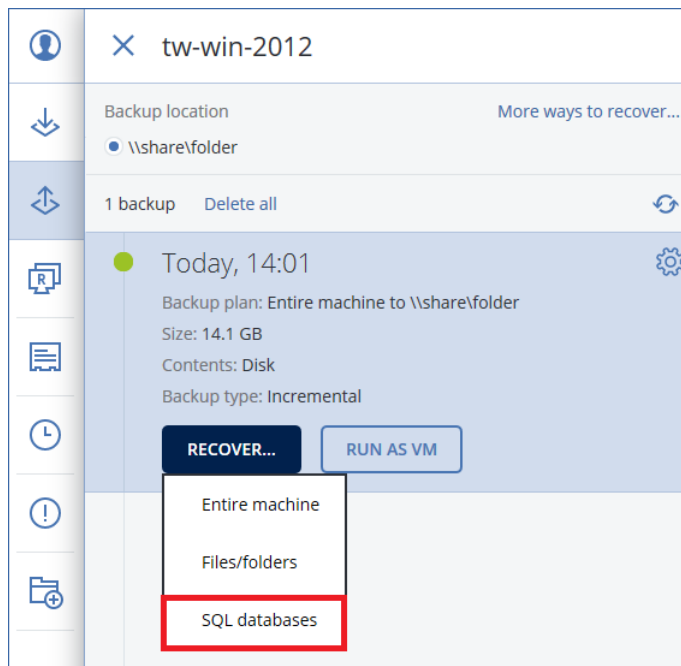
6. On the backup plan panel, click **Create**.
7. Click **Run now**.

The backup starts immediately. The backup progress is shown on the **Activities** tab.
8. Wait until the backup is complete.

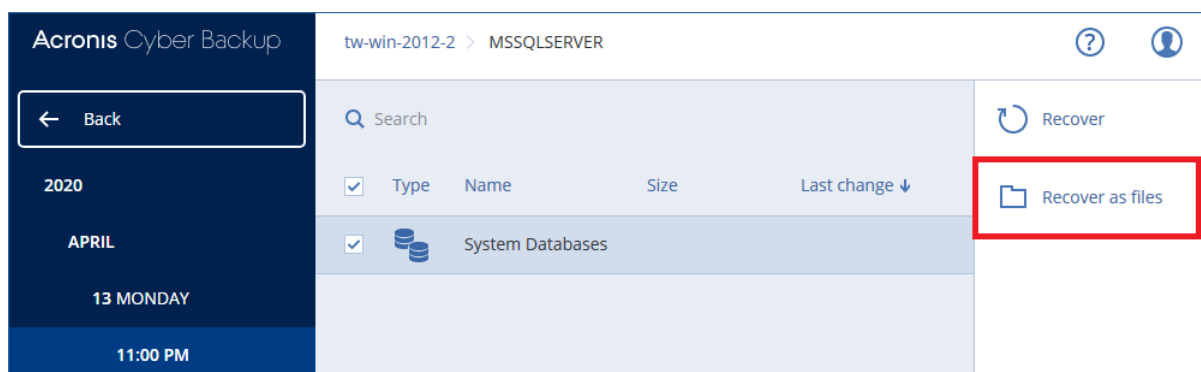
To learn more about application-aware backup, refer to:  
<http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html#35509.html>.

## To recover a database from the backup

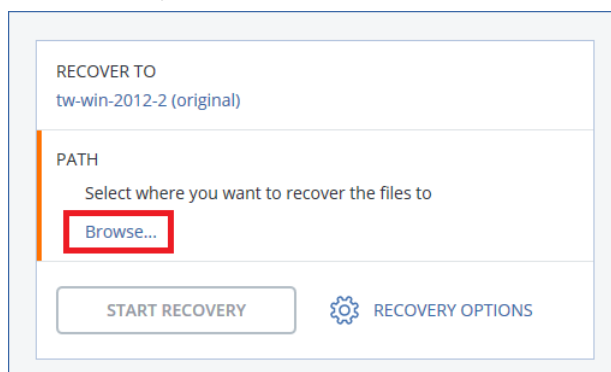
1. Select the machine that you backed up, and then click **Recovery**.
2. Select the recovery point, and then click **Recover > SQL databases**.



3. Select the data that you want to recover. Double-click an instance to view the databases it contains.
4. Click **Recover as files**.



5. Click **Browse**, select a local folder to save the files to, and then click **Done**.





6. Click **Start recovery**.

The recovery progress is shown on the **Activities** tab.

---

*To learn more about recovery of SQL databases, refer to:*

<http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html#33592.html>.

---

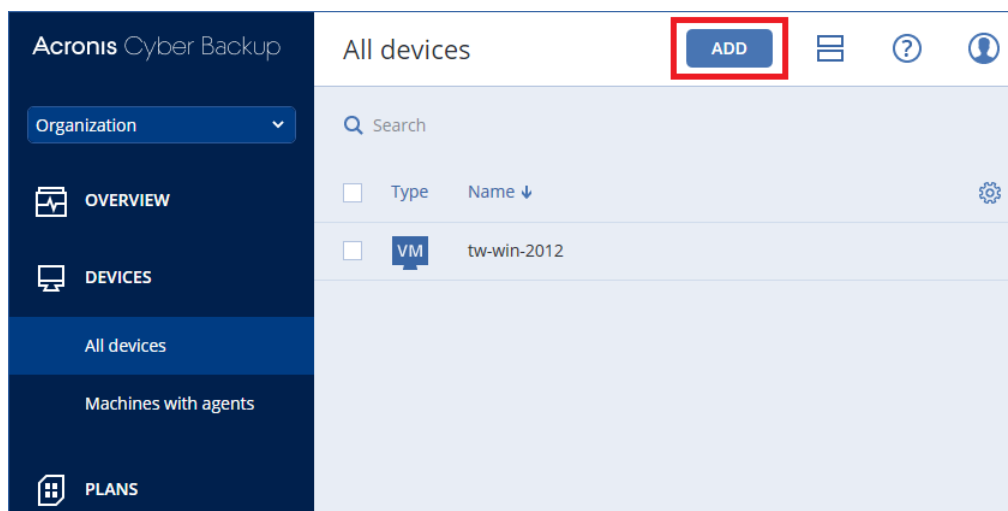
## 5.4 Virtual machine backup and recovery

*In this scenario, you will install Agent for Hyper-V, back up a Hyper-V virtual machine, and recover it to a new virtual machine.*

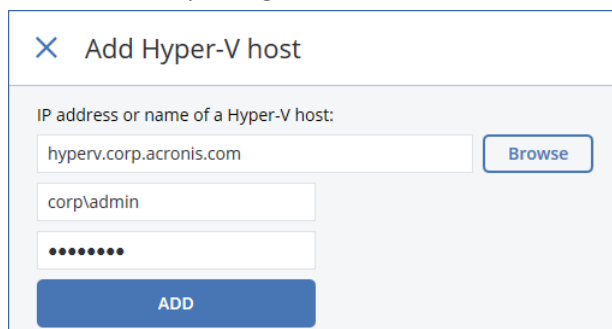
If you have a VMware ESXi environment, you can perform similar steps for VMware ESXi virtual machines.

### To install Agent for Hyper-V

1. Click **Devices**, and then click the **Add** button above the list of devices.

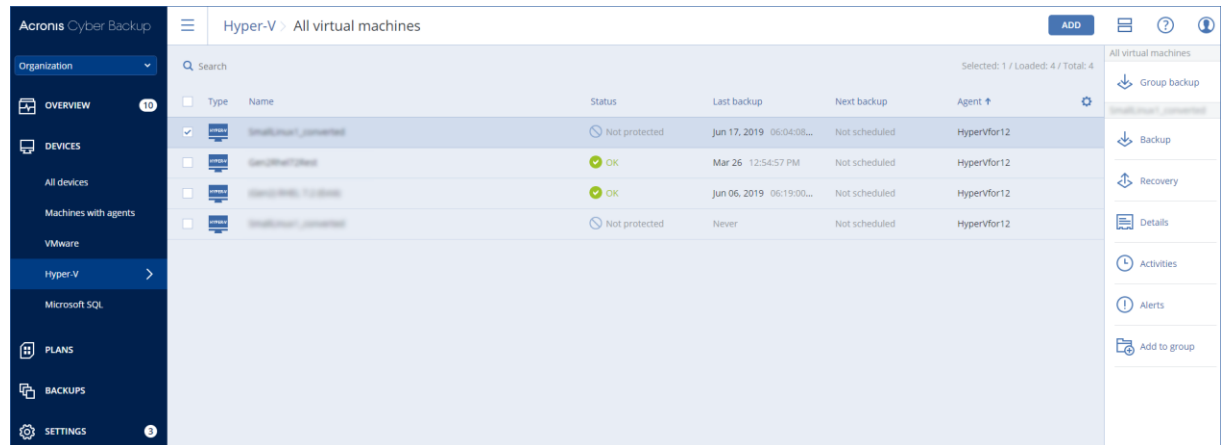


2. Click **Hyper-V**.
3. Specify the host name or IP address of the Hyper-V host and the credentials of an account with administrative privileges on the machine.

The screenshot shows a dialog box titled 'Add Hyper-V host'. It contains three input fields: 'IP address or name of a Hyper-V host:' with the value 'hyperv.corp.acronis.com', a 'Browse' button, a field for 'corpadmin', and a password field represented by dots. At the bottom is a large blue 'ADD' button.

4. Click **Add**.

The agent will be silently deployed to the selected machine. The virtual machines will appear under **Devices** on the **Hyper-V** tab.

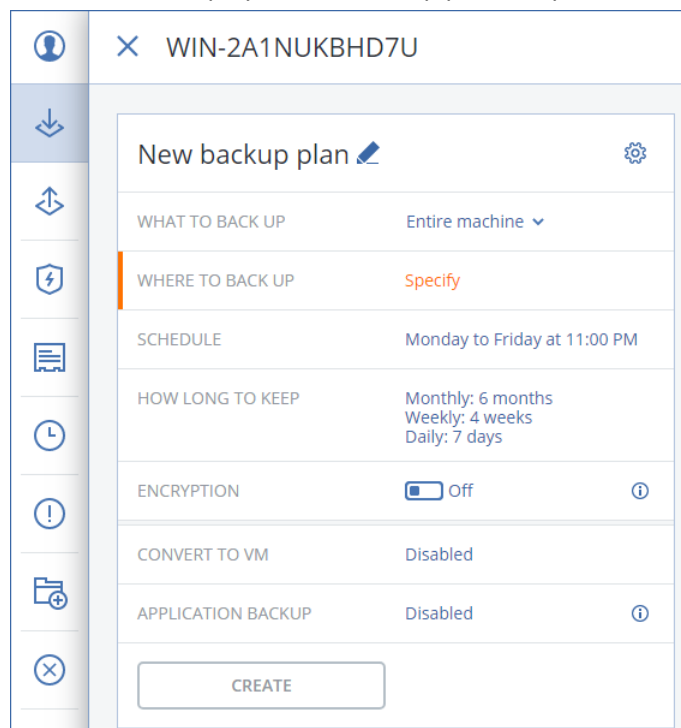


If you have problems with the installation, refer to the preparatory steps described at:  
<http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html#36533.html>.

## To back up a Hyper-V virtual machine

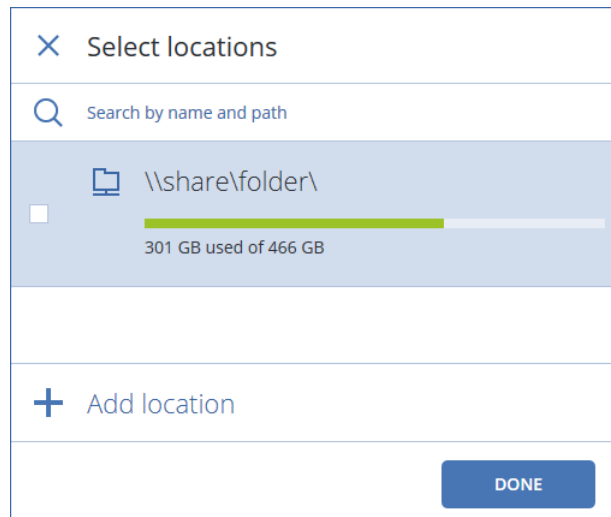
1. Select the virtual machine that you want to back up.
2. Click **Backup**.

The software displays a new backup plan template.



3. Click **Where to backup**, and then do one of the following:
  - Select the shared folder you created earlier, and then click **Done**.

- To add a new backup location, click **Add location**.



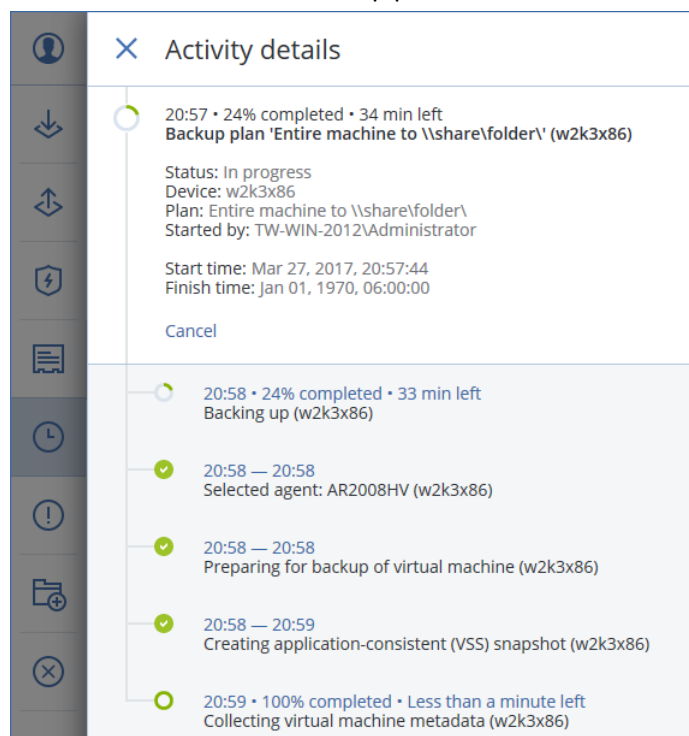
4. On the backup plan panel, click **Create**.

5. Click **Run now**.

The backup starts immediately.

6. Click **Activities**.

The software shows the backup process details.

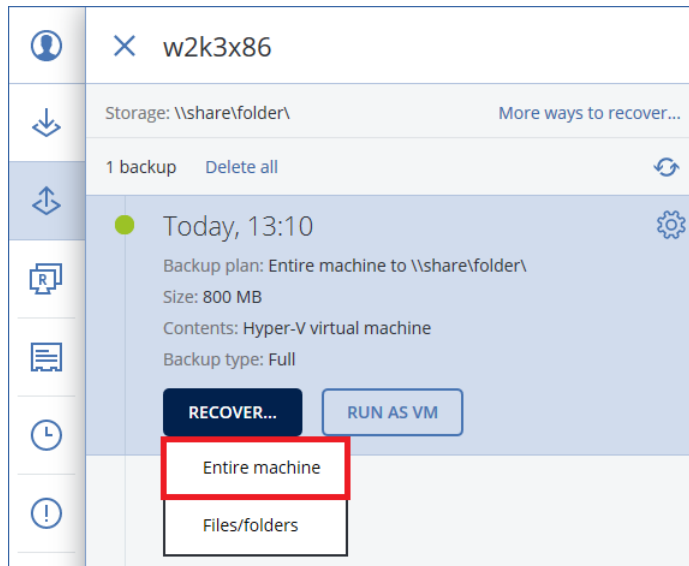


7. Wait until the backup is complete.

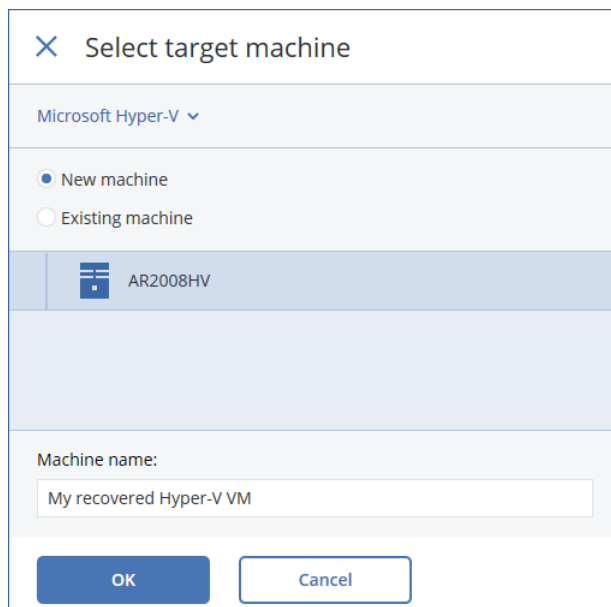
## To recover a virtual machine

1. Select the virtual machine that you backed up, and then click **Recovery**.

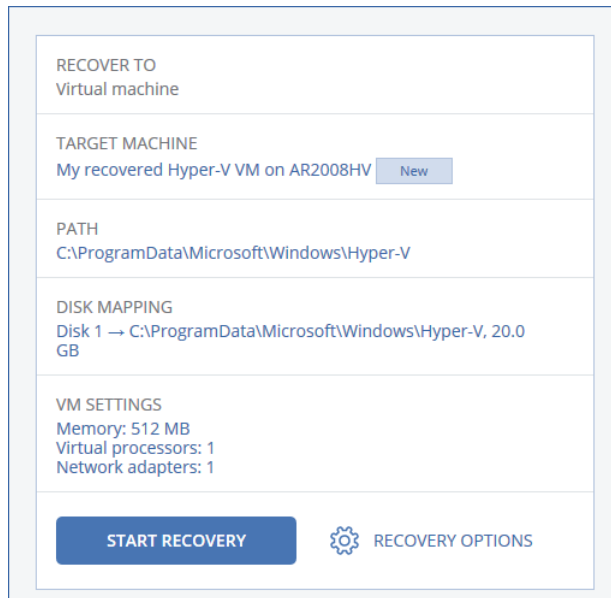
2. Select a recovery point, and then click **Recover** > **Entire machine**.



3. The software automatically selects the original machine as the target machine. Click **Target machine**, and then do the following:
- Click **New machine**.
  - Select the Hyper-V host.
  - In **Machine name**, specify the new machine name.
  - Click **OK**.



4. Click **Start recovery**.



The screenshot shows a configuration window for a virtual machine recovery. It is divided into several sections: 'RECOVER TO' with the value 'Virtual machine'; 'TARGET MACHINE' with the value 'My recovered Hyper-V VM on AR2008HV' and a 'New' button; 'PATH' with the value 'C:\ProgramData\Microsoft\Windows\Hyper-V'; 'DISK MAPPING' with the value 'Disk 1 → C:\ProgramData\Microsoft\Windows\Hyper-V, 20.0 GB'; and 'VM SETTINGS' with values 'Memory: 512 MB', 'Virtual processors: 1', and 'Network adapters: 1'. At the bottom, there is a blue 'START RECOVERY' button and a 'RECOVERY OPTIONS' link with a gear icon.

RECOVER TO Virtual machine
TARGET MACHINE My recovered Hyper-V VM on AR2008HV <a href="#">New</a>
PATH C:\ProgramData\Microsoft\Windows\Hyper-V
DISK MAPPING Disk 1 → C:\ProgramData\Microsoft\Windows\Hyper-V, 20.0 GB
VM SETTINGS Memory: 512 MB Virtual processors: 1 Network adapters: 1
<a href="#">START RECOVERY</a> <a href="#">RECOVERY OPTIONS</a>

The recovery progress is shown on the **Activities** tab.

The recovered machine is powered off by default, because the original machine may still be online and so there is a chance that the original machine's clone will appear on the network. To be on the safe side, power on the recovered virtual machine manually, after you take the necessary precautions.

## 5.5 Acronis Instant Restore

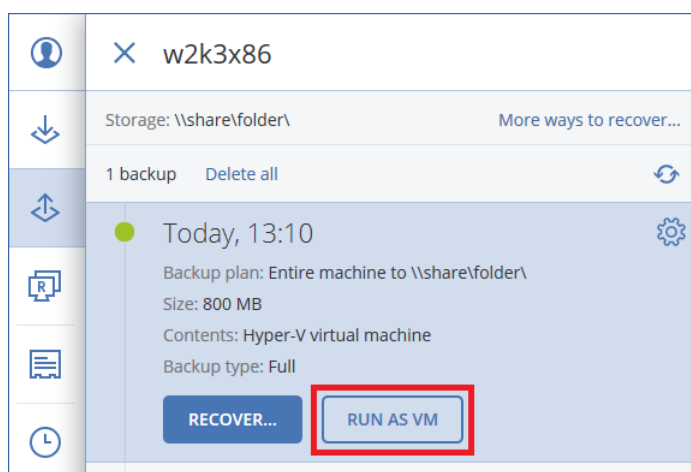
*In this scenario, you will run a Hyper-V virtual machine from a backup of a machine running Microsoft SQL Server. You can use the backup created in the "Application-aware backup and SQL database recovery" (p. 14) scenario.*

If you have a VMware ESXi environment, you can perform similar steps to run a VMware ESXi virtual machine from a backup.

A virtual machine can be created from a disk-level backup that contains an operating system. This operation, also known as Instant Restore, enables you to spin up a virtual server in seconds. The virtual disks are emulated directly from the backup and thus do not consume space on the datastore (storage). The storage space is required only to keep changes to the virtual disks.

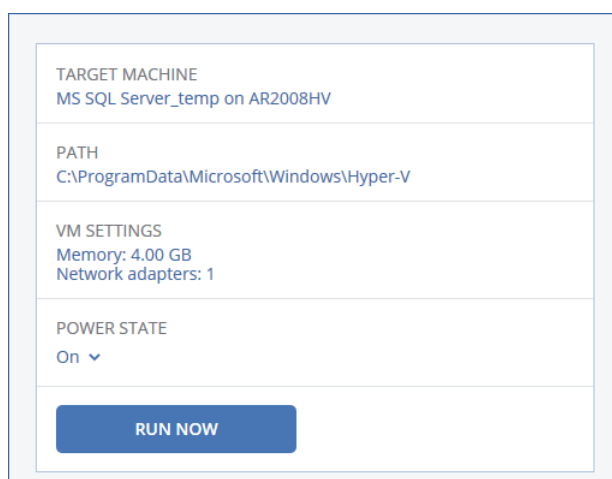
### To run a virtual machine from a backup

1. Select a backed-up machine, click **Recovery**, and then select a recovery point.
2. Click **Run as VM**.



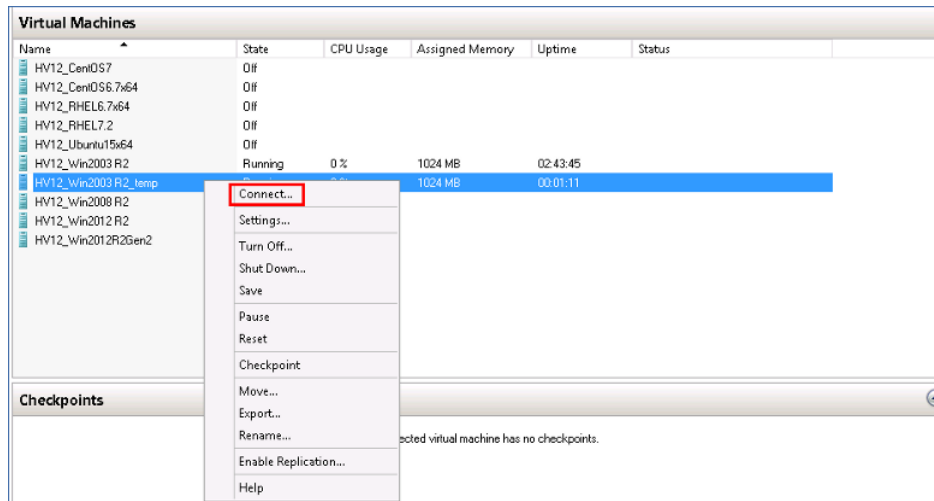
The software automatically selects the host and other required parameters.

3. Click **Run now**.



As a result, the machine appears in the **All machines** list with the following icon:

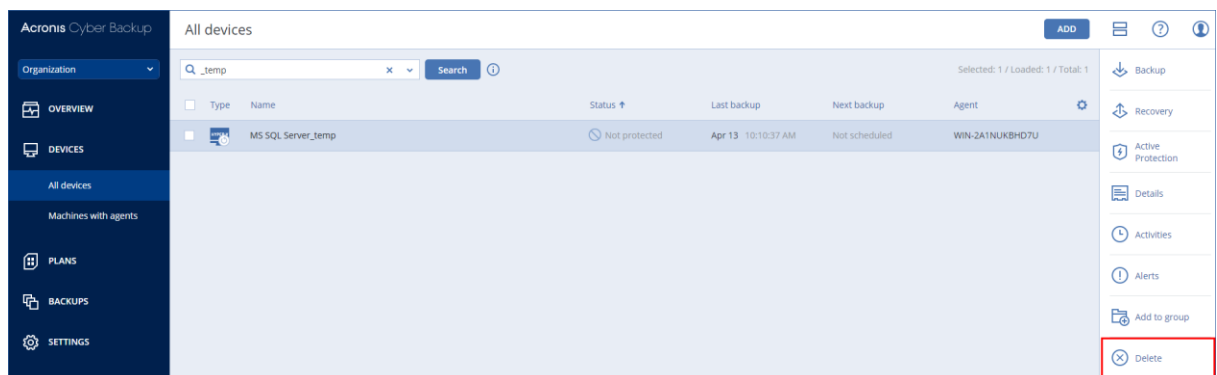
4. In Hyper-V Manager, right-click the machine running from a backup, and then click **Connect**.



5. Verify that the machine running from a backup functions properly. For example, start SQL Server Management Studio and connect to a SQL Server instance that is running on the machine.

### To delete a virtual machine that is running from a backup

1. Select a machine that is running from a backup.
2. Click **Delete**.



3. Confirm your decision.

The machine is removed from the backup console. It is also removed from the Hyper-V inventory and storage. All changes that occurred to the data while the machine was running are lost.

To learn more about Instant Restore, refer to:

<http://dl.managed-protection.com/u/backup/help/12.5/user/en-US/index.html#38848.html>.



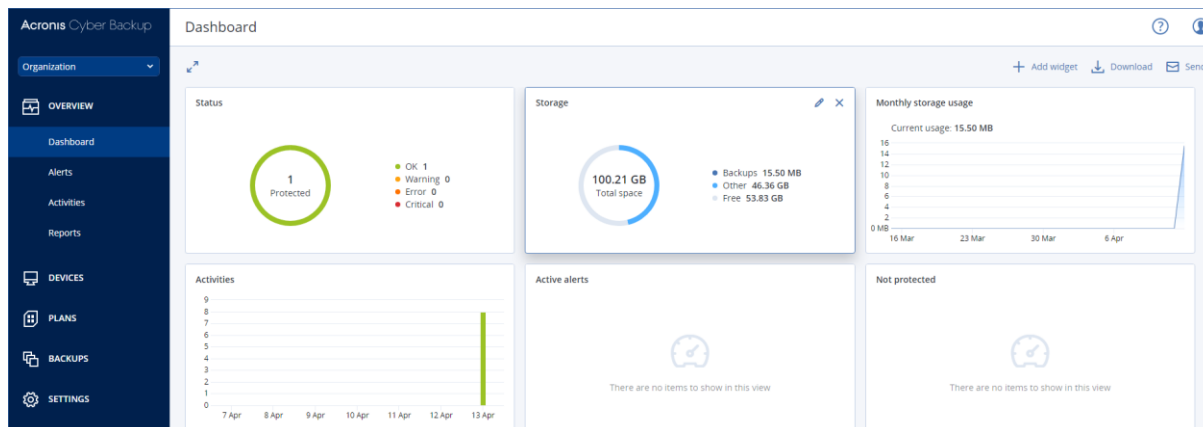
## 5.6 Using the Dashboard

*In this scenario, you will inspect the current state of your backup infrastructure by using the **Dashboard** tab and customize a widget.*

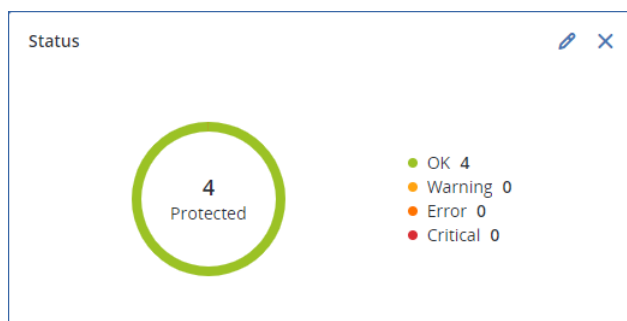
The dashboard provides a number of customizable, dynamic widgets that give an overview of your backup infrastructure and backed-up devices. The widgets are updated in real time.

### To view the dashboard

1. Click **Dashboard**.



2. Inspect the **Status** widget. It shows a summary of protection status of all protected devices. Click a status view the list of devices that have this status.



## To customize a widget

You can customize the **Status** widget so that it shows the status of specific machines only. To open the widget settings, click the Pencil icon. In **Device group**, expand **All**, and then select your desired group.

The screenshot displays the 'Status' widget settings. The main area shows a 'Status' widget with a green circle indicating '2 Protected' machines. A legend shows: OK 2 (green), Warning 0 (yellow), Error 0 (orange), and Critical 0 (red). The right sidebar shows the 'Status' settings panel with a 'Name' field set to 'Status' and a 'Device group' dropdown set to 'Hyper-V'. The dropdown menu is expanded, showing a tree structure: 'All' (expanded) with sub-items 'Machines with agents', 'VMware', 'Hyper-V' (selected), 'Hosts and clusters', 'Important VMs', and 'Microsoft SQL'.

## 5.7 Group management

*In this scenario, you will create a group of machines, apply a backup plan to this group, run the plan, and then check the plan execution status.*

Groups are designed for convenient managing a large number of machines. You can apply a backup plan to a group rather than to each machine separately. Once a new machine appears in the group, the plan is automatically applied to it.

You can create static and dynamic groups. A static group content never changes unless you explicitly add or delete a machine. Dynamic groups are populated automatically according to the search criteria you specify.

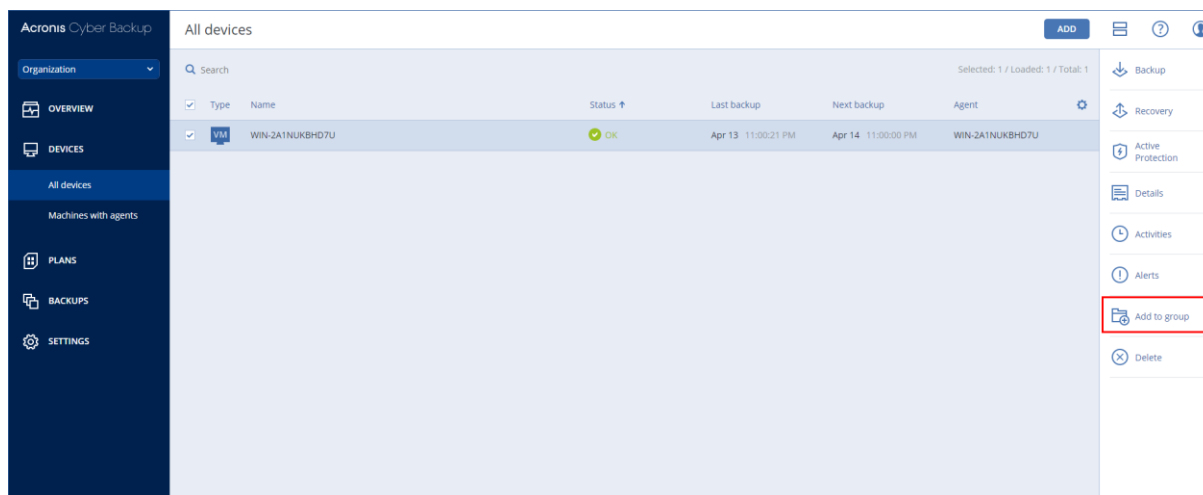
Only machines of the same type can be added to a group. For example, under **Hyper-V** you can create a group of Hyper-V virtual machines. Under **Machines with agents**, you can create a group of machines with installed agents. Under **All machines**, you cannot create a group.

Besides machines, you can also create groups of Exchange databases, Exchange mailboxes, SQL Server databases, and Office 365 mailboxes.

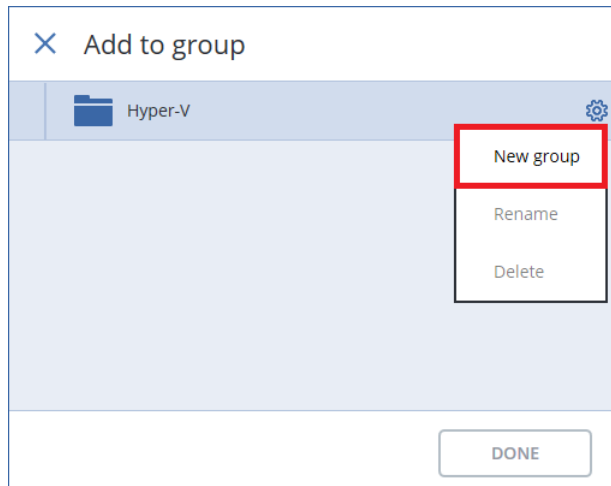
In this scenario, we will create a static group of virtual machines.

### To create a group of machines

1. Click **All machines** or **Hyper-V**, and then select a Hyper-V virtual machine.
2. Click **Add to group**.



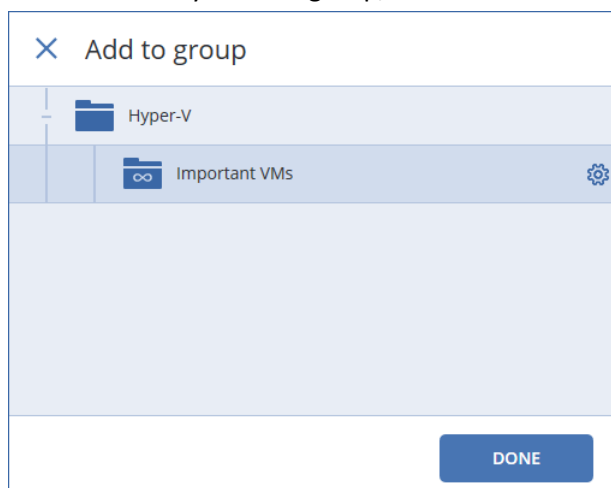
3. Click the gear icon next to the **Hyper-V** group, and then click **New group**.



4. Specify the name of the new group, and then click **OK**.

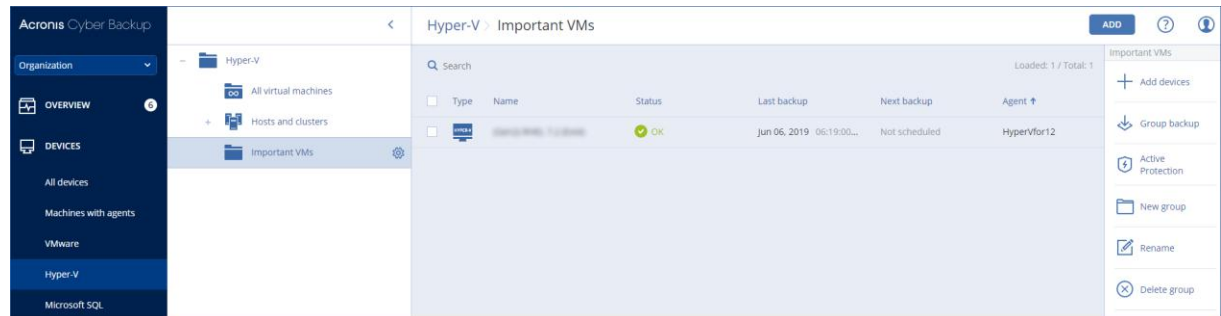
A screenshot of a "Create new group" dialog box. It has a title bar "Create new group". Below the title bar, there is a label "Enter the name for the group" followed by a text input field containing the text "Important VMs". Below that is a label "Comment" followed by a large empty text area. At the bottom left, it says "0 / 512 characters". At the bottom right, there are two buttons: "OK" and "CANCEL".

5. Select the newly created group, and then click **Done**.



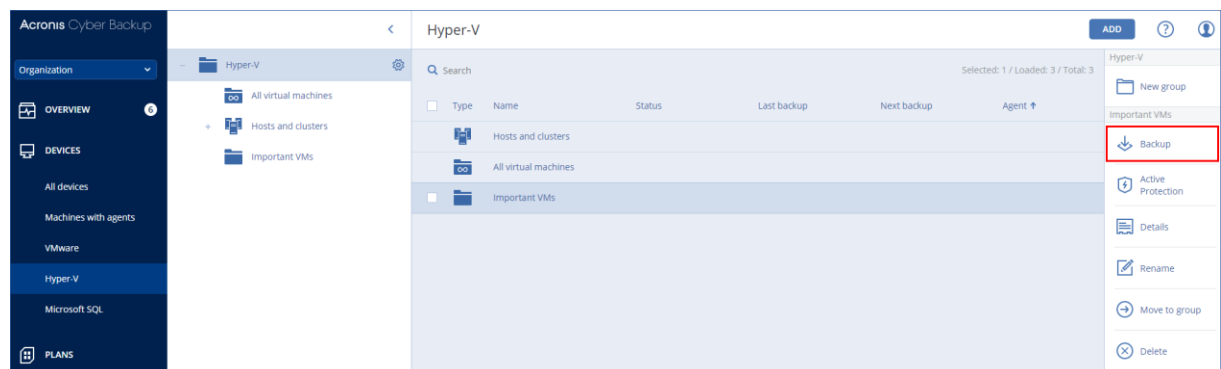
6. Add another machine to the newly created group:
- Select another Hyper-V virtual machine.
  - Click **Add to group**.
  - Select the group, and then click **Done**.

- Under **Devices**, go to the **Hyper-V** section.
- The software displays the list of groups, including the built-in groups (**All virtual machines**, **Hosts and clusters**), and the newly created group. The new group contains two machines.

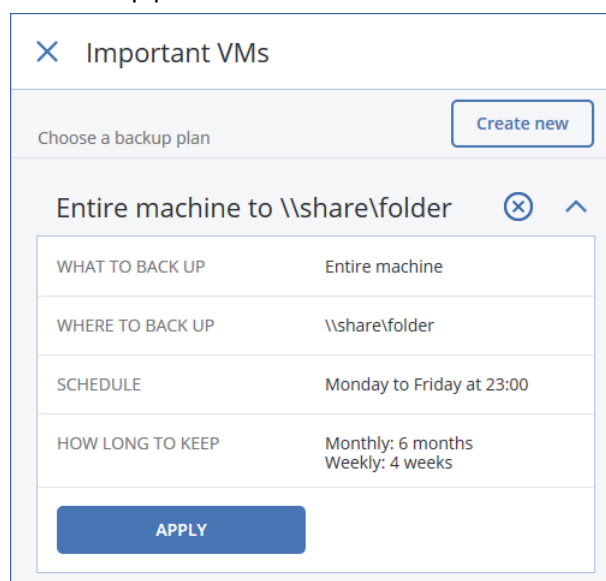


## To apply a backup plan to a group of machines

- In the groups tree, select the **Hyper-V** group.  
The software displays the list of child groups.
- Select the newly created group, and then click **Backup**.



The software displays an existing backup plan from one of the previous scenarios. You can apply this backup plan or create a new one.



- Click **Apply**.
- Click **Run now**. The backup will be started on all machines to which the plan is applied.

## To check the plan execution status

- Click the **Plans** tab, and then click **Backup**.

2. Select the backup plan, and then click the diagram in the **Status** column.  
The software displays the plan execution status.

Acronis Cyber Backup

Backup plans

Organization

Search

Selected: 1 / Loaded: 2

+ Create plan

Import

Details

Run now

Stop

Type	Name	Devices	Status	Schedule	Destination
Entire machine to \\share\\folder	1	OK	Monday to Friday at 1...	WIN-2A1NUKBHD7U: ...	
New backup plan	1	OK	Monday to Friday at 1...	WIN-2A1NUKBHD7U: ...	

## 5.8 Acronis Active Protection

*In this scenario, you will enable Acronis Active Protection on a machine, emulate an activity that encrypts some test files, and see how Acronis Cyber Backup handles the situation.*

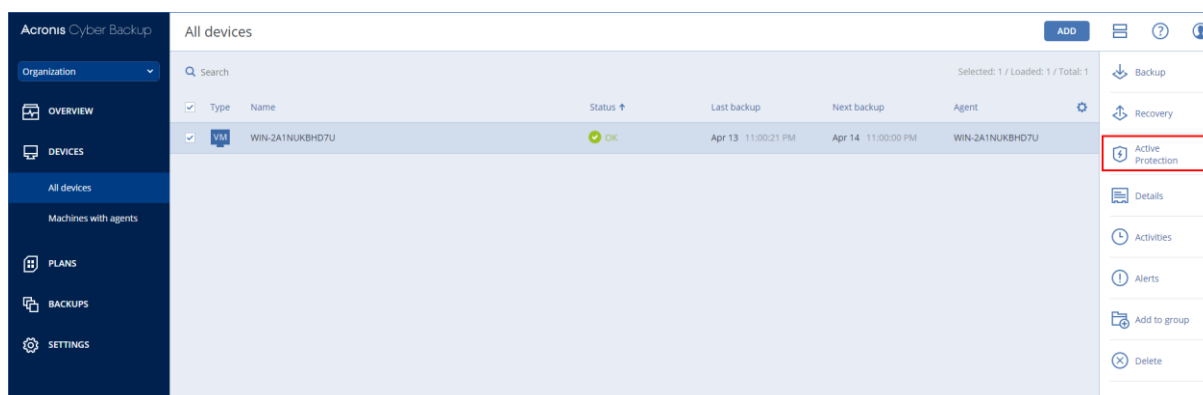
**Note** The encryption only affects the files located in the test folder. After the evaluation is finished, you can safely delete this folder from the machine.

Acronis Active Protection protects your system from malicious software (also known as ransomware) that encrypts files and demands a ransom for the encryption key. When enabled, Active Protection monitors the processes running on the machine. When a third-party process that tries to encrypt files is detected, Active Protection generates an alert, stops the process and reverts the file changes by using the service cache.

Active Protection is available for machines running Windows Vista and later, Windows Server 2008 and later. Agent for Windows must be installed on the machine.

### To enable Acronis Active Protection on a machine

1. Under **All machines**, select the machine for which you want to enable Acronis Active Protection.
2. Click **Active Protection**.



3. Click **Apply**.

### Active Protection Plan ⓘ

ACTION ON DETECTION	Stop the process
TRUSTED PROCESSES	None
HARMFUL PROCESSES	None
FOLDER EXCLUSIONS	None
SELF-PROTECTION	On
PROTECTION OPTIONS	Backups - On Cryptomining protection - Off Mapped drives - Off

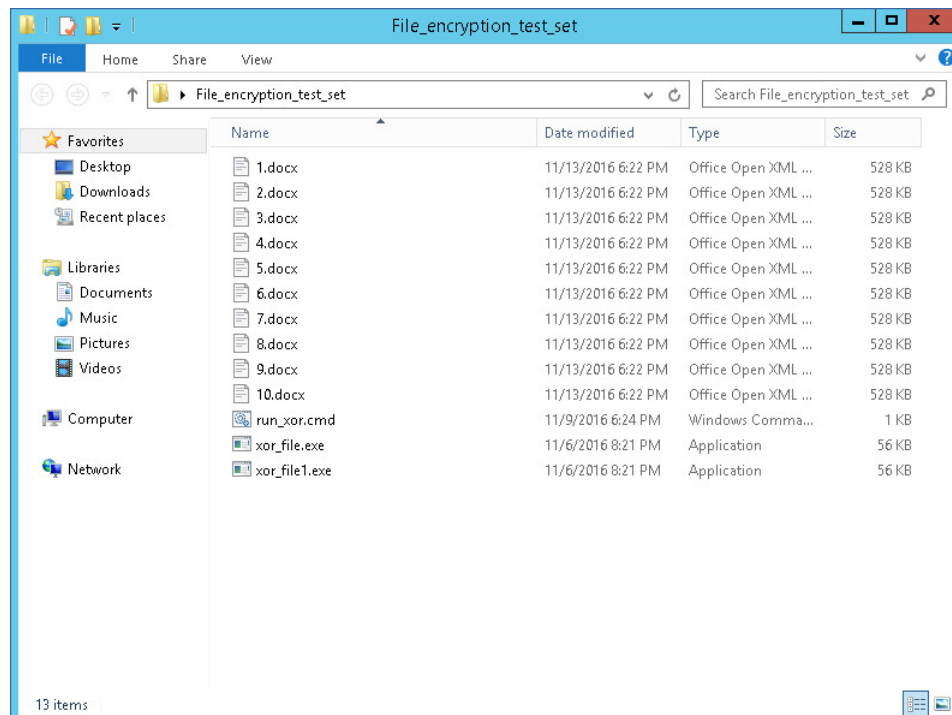
APPLYEDIT

### To emulate an encryption activity

1. Download the archive: <http://dl2.acronis.com/u/EncryptionTest/FileEncryptionTestSet.zip>

2. Unpack the archive to a local folder of the machine for which Acronis Active Protection is enabled.

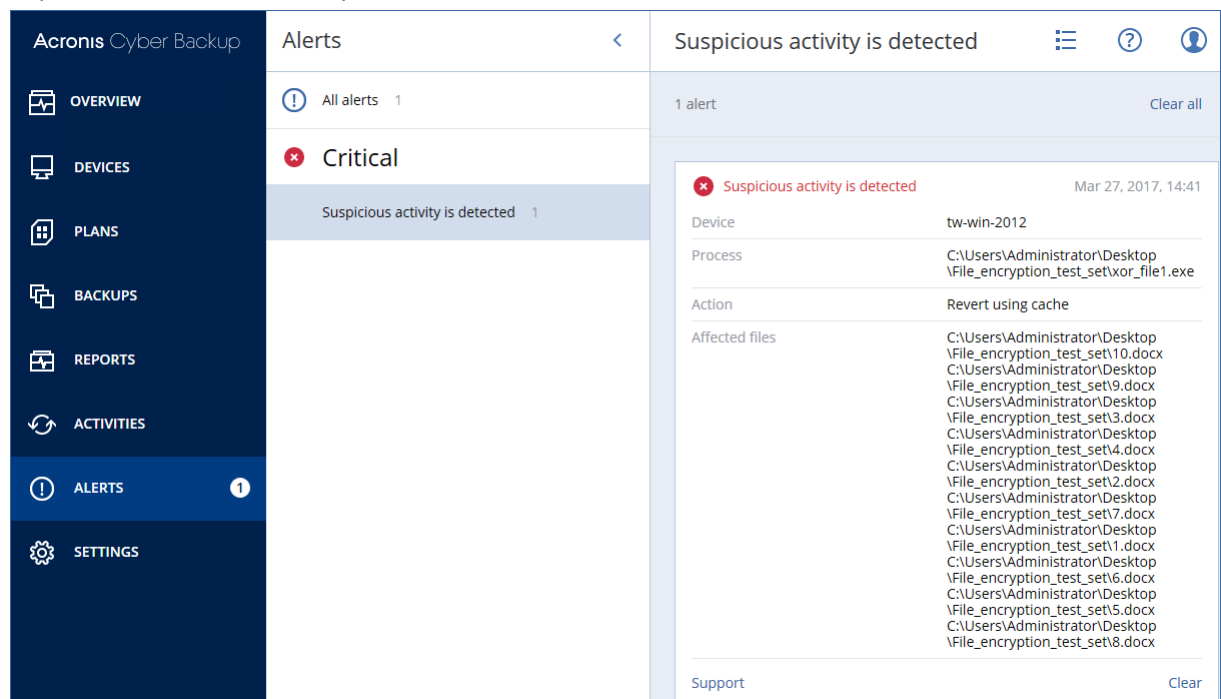
The archive contains the encryption tool and several .docx files.



3. Double click the run\_xor.cmd file.

The tool starts encrypting the .docx files in the folder.

4. Check the **Alerts** tab in the backup console. The software generates an alert, stops the test file encryption process, and then reverts the file changes by using the service cache (temporary copies of the files created by the Acronis Active Protection service).



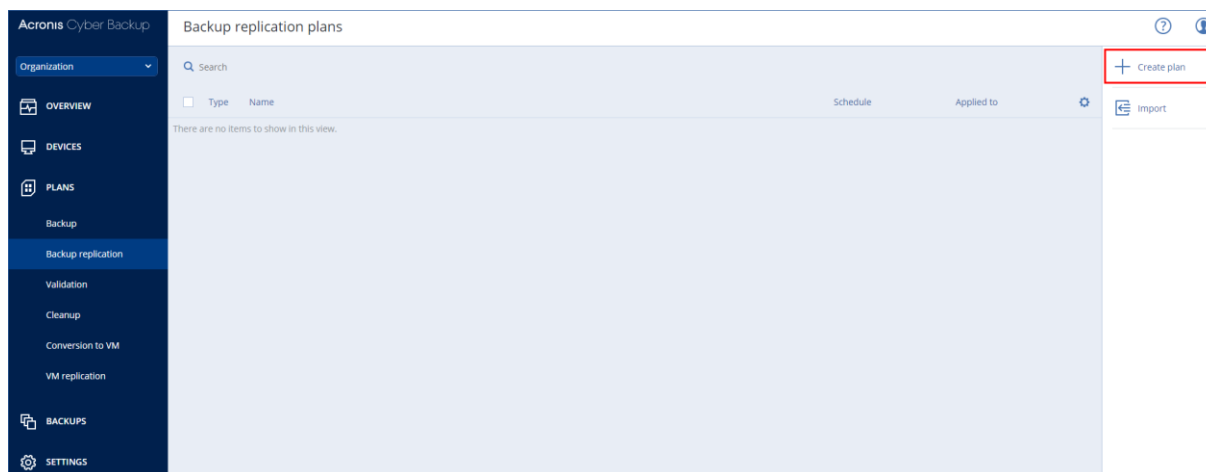


## 5.9 Off-host replication of backups to cloud storage

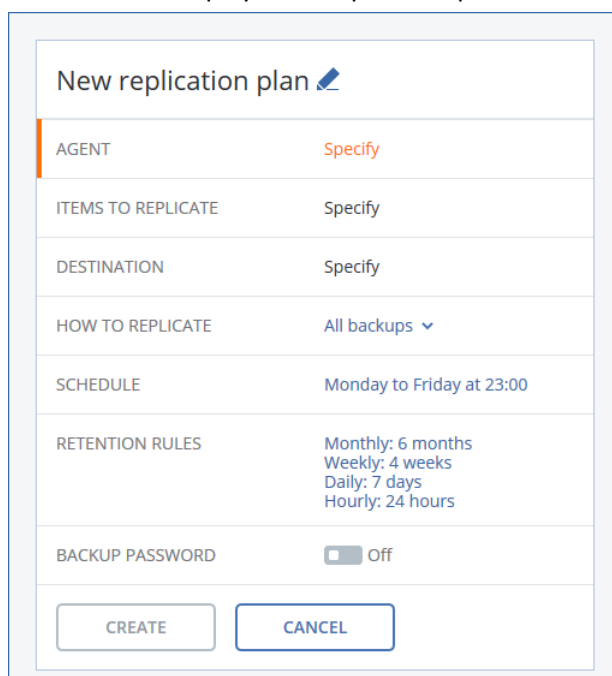
*In this scenario, you will schedule replication of backups from a network share to the cloud storage. The replication plan will be executed by an agent different from the one(s) that create the backups. This capability is designed to relieve the production servers of unnecessary CPU load.*

### To create a backup replication plan

1. Click **Plans > Backup replication**.
2. Click **Create plan**.



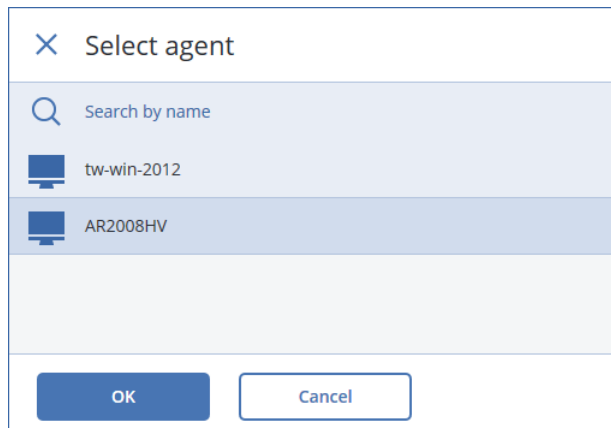
The software displays a new plan template.



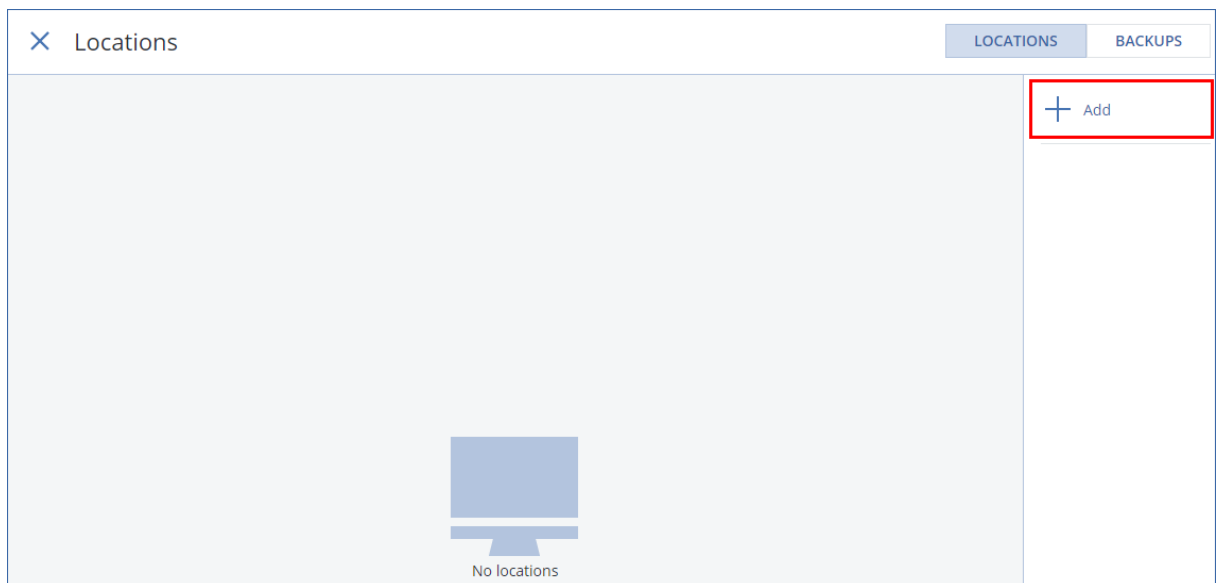
New replication plan	
AGENT	Specify
ITEMS TO REPLICATE	Specify
DESTINATION	Specify
HOW TO REPLICATE	All backups
SCHEDULE	Monday to Friday at 23:00
RETENTION RULES	Monthly: 6 months Weekly: 4 weeks Daily: 7 days Hourly: 24 hours
BACKUP PASSWORD	<input type="checkbox"/> Off
<div>CREATE CANCEL</div>	

3. Click **Agent**, select the agent that will perform the replication, and then click **OK**.

You can select any agent that is registered on the management server and has access to the backup location. To showcase this scenario, we recommend that you select an agent different from the one that executes the backup plan.

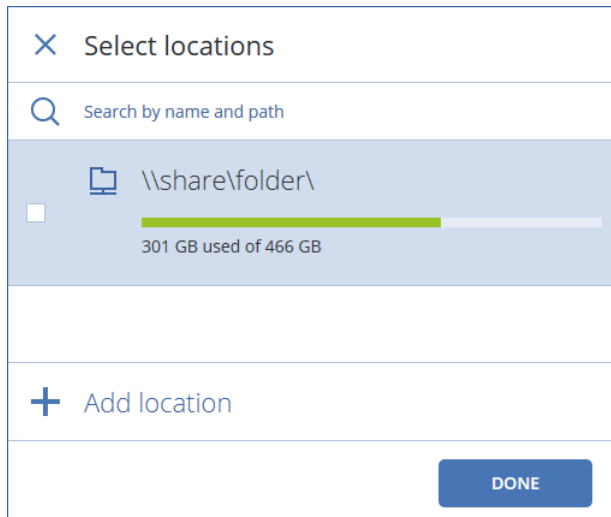


4. We will configure the plan to replicate the entire backup location; in our case, the shared folder.  
Click **Items to replicate**, and then do the following:
  - a. Click **Add**.



The software displays the previously used backup locations.

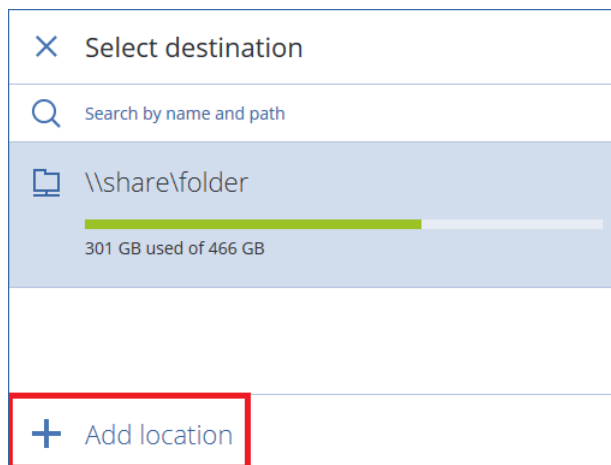
- b. Select the shared folder that contains backups, and then click **Done**.



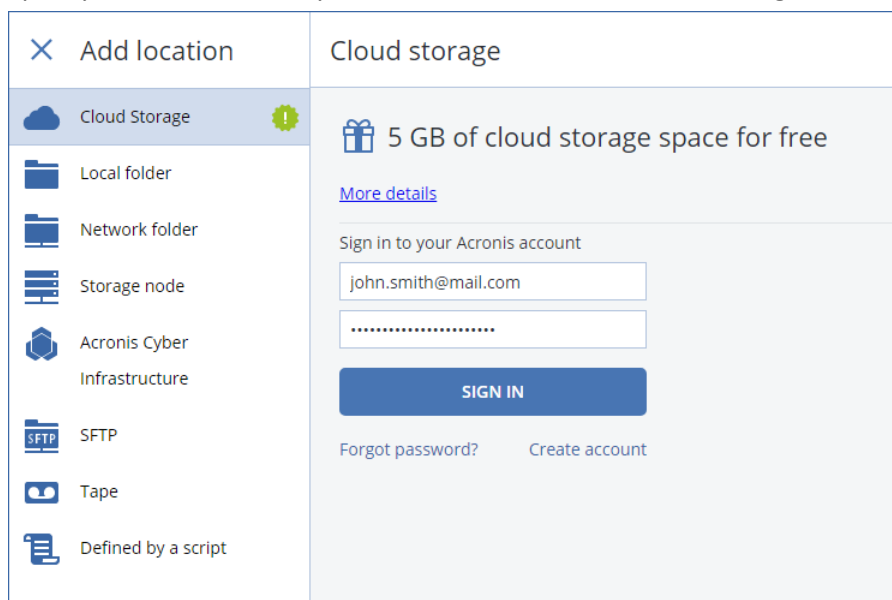
- c. Click **Done**. If prompted, specify the user name and password for the shared folder.

5. Click **Destination**.

6. Click **Add location > Cloud storage**.



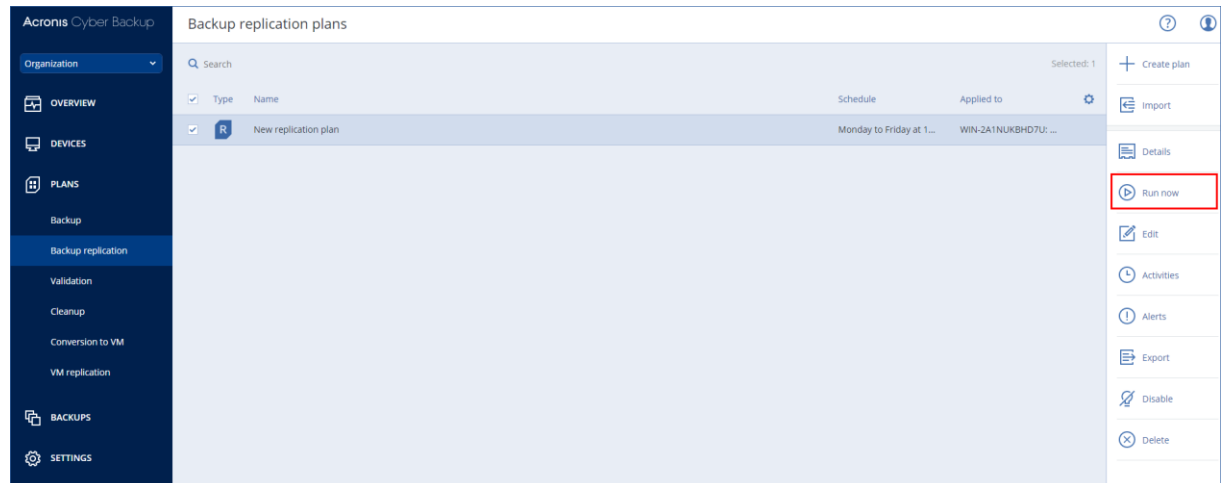
7. Specify the credentials of your Acronis account, and then click **Sign in**.



8. On the new plan panel, click **Create**.

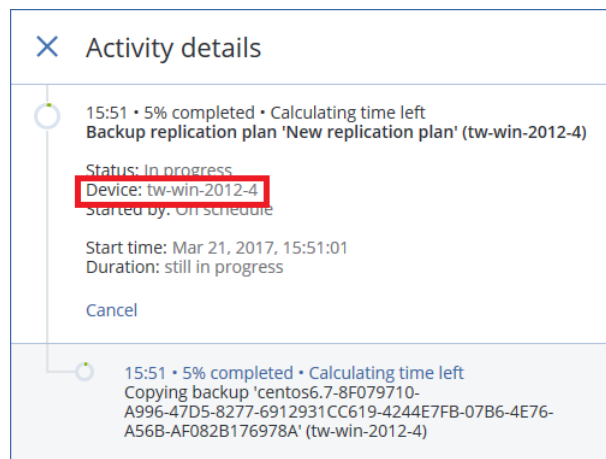
## To run the replication plan

1. Under **Plans > Backup replication**, select the newly created plan.
2. Click **Run now**.



## To check the plan execution status

1. Click **Activities**.
2. Click the running activity to view the details. The **Device** field shows the agent that is executing the plan.



3. Wait until the replication is finished.
4. Click the **Backups** tab.
5. In **Locations**, select **Cloud Storage**. Browse the cloud storage to ensure that the backups were replicated.

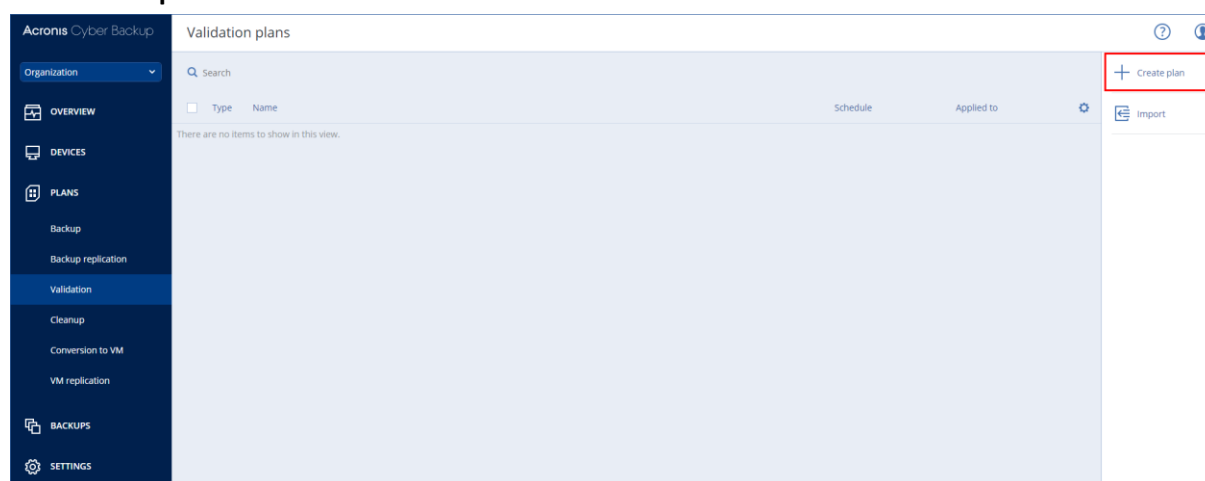
## 5.10 Off-host validation of backups by calculating checksum and Instant Restore

*In this scenario, you will schedule validation of backups that are stored on a network share. The software will simultaneously use two validation methods:*

- *Calculating a checksum for every data block saved in a backup.*
- *Running a Hyper-V virtual machine from a backup, and then connecting to Hyper-V Heartbeat Service to ensure that the operating system has started successfully. This method works only for disk-level backups that contain an operating system.*

### To create a validation plan

1. Click **Plans > Validation**.
2. Click **Create plan**.



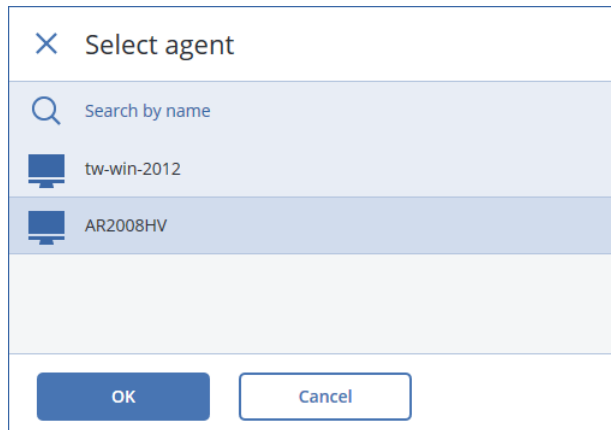
The software displays a new plan template.

The 'New validation plan' dialog box is displayed. It contains the following fields and values:

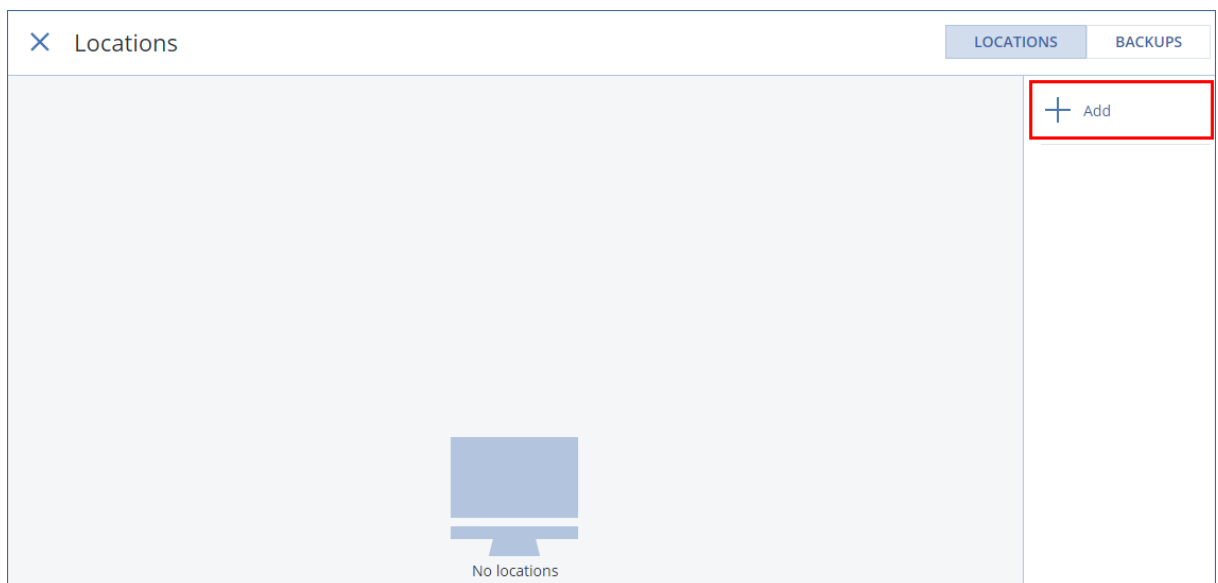
Field	Value
AGENT	Specify
ITEMS TO VALIDATE	Specify
WHAT TO VALIDATE	All backups
HOW TO VALIDATE	Checksum verification
SCHEDULE	Monday to Friday at 23:00
BACKUP PASSWORD	Off

At the bottom of the dialog are two buttons: 'CREATE' and 'CANCEL'.

3. Click **Agent**, select Agent for Hyper-V that will perform the validation, and then click **OK**.

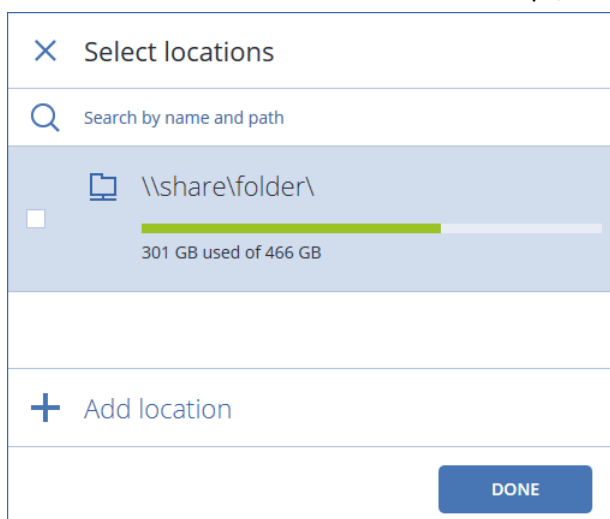


4. We will configure the plan to validate the entire backup location; in our case, the shared folder.  
Click **Items to validate**, and then do the following:
- a. Click **Add**.



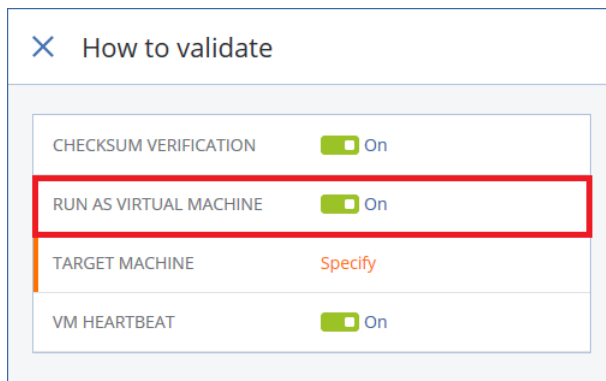
The software displays the previously used backup locations.

- b. Select the shared folder that contains backups, and then click **Done**.



- c. Click **Done**. If prompted, specify the user name and password for the shared folder.

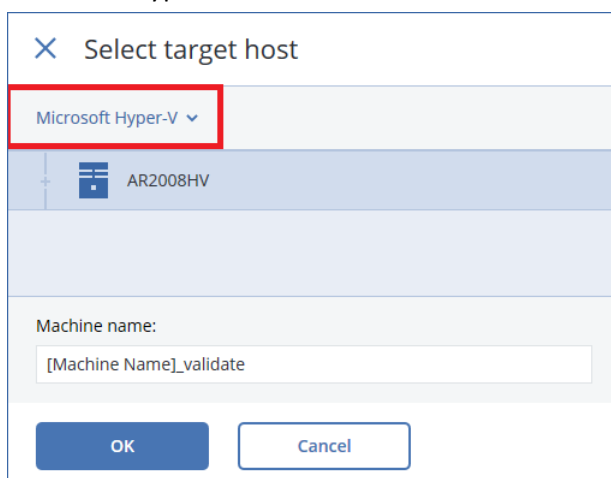
5. To configure the plan to use both validation methods, click **How to validate**, and then do the following:
- Enable the **Run as a virtual machine** switch.



How to validate

CHECKSUM VERIFICATION	<input checked="" type="checkbox"/> On
RUN AS VIRTUAL MACHINE	<input checked="" type="checkbox"/> On
TARGET MACHINE	Specify
VM HEARTBEAT	<input checked="" type="checkbox"/> On

- Click **Target machine**.
- In the virtual machine type selector, select **Microsoft Hyper-V**.
- Select the Hyper-V host where the virtual machines will run, and then click **OK**.



Select target host

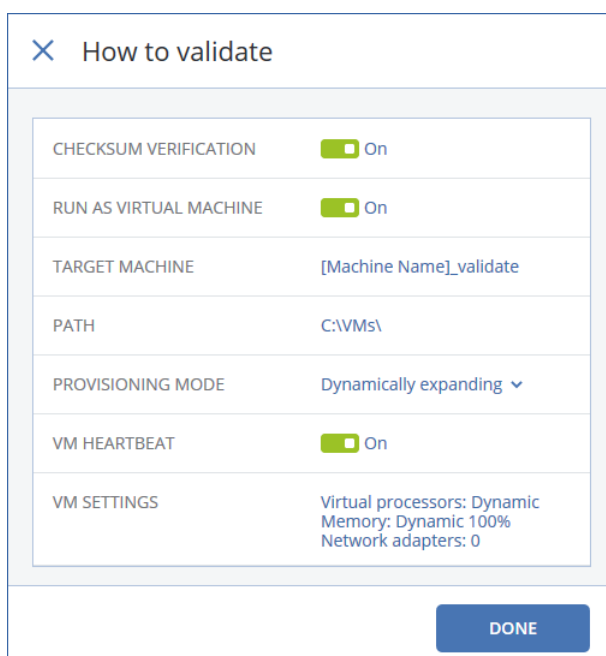
Microsoft Hyper-V ▾

AR2008HV

Machine name:  
[Machine Name]\_validate

OK Cancel

- Click **Path**, specify a folder on the Hyper-V server where the machines will be located, and then click **Done**.



How to validate

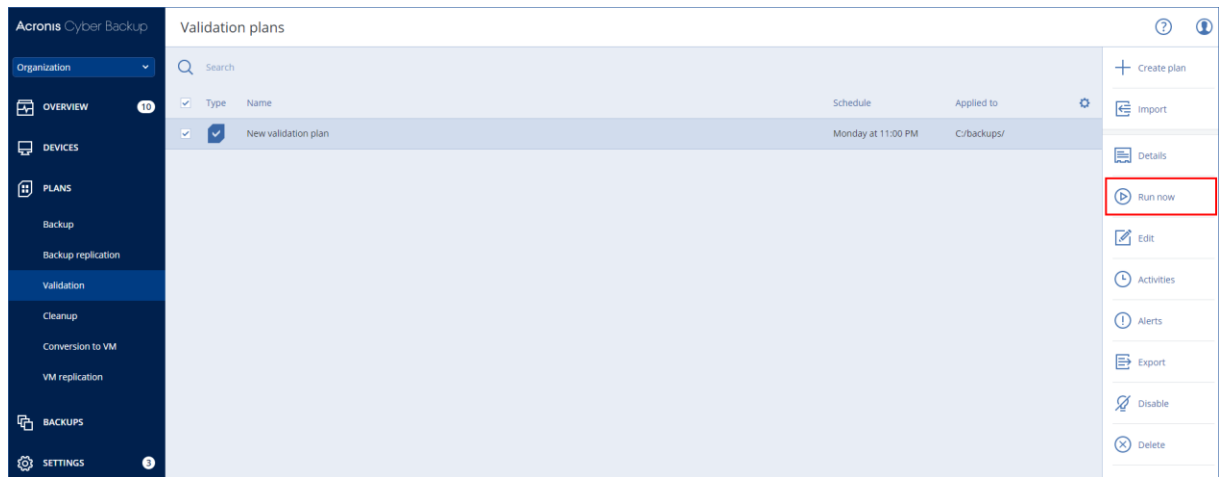
CHECKSUM VERIFICATION	<input checked="" type="checkbox"/> On
RUN AS VIRTUAL MACHINE	<input checked="" type="checkbox"/> On
TARGET MACHINE	[Machine Name]_validate
PATH	C:\VMs\
PROVISIONING MODE	Dynamically expanding ▾
VM HEARTBEAT	<input checked="" type="checkbox"/> On
VM SETTINGS	Virtual processors: Dynamic Memory: Dynamic 100% Network adapters: 0

DONE

6. On the new plan panel, click **Create**.

### To run the validation plan

1. Under **Plans > Validation**, select the newly created plan.
2. Click **Run now**.



### To check the plan execution status

1. Click **Activities**.  
The software shows two validation activities per backup - one for each of the validation methods.
2. You can click an activity to view its details.



The **Device** field shows the agent that executed the activity.

**Activity details**

14:00 — 14:07  
Running validation plan 'New validation plan' (AR2008HV)  
Status: Succeeded  
Device: AR2008HV  
Started by: PolicyManager  
Start time: Mar 23, 2017, 14:00:08  
Finish time: Mar 23, 2017, 14:07:02  
Duration: 6 min  
[Download log](#)

- 14:00 — 14:00  
Validating backup 'w7x86-E7202A5B-8432-4403-BB0C-8888B2ECA4FB-CD482E64-5EDB-4A4A-A25C-97BA96ECFEADA'. (AR2008HV)
- 14:00 — 14:06  
Running machine from backup (w7x86\_validate)
- 14:00 — 14:03  
Creating and configuring temporary machine (AR2008HV)
- 14:00 — 14:00  
Preparing datastore (AR2008HV)
- 14:03 — 14:03  
Fixing virtual machine bootability (AR2008HV)
- 14:03 — 14:03  
Starting temporary machine (w7x86\_validate)
- 14:03 — 14:04  
Waiting for 1 minutes (the initial timeout). (w7x86\_validate)
- 14:04 — 14:06  
Waiting for 2 minutes (the retry timeout). (w7x86\_validate)
- 14:06 — 14:07  
Deleting machine running from backup (w7x86\_validate)
- 14:06 — 14:06  
The heartbeat is received. (w7x86\_validate)

3. Wait until the validation is finished for all backups. If some of the backups are corrupted, the software will generate alerts.

## 5.11 Tape management

In this scenario, you will back up a machine running Windows to a locally attached tape device and recover a folder from this backup.

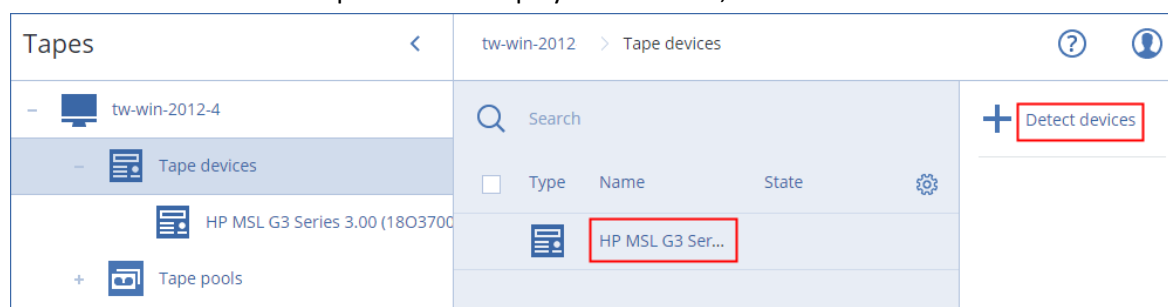
### Before backing up

1. Ensure that the tape device is attached to the machine in accordance with the manufacturer's instructions.
2. If third-party software with proprietary tape management tools is installed on the machine, uninstall or deactivate this software.
3. When detecting a tape device, Acronis Cyber Backup disables the device from Windows Removable Storage Manager (RSM). If the machine has third-party software that uses RSM, make sure that neither a user nor third-party software enables the device in RSM until the evaluation is completed.
4. Load tapes to the tape device.

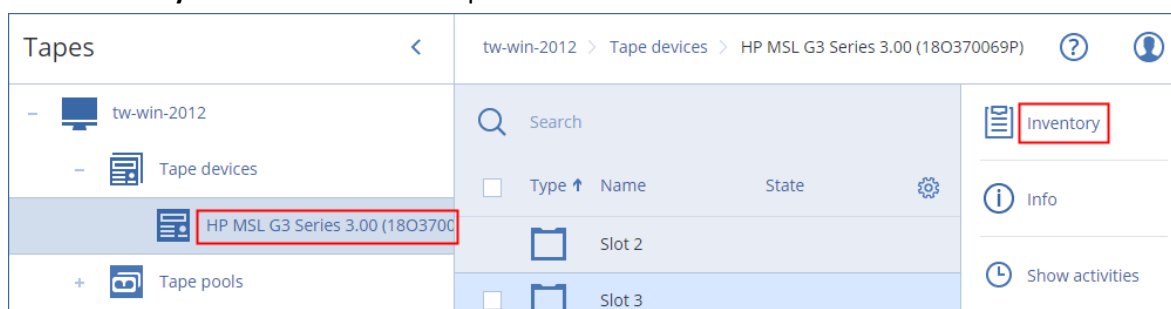
The total capacity of tapes that you need roughly equals the total occupied space of the machine's disks.

**Warning** The tapes will be overwritten. Please ensure that you do not need the data stored of these tapes.

5. In **Settings > Tape management**, expand the node with the machine name, and then click **Tape devices**.
6. Ensure that the attached tape device is displayed. If it is not, click **Detect devices**.

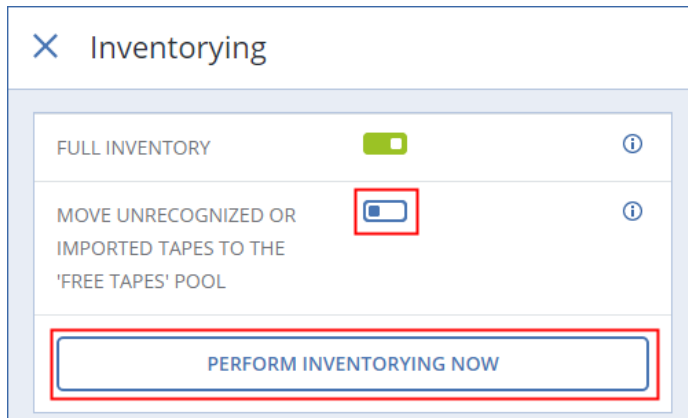


7. If your tape device is a stand-alone drive, skip this step. Otherwise, do the following:
  - a. Click the tape device name.
  - b. Click **Inventory** to detect the loaded tapes.



- c. Keep **Full inventory** turned on. Enable the **Move unrecognized or imported tapes to the 'Free tapes' pool** switch, and then click **Perform inventorying now**.

Full inventorying of an entire tape device may take a long time.

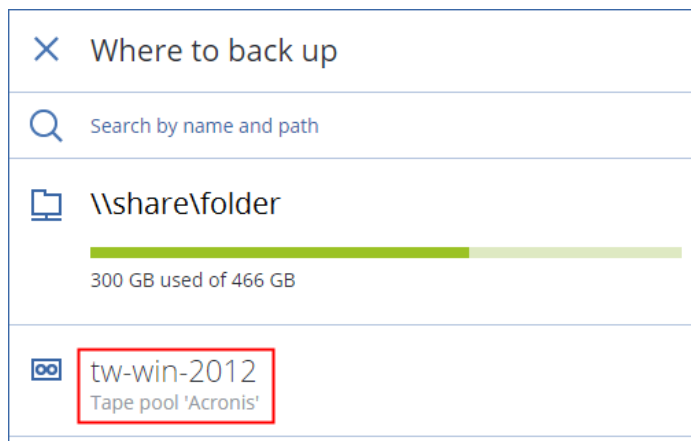


As a result, the loaded tapes are detected and moved to the **Free tapes** pool.

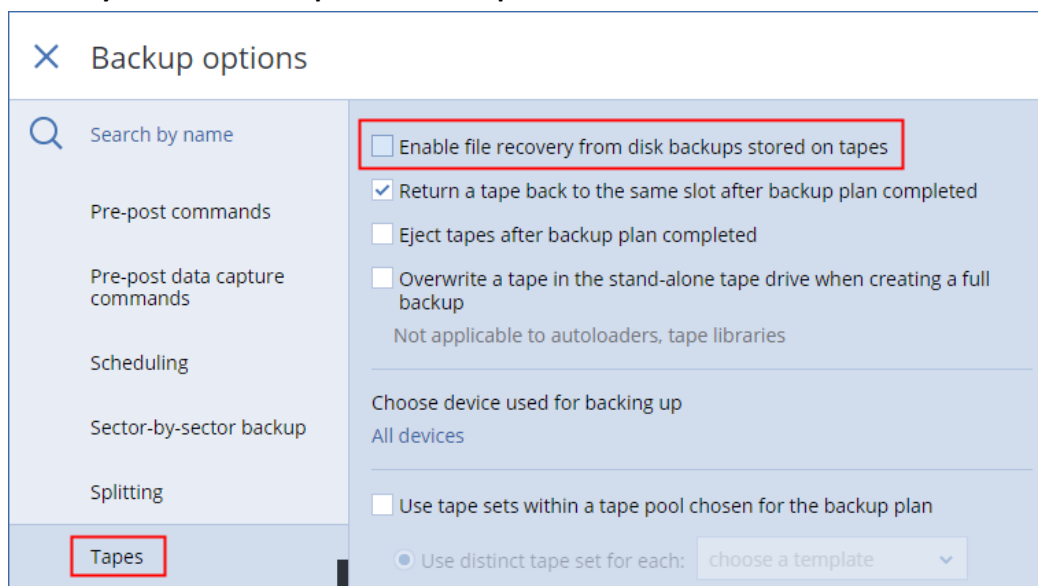
## To back up the machine

Perform the backup as described in "Windows: Backup and granular file recovery" (p. 10) with the following specifics:

- When specifying the backup location, select **Tape pool 'Acronis'**.

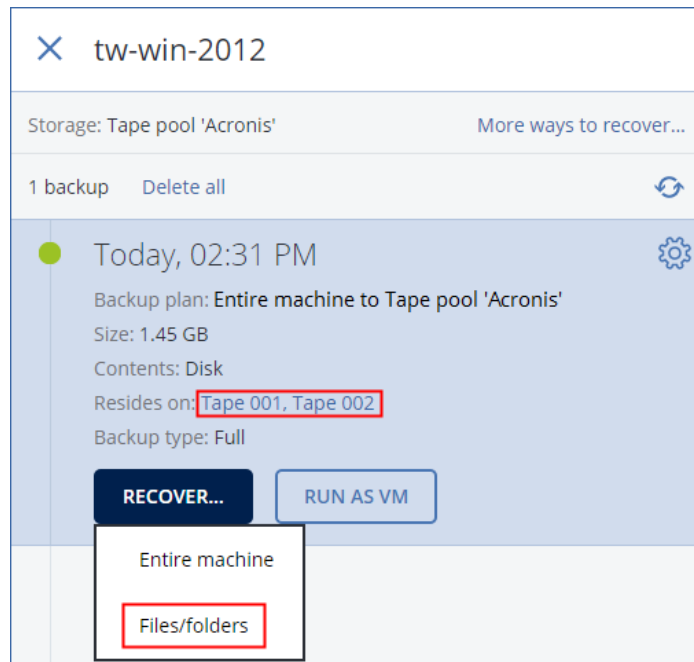


- Click the gear icon to modify the backup options, click **Tapes**, and then select the **Enable file recovery from disk backups stored on tapes** check box.



## To recover a folder from the backup

1. In the backup console, select your machine, and then click **Recovery**.
2. Select the recovery point.
3. The software displays the tapes on which the backup is stored. Ensure that these tapes are present in the tape device.
4. Click **Recover** > **Files/folders**.



5. Follow the recovery steps described in "Windows: Backup and granular file recovery" (p. 10), starting from step 3.

## 5.12 Reporting

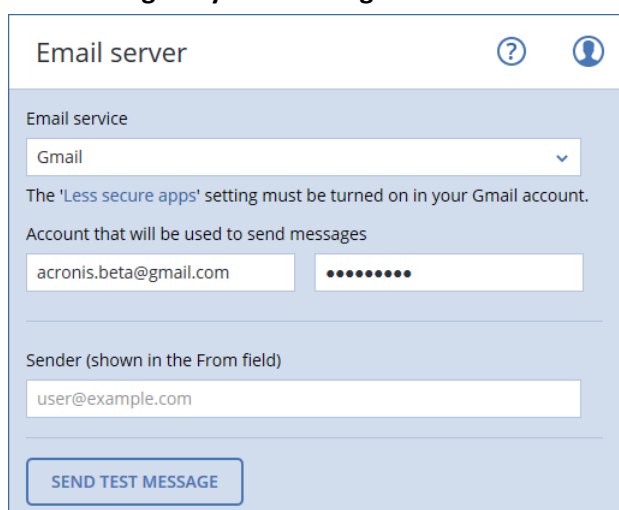
*In this scenario, you will configure the email notification settings, generate a summary report about your backup infrastructure, send the report to the specified email address, and then schedule sending the report.*

You can specify a custom SMTP server for sending email notifications from the management server. For example, it is possible to use Microsoft Exchange Server that is installed on your premises, or your Office 365 mailbox.

For simplicity, we recommend that you use an existing or create a new account in the Gmail email service. The **Less secure apps** setting must be turned on in this Gmail account. For more information, refer to <https://support.google.com/accounts/answer/6010255>.

### To configure the email notification settings

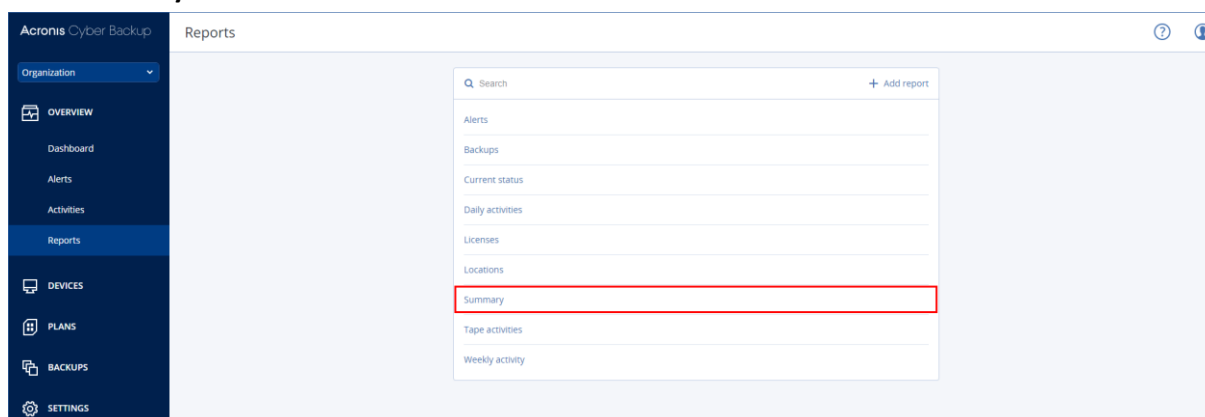
1. Click **Settings > System settings > Email server**.



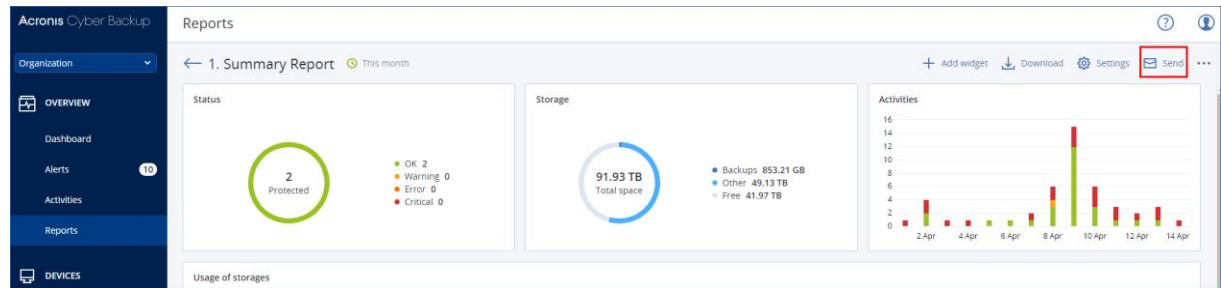
2. In **Email service**, select **Gmail**.
3. Specify the credentials of an account that will be used to send the report.
4. Leave the **Sender** field empty. This setting is not effective when using the Gmail email service.
5. Click **Save**.

### To generate and send a summary report

1. Click the **Reports** tab.
2. Click **Summary**.



The software shows the summary report which includes the dashboard widgets and tables that provide historical data.



3. Click **Send**.
4. Specify the recipient's email address.
5. In **File format**, select **PDF**.

Send report

Recipients

john.smith@mail.com

File format

PDF

**SEND**

Cancel

6. Click **Send**.
7. Check the inbox of the email account that you specified in step 4.

### To schedule sending the summary report

1. Click **Settings**.
2. Enable the **Send a scheduled report** switch.
3. Select the **Send by email** check box.
4. In **Recipients**, specify the recipient's email address.
5. In **Schedule**, select the day of the month on which the report will be generated and sent.

6. In **Send at**, select the time when the report will be generated.

The screenshot shows a configuration window for a backup task. The 'General' tab is active, showing the task name 'Daily activities' and a range of '7 days'. The 'Scheduled' tab is also visible, showing a green toggle switch for scheduling. Under the 'Scheduled' tab, the 'Send by email on a schedule' checkbox is checked, with the recipient email address 'john.smith@mail.com' entered. The 'Save the file to a local folder on a schedule' checkbox is unchecked. The 'File format' is set to 'Excel and PDF'. The 'Days of week' and 'Monthly' tabs are visible, with 'Monthly' selected. The 'days of month' is set to '1', and the 'Send at' time is set to '12:00 AM'.

General

Name  
Daily activities

Range  
7 days

Scheduled

☒ Send by email on a schedule

Recipients  
john.smith@mail.com

☐ Save the file to a local folder on a schedule

File format  
Excel and PDF

Days of week Monthly

days of month  
1

Send at  
12:00 AM

## 6 Disclaimer

This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Technical changes and differences from the illustrations are reserved; errors are excepted.

Acronis and Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners.