Acronis

Acronis SCS

Cyber Backup 12.5 Hardened Edition Update 4.10

USER GUIDE

1 Installation

1.1 Components

Agents

Agents are applications that perform data backup, recovery, and other operations on the machines managed by Acronis SCS Cyber Backup 12.5 Hardened Edition.

Choose an agent, depending on what you are going to back up. The following table summarizes the information, to help you decide.

Note that Agent for Windows is installed along with Agent for Exchange, Agent for SQL, Agent for Active Directory, and Agent for Oracle. If you install, for example, Agent for SQL, you also will be able to back up the entire machine where the agent is installed.

What are you going to back up?	Which agent to install?	Where to install it?
Physical machines		
Disks, volumes, and files on physical machines running Windows	Agent for Windows	On the machine that will be backed up.
Disks, volumes, and files on physical machines running Linux	Agent for Linux	
Applications		
SQL databases	Agent for SQL	On the machine running Microsoft SQL Server.
Exchange databases and mailboxes	Agent for Exchange	On the machine running the Mailbox role of Microsoft Exchange Server. If only mailbox backup is required, the agent can be installed on any Windows machine that has network access to the machine running the Client Access role of Microsoft Exchange Server.
Machines running Active Directory Domain Services	Agent for Active Directory	On the domain controller.
Machines running Oracle Database	Agent for Oracle	On the machine running Oracle Database
Virtual machines		
VMware ESXi virtual machines	Agent for VMware (Windows)	On a Windows machine that has network access to vCenter Server and to the virtual machine storage.*
	Agent for VMware (Virtual Appliance)	On the ESXi host.

What are you going to back up?	Which agent to install?	Where to install it?
Hyper-V virtual machines	Agent for Hyper-V	On the Hyper-V host.
Citrix XenServer virtual machines***	The same as for physical machines**	On the machine that will be backed up.
Red Hat Virtualization (RHV/RHEV) virtual machines***		
Kernel-based Virtual Machines (KVM)***		
Oracle virtual machines***		
Nutanix AHV virtual machines***		

*If your ESXi uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESXi host and LAN. For detailed instructions, refer to "LAN-free backup" (Section 14.2.2).

**A virtual machine is considered virtual if it is backed up by an external agent. If an agent is installed in the guest system, the backup and recovery operations are the same as with a physical machine.

***With an Acronis SCS Cyber Backup 12.5 Hardened Edition Advanced Virtual Host license, these virtual machines are considered as virtual (per host licensing is used). With an Acronis SCS Cyber Backup 12.5 Hardened Edition Virtual Host license, these machines are considered as physical (per machine licensing is used).

Other components

Component	Function	Where to install it?
Management Server	Manages the agents. Provides the web interface to users.	On a machine running Windows or Linux.
Components for Remote Installation	Saves agent installation packages to a local folder.	On the Windows machine running the management server.
Monitoring Service	Provides the dashboard and reporting functionality.	On the machine running the management server.
Bootable Media Builder	Creates bootable media.	On a machine running Windows or Linux.
Command-Line Tool	Provides the command-line interface.	On a machine running Windows or Linux.
Backup Monitor	Enables users to monitor backups outside the web interface.	On a machine running Windows.

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Azure virtual machines		+

* In these editions, the HotAdd transport for virtual disks is supported on vSphere 5.0 and later. On version 4.1, backups may run slower.

** Backup at a hypervisor level is not supported for vSphere Hypervisor because this product restricts access to Remote Command Line Interface (RCLI) to read-only mode. The agent works during the vSphere Hypervisor evaluation period while no serial key is entered. Once you enter a serial key, the agent stops functioning.

Limitations

- **Fault tolerant machines**
  Agent for VMware backs up a fault tolerant machine only if fault tolerance was enabled in VMware vSphere 6.0 and later. If you upgraded from an earlier vSphere version, it is enough to disable and enable fault tolerance for each machine. If you are using an earlier vSphere version, install an agent in the guest operating system.
- **Independent disks and RDM**
  Agent for VMware does not back up Raw Device Mapping (RDM) disks in physical compatibility mode or independent disks. The agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding independent disks and RDMs in physical compatibility mode from the backup plan. If you want to back up these disks or data on these disks, install an agent in the guest operating system.
- **Pass-through disks**
  Agent for Hyper-V does not back up pass-through disks. During backup, the agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding pass-through disks from the backup plan. If you want to back up these disks or data on these disks, install an agent in the guest operating system.
- **Hyper-V guest clustering**
  Agent for Hyper-V does not support backup of Hyper-V virtual machines that are nodes of a Windows Server Failover Cluster. A VSS snapshot at the host level can even temporarily disconnect the external quorum disk from the cluster. If you want to back up these machines, install agents in the guest operating systems.
- **In-guest iSCSI connection**
  Agent for VMware and Agent for Hyper-V do not back up LUN volumes connected by an iSCSI initiator that works within the guest operating system. Because the ESXi and Hyper-V hypervisors are not aware of such volumes, the volumes are not included in hypervisor-level snapshots and are omitted from a backup without a warning. If you want to back up these volumes or data on these volumes, install an agent in the guest operating system.
- **Linux machines containing logical volumes (LVM)**
  Agent for VMware and Agent for Hyper-V do not support the following operations for Linux machines with LVM:
  - P2V and V2P migration. Use Agent for Linux or bootable media to create the backup and bootable media to recover.
  - Running a virtual machine from a backup created by Agent for Linux or bootable media.
  - Converting a backup created by Agent for Linux or bootable media to a virtual machine.
- **Encrypted virtual machines** (introduced in VMware vSphere 6.5)
  - Encrypted virtual machines are backed up in an unencrypted state. If encryption is critical to you, enable encryption of backups when creating a backup plan (Section 5.6 Encryption).

- Recovered virtual machines are always unencrypted. You can manually enable encryption after the recovery is complete.
- If you back up encrypted virtual machines, we recommend that you also encrypt the virtual machine where Agent for VMware is running. Otherwise, operations with encrypted machines may be slower than expected. Apply the **VM Encryption Policy** to the agent's machine by using vSphere Web Client.
- Encrypted virtual machines will be backed up via LAN, even if you configure the SAN transport mode for the agent. The agent will fall back on the NBD transport because VMware does not support SAN transport for backing up encrypted virtual disks.
- **Secure Boot** (introduced in VMware vSphere 6.5)

  Secure Boot is disabled after a virtual machine is recovered as a new virtual machine. You can manually enable this option after the recovery is complete.
- **ESXi configuration backup** is not supported for VMware vSphere 6.7.

1.2.8 Linux packages

To add the necessary modules to the Linux kernel, the setup program needs the following Linux packages:

- The package with kernel headers or sources. The package version must match the kernel version.
- The GNU Compiler Collection (GCC) compiler system. The GCC version must be the one with which the kernel was compiled.
- The Make tool.
- The Perl interpreter.
- The **`libelf-dev`**, **`libelf-devel`**, or **`elfutils-libelf-devel`** libraries for building kernels starting with 4.15 and configured with CONFIG_UNWINDER_ORC=y. For some distributions, such as Fedora 28, they need to be installed separately from kernel headers.

The names of these packages vary depending on your Linux distribution.

In Red Hat Enterprise Linux, CentOS, and Fedora, the packages normally will be installed by the setup program. In other distributions, you need to install the packages if they are not installed or do not have the required versions.

Are the required packages already installed?

To check whether the packages are already installed, perform these steps:

1. Run the following command to find out the kernel version and the required GCC version:

   ```
   cat /proc/version
   ```

   This command returns lines similar to the following: **`Linux version 2.6.35.6`** and **`gcc version 4.5.1`**
2. Run the following command to check whether the Make tool and the GCC compiler are installed:

   ```
   make -v
   gcc -v
   ```

   For **gcc**, ensure that the version returned by the command is the same as in the **`gcc version`** in step 1. For **make**, just ensure that the command runs.
3. Check whether the appropriate version of the packages for building kernel modules is installed:
   - In Red Hat Enterprise Linux, CentOS, and Fedora, run the following command:

     ```
     yum list installed | grep kernel-devel
     ```

- In Ubuntu, run the following commands:

```
dpkg --get-selections | grep linux-headers
dpkg --get-selections | grep linux-image
```

In either case, ensure that the package versions are the same as in **`Linux version`** in step 1.

4. Run the following command to check whether the Perl interpreter is installed:

```
perl --version
```

If you see the information about the Perl version, the interpreter is installed.

5. In Red Hat Enterprise Linux, CentOS, and Fedora, run the following command to check whether **`elfutils-libelf-devel`** is installed:

```
yum list installed | grep elfutils-libelf-devel
```

If you see the information about the library version, the library is installed.

Installing the packages from the repository

The following table lists how to install the required packages in various Linux distributions.

Linux distribution	Package names	How to install
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	The setup program will download and install the packages automatically by using your Red Hat subscription.
	perl	Run the following command: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	The setup program will download and install the packages automatically.
	perl	Run the following command: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Run the following commands:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source
	gcc
	make
	perl
		`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

The packages will be downloaded from the distribution's repository and installed.

For other Linux distributions, please refer to the distribution's documentation regarding the exact names of the required packages and the ways to install them.

Installing the packages manually

You may need to install the packages **manually** if:

- The machine does not have an active Red Hat subscription or Internet connection.
- The setup program cannot find the **kernel-devel** or **gcc** version corresponding to the kernel version. If the available **kernel-devel** is more recent than your kernel, you need to either update the kernel or install the matching **kernel-devel** version manually.
- You have the required packages on the local network and do not want to spend time for automatic search and downloading.

Obtain the packages from your local network or a trusted third-party website, and install them as follows:

- In Red Hat Enterprise Linux, CentOS, or Fedora, run the following command as the root user:
  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```
- In Ubuntu, run the following command:
  ```
  sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

Example: Installing the packages manually in Fedora 14

Follow these steps to install the required packages in Fedora 14 on a 32-bit machine:

1. Run the following command to determine the kernel version and the required GCC version:
   ```
   cat /proc/version
   ```
   The output of this command includes the following:
   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```
2. Obtain the **kernel-devel** and **gcc** packages that correspond to this kernel version:
   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```
3. Obtain the **make** package for Fedora 14:
   ```
   make-3.82-3.fc14.i686
   ```
4. Install the packages by running the following commands as the root user:
   ```
   rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   rpm -ivh gcc-4.5.1.fc14.i686.rpm
   rpm -ivh make-3.82-3.fc14.i686
   ```
   You can specify all these packages in a single **rpm** command. Installing any of these packages may require installing additional packages to resolve dependencies.

1.2.9 Compatibility with encryption software

There are no limitations on backing up and recovering data that is encrypted by *file-level* encryption software.

Disk-level encryption software encrypts data on the fly. This is why data contained in the backup is not encrypted. Disk-level encryption software often modifies system areas: boot records, or partition tables, or file system tables. These factors affect disk-level backup and recovery, the ability of the recovered system to boot and access to Secure Zone.

You can back up the data encrypted by the following disk-level encryption software:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption.

To ensure reliable disk-level recovery, follow the common rules and software-specific recommendations.

Common installation rule

The strong recommendation is to install the encryption software before installing the backup agents.

The way of using Secure Zone

Secure Zone must not be encrypted with disk-level encryption. This is the only way to use Secure Zone:

1. Install the encryption software; then, install the agent.
2. Create Secure Zone.
3. Exclude Secure Zone when encrypting the disk or its volumes.

Common backup rule

You can do a disk-level backup in the operating system. Do not try to back up using bootable media.

Software-specific recovery procedures

Microsoft BitLocker Drive Encryption

To recover a system that was encrypted by BitLocker:

1. Boot from the bootable media.
2. Recover the system. The recovered data will be unencrypted.
3. Reboot the recovered system.
4. Turn on BitLocker.

If you only need to recover one partition of a multi-partitioned disk, do so under the operating system. Recovery under bootable media may make the recovered partition undetectable for Windows.

McAfee Endpoint Encryption and PGP Whole Disk Encryption

You can recover an encrypted system partition by using bootable media only.

If the recovered system fails to boot, rebuild Master Boot Record as described in the following Microsoft knowledge base article: https://support.microsoft.com/kb/2622803

1.3 System requirements

The following table summarizes disk space and memory requirements for typical installation cases. The installation is performed with the default settings.

Components to be installed	Occupied disk space	Minimum memory consumption
Agent for Windows	850 MB	150 MB
Agent for Windows and one of the following agents: ▪ Agent for SQL ▪ Agent for Exchange	950 MB	170 MB

Agent for Windows and one of the following agents: ▪ Agent for VMware (Windows) ▪ Agent for Hyper-V	1170 MB	180 MB
Agent for Linux	720 MB	130 MB
Management Server in Windows	1.7 GB	200 MB
Management Server in Linux	0.6 GB	200 MB
Management Server and Agent for Windows	2.4 GB	360 MB
Management Server and agents on a machine running Windows, Microsoft SQL Server, Microsoft Exchange Server, and Active Directory Domain Services	3.35 GB	400 MB
Management Server and Agent for Linux	1.2 GB	340 MB

Note *To comply with FIPS certification standards, install backup agents for Windows on machines that support RDRAND CPU instructions.*
To comply with Common Criteria certification standards, install backup agents for Linux on operating systems that support D-bus.

While backing up, an agent typically consumes about 350 MB of memory (measured during a 500-GB volume backup). The peak consumption may reach 2 GB, depending on the amount and type of data being processed.

Bootable media or a disk recovery with a reboot requires at least 1 GB of memory.

A management server with one registered machine consumes 200 MB of memory. Each of the newly registered machines adds about 2 MB. Thus, a server with 100 registered machines consumes approximately 400 MB above the operating system and running applications. The maximum number of registered machines is 900-1000. This limitation originates from the management server's embedded SQLite.

You can overcome this limitation by specifying an external Microsoft SQL Server instance during the management server installation. With an external SQL database, up to 8000 machines can be registered without significant performance degradation. The SQL Server will then consume about 8 GB of RAM. For better backup performance, we recommend managing the machines by groups, with approximately 100 machines in each.

1.4 Supported file systems

A backup agent can back up any file system that is accessible from the operating system where the agent is installed. For example, Agent for Windows can back up and recover an ext4 file system if the corresponding driver is installed in Windows.

The following table summarizes the file systems that can be backed up and recovered. The limitations apply to both the agents and bootable media.

File system	Supported by			Limitations
	Agents	WinPE bootable media	Linux-based bootable media	

File system	Supported by			Limitations
	Agents	WinPE bootable media	Linux-based bootable media	
FAT16/32	All agents	+	+	No limitations
NTFS		+	+	
ext2/ext3/ext4		+	+	
JFS	Agent for Linux	-	+	▪ Files cannot be excluded from a disk backup ▪ Fast incremental/ differential backup cannot be enabled
ReiserFS3		-	+	
ReiserFS4		-	+	▪ Files cannot be excluded from a disk backup ▪ Fast incremental/ differential backup cannot be enabled ▪ Volumes cannot be resized during a recovery
ReFS	All agents	+	+	
XFS		+	+	
Linux swap	Agent for Linux	-	+	No limitations
exFAT	All agents	+	+ Bootable media cannot be used for recovery if the backup *is stored on* exFAT	▪ Only disk/volume backup is supported ▪ Files cannot be excluded from a backup ▪ Individual files cannot be recovered from a backup

The software automatically switches to the sector-by-sector mode when backing up drives with unrecognized or unsupported file systems. A sector-by-sector backup is possible for any file system that:

- is block-based
- spans a single disk
- has a standard MBR/GPT partitioning scheme

If the file system does not meet these requirements, the backup fails.

1.5 Limitations of the Acronis SCS Cyber Backup 12.5 Hardened Edition builds

Because Acronis SCS Cyber Backup 12.5 Hardened Edition is purpose-built to work with zero connectivity and has specific encryption and certification mechanisms, it has the following limitations related to them.

- Acronis SCS Cyber Backup 12.5 Hardened Edition Storage Node is not available.
- No support for Mac.
- No support for backups to cloud due to the restriction to access the Internet.
- Acronis SCS Cyber Backup 12.5 Hardened Edition appliance is not available.
- If you install Acronis SCS Cyber Backup 12.5 Hardened Edition on hardware that does not support RDRAND CPU instructions, Acronis SCS Cyber Backup 12.5 Hardened Edition will not be compliant to the FIPS certification standard.
- If you install Acronis SCS Cyber Backup 12.5 Hardened Edition on a Linux OS that does not support D-bus, Acronis SCS Cyber Backup 12.5 Hardened Edition will not be compliant to the Common Criteria certification requirements.

1.6 Installing the management server

1.6.1 Installation in Windows

To install the management server

1. Log on as an administrator and start the Acronis SCS Cyber Backup 12.5 Hardened Edition setup program.
2. Leave the default setting **Install a backup agent and Acronis SCS Cyber Backup 12.5 Hardened Edition Management Server**.
3. Do any of the following:
   - Click **Install Acronis SCS Cyber Backup 12.5 Hardened Edition**.
     This is the easiest way to install the product. Most of the installation parameters will be set to their default values.
     The following components will be installed:
     - Management Server
     - Components for Remote Installation
     - Monitoring Service
     - Agent for Windows
     - Other agents (Agent for Hyper-V, Agent for Exchange, Agent for SQL, and Agent for Active Directory), if the respective hypervisor or application is detected on the machine
     - Bootable Media Builder
     - Command-Line Tool
     - Backup Monitor
   - Click **Customize installation settings** to configure the setup.
     You will be able to select the components to be installed and to specify additional parameters. For details, refer to "Customizing installation settings" (Section 1.6.1.1).
   - Click **Create .mst and .msi files for unattended installation** to extract the installation packages. Review or modify the installation settings that will be added to the .mst file, and then click **Generate**. Further steps of this procedure are not required.
     If you want to deploy agents through Group Policy, refer to "Deploying agents through Group Policy" (Section 1.12).
4. Proceed with the installation.

5. After the installation completes, click **Close**.

1.6.1.1 Customizing installation settings

This section describes settings that can be changed during installation.

Common settings

- The components to be installed.
- The folder where the product will be installed.
- The accounts under which the services will run.

  You can choose one of the following:

  - **Use Service User Accounts** (default for the agent service)
    Service User Accounts are Windows system accounts that are used to run services. The advantage of this setting is that the domain security policies do not affect these accounts' user rights. By default, the agent runs under the **Local System** account.
  - **Create a new account** (default for the management server service)
    The account names will be **Acronis SCS Agent User**, and **AMS User** for the agent, and management server, respectively.
  - **Use the following account**
    If you install the product on a domain controller, the setup program prompts you to specify existing accounts (or the same account) for each service. For security reasons, the setup program does not automatically create new accounts on a domain controller.
    Also, choose this setting if you want the management server to use an existing Microsoft SQL server installed on a different machine and use Windows Authentication for the SQL Server.

  If you chose the **Create a new account** or **Use the following account** option, ensure that the domain security policies do not affect the related accounts' rights. If an account is deprived of the user rights assigned during the installation, the component may work incorrectly or not work.

Management server installation

- The database to be used by the management server. By default, the built-in SQLite database is used.

  You can select any edition of the following Microsoft SQL Server versions:

  - Microsoft SQL Server 2012
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2017 (running in Windows)

  The instance you choose can also be used by other programs.

  Before selecting an instance installed on another machine, ensure that SQL Server Browser Service and the TCP/IP protocol are enabled on that machine. For instructions on how to start SQL Server Browser Service, refer to: http://msdn.microsoft.com/en-us/library/ms189093.aspx. You can enable the TCP/IP protocol by using a similar procedure.
- The port that will be used by a web browser to access the management server (by default, 9877) and the port that will be used for communication between the product components (by default, 7780). Changing the latter port after the installation will require re-registering of all of the components.

Windows Firewall is configured automatically during the installation. If you use a different firewall, ensure that the ports are open for both incoming and outgoing requests through that firewall.

1.6.2 Installation in Linux

Preparation

1. Before installing the product on a system that does not use RPM Package Manager, such as an Ubuntu system, you need to install this manager manually; for example, by running the following command (as the root user): **`apt-get install rpm`**.
2. If you want to install Agent for Linux along with the management server, ensure that the necessary Linux packages (Section 1.2.8) are installed on the machine.
3. Choose the database to be used by the management server.

   By default, the built-in SQLite database is used. As an alternative, you can use PostgreSQL.

   Note *If you switch to PostgreSQL after the management server has been working for some time, you will have to add devices, configure backup plans and other settings from scratch.*

Installation

To install the management server

1. As the root user, run the installation file.
2. Accept the terms of the license agreement.
3. [Optional] Select the components that you want to install.

   By default, the following components will be installed:

   - Management Server
   - Agent for Linux
   - Bootable Media Builder
4. Specify the port that will be used by a web browser to access the management server. The default value is 9877.
5. Specify the port that will be used for communication between the product components. The default value is 7780.
6. Click **Next** to proceed with the installation.
7. After the installation completes, select **Open web console**, and then click **Exit**. The backup console will open in your default web browser.

1.6.3 Adding a machine running Linux

1. Click **All devices** > **Add**.
2. Click **Linux**. This will download the installation file.
3. On the machine that you want to protect, run the setup program locally (Section 1.8.2).

1.7 Adding machines via the web interface

To start adding a machine to the management server, click **All devices** > **Add**.

If the management server is installed in Linux, you will be asked to select the setup program based on the type of the machine that you want to add. Once the setup program is downloaded, run it locally on that machine.

Adding the machine

1. Click **All devices** > **Add**.
2. Click **Windows** or the button that corresponds to the application that you want to protect. Depending on the button you click, one of the following options is selected:
   - Agent for Windows
   - Agent for Hyper-V
   - Agent for SQL + Agent for Windows
   - Agent for Exchange + Agent for Windows
     If you clicked **Microsoft Exchange Server** > **Exchange mailboxes**, and at least one Agent for Exchange is already registered, you are taken directly to step 5.
   - Agent for Active Directory + Agent for Windows
3. Specify the host name or IP address of the machine, and the credentials of an account with administrative privileges on that machine.
4. Select the name or IP address that the agent will use to access the management server.
   By default, the server name is chosen. You may need to change this setting if the DNS server is unable to resolve the name to the IP address, which results in an agent registration failure.
5. Click **Add**.
6. If you clicked **Microsoft Exchange Server** > **Exchange mailboxes** in step 2, specify the machine where the **Client Access** server role (CAS) of Microsoft Exchange Server is enabled. For more information, refer to "Mailbox backup" (Section 11.4).

1.7.1.1 Requirements on User Account Control (UAC)

On a machine that is running Windows Vista or later and is not a member of an Active Directory domain, centralized management operations (including remote installation) require that UAC and UAC remote restrictions be disabled.

To disable UAC

Do one of the following depending on the operating system:

- **In a Windows operating system prior to Windows 8:**
  Go to **Control panel > View by: Small icons > User Accounts > Change User Account Control Settings**, and then move the slider to **Never notify**. Then, restart the machine.
- **In any Windows operating system**:
  1. Open Registry Editor.
  2. Locate the following registry key:
     HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
  3. For the **EnableLUA** value, change the setting to **0**.
  4. Restart the machine.

To disable UAC remote restrictions

1. Open Registry Editor.
2. Locate the following registry key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. For **LocalAccountTokenFilterPolicy** value, change the setting to **1**.
   If the **LocalAccountTokenFilterPolicy** value does not exist, create it as DWORD (32-bit). For more information about this value, refer to the Microsoft documentation:

https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Note *For security reasons, it is recommended that after finishing the management operation – for example, remote installation, both of the settings be reverted to their original state:* ***EnableLUA*****=1** *and* ***LocalAccountTokenFilterPolicy*** *=* ***0***

1.7.2 Adding a vCenter or an ESXi host

There are four methods of adding a vCenter or a stand-alone ESXi host to the management server:

- Deploying Agent for VMware (Virtual Appliance) (Section 1.7.2.1)
  This method is recommended in most cases. The virtual appliance will be automatically deployed to every host managed by the vCenter you specify. You can select the hosts and customize the virtual appliance settings.
- Installing Agent for VMware (Windows) (Section 1.7.2.2)
  You may want to install Agent for VMware on a physical machine running Windows for the purpose of an offloaded or LAN-free backup.
  - **Offloaded backup**
    Use if your production ESXi hosts are so heavily loaded that running the virtual appliances is not desirable.
  - **LAN-free backup**
    If your ESXi uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESXi host and LAN. For detailed instructions, refer to "LAN-free backup" (Section 14.2.2).

  If the management server is running in Windows, the agent will be automatically deployed to the machine you specify. Otherwise, you need to install the agent manually.
- Registering an already installed Agent for VMware (Section 1.7.2.3)
  This is a necessary step after you have re-installed the management server. Also, you can register and configure Agent for VMware (Virtual Appliance) that is deployed from an OVF template.
- Configuring an already registered Agent for VMware (Section 1.7.2.4)
  This is a necessary step after you have installed Agent for VMware (Windows) manually or deployed Acronis SCS Cyber Backup 12.5 Hardened Edition appliance. Also, you can associate an already configured Agent for VMware with another vCenter Server or stand-alone ESXi host.

1.7.2.1 Deploying Agent for VMware (Virtual Appliance) via the web interface

1. Click **All devices** > **Add**.
2. Click **VMware ESXi**.
3. Select **Deploy as a virtual appliance to each host of a vCenter**.
4. Specify the address and access credentials for the vCenter Server or stand-alone ESXi host. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges (Section 14.2.7) on the vCenter Server or ESXi.
5. Select the name or IP address that the agent will use to access the management server.
   By default, the server name is chosen. You may need to change this setting if the DNS server is unable to resolve the name to the IP address, which results in an agent registration failure.
6. [Optional] Click **Settings** to customize the deployment settings:

- ESXi hosts that you want to deploy the agent to (only if a vCenter Server was specified in the previous step).
- The virtual appliance name.
- The datastore where the appliance will be located.
- The resource pool or vApp that will contain the appliance.
- The network that the virtual appliance's network adapter will be connected to.
- Network settings of the virtual appliance. You can choose DHCP auto configuration or specify the values manually, including a static IP address.

7. Click **Deploy**.

1.7.2.2 Installing Agent for VMware (Windows)

Preparation

Follow the preparatory steps described in the "Adding a machine running Windows" (Section 1.7.1).

Installation

1. Click **All devices** > **Add**.
2. Click **VMware ESXi**.
3. Select **Remotely install on a machine running Windows**.
4. Specify the host name or IP address of the machine, and the credentials of an account with administrative privileges on that machine.
5. Select the name or IP address that the agent will use to access the management server.
   By default, the server name is chosen. You may need to change this setting if the DNS server is unable to resolve the name to the IP address, which results in an agent registration failure.
6. Click **Connect**.
7. Specify the address and credentials for the vCenter Server or stand-alone ESXi host, and then click **Connect**. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges (Section 14.5.1) on the vCenter Server or ESXi.
8. Click **Install** to install the agent.

1.7.2.3 Registering an already installed Agent for VMware

This section describes registering Agent for VMware via the web interface.

Alternative registration methods:

- You can register Agent for VMware (Virtual Appliance) by specifying the management server in the virtual appliance UI. See step 3 under "Configuring the virtual appliance" in the "Deploying Agent for VMware (Virtual Appliance) from an OVF template" section.
- Agent for VMware (Windows) is registered during its local installation (section 1.8.1).

To register Agent for VMware

1. Click **All devices** > **Add**.
2. Click **VMware ESXi**.
3. Select **Register an already installed agent**.
4. If you register *Agent for VMware (Windows)*, specify the host name or IP address of the machine where the agent is installed, and credentials of an account with administrative privileges on that machine.

If you register *Agent for VMware (Virtual Appliance)*, specify the host name or IP address of the virtual appliance, and credentials for the vCenter Server or the stand-alone ESXi host where the appliance is running.

5. Select the name or IP address that the agent will use to access the management server.
   By default, the server name is chosen. You may need to change this setting if the DNS server is unable to resolve the name to the IP address, which results in an agent registration failure.
6. Click **Connect**.
7. Specify the host name or IP address of the vCenter Server or the ESXi host, and credentials to access it, and then click **Connect**. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges (Section 14.5.1) on the vCenter Server or ESXi.
8. Click **Register** to register the agent.

1.7.2.4 Configuring an already registered Agent for VMware

This section describes how to associate Agent for VMware with a vCenter Server or ESXi in the web interface. As an alternative, you can do this in the Agent for VMware (Virtual Appliance) console.

By using this procedure, you can also change the existing association of the agent with a vCenter Server or ESXi. Alternatively, you can do this in the Agent for VMware (Virtual Appliance) console or by clicking **Settings** > **Agents** > the agent > **Details** > **vCenter/ESXi**.

To configure Agent for VMware

1. Click **All devices** > **Add**.
2. Click **VMware ESXi**.
3. The software shows the unconfigured Agent for VMware that appears first alphabetically.
   If all of the agents registered on the management server are configured, click **Configure an already registered agent**, and the software will show the agent that appears first alphabetically.
4. If necessary, click **Machine with agent** and select the agent to be configured.
5. Specify or change the host name or IP address of the vCenter Server or the ESXi host, and credentials to access it. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges (Section 14.5.1) on the vCenter Server or ESXi.
6. Click **Configure** to save the changes.

1.8 Installing agents locally

1.8.1 Installation in Windows

To install Agent for Windows, Agent for Hyper-V, Agent for Exchange, Agent for SQL, or Agent for Active Directory

1. Log on as an administrator and start the Acronis SCS Cyber Backup 12.5 Hardened Edition setup program.
2. Select **Install a backup agent**.
3. Do any of the following:
   - Click **Install Acronis SCS Cyber Backup 12.5 Hardened Edition**.
     This is the easiest way to install the product. Most of the installation parameters will be set to their default values.
     The following components will be installed:

- Agent for Windows
- Other agents (Agent for Hyper-V, Agent for Exchange, Agent for SQL, and Agent for Active Directory), if the respective hypervisor or application is detected on the machine
- Bootable Media Builder
- Command-Line Tool
- Backup Monitor

- Click **Customize installation settings** to configure the setup.
  You will be able to select the components to be installed and to specify additional parameters. For details, refer to "Customizing installation settings" (Section 1.6.1.1).
- Click **Create .mst and .msi files for unattended installation** to extract the installation packages. Review or modify the installation settings that will be added to the .mst file, and then click **Generate**. Further steps of this procedure are not required.
  If you want to deploy agents through Group Policy, proceed as described in "Deploying agents through Group Policy" (Section 1.12).

4. Specify the management server where the machine with the agent will be registered:
   a. Specify the host name or IP address of the machine where the management server is installed.
   b. Specify the credentials of a management server administrator or a registration token.
      For more information on how to generate a registration token, refer to "Deploying agents through Group Policy" (Section 1.12).
      If you are not a management server administrator, you still can register the machine, by selecting the **Connect without authentication** option. This works on the condition that the management server allows anonymous registration, which may be disabled (Section 18.5).
   c. Click **Done**.
5. If prompted, select whether the machine with the agent will be added to the organization or to one of the units.
   This prompt appears if you administer more than one unit, or an organization with at least one unit. Otherwise, the machine will be silently added to the unit you administer or to the organization. For more information, refer to "Administrators and units" (Section 19.1).
6. Proceed with the installation.
7. After the installation completes, click **Close**.
8. If you installed Agent for Exchange, you will be able to back up Exchange databases. If you want to back up Exchange mailboxes, open the backup console, click **Add** > **Microsoft Exchange Server** > **Exchange mailboxes**, and then specify the machine where the **Client Access** server role (CAS) of Microsoft Exchange Server is enabled. For more information, refer to "Mailbox backup" (Section 11.4)

To install Agent for VMware (Windows), Agent for Oracle, or Agent for Exchange on a machine without Microsoft Exchange Server

1. Log on as an administrator and start the Acronis SCS Cyber Backup 12.5 Hardened Edition setup program.
2. Select **Install a backup agent**, and then click **Customize installation settings**.
3. Next to **What to install**, click **Change**.
4. Select the check box corresponding to the agent that you want to install. Clear the check boxes for the components that you do not want to install. Click **Done** to continue.
5. Specify the management server where the machine with the agent will be registered:
   a. Next to **Acronis SCS Cyber Backup 12.5 Hardened Edition Management Server**, click **Specify**.

b. Specify the host name or IP address of the machine where the management server is installed.

c. Specify the credentials of a management server administrator or a registration token. For more information on how to generate a registration token, refer to "Deploying agents through Group Policy" (Section 1.12).
If you are not a management server administrator, you still can register the machine, by selecting the **Connect without authentication** option. This works on the condition that the management server allows anonymous registration, which may be disabled (Section 18.5).

d. Click **Done**.

6. If prompted, select whether the machine with the agent will be added to the organization or to one of the units.
This prompt appears if you administer more than one unit, or an organization with at least one unit. Otherwise, the machine will be silently added to the unit you administer or to the organization. For more information, refer to "Administrators and units" (Section 19.1).
7. [Optional] Change other installation settings as described in "Customizing installation settings" (Section 1.6.1.1).
8. Click **Install** to proceed with the installation.
9. After the installation completes, click **Close**.
10. [Only when installing Agent for VMware (Windows)] Perform the procedure described in "Configuring an already registered Agent for VMware" (Section 1.7.2.4).
11. [Only when installing Agent for Exchange] Open the backup console, click **Add** > **Microsoft Exchange Server** > **Exchange mailboxes**, and then specify the machine where the **Client Access** server role (CAS) of Microsoft Exchange Server is enabled. For more information, refer to "Mailbox backup" (Section 11.4).

1.8.2 Installation in Linux

Preparation

1. Before installing the product on a system that does not use RPM Package Manager, such as an Ubuntu system, you need to install this manager manually; for example, by running the following command (as the root user): **`apt-get install rpm`**.
2. Ensure that the necessary Linux packages (Section 1.2.8) are installed on the machine.

Installation

To install Agent for Linux, you need at least 2.0 GB of free disk space.

To install Agent for Linux

1. As the root user, run the appropriate installation file (an .i686 or an .x86_64 file).
2. Accept the terms of the license agreement.
3. Specify the components to install:
   a. Clear the **Acronis SCS Cyber Backup 12.5 Hardened Edition Management Server** check box.
   b. Select the check boxes for the agents that you want to install. The following agents are available:
      - **Agent for Linux**
      - **Agent for Oracle**

      Agent for Oracle requires that Agent for Linux is also installed.
   c. Click **Next**.

4. Specify the management server where the machine with the agent will be registered:
   a. Specify the host name or IP address of the machine where the management server is installed.
   b. Specify the user name and password of a management server administrator or choose anonymous registration.
      Specifying the credentials makes sense if your organization has units, in order to add the machine to the unit managed by the specified administrator. With anonymous registration, the machine is always added to the organization. For more information, refer to "Administrators and units" (Section 19.1).
      Specifying the credentials is necessary if anonymous registration on the management server is disabled (Section 18.5).
   c. Click **Next**.
5. If prompted, select whether the machine with the agent will be added to the organization or to one of the units, and then press **Enter**.
   This prompt appears if the account specified in the previous step administers more than one unit or an organization with at least one unit.
6. If UEFI Secure Boot is enabled on the machine, you are informed that you need to restart the system after the installation. Be sure to remember what password (the one of the root user or "acronis") should be used.

   Note *During the installation, the Acronis key is generated, used to sign the* ***`snapapi`*** *module, and registered as a Machine Owner Key (MOK). The restart is mandatory in order to enroll this key. Without enrolling the key, the agent will not be operational. If you enable UEFI Secure Boot after the agent installation, repeat the installation including step 6.*

7. After the installation completes, do one of the following:
   - Click **Restart**, if you were prompted to restart the system in the previous step.
     During the system restart, opt for MOK (Machine Owner Key) management, choose **Enroll MOK**, and then enroll the key by using the password recommended in the previous step.
   - Otherwise, click **Exit**.

Troubleshooting information is provided in the file:
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

1.9 Unattended installation or uninstallation

1.9.1 Unattended installation or uninstallation in Windows

This section describes how to install or uninstall Acronis SCS Cyber Backup 12.5 Hardened Edition in the unattended mode on a machine running Windows, by using Windows Installer (the **`msiexec`** program). In an Active Directory domain, another way of performing unattended installation is through Group Policy—see "Deploying agents through Group Policy" (Section 1.12).

During the installation, you can use a file known as a **transform** (an .mst file). A transform is a file with installation parameters. As an alternative, you can specify installation parameters directly in the command line.

Creating the .mst transform and extracting the installation packages

1. Log on as an administrator and start the setup program.
2. Click **Create .mst and .msi files for unattended installation**.

3. In **What to install**, select the components that you want to install. The installation packages for these components will be extracted from the setup program.
4. Review or modify other installation settings that will be added to the .mst file.
5. Click **Generate**.

As a result, the .mst transform is generated and the .msi and .cab installation packages are extracted to the folder you specified.

Installing the product by using the .mst transform

Run the following command:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Here:

- `<package name>` is the name of the .msi file. This name is **AB_SCS.msi** or **AB_SCS64.msi**, depending on the operating system bitness.
- `<transform name>` is the name of the transform. This name is **AB_SCS.msi.mst** or **AB_SCS64.msi.mst**, depending on the operating system bitness.

For example, **`msiexec /i AB_SCS64.msi TRANSFORMS=AB_SCS64.msi.mst`**

Installing or uninstalling the product by specifying parameters manually

Run the following command:

```
msiexec /i <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Here, `<package name>` is the name of the .msi file. This name is **AB.msi** or **AB64.msi**, depending on the operating system bitness.

*The supplemental SSL installer needs to be run per machine the MSI is deployed to.

Available parameters and their values are described in "Unattended installation or uninstallation parameters" (Section 1.9.1.1).

Examples

- Installing Management Server and Components for Remote Installation.
```
msiexec.exe /i AB_SCS64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature T
ARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress
AMS_USE_SYSTEM_ACCOUNT=1
```
- Installing Agent for Windows, Command-Line Tool, and Backup Monitor. Registering the machine with the agent on a previously installed management server.
```
msiexec.exe /i AB_SCS64.msi /l*v my_log.txt /qn
ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonito r
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress
MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
```

1.9.1.1 Unattended installation or uninstallation parameters

This section describes parameters that are used during unattended installation or uninstallation in Windows.

In addition to these parameters, you can use other parameters of **`msiexec`**, as described at https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Installation parameters

Common parameters

ADDLOCAL=<list of components>

The components to be installed, separated by commas without space characters. All of the specified components must be extracted from the setup program prior to installation.

The full list of the components is as follows.

Component	Must be installed together with	Bitness	Component name / description
AcronisCentralizedManagementServer	WebConsole	32-bit/64-bit	Management Server
WebConsole	AcronisCentralizedManagementServer	32-bit/64-bit	Web Console
MonitoringServer	AcronisCentralizedManagementServer	32-bit/64-bit	Monitoring Service
ComponentRegisterFeature	AcronisCentralizedManagementServer	32-bit/64-bit	Components for Remote Installation
AgentsCoreComponents		32-bit/64-bit	Core components for agents
BackupAndRecoveryAgent	AgentsCoreComponents	32-bit/64-bit	Agent for Windows
ArxAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for SQL
ARADAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Oracle
AcronisESXSupport	AgentsCoreComponents	32-bit/64-bit	Agent for VMware (Windows)
HyperVAgent	AgentsCoreComponents	32-bit/64-bit	Agent for Hyper-V
ESXVirtualAppliance		32-bit/64-bit	Agent for VMware (Virtual Appliance)
CommandLineTool		32-bit/64-bit	Command-Line Tool
TrayMonitor	BackupAndRecoveryAgent	32-bit/64-bit	Backup Monitor
BackupAndRecoveryBootableComponents		32-bit/64-bit	Bootable Media Builder
PXEServer		32-bit/64-bit	PXE Server

TARGETDIR=<path>

The folder where the product will be installed.

REBOOT=ReallySuppress

If the parameter is specified, the machine reboot is forbidden.

REGISTRATION_ADDRESS=<host name or IP address>:<port>

The host name or IP address of the machine where the management server is installed. Agents specified in the **ADDLOCAL** parameter will be registered on this management server. The port number is mandatory if it is different from the default value (9877).

If anonymous registration on the management server is disabled (Section 18.5), you must specify either the **REGISTRATION_TOKEN** parameter, or the **REGISTRATION_LOGIN** and **REGISTRATION_PASSWORD** parameters.

REGISTRATION_TOKEN=<token>

The registration token that was generated in the backup console as described in Deploying agents through Group Policy (Section 1.12).

REGISTRATION_LOGIN=<user name>, **REGISTRATION_PASSWORD=**<password>

The user name and password of a management server administrator.

REGISTRATION_TENANT=<unit ID>

The unit within the organization. Agents specified in the **ADDLOCAL** parameter will be added to this unit.

To learn a unit ID, in the backup console, click **Settings** > **Administrators**, select the unit, and click **Details**.

This parameter does not work without **REGISTRATION_TOKEN**, or **REGISTRATION_LOGIN** and **REGISTRATION_PASSWORD**. In this case, the components will be added to the organization.

Without this parameter, the components will be added to the organization.

REGISTRATION_REQUIRED={0,1}

The installation result in case the registration fails. If the value is **1**, the installation fails. If the value is **0**, the installation completes successfully even though the component was not registered.

REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<public key value>

These mutually exclusive parameters define the method of the management server certificate check during the registration. Check the certificate if you want to verify the authenticity of the management server to prevent MITM attacks.

If the value is **1**, the verification uses the system CA, or the CA bundle delivered with the product, correspondingly. If a pinned public key is specified, the verification uses this key. If the value is **0** or the parameters are not specified, the certificate verification is not performed, but the registration traffic remains encrypted.

/l*v <log file>

If the parameter is specified, the installation log in the verbose mode will be saved to the specified file. The log file can be used for analyzing the installation issues.

Management server installation parameters

WEB_SERVER_PORT=<port number>

The port that will be used by a web browser to access the management server. By default, 9877.

AMS_ZMQ_PORT=<port number>

The port that will be used for communication between the product components. By default, 7780.

SQL_INSTANCE=<instance>

The database to be used by the management server. You can select any edition of Microsoft SQL Server 2012, Microsoft SQL Server 2014, or Microsoft SQL Server 2016. The instance you choose can also be used by other programs.

Without this parameter, the built-in SQLite database will be used.

SQL_USER_NAME=<user name> and **SQL_PASSWORD=**<password>

Credentials of a Microsoft SQL Server login account. The management server will use these credentials to connect to the selected SQL Server instance. Without these parameters, the management server will use the credentials of the management server service account (**AMS User**).

Account under which the management server service will run

Specify one of the following parameters:

- **AMS_USE_SYSTEM_ACCOUNT={0,1}**
  If the value is **1**, the system account will be used.
- **AMS_CREATE_NEW_ACCOUNT={0,1}**
  If the value is **1**, a new account will be created.
- **AMS_SERVICE_USERNAME=**<user name> and **AMS_SERVICE_PASSWORD=**<password>
  The specified account will be used.

Agent installation parameters

SET_ESX_SERVER={0,1}

If the value is **0**, Agent for VMware being installed will not be connected to a vCenter Server or an ESXi host. After the installation, proceed as described in "Configuring an already registered Agent for VMware" (Section 1.7.2.4).

If the value is **1**, specify the following parameters:

ESX_HOST=<host name or IP address>

The host name or IP address of the vCenter Server or the ESXi host.

ESX_USER=<user name> and **ESX_PASSWORD=**<password>

Credentials to access the vCenter Server or ESXi host.

Account under which the agent service will run

Specify one of the following parameters:

- **MMS_USE_SYSTEM_ACCOUNT={0,1}**
  If the value is **1**, the system account will be used.
- **MMS_CREATE_NEW_ACCOUNT={0,1}**
  If the value is **1**, a new account will be created.
- **MMS_SERVICE_USERNAME=**<user name> and **MMS_SERVICE_PASSWORD=**<password>
  The specified account will be used.

Uninstallation parameters

REMOVE={<list of components>**|ALL}**

The components to be removed, separated by commas without space characters.

Available components are described earlier in this section.

If the value is **ALL**, all of the product components will be uninstalled. Additionally, you can specify the following parameter:

DELETE_ALL_SETTINGS={0, 1}

If the value is **1**, the product's logs, tasks, and configuration settings will be removed.

1.9.2 Unattended installation or uninstallation in Linux

This section describes how to install or uninstall Acronis SCS Cyber Backup 12.5 Hardened Edition in the unattended mode on a machine running Linux, by using the command line.

To install or uninstall the product

1. Open Terminal.
2. Run the following command:

   ```
   <package name> -a <parameter 1> ... <parameter N>
   ```

   Here, `<package name>` is the name of the installation package (an .i686 or an .x86_64 file).
3. [Only when installing Agent for Linux] If UEFI Secure Boot is enabled on the machine, you are informed that you need to restart the system after the installation. Be sure to remember what password (the one of the root user or "acronis") should be used. During the system restart, opt for MOK (Machine Owner Key) management, choose **Enroll MOK**, and then enroll the key by using the recommended password.

If you enable UEFI Secure Boot after the agent installation, repeat the installation including step 3. Otherwise, backups will fail.

Installation parameters

Common parameters

{-i |--id=}`<list of components>`

The components to be installed, separated by commas without space characters.

The following components are available for installation:

Component	Component description
AcronisCentralizedManagementServer	Management Server
BackupAndRecoveryAgent	Agent for Linux
BackupAndRecoveryBootableComponents	Bootable Media Builder
MonitoringServer	Monitoring Service

Without this parameter, all of the above components will be installed.

{-d|--debug}

If the parameter is specified, the installation log is written in the verbose mode. The log is located in the file **/var/log/trueimage-setup.log**.

{-t|--strict}

If the parameter is specified, any warning that occurs during the installation results in the installation failure. Without this parameter, the installation completes successfully even in the case of warnings.

{-n|--nodeps}

If the parameter is specified, absence of required Linux packages will be ignored during the installation.

Management server installation parameters

{-W |--web-server-port=}<port number>

The port that will be used by a web browser to access the management server. By default, 9877.

--ams-tcp-port=<port number>

The port that will be used for communication between the product components. By default, 7780.

Agent installation parameters

Specify one of the following parameters:

- **--skip-registration**

  Do not register the agent on the management server.

- **{-C |--ams=}**<host name or IP address>

  The host name or IP address of the machine where the management server is installed. The agent will be registered on this management server.

  If you install the agent and the management server within one command, the agent will be registered on this management server regardless of the **-C** parameter.

  If anonymous registration on the management server is disabled (Section 18.5), you must specify either the **token** parameter, or the **login** and **password** parameters.

  --token=<token>

  The registration token that was generated in the backup console as described in Deploying agents through Group Policy (Section 1.12).

  {-g |--login=}<user name> and **{-w |--password=}**<password>

  Credentials of a management server administrator.

  --unit=<unit ID>

  The unit within the organization. The agent will be added to this unit.

  To learn a unit ID, in the backup console, click **Settings** > **Administrators**, select the unit, and click **Details**.

  Without this parameter, the agent will be added to the organization.

  --reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}

  The method of the management server certificate check during the registration. Check the certificate if you want to verify the authenticity of the management server to prevent MITM attacks.

  If the value is **https** or the parameter is not specified, the certificate check is not performed, but the registration traffic remains encrypted. If the value is *not* **https**, the check uses the system CA, or the CA bundle delivered with the product or the pinned public key, correspondingly.

  --reg-transport-pinned-public-key=<public key value>

  The pinned public key value. This parameter should be specified together or instead of the **--reg-transport=https-pinned-public-key** parameter.

Uninstallation parameters

{-u|--uninstall}

Uninstalls the product.

--purge -a

Removes the product's logs, tasks, plans, vaults, and configuration settings.

Information parameters

{-?|--help}

Shows the description of parameters.

--usage

Shows a brief description of the command usage.

{-v|--version}

Shows the installation package version.

--product-info

Shows the product name and the installation package version.

Examples

- Installing Management Server.

```
./AcronisBackup_12.5_SCS_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Installing Management Server and Monitoring Service. Specifying custom ports.

```
./AcronisBackup_12.5_SCS_64-bit.x86_64 -a -i
AcronisCentralizedManagementServer,MonitoringServer --web-server-port 6543
--ams-tcp-port 8123
```

- Installing Agent for Linux and registering it on the specified management server.

```
./AcronisBackup_12.5_SCS_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams
10.10.1.1 --login root --password 123456
```

- Installing Agent for Linux and registering it on the specified management server, in the specified unit.

```
./AcronisBackup_12.5_SCS_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams
10.10.1.1 --login root --password 123456 –unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

1.10 Deploying Agent for VMware (Virtual Appliance) from an OVF template

The Agent for VMware (Virtual Appliance) is provided as an .ovf template ready to be deployed to VMware vSphere ESXi hosts versions 6.0 or higher. For ESXi versions 4.1, 5.0, 5.1, and 5.5, use the Agent for VMware (Windows).

1.10.1 Before you start

System requirements for the agent

By default, the virtual appliance is assigned 4 GB of RAM and 2 vCPUs, which is optimal and sufficient for most operations.

We recommend increasing these resources to 8 GB of RAM and 4 vCPUs if the backup traffic bandwidth is expected to exceed 100 MB per second (for example, in 10-GBit networks), in order to improve backup performance.

The appliance's own virtual disks occupy no more than 6 GB. Thick or thin disk format does not matter, it does not affect the appliance performance.

How many agents do I need?

Even though one virtual appliance is able to protect an entire vSphere environment, the best practice is deploying one virtual appliance per vSphere cluster (or per host, if there are no clusters). This makes for faster backups because the appliance can attach the backed-up disks by using the HotAdd transport, and therefore the backup traffic is directed from one local disk to another.

It is normal to use both the virtual appliance and Agent for VMware (Windows) at the same time, as long as they are connected to the same vCenter Server *or* they are connected to different ESXi hosts. Avoid cases when one agent is connected to an ESXi directly and another agent is connected to the vCenter Server which manages this ESXi.

We do not recommend using locally attached storage (i.e. storing backups on virtual disks added to the virtual appliance) if you have more than one agent. For more considerations, see "Using a locally attached storage" (Section 14.2.4).

Disable automatic DRS for the agent

If the virtual appliance is deployed to a vSphere cluster, be sure to disable automatic vMotion for it. In the cluster DRS settings, enable individual virtual machine automation levels, and then set **Automation level** for the virtual appliance to **Disabled**.

1.10.2 Deploying the OVF template

Location of the OVF template

The OVF template consists of one .ovf file and two .vmdk files.

After the management server is installed, the OVF package of the virtual appliance is located in the following folder.

- In Windows: **%ProgramFiles%\Acronis\ESXAppliance**
- In Linux: **/usr/lib/Acronis/ESXAppliance**

Deploying the OVF template

The instructions in this section apply to VMware vSphere Host Client connected to a standalone VMware ESXi host version 6.5. The OVF deployment steps for other vSphere versions and/or different vSphere setups may vary. Please refer to the VMware documentation portal for details.

1. Verify that the OVF template files of Agent for VMware (Virtual Appliance) can be accessed from the machine where the vSphere Client is running.
2. Connect the VMware vSphere Client to the ESXi host.
3. Click **Create/register VM** and select **Deploy a virtual machine from an OVF or OVA file**.
4. Browse and select the OVF and VMDK files of Agent for VMware (Virtual Appliance) and enter a name for the deployed virtual machine.
5. Follow the steps in the OVF deployment wizard to configure storage and other deployment options.
   - When configuring storage, select the shared datastore, if it exists.
   - The disk provisioning format does not affect the performance of the appliance, so you can select **Thin** to save space.
   - When configuring network connections, be sure to select a network that includes the management server, so that the agent can properly register itself.
6. Review the summary and click **Finish**.

1.10.3 Configuring the virtual appliance

After you deploy the OVF template of the backup Agent for VMware (Virtual Appliance), you have to configure the appliance.

1. **Starting the virtual appliance**
   a. In the vSphere Client Navigator, right-click the virtual appliance that you deployed, and select **Power** > **Power On**.
   b. Click the **Console** tab.
2. **Proxy server**

   Follow this procedure if a proxy server is enabled in your network. Otherwise, skip to the next step.
   a. To start the command shell, press CTRL+SHIFT+F2 while in the virtual appliance console.
   b. Open the file **/etc/Acronis/Global.config** in a text editor.
   c. Find the following section:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"0"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

   d. Replace **0** with **1**.
   e. Replace ADDRESS with the new proxy server host name/IP address, and PORT with the decimal value of the port number.
   f. If your proxy server requires authentication, replace LOGIN and PASSWORD with the proxy server credentials. Otherwise, delete these lines from the file.
   g. Save the file.
   h. Execute the **reboot** command.
3. **Network settings**

   The agent's network connection is configured automatically by using Dynamic Host Configuration Protocol (DHCP). To change the default configuration, under **Agent options**, in **eth0**, click **Change** and specify the desired network settings.
4. **vCenter/ESXi**
   a. Under **Agent options**, in **vCenter/ESX(i)**, click **Change** and specify the name or IP address of the vCenter Server or the ESXi host whose virtual machines you want to back up and recover.
      - If you use vCenter Server, the agent will be able to back up and recover any virtual machine managed by the vCenter Server.
      - If you use an ESXi host, the agent will be able to backup and recover any virtual machines on the ESXi host. Normally, backups run faster when the agent backs up virtual machines hosted on its own ESXi host.

   b. Specify the credentials that the agent will use to connect to the vCenter Server or ESXi. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges (Section 14.5.1) on the vCenter Server or ESXi.
   c. Click **Check connection** to ensure the access credentials are correct.
5. **Management server**
   a. Under **Agent options**, in **Management Server**, click **Change**.

b. In **Server name/IP**, select **Local**. Specify the host name or IP address of the machine where the management server is installed.

c. In **User name** and **Password**, specify the user name and password of a management server administrator.

6. **Time zone**
   a. Under **Virtual machine**, in **Time zone**, click **Change**.
   b. Select the time zone of your location to ensure that the scheduled operations run at the appropriate time.
7. **[Optional] Local storages**
   You can attach an additional disk to the virtual appliance so the Agent for VMware can back up to this locally attached storage (Section 14.2.4).
   a. Add the disk by editing the settings of the virtual machine and click **Refresh**. The **Create storage** link becomes available.
   b. Click this link, select the disk, and then specify a label for it.
8. **Disable vMotion for the virtual appliance**
   If you deploy Agent for VMware (Virtual Appliance) in a vSphere HA cluster environment, disable automatic vSphere vMotion for this virtual machine.
   a. In the vSphere cluster settings, under **vSphere DRS**, expand the **DRS Automation** section.
   b. Under **Virtual Machine Automation**, select the **Enable individual virtual machine automation levels** check box and click **OK**.
   c. Click the **Configuration** tab of the vSphere HA cluster, select **VM Overrides**, and click **Add**.
   d. Use the + button to select the Agent for VMware (Virtual Appliance) machine to apply the overrides.
   e. Click **OK**.

1.11 Managing licenses

Licensing of Acronis SCS Cyber Backup 12.5 Hardened Edition is based on the number of the backed-up physical machines and virtualization hosts.

To start using Acronis SCS Cyber Backup 12.5 Hardened Edition, you need to add at least one license key to the management server. A license is automatically assigned to a machine when a backup plan is applied.

Licenses can also be assigned and revoked manually. Manual operations with licenses are available only to organization administrators (Section 19.1).

To access the Licenses page

1. Do one of the following:
   - Click **Settings**.
   - Click the account icon in the top-right corner.
2. Click **Licenses**.

To add a license key

1. Click **Add keys**.
2. Enter the license keys.
3. Click **Add**.
4. Click **Done**.

Managing licenses

To assign a license to a machine

1. Select a license.

   The software displays the license keys that correspond to the selected license.
2. Select the key to assign.
3. Click **Assign**.

   The software displays the machines that the selected key can be assigned to.
4. Select the machine, and then click **Done**.

To revoke a license from a machine

1. Select a license.

   The software displays the license keys that correspond to the selected license. The machine that the key is assigned to is shown in the **Assigned to** column.
2. Select the license key to revoke.
3. Click **Revoke**.
4. Confirm your decision.

   The revoked key will remain in the license keys list. It can be assigned to another machine.

1.12 Deploying agents through Group Policy

You can centrally install (or deploy) Agent for Windows onto machines that are members of an Active Directory domain, by using Group Policy.

In this section, you will find out how to set up a Group Policy object to deploy agents onto machines in an entire domain or in its organizational unit.

Every time a machine logs on to the domain, the resulting Group Policy object will ensure that the agent is installed and registered.

Prerequisites

Before proceeding with agent deployment, ensure that:

- You have an Active Directory domain with a domain controller running Microsoft Windows Server 2003 or later.
- You are a member of the **Domain Admins** group in the domain.
- You have downloaded the **All agents for installation in Windows** setup program. The download link is available on the **Add devices** page in the backup console.

Step 1: Generating a registration token

A registration token passes your identity to the setup program without storing your login and password for the backup console. This enables you to register any number of machines under your account. For more security, a token has limited lifetime.

To generate a registration token

1. Sign in to the backup console by using the credentials of the account to which the machines should be assigned.
2. Click **All devices** > **Add**.
3. Scroll down to **Registration token**, and then click **Generate**.
4. Specify the token lifetime, and then click **Generate token**.

5. Copy the token or write it down. Be sure to save the token if you need it for further use.

   You can click **Manage active tokens** to view and manage the already generated tokens. Please be aware that for security reasons, this table does not display full token values.

Step 2: Creating the .mst transform and extracting the installation package

1. Log on as an administrator on any machine in the domain.
2. Create a shared folder that will contain the installation packages. Ensure that domain users can access the shared folder—for example, by leaving the default sharing settings for **Everyone**.
3. Start the setup program.
4. Click **Create .mst and .msi files for unattended installation**.
5. Review or modify the installation settings that will be added to the .mst file. When specifying the method of connection to the management server, select **Use a registration token**, and then enter the token you generated.
6. Click **Proceed**.
7. In **Save the files to**, specify the path to the folder you created.
8. Click **Generate**.

As a result, the .mst transform is generated and the .msi and .cab installation packages are extracted to the folder you created.

*The supplemental SSL installer needs to be run per machine the MSI is deployed to.

Step 3: Setting up the Group Policy objects

1. Log on to the domain controller as a domain administrator; if the domain has more than one domain controller, log on to any of them as a domain administrator.
2. If you are planning to deploy the agent in an organizational unit, ensure that the organizational unit exists in the domain. Otherwise, skip this step.
3. In the **Start** menu, point to **Administrative Tools**, and then click **Active Directory Users and Computers** (in Windows Server 2003) or **Group Policy Management** (in Windows Server 2008 or later).
4. In Windows Server 2003:
   - Right-click the name of the domain or organizational unit, and then click **Properties**. In the dialog box, click the **Group Policy** tab, and then click **New**.

   In Windows Server 2008 or later:
   - Right-click the name of the domain or organizational unit, and then click **Create a GPO in this domain, and Link it here**.
5. Name the new Group Policy object **Agent for Windows.**
6. Open the **Agent for Windows** Group Policy object for editing, as follows:
   - In Windows Server 2003, click the Group Policy object, and then click **Edit**.
   - In Windows Server 2008 or later, under **Group Policy Objects**, right-click the Group Policy object, and then click **Edit**.
7. In the Group Policy object editor snap-in, expand **Computer Configuration**.
8. In Windows Server 2003 and Windows Server 2008:
   - Expand **Software Settings**.

   In Windows Server 2012 or later:
   - Expand **Policies** > **Software Settings**.
9. Right-click **Software installation**, then point to **New**, and then click **Package**.

5. If you are planning to install the agent again, skip this step. Otherwise, in the backup console, click **Settings** > **Agents**, select the machine where the agent was installed, and then click **Delete**.

In Linux

1. As the root user, run **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Optional] Select the **Clean up all product traces (Remove the product's logs, tasks, vaults, and configuration settings)** check box.

   Keep this check box cleared if you are uninstalling an agent and are planning to install it again. If you select the check box, the machine may be duplicated in the backup console and the backups of the old machine may not be associated with the new machine.
3. Confirm your decision.
4. If you are planning to install the agent again, skip this step. Otherwise, in the backup console, click **Settings** > **Agents**, select the machine where the agent was installed, and then click **Delete**.

Removing Agent for VMware (Virtual Appliance)

1. Start the vSphere Client and log on to the vCenter Server.
2. If the virtual appliance (VA) is powered on, right-click it, and then click **Power** > **Power Off**. Confirm your decision.
3. If the VA uses a locally attached storage on a virtual disk and you want to preserve data on that disk, do the following:
   a. Right-click the VA, and then click **Edit Settings**.
   b. Select the disk with the storage, and then click **Remove**. Under **Removal Options**, click **Remove from virtual machine**.
   c. Click **OK**.

   As a result, the disk remains in the datastore. You can attach the disk to another VA.
4. Right-click the VA, and then click **Delete from Disk**. Confirm your decision.
5. If you are planning to install the agent again, skip this step. Otherwise, in the backup console, click **Settings** > **Agents**, select the virtual appliance, and then click **Delete**.

This is the easiest way to sign in from the same machine where the management server is installed.

If the management server is installed on a different machine, this method works on the conditions that:

- The machine you are signing in from is in the same Active Directory domain as the management server.
- You are logged on as a domain user.

We recommend configuring your web browser for Integrated Windows Authentication (Section 3.1). Otherwise, the browser will ask for a user name and password.

- Click **Enter user name and password**, and then specify the user name and password.

In any case, your account must be in the list of the management server administrators. By default, this list contains the **Administrators** group on the machine running the management server. For more information, refer to "Administrators and units" (Section 19.1).

In Linux

If the management server is installed in Linux, specify the user name and password of an account that is in the list of the management server administrators. By default, this list contains only the **root** user on the machine running the management server. For more information, refer to "Administrators and units" (Section 19.1).

3.1 Configuring a web browser for Integrated Windows Authentication

Integrated Windows Authentication is possible if you access the backup console from a machine running Windows and any supported browser (Section 1.2.2).

We recommend configuring your web browser for Integrated Windows Authentication. Otherwise, the browser will ask for a user name and password.

Configuring Internet Explorer, Microsoft Edge, Opera, and Google Chrome

If the machine running the browser is in the same Active Directory domain as the machine running the management server, add the console's login page to the list of **Local intranet** sites.

Otherwise, add the console's login page to the list of **Trusted sites** and enable the **Automatic logon with current user name and password** setting.

The step-by-step instructions are provided later in this section. Because these browsers use Windows settings, it is also possible to configure them by using Group Policy in an Active Directory domain.

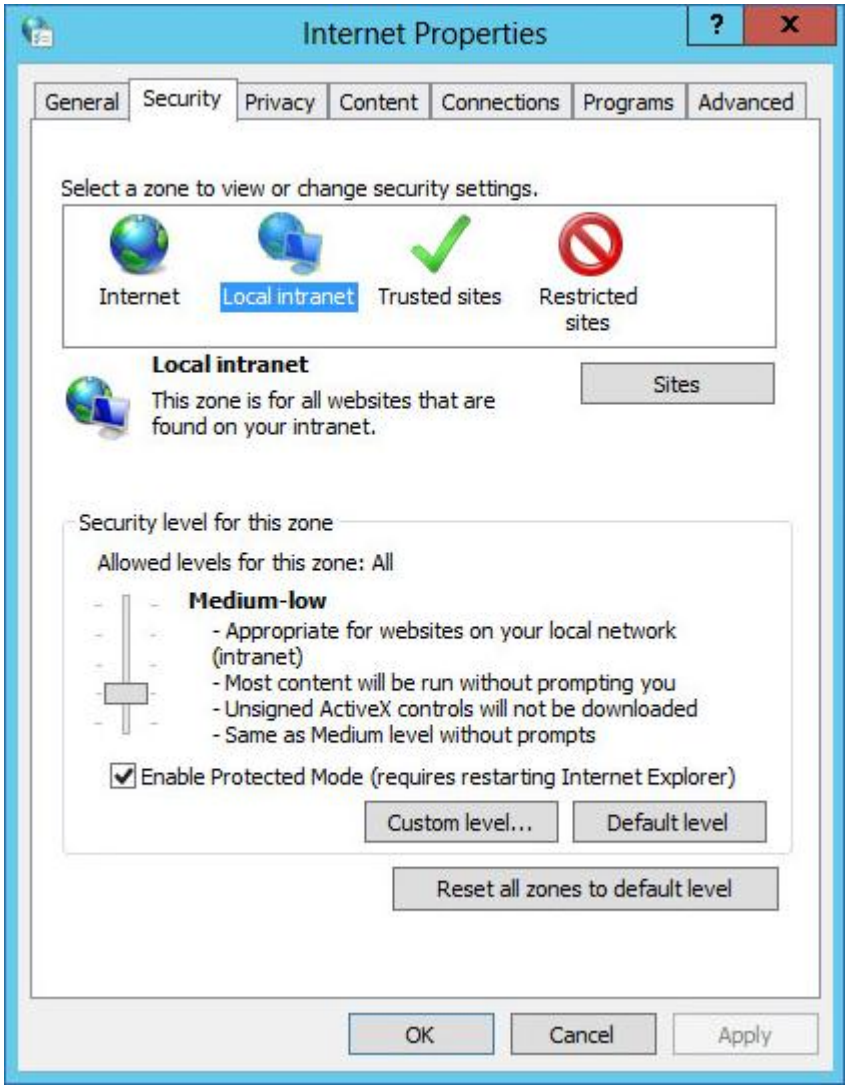
Configuring Mozilla Firefox

1. In Firefox, navigate to the URL `about:config`, and then click the **I accept the risk** button.
2. In the **Search** field, search for the `network.negotiate-auth.trusted-uris` preference.
3. Double-click the preference, and then enter the address of the backup console login page.
4. Repeat steps 2-3 for the `network.automatic-ntlm-auth.trusted-uris` preference.
5. Close the `about:config` window.

3.1.1 Adding the console to the list of local intranet sites

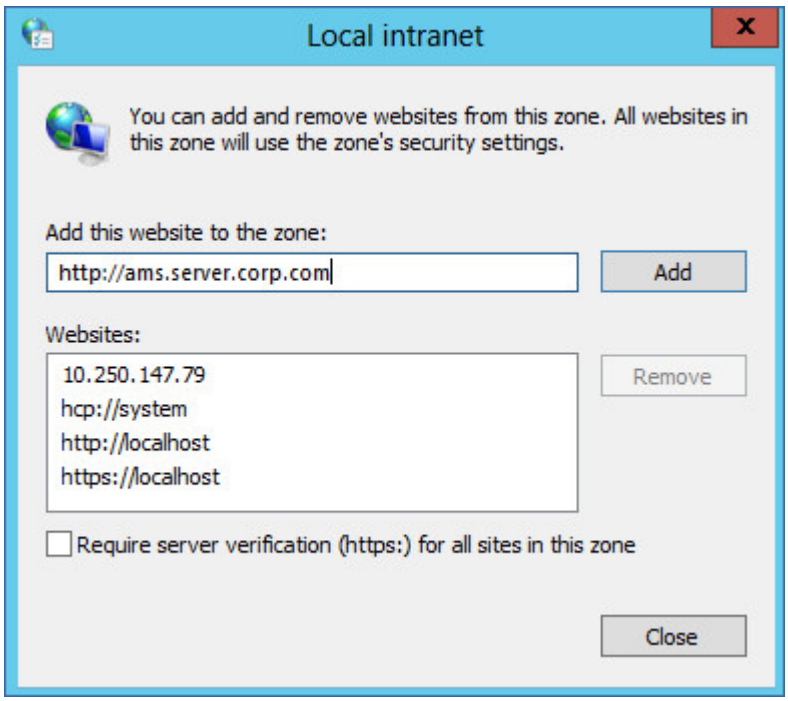
1. Go to **Control Panel** > **Internet Options**.

2. On the **Security** tab, select **Local intranet**.



3. Click **Sites**.

4. In **Add this website to the zone**, enter the address of the backup console login page, and then click **Add**.

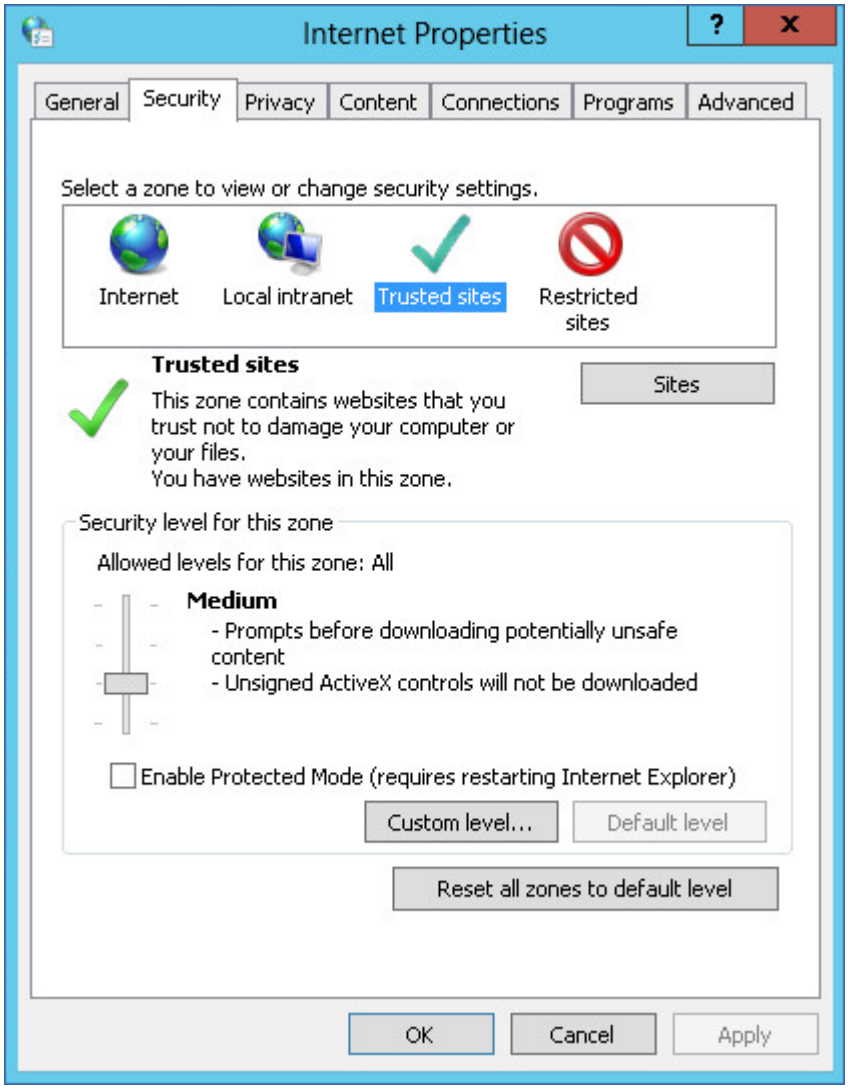


5. Click **Close**.
6. Click **OK**.

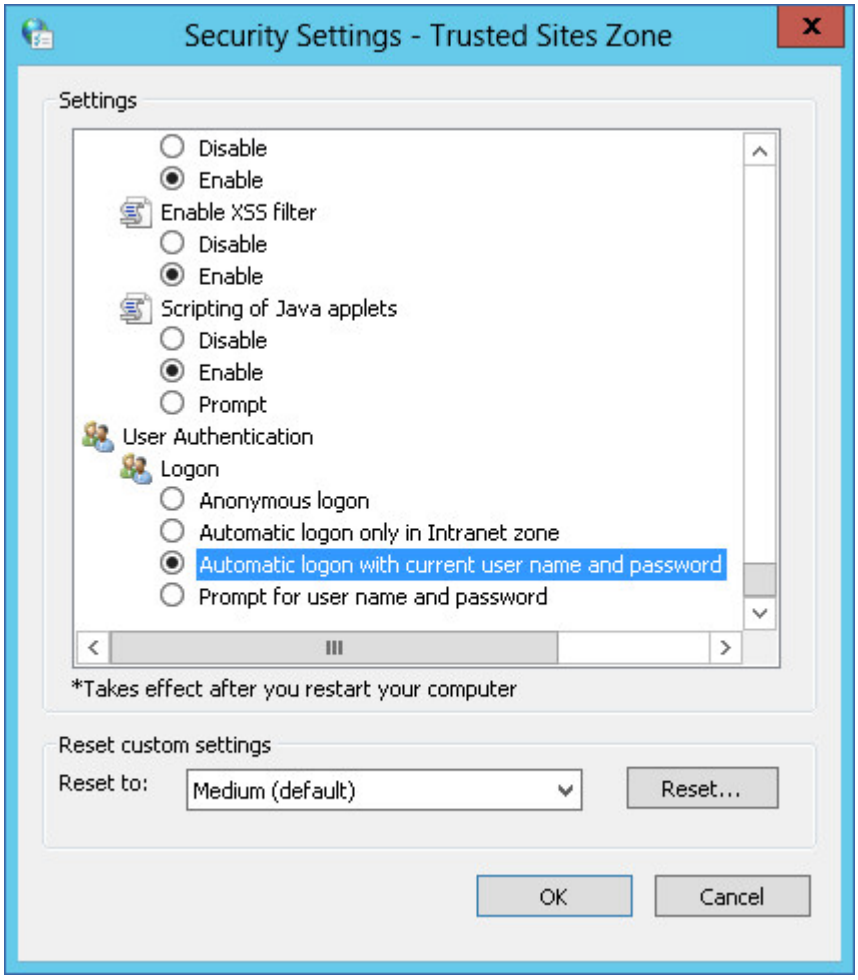
3.1.2 Adding the console to the list of trusted sites

1. Go to **Control Panel** > **Internet Options**.

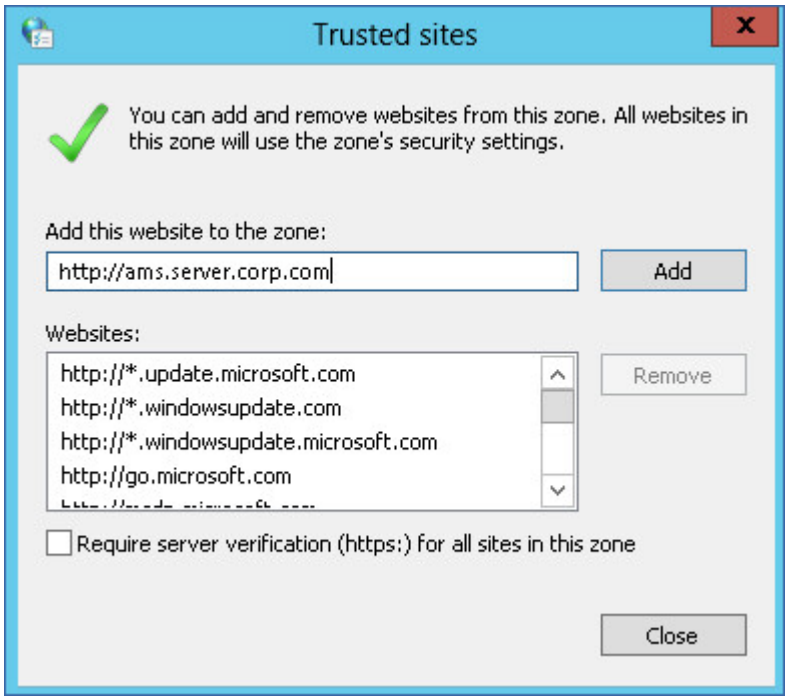
2. On the **Security** tab, select **Trusted sites**, and then click **Custom Level**.



3. Under **Logon**, select **Automatic logon with current user name and password**, and then click **OK**.



4. On the **Security** tab, with **Trusted sites** still selected, click **Sites**.
5. In **Add this website to the zone**, enter the address of the backup console login page, and then click **Add**.



6. Click **Close**.
7. Click **OK**.

3.2 Changing the SSL certificate settings

This section describes how to change the self-signed Secure Socket Layer (SSL) certificate generated by the management server to a certificate issued by a trusted certificate authority, such as GoDaddy, Comodo, or GlobalSign. If you do this, the certificate used by the management server will be trusted on any machine. The browser security alert will not appear when logging in to the backup console by using the HTTPS protocol.

Optionally, you can configure the management server to prohibit accessing the backup console via HTTP, by redirecting all users to HTTPS.

To change the SSL certificate settings

1. Ensure that you have all of the following:
   - The certificate file (.pem, .cert, or other format)
   - The file with the private key for the certificate (usually .key)
   - The private key passphrase, if the key is encrypted
2. Copy the files to the machine running the management server.
3. On this machine, open the following configuration file with a text editor:
   - In Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - In Linux: **/var/lib/Acronis/ApiGateway/api_gateway.json**
4. Locate the following section:

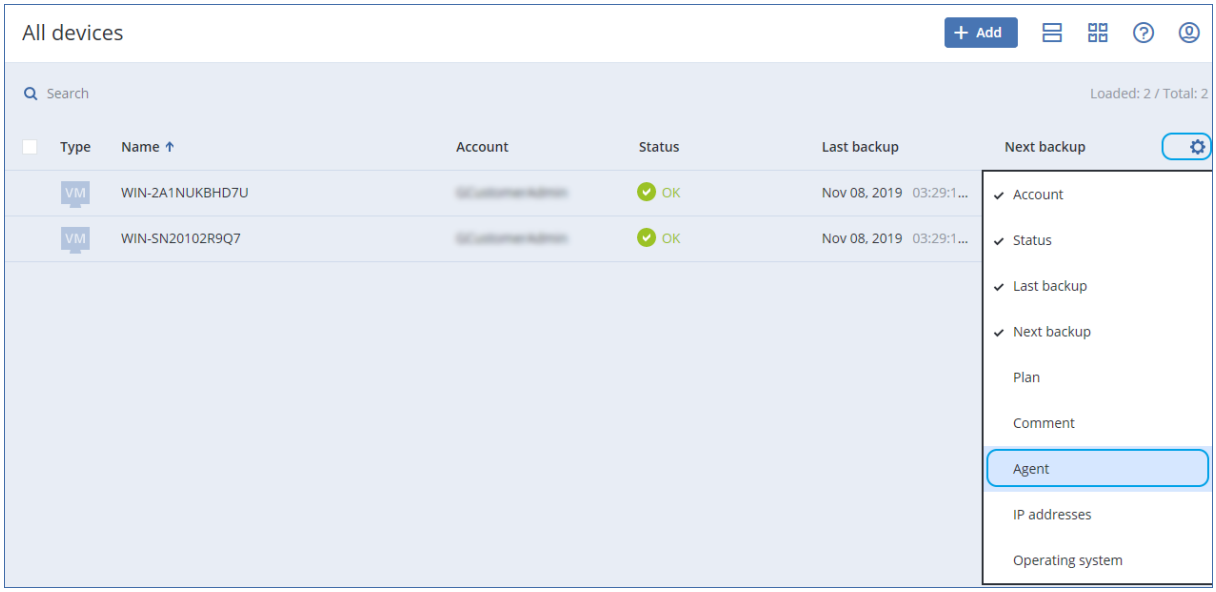
```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
    "auto_redirect": false
}
```

5. Between the quotation marks in the **"cert_file"** line, specify the full path to the certificate file. For example:
   - In Windows (note the forward slashes): **"cert_file": "C:/certificate/local-domain.ams.cert"**
   - In Linux: **"cert_file": "/home/user/local-domain.ams.cert"**
6. Between the quotation marks in the **"key_file"** line, specify the full path to the private key file. For example:
   - In Windows (note the forward slashes): **"key_file": "C:/certificate/private.key"**
   - In Linux: **"key_file": "/home/user/private.key"**
7. If the private key is encrypted, between the quotation marks in the **"passphrase"** line, specify the private key passphrase. For example: **"passphrase": "my secret passphrase"**
8. If you want to prohibit accessing the backup console via HTTP, by redirecting all users to HTTPS, change the **"auto_redirect"** value from **false** to **true**. Otherwise, skip this step.
9. Save the **api_gateway.json** file.

   Important *Please be careful and do not accidentally delete any commas, brackets, and quotation marks in the configuration file.*

10. Restart Acronis SCS Service Manager Service as described below.

2. Click the gear icon in the upper right corner and enable the **Agent** column.



3. In the **Agent** column, check the name of the machine where the respective agent is installed.
4. Delete this machine from the service console. This will also delete all of the machines that are backed up by its agent.
5. Uninstall the agent from the deleted machine as described in "Uninstalling agents" (Section 1.14).

5 Backup

A backup plan is a set of rules that specify how the given data will be protected on a given machine.

A backup plan can be applied to multiple machines at the time of its creation, or later.

To create the first backup plan

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

WHAT TO BACK UP	ITEMS TO BACK UP Selection methods	WHERE TO BACK UP	SCHEDULE Backup schemes	HOW LONG TO KEEP
Exchange databases		Network folder (Section 5.3) Tape device (Section 5.3)	incremental (Section 5.4) Custom (F-I) (Section 5.4)	
Exchange mailboxes		Local folder (Section 5.3) Network folder (Section 5.3)	Always incremental (Single-file) (Section 5.4)	

* See the limitations below.

Limitations

SFTP server and tape device

- These locations cannot be a destination for application-aware backups.
- The **Always incremental (single-file)** backup scheme is not available when backing up to these locations.
- The **By total size of backups** retention rule is not available for these locations.

NFS

- Backup to NFS shares is not available in Windows.

Secure Zone

- Secure Zone cannot be created on a Mac.

Always incremental (single-file)

- The **Always incremental (single-file)** backup scheme is not available when backing up to an SFTP server or a tape device.

By total size of backups

- The **By total size of backups** retention rule is not available:
  - If the backup scheme is set to **Always incremental (single-file)**
  - When backing up to an SFTP server, a tape device, or a managed location with enabled deduplication.

5.2 Selecting data to back up

5.2.1 Selecting files/folders

File-level backup is available for physical machines and virtual machines backed up by an agent installed in the guest system.

A file-level backup is not sufficient for recovery of the operating system. Choose file backup if you plan to protect only certain data (the current project, for example). This will reduce the backup size, thus saving storage space.

There are two ways of selecting files: directly on each machine or by using policy rules. Either method allows you to further refine the selection by setting the file filters (Section 5.10.13).

Direct selection

1. In **What to back up**, select **Files/folders**.
2. Click **Items to back up**.
3. In **Select items for backup**, select **Directly**.
4. For each of the machines included in the backup plan:
   a. Click **Select files and folders**.
   b. Click **Local folder** or **Network folder**.
      The share must be accessible from the selected machine.
   c. Browse to the required files/folders or enter the path and click the arrow button. If prompted, specify the user name and password for the shared folder.
      Backing up a folder with anonymous access is not supported.
   d. Select the required files/folders.
   e. Click **Done**.

Using policy rules

1. In **What to back up**, select **Files/folders**.
2. Click **Items to back up**.
3. In **Select items for backup**, select **Using policy rules**.
4. Select any of the predefined rules, type your own rules, or combine both.
   The policy rules will be applied to all of the machines included in the backup plan. If no data meeting at least one of the rules is found on a machine when the backup starts, the backup will fail on that machine.
5. Click **Done**.

Selection rules for Windows

- Full path to a file or folder, for example **D:\Work\Text.doc** or **C:\Windows**.
- Templates:
  - **`[All Files]`** selects all files on all volumes of the machine.
  - **`[All Profiles Folder]`** selects the folder where all user profiles are located (typically, **C:\Users** or **C:\Documents and Settings**).
- Environment variables:
  - **`%ALLUSERSPROFILE%`** selects the folder where the common data of all user profiles is located (typically, **C:\ProgramData** or **C:\Documents and Settings\All Users**).
  - **`%PROGRAMFILES%`** selects the Program Files folder (for example, **C:\Program Files**).
  - **`%WINDIR%`** selects the folder where Windows is located (for example, **C:\Windows**).

  You can use other environment variables or a combination of environment variables and text. For example, to select the Java folder in the Program Files folder, type: **%PROGRAMFILES%\Java**.

Selection rules for Linux

- Full path to a file or directory. For example, to back up **file.txt** on the volume **/dev/hda3** mounted on **/home/usr/docs**, specify **/dev/hda3/file.txt** or **/home/usr/docs/file.txt**.
  - **`/home`** selects the home directory of the common users.
  - **`/root`** selects the root user's home directory.
  - **`/usr`** selects the directory for all user-related programs.
  - **`/etc`** selects the directory for system configuration files.

- Templates:
  - **[All Profiles Folder]** selects **/home**. This is the folder where all user profiles are located by default.

5.2.2 Selecting disks/volumes

A disk-level backup contains a copy of a disk or a volume in a packaged form. You can recover individual disks, volumes, or files from a disk-level backup. A backup of an entire machine is a backup of all its disks.

There are two ways of selecting disks/volumes: directly on each machine or by using policy rules. You can exclude files from a disk backup by setting the file filters (Section 5.10.13).

Direct selection

Direct selection is available only for physical machines.

1. In **What to back up**, select **Disks/volumes**.
2. Click **Items to back up**.
3. In **Select items for backup**, select **Directly**.
4. For each of the machines included in the backup plan, select the check boxes next to the disks or volumes to back up.
5. Click **Done**.

Using policy rules

1. In **What to back up**, select **Disks/volumes**.
2. Click **Items to back up**.
3. In **Select items for backup**, select **Using policy rules**.
4. Select any of the predefined rules, type your own rules, or combine both.

   The policy rules will be applied to all of the machines included in the backup plan. If no data meeting at least one of the rules is found on a machine when the backup starts, the backup will fail on that machine.
5. Click **Done**.

Rules for Windows and Linux

- **[All volumes]** selects all volumes on machines running Windows and all mounted volumes on machines running Linux.

Rules for Windows

- Drive letter (for example **C:**) selects the volume with the specified drive letter.
- **[Fixed Volumes (Physical machines)]** selects all volumes of physical machines, other than removable media. Fixed volumes include volumes on SCSI, ATAPI, ATA, SSA, SAS, and SATA devices, and on RAID arrays.
- **[BOOT+SYSTEM]** selects the system and boot volumes. This combination is the minimal set of data that ensures recovery of the operating system from the backup.
- **[Disk 1]** selects the first disk of the machine, including all volumes on that disk. To select another disk, type the corresponding number.

Rules for Linux

- **/dev/hda1** selects the first volume on the first IDE hard disk.
- **/dev/sda1** selects the first volume on the first SCSI hard disk.
- **/dev/md1** selects the first software RAID hard disk.

To select other basic volumes, specify **/dev/xdyN**, where:

- "x" corresponds to the disk type
- "y" corresponds to the disk number (a for the first disk, b for the second disk, and so on)
- "N" is the volume number.

To select a logical volume, specify its path as it appears after running the **ls /dev/mapper** command under the root account. For example:

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

This output shows two logical volumes, **lv1** and **lv2**, that belong to the volume group **vg_1**. To back up these volumes, enter:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

5.2.2.1 What does a disk or volume backup store? [for SCS]

A disk or volume backup stores a disk or a volume **file system** as a whole and includes all of the information necessary for the operating system to boot. It is possible to recover disks or volumes as a whole from such backups as well as individual folders or files.

With the **sector-by-sector (raw mode)** backup option (Section 5.10.24) enabled, a disk backup stores all the disk sectors. The sector-by-sector backup can be used for backing up disks with unrecognized or unsupported file systems and other proprietary data formats.

Windows

A volume backup stores all files and folders of the selected volume independent of their attributes (including hidden and system files), the boot record, the file allocation table (FAT) if it exists, the root and the zero track of the hard disk with the master boot record (MBR).

A disk backup stores all volumes of the selected disk (including hidden volumes such as the vendor's maintenance partitions) and the zero track with the master boot record.

The following items are *not* included in a disk or volume backup (as well as in a file-level backup):

- The swap file (pagefile.sys) and the file that keeps the RAM content when the machine goes into hibernation (hiberfil.sys). After recovery, the files will be re-created in the appropriate place with the zero size.
- If the backup is performed under the operating system (as opposed to bootable media or backing up virtual machines at a hypervisor level):
  - Windows shadow storage. The path to it is determined in the registry value **VSS Default Provider** which can be found in the registry key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBa**

ckup. This means that in operating systems starting with Windows Vista, Windows Restore Points are not backed up.

- If the **Volume Shadow Copy Service (VSS)** backup option (Section 5.10.28) is enabled, files and folders that are specified in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** registry key.

Linux

A volume backup stores all files and directories of the selected volume independent of their attributes, a boot record, and the file system super block.

A disk backup stores all disk volumes as well as the zero track with the master boot record.

5.2.3 Selecting ESXi configuration

A backup of an ESXi host configuration enables you to recover an ESXi host to bare metal. The recovery is performed under bootable media.

The virtual machines running on the host are not included in the backup. They can be backed up and recovered separately.

A backup of an ESXi host configuration includes:

- The bootloader and boot bank partitions of the host.
- The host state (configuration of virtual networking and storage, SSL keys, server network settings, and local user information).
- Extensions and patches installed or staged on the host.
- Log files.

Prerequisites

- SSH must be enabled in the **Security Profile** of the ESXi host configuration.
- You must know the password for the 'root' account on the ESXi host.

Limitations

- ESXi configuration backup is not supported for VMware vSphere 6.7.

To select an ESXi configuration

1. Click **Devices** > **All devices**, and then select the ESXi hosts that you want to back up.
2. Click **Backup**.
3. In **What to back up**, select **ESXi configuration**.
4. In **ESXi 'root' password**, specify a password for the 'root' account on each of the selected hosts or apply the same password to all of the hosts.

5.3 Selecting a destination

To select a backup location

1. Click **Where to back up**.
2. Do one of the following:
   - Select a previously used or predefined backup location
   - Click **Add location**, and then specify a new backup location.

Supported locations

- **Local folder**

  If a single machine is selected, browse to a folder on the selected machine or type the folder path.

  If multiple machines are selected, type the folder path. Backups will be stored in this folder on each of the selected physical machines or on the machine where the agent for virtual machines is installed. If the folder does not exist, it will be created.

- **Network folder**

  This is a folder shared via SMB/CIFS/DFS.

  Browse to the required shared folder or enter the path in the following format:

  - For SMB/CIFS shares: `\\<host name>\<path>\` or `smb://<host name>/<path>/`
  - For DFS shares: `\\<full DNS domain name>\<DFS root>\<path>`

    For example, `\\example.company.com\shared\files`

  Then, click the arrow button. If prompted, specify the user name and password for the shared folder.

  Backing up to a folder with anonymous access is not supported.

- **NFS folder** (available for machines running Linux)

  Browse to the required NFS folder or enter the path in the following format:

  `nfs://<host name>/<exported folder>:/<subfolder>`

  Then, click the arrow button.

  It is not possible to back up to an NFS folder protected with a password.

- **Secure Zone** (available if it is present on each of the selected machines)

  Secure Zone is a secure partition on a disk of the backed-up machine. This partition has to be created manually prior to configuring a backup. For information about how to create Secure Zone, its advantages and limitations, refer to "About Secure Zone" (Section 5.3.1).

- **SFTP**

  Type the SFTP server name or address. The following notations are supported:

  `sftp://<server>`

  `sftp://<server>/<folder>`

  After entering the user name and password, you can browse the server folders.

  In either notation, you can also specify the port, user name, and password:

  `sftp://<server>:<port>/<folder>`

  `sftp://<user name>@<server>:<port>/<folder>`

  `sftp://<user name>:<password>@<server>:<port>/<folder>`

  If the port number is not specified, port 22 is used.

  Users, for whom SFTP access with no password is configured, cannot back up to SFTP.

  Backing up to FTP servers is not supported.

Advanced storage options

Note *This functionality is available only with the Acronis SCS Cyber Backup 12.5 Hardened Edition Advanced license.*

- **Defined by a script** (available for machines running Windows)

  You can store each machine's backups in a folder defined by a script. The software supports scripts written in JScript, VBScript, or Python 3.5. When deploying the backup plan, the software runs the script on each machine. The script output for each machine should be a local or network folder path. If a folder does not exist, it will be created (limitation: scripts written in Python

cannot create folders on network shares). On the **Backups** tab, each folder is shown as a separate backup location.

In **Script type**, select the script type (**JScript**, **VBScript**, or **Python**), and then import, or copy and paste the script. For network folders, specify the access credentials with the read/write permissions.

Example. The following JScript script outputs the backup location for a machine in the format **\\bkpsrv**<machine name>:

```
WScript.echo("\\\\bkpsrv\\" +
WScript.CreateObject("WScript.Network").ComputerName);
```

As a result, the backups of each machine will be saved in a folder of the same name on the server **bkpsrv**.

- **Tape**

  If a tape device is attached to the backed-up machine, the location list shows the default tape pool. This pool is created automatically.

  You can select the default pool or create a new one by clicking **Add location** > **Tape**. For information about pool settings, refer to "Creating a pool" (Section 17.1.4.3).

5.3.1 About Secure Zone

Secure Zone is a secure partition on a disk of the backed-up machine. It can store backups of disks or files of this machine.

Should the disk experience a physical failure, the backups located in the Secure Zone may be lost. That's why Secure Zone should not be the only location where a backup is stored. In enterprise environments, Secure Zone can be thought of as an intermediate location used for backup when an ordinary location is temporarily unavailable or connected through a slow or busy channel.

Why use Secure Zone?

Secure Zone:

- Enables recovery of a disk to the same disk where the disk's backup resides.
- Offers a cost-effective and handy method for protecting data from software malfunction, virus attack, human error.
- Eliminates the need for a separate media or network connection to back up or recover the data. This is especially useful for roaming users.
- Can serve as a primary destination when using replication of backups.

Limitations

- Secure Zone cannot be organized on a Mac.
- Secure Zone is a partition on a basic disk. It cannot be organized on a dynamic disk or created as a logical volume (managed by LVM).
- Secure Zone is formatted with the FAT32 file system. Because FAT32 has a 4-GB file size limit, larger backups are split when saved to Secure Zone. This does not affect the recovery procedure and speed.
- Secure Zone does not support the single-file backup format (Glossary). When you change the destination to Secure Zone in a backup plan that has the **Always incremental (Single-file)** backup scheme, the scheme is changed to **Weekly full, daily incremental**.

How creating Secure Zone transforms the disk

- Secure Zone is always created at the end of the hard disk.
- If there is no or not enough unallocated space at the end of the disk, but there is unallocated space between volumes, the volumes will be moved to add more unallocated space to the end of the disk.
- When all unallocated space is collected but it is still not enough, the software will take free space from the volumes you select, proportionally reducing the volumes' size.
- However, there should be free space on a volume, so that the operating system and applications can operate; for example, create temporary files. The software will not decrease a volume where free space is or becomes less than 25 percent of the total volume size. Only when all volumes on the disk have 25 percent or less free space, will the software continue decreasing the volumes proportionally.

As is apparent from the above, specifying the maximum possible Secure Zone size is not advisable. You will end up with no free space on any volume, which might cause the operating system or applications to work unstably and even fail to start.

Important *Moving or resizing the volume from which the system is booted requires a reboot.*

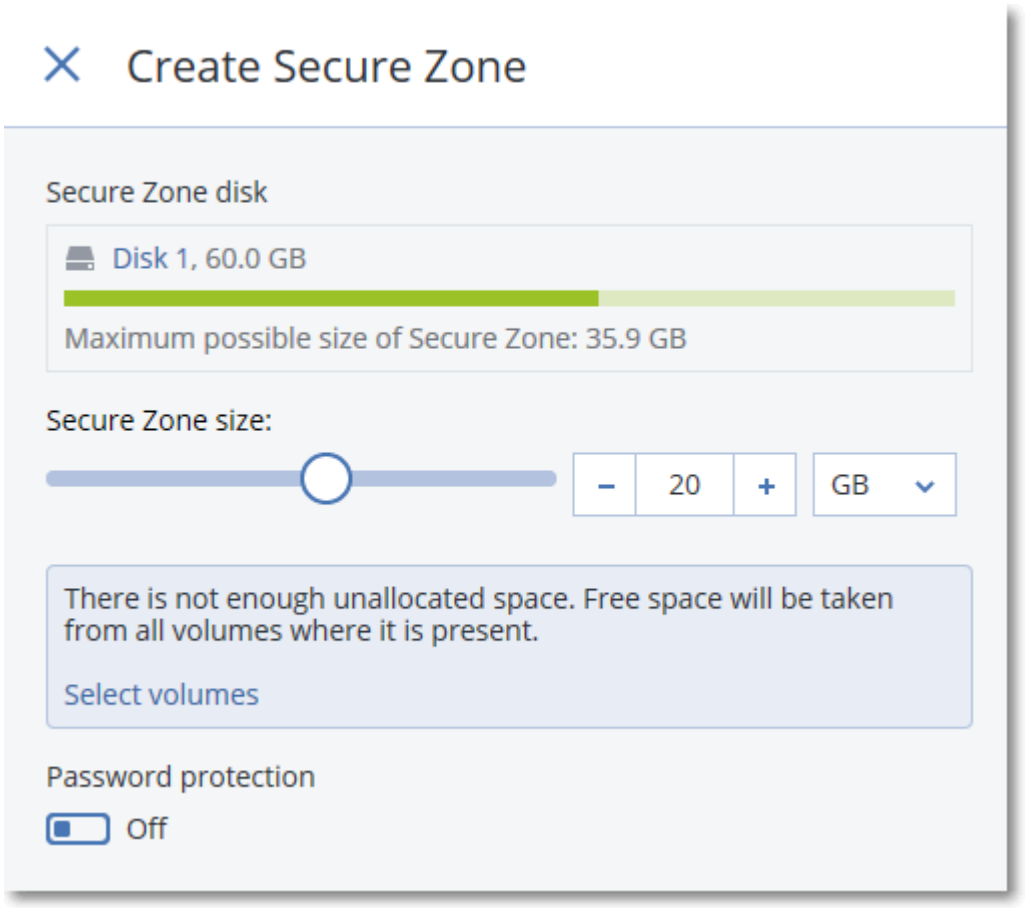
How to create Secure Zone

1. Select the machine that you want to create Secure Zone on.
2. Click **Details** > **Create Secure Zone**.
3. Under **Secure Zone disk**, click **Select**, and then select a hard disk (if several) on which to create the zone.

   The software calculates the maximum possible size of Secure Zone.
4. Enter the Secure Zone size or drag the slider to select any size between the minimum and the maximum ones.

   The minimum size is approximately 50 MB, depending on the geometry of the hard disk. The maximum size is equal to the disk's unallocated space plus the total free space on all of the disk's volumes.

5. If all unallocated space is not enough for the size you specified, the software will take free space from the existing volumes. By default, all volumes are selected. If you want to exclude some volumes, click **Select volumes**. Otherwise, skip this step.



6. [Optional] Enable the **Password protection** switch and specify a password.

   The password will be required to access the backups located in Secure Zone. Backing up to Secure Zone does not require a password, unless the backup if performed under bootable media.
7. Click **Create**.

   The software displays the expected partition layout. Click **OK**.
8. Wait while the software creates Secure Zone.

You can now choose Secure Zone in **Where to back up** when creating a backup plan.

How to delete Secure Zone

1. Select a machine with Secure Zone.
2. Click **Details**.
3. Click the gear icon next to **Secure Zone**, and then click **Delete**.
4. [Optional] Specify the volumes to which the space freed from the zone will be added. By default, all volumes are selected.

   The space will be distributed equally among the selected volumes. If you do not select any volumes, the freed space will become unallocated.

   Resizing the volume from which the system is booted requires a reboot.
5. Click **Delete**.

As a result, Secure Zone will be deleted along with all backups stored in it.

5.3.2 About Optical Drive Support

Acronis SCS Cyber Backup 12.5 Hardened Edition supports drives for both read and write operations.

Note: Feature Enforcement and Licensing
This feature is allowed if local backup is allowed by the licesnse.

You can allow full access, read-only access, or deny access to optical drives to control data copy operations to and from any optical drive on a protected computer. Disk level recovery, volume level recovery, and file level recovery are supported. Full, incremental, and differential backup are supported as well as multi-disk support.

Optical drives (access control by device type) - External and internal CD/DVD/BD drives (including writers) with any interface for connecting to a computer (IDE, SATA, USB, FireWire, PCMCIA, etc.). You can allow full access, allow read-only access, or deny access to optical drives to control data copy operations to and from any optical drive on a protected computer.

Supported backup types

- Allow to back up to CD/DVD
    - Support backup splitting
    - Support placing bootable media components on CD/DVD (making it bootable)
    - Support backup configuration via Web Console Interface (add new type of location- on CD/DVD)

Backup via the following agents:

AgentforWindows

- Agent for Linux
- Bootable Media Linux x64
- Bootable Media WinPEx32
- Allow to recover from CD/DVD

Supported recovery types

Recoverytypessupported for both disk/volume, and file recovery,

Limitations

- Catalog is not supported for backup on CD/DVD/BD
- CD/DVD supported only during recovery using bootable media
- CD/DVD is not supported by Windows 11
- Blue-ray not supported
- No replication to/from CD/DVD
- Recovery via media only
- Archive version 11 support only
- Backup storage
    - Refresh the Arhchive list every time the vault is opened by the user (using last disk)
    - If no disk is in the drive- ask user to put disk into the drive
    - If disk does not contain the last part of the archive (last volume) - show error that is not the last disk into the drive

Archive Browsing on CD/DVD:

1. The last CD/DVD should be inserted into the drive every time the user wants to browse the list of archives.
2. If there is no disk on the drive, the product will ask the user to insert the disk into the drive

How to Backup with CD/DVD

1. Boot into a BM using a Windows or Linux Machine
2. Click '**Manage this machine locally**'
3. Disconnect the BM ISO, or have a secondary CD/ROM attached to the machine.
4. Select '**Back Up Now**'
5. Using default or changing to specific files you want to backup
6. Select the Empty CD/DVD or secondary CD Drive CD/DVD
7. Select **Backup** or **Start**
8. Should succeed successfully backing up any content to the CD or DVD

Main Success Scenario (Basic Flow):

1. User has old backup plans that create backups to CD/DVD.
2. After upgrade the user is shown a notification that old backups to CD/DVD are only supported for recovery. Existing backup plans to CD/DVD are shown in the local console.
3. User is allowed to reconfigure the existing backup plan using another destinations.
4. The application does not allow to continue backups to CD/DVD
5. The application allows to add exisiting backups to CD/DVD into the local console in the recovery tab
6. User can recovery backups to CD/DVD via local console or via bootable media (Windows-based; Linux-based)

To create bootable media in Windows or Linux:

1. Download the bootable media ISO file. To download the file, select a machine, and then click **Recover** > **More ways to recover...**>**Download ISO image**.
2. Do any of the following:
    a. Burn a CD/DVD using the ISO file
    b. Create a bootable USB flash drive by using the ISO file and one of the free tools available.
    c. Connect the is file as a CD/DVD drive to the virtual machine that you want to recover.

You can also create bootable media by using **Bootable Media Builder .**
Please refer **to this page** for more detailed instructions.

5.4 Schedule

You can choose one of the predefined backup schemes or create a custom scheme. A backup scheme is a part of the backup plan that includes the backup schedule and the backup methods.

In **Backup scheme**, select one of the following:

- [Only for disk-level backups] **Always incremental (single-file)**
  By default, backups are performed on a daily basis, Monday to Friday. You can select the time to run the backup.
  If you want to change the backup frequency, move the slider, and then specify the backup schedule.
  The backups use the new single-file backup format (Glossary).
  This scheme is not available when backing up to a tape device, an SFTP server, or Secure Zone.
- **Always full**
  By default, backups are performed on a daily basis, Monday to Friday. You can select the time to run the backup.
  If you want to change the backup frequency, move the slider, and then specify the backup schedule.
  All backups are full.
- **Weekly full, Daily incremental**
  By default, backups are performed on a daily basis, Monday to Friday. You can modify the days of the week and the time to run the backup.
  A full backup is created once a week. All other backups are incremental. The day on which the full backup is created depends on the **Weekly backup** option (click the gear icon, then **Backup options** > **Weekly backup**).
- **Monthly full, Weekly differential, Daily incremental (GFS)**
  By default, incremental backups are performed on a daily basis, Monday to Friday; differential backups are performed every Saturday; full backups are performed on the first day of each month. You can modify these schedules and the time to run the backup.
  This backup scheme is displayed as a **Custom** scheme on the backup plan panel.
- **Custom**
  Specify schedules for full, differential, and incremental backups.
  Differential backup is not available when backing up SQL data or Exchange data.

With any backup scheme, you can schedule the backup to run by events, instead of by time. To do this, select the event type in the schedule selector. For more information, refer to "Schedule by events" (Section 5.4.1).

Additional scheduling options

With any destination, you can do the following:

- Specify the backup start conditions, so that a scheduled backup is performed only if the conditions are met. For more information, refer to "Start conditions" (Section 5.4.2).
- Set a date range for when the schedule is effective. Select the **Run the plan within a date range** check box, and then specify the date range.
- Disable the schedule. While the schedule is disabled, the retention rules are not applied unless a backup is started manually.

- Introduce a delay from the scheduled time. The delay value for each machine is selected randomly and ranges from zero to the maximum value you specify. You may want to use this setting when backing up multiple machines to a network location, to avoid excessive network load.

  Click the gear icon, then **Backup options** > **Scheduling**. Select **Distribute backup start times within a time window**, and then specify the maximum delay. The delay value for each machine is determined when the backup plan is applied to the machine and remains the same until you edit the backup plan and change the maximum delay value.
- Click **Show more** to access the following options:
  - **If the machine is turned off, run missed tasks at the machine startup** (disabled by default)
  - **Prevent the sleep or hibernate mode during backup** (enabled by default)

    This option is effective only for machines running Windows.
  - **Wake up from the sleep or hibernate mode to start a scheduled backup** (disabled by default)

    This option is effective only for machines running Windows. This option is not effective when the machine is powered off, i.e. the option does not employ the Wake-on-LAN functionality.

5.4.1 Schedule by events

When setting up a schedule for a backup plan, you can select the event type in the schedule selector. The backup will be launched as soon as the event occurs.

You can choose one of the following events:

- **Upon time since last backup**

  This is the time since the completion of the last successful backup within the same backup plan. You can specify the length of time.
- **When a user logs on to the system**

  By default, logging on of any user will initiate a backup. You can change any user to a specific user account.
- **When a user logs off the system**

  By default, logging off of any user will initiate a backup. You can change any user to a specific user account.

  Note *The backup will not run at a system shutdown because shutting down is not the same as logging off.*
- **On the system startup**
- **On the system shutdown**
- **On Windows Event Log event**

  You must specify the event properties (Section 5.4.1.1).

The table below lists the events available for various data under Windows and Linux.

WHAT TO BACK UP	Upon time since last backup	When a user logs on to the system	When a user logs off the system	On the system startup	On the system shutdown	On Windows Event Log event
Disks/volumes or files (physical machines)	Windows, Linux	Windows	Windows	Windows, Linux	Windows	Windows
Disks/volumes (virtual machines)	Windows, Linux	–	–	–	–	–

ESXi configuration	Windows, Linux	–	–	–	–	–
Exchange databases and mailboxes	Windows	–	–	–	–	Windows
SQL databases	Windows	–	–	–	–	Windows

5.4.1.1 On Windows Event Log event

You can schedule a backup to start when a certain Windows event has been recorded in one of the event logs, such as the **Application**, **Security**, or **System** log.

For example, you may want to set up a backup plan that will automatically perform an emergency full backup of your data as soon as Windows discovers that your hard disk drive is about to fail.

To browse the events and view the event properties, use the **Event Viewer** snap-in available in the **Computer Management** console. To be able to open the **Security** log, you must be a member of the **Administrators** group.

Event properties

Log name

Specifies the name of the log. Select the name of a standard log (**Application**, **Security**, or **System**) from the list, or type a log name—for example: **Microsoft Office Sessions**

Event source

Specifies the event source, which typically indicates the program or the system component that caused the event—for example: **disk**

Any event source that contains the specified string will trigger the scheduled backup. This option is not case sensitive. Thus, if you specify the string **service**, both **Service Control Manager** and **Time-Service** event sources will trigger a backup.

Event type

Specifies the event type: **Error**, **Warning**, **Information**, **Audit success**, or **Audit failure**.

Event ID

Specifies the event number, which typically identifies the particular kind of events among events from the same source.

For example, an **Error** event with Event source **disk** and Event ID **7** occurs when Windows discovers a bad block on a disk, whereas an **Error** event with Event source **disk** and Event ID **15** occurs when a disk is not ready for access yet.

Example: "Bad block" emergency backup

One or more bad blocks that have suddenly appeared on a hard disk usually indicate that the hard disk drive will soon fail. Suppose that you want to create a backup plan that will back up hard disk data as soon as such a situation occurs.

When Windows detects a bad block on a hard disk, it records an event with the event source **disk** and the event number **7** into the **System** log; the type of this event is **Error**.

When creating the plan, type or select the following in the **Schedule** section:

- **Log name**: **System**
- **Event source**: **disk**

- **Event type**: **Error**
- **Event ID**: **7**

Important *To ensure that such a backup will complete despite the presence of bad blocks, you must make the backup ignore bad blocks. To do this, in* ***Backup options****, go to* ***Error handling****, and then select the* ***Ignore bad sectors*** *check box.*

5.4.2 Start conditions

These settings add more flexibility to the scheduler, enabling it to execute a backup with respect to certain conditions. With multiple conditions, all of them must be met simultaneously to enable a backup to start. Start conditions are not effective when a backup is started manually.

To access these settings, click **Show more** when setting up a schedule for a backup plan.

The scheduler behavior, in case the condition (or any of multiple conditions) is not met, is defined by the Backup start conditions (Section 5.10.6) backup option. To handle the situation when the conditions are not met for too long and further delaying the backup is becoming risky, you can set the time interval after which the backup will run irrespective of the condition.

The table below lists the start conditions available for various data under Windows and Linux.

WHAT TO BACK UP	Disks/volumes or files (physical machines)	Disks/volumes (virtual machines)	ESXi configuration	Exchange databases and mailboxes	SQL databases
User is idle (Section 5.4.2.1)	Windows	–	–	–	–
The backup location's host is available (Section 5.4.2.2)	Windows, Linux	Windows, Linux	Windows, Linux	Windows	Windows
Users logged off (Section 5.4.2.3)	Windows	–	–	–	–
Fits the time interval (Section 5.4.4)	Windows, Linux	Windows, Linux	–	–	–
Save battery power (Section 5.4.2.5)	Windows	–	–	–	–
Do not start when on metered connection Section 5.4.2.6)	Windows	–	–	–	–
Do not start when connected to the following Wi-Fi networks (Section 5.4.2.7)	Windows	–	–	–	–
Check device IP address (Section 5.4.2.8)	Windows	–	–	–	–

5.4.2.1 User is idle

"User is idle" means that a screen saver is running on the machine or the machine is locked.

Example

Run the backup on the machine every day at 21:00, preferably when the user is idle. If the user is still active by 23:00, run the backup anyway.

- Schedule: Daily, Run every day. Start at: **21:00**.
- Condition: **User is idle**.
- Backup start conditions: **Wait until the conditions are met, Start the backup anyway after 2** hour(s).

As a result,

(1) If the user becomes idle before 21:00, the backup will start at 21:00.

(2) If the user becomes idle between 21:00 and 23:00, the backup will start immediately after the user becomes idle.

(3) If the user is still active at 23:00, the backup will start at 23:00.

5.4.2.2 The backup location's host is available

"The backup location's host is available" means that the machine hosting the destination for storing backups is available over the network.

This condition does not cover the availability of the location itself — only the host availability. For example, if the host is available, but the network folder on this host is not shared or the credentials for the folder are no longer valid, the condition is still considered met.

Example

Data is backed up to a network folder every workday at 21:00. If the machine that hosts the folder is not available at that moment (for instance, due to maintenance work), you want to skip the backup and wait for the scheduled start on the next workday.

- Schedule: Daily, Run Monday to Friday. Start at: **21:00**.
- Condition: **The backup location's host is available**.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

(1) If 21:00 comes and the host is available, the backup will start immediately.

(2) If 21:00 comes but the host is unavailable, the backup will start on the next workday if the host is available.

(3) If the host is never available on workdays at 21:00, the backup will never start.

5.4.2.3 Users logged off

Enables you to put a backup on hold until all users log off from Windows.

Example

Run the backup at 20:00 every Friday, preferably when all users are logged off. If one of the users is still logged on at 23:00, run the backup anyway.

- Schedule: Weekly, on Fridays. Start at: **20:00**.
- Condition: **Users logged off**.
- Backup start conditions: **Wait until the conditions are met**, **Start the backup anyway after 3** hour(s).

As a result:

(1) If all users are logged off at 20:00, the backup will start at 20:00.

(2) If the last user logs off between 20:00 and 23:00, the backup will start immediately after the user logs off.

(3) If any user is still logged on at 23:00, the backup will start at 23:00.

5.4.2.4 Fits the time interval

Restricts a backup start time to a specified interval.

Example

A company uses different locations on the same network-attached storage for backing up users' data and servers. The workday starts at 08:00 and ends at 17:00. Users' data should be backed up as soon as the users log off, but not earlier than 16:30. Every day at 23:00 the company's servers are backed up. So, all the users' data should preferably be backed up before this time, in order to free network bandwidth. It is assumed that backing up user's data takes no more than one hour, so the latest backup start time is 22:00. If a user is still logged on within the specified time interval, or logs off at any other time – do not back up the users' data, i.e., skip backup execution.

- Event: **When a user logs off the system**. Specify the user account: **Any user**.
- Condition: **Fits the time interval** from **16:30** to **22:00**.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

(1) if the user logs off between 16:30 and 22:00, the backup will start immediately following the logging off.

(2) if the user logs off at any other time, the backup will be skipped.

5.4.2.5 Save battery power

Prevents a backup if the device (a laptop or a tablet) is not connected to a power source. Depending on the value of the Backup start conditions (Section 5.10.6) backup option, the skipped backup will or will not be started after the device is connected to a power source. The following options are available:

- **Do not start when on battery**

  A backup will start only if the device is connected to a power source.
- **Start when on battery if the battery level is higher than**

  A backup will start if the device is connected to a power source or if the battery level is higher than the specified value.

Example

Data is backed up every workday at 21:00. If the device is not connected to a power source (for instance, the user is attending a late meeting), you want to skip the backup to save the battery power and wait until the user connects the device to a power source.

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.
- Condition: **Save battery power**, **Do not start when on battery**.
- Backup start conditions: **Wait until the conditions are met**.

As a result:

(1) If 21:00 comes and the device is connected to a power source, the backup will start immediately.

(2) If 21:00 comes and the device is running on battery power, the backup will start as soon as the device is connected to a power source.

5.4.2.6 Do not start when on metered connection

Prevents a backup (including a backup to a local disk) if the device is connected to the Internet by using a connection that is set as metered in Windows. For more information about metered connections in Windows, refer to https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

As an additional measure to prevent backups over mobile hotspots, when you enable the **Do not start when on metered connection** condition, the condition **Do not start when connected to the following Wi-Fi networks** is enabled automatically. The following network names are specified by default: "android", "phone", "mobile", and "modem". You can delete these names from the list by clicking on the X sign.

Example

Data is backed up every workday at 21:00. If the device is connected to the Internet by using a metered connection (for instance, the user is on a business trip), you want to skip the backup to save the network traffic and wait for the scheduled start on the next workday.

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.
- Condition: **Do not start when on metered connection**.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

(1) If 21:00 comes and the device is not connected to the Internet by using a metered connection, the backup will start immediately.

(2) If 21:00 comes and the device is connected to the Internet by using a metered connection, the backup will start on the next workday.

(3) If the device is always connected to the Internet by using a metered connection on workdays at 21:00, the backup will never start.

5.4.2.7 Do not start when connected to the following Wi-Fi networks

Prevents a backup (including a backup to a local disk) if the device is connected to any of the specified wireless networks. You can specify the Wi-Fi network names, also known as service set identifiers (SSID).

The restriction applies to all networks that contain the specified name as a substring in their name, case-insensitive. For example, if you specify "phone" as the network name, the backup will not start when the device is connected to any of the following networks: "John's iPhone", "phone_wifi", or "my_PHONE_wifi".

This condition is useful to prevent backups when the device is connected to the Internet by using a mobile phone hotspot.

As an additional measure to prevent backups over mobile hotspots, the **Do not start when connected to the following Wi-Fi** condition is enabled automatically when you enable the **Do not start when on metered connection** condition. The following network names are specified by default: "android", "phone", "mobile", and "modem". You can delete these names from the list by clicking on the X sign.

Example

Data is backed up every workday at 21:00. If the device is connected to the Internet by using a mobile hotspot (for example, a laptop is connected in the tethering mode), you want to skip the backup and wait for the scheduled start on the next workday.

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.
- Condition: **Do not start when connected to the following networks**, **Network name**: `<SSID of the hotspot network>`.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

(1) If 21:00 comes and the machine is not connected to the specified network, the backup will start immediately.

(2) If 21:00 comes and the machine is connected to the specified network, the backup will start on the next workday.

(3) If the machine is always connected to the specified network on workdays at 21:00, the backup will never start.

5.4.2.8 Check device IP address

Prevents a backup (including a backup to a local disk) if any of the device IP addresses are within or outside of the specified IP address range. The following options are available:

- **Start if outside IP range**
- **Start if within IP range**

With either option, you can specify several ranges. Only IPv4 addresses are supported.

This condition is useful in the event of a user being overseas, to avoid large data transit charges. Also, it helps to prevent backups over a Virtual Private Network (VPN) connection.

Example

Data is backed up every workday at 21:00. If the device is connected to the corporate network by using a VPN tunnel (for instance, the user is working from home), you want to skip the backup and wait until the user brings the device to the office.

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.

- Condition: **Check device IP address**, **Start if outside IP range**, **From**: <beginning of the VPN IP address range>, **To**: <end of the VPN IP address range>.
- Backup start conditions: **Wait until the conditions are met**.

As a result:

(1) If 21:00 comes and the machine IP address is not in the specified range, the backup will start immediately.

(2) If 21:00 comes and the machine IP address is in the specified range, the backup will start as soon as the device obtains a non-VPN IP address.

(3) If the machine IP address is always in the specified range on workdays at 21:00, the backup will never start.

5.5 Retention rules

1. Click **How long to keep**.
2. In **Cleanup**, choose one of the following:
   - **By backup age** (default)
     Specify how long to keep backups created by the backup plan. By default, the retention rules are specified for each backup set (**Glossary**) separately. If you want to use a single rule for all backups, click **Switch to single rule for all backup sets**.
   - **By number of backups**
     Specify the maximum number of backups to keep.
   - **By total size of backups**
     Specify the maximum total size of backups to keep.
     This setting is not available with the **Always incremental (single-file)** backup scheme, or when backing up to an SFTP server or a tape device.
   - **Keep backups indefinitely**
3. Select when to start the cleanup:
   - **After backup** (default)
     The retention rules will be applied after a new backup is created.
   - **Before backup**
     The retention rules will be applied before a new backup is created.
     This setting is not available when backing up Microsoft SQL Server clusters or Microsoft Exchange Server clusters.

What else you need to know

- The last backup created by the backup plan always will be kept, even if a retention rule violation is detected. Please do not try to delete the only backup you have by applying the retention rules before backup.
- Backups stored on tapes are not deleted until the tape is overwritten.
- If, according to the backup scheme and backup format, each backup is stored as a separate file, this file cannot be deleted until the lifetime of all its dependent (incremental and differential) backups expires. This requires extra space for storing backups whose deletion is postponed. Also, the backup age, number, or size of backups may exceed the values you specify.
  This behavior can be changed by using the "Backup consolidation" (Section 5.10.2) backup option.

- Retention rules are a part of a backup plan. They stop working for a machine's backups as soon as the backup plan is revoked from the machine, or deleted, or the machine itself is deleted from the management server. If you no longer need the backups created by the plan, delete them as described in "Deleting backups" (Section 7.4).

5.6 Encryption

Important *There is no way to recover encrypted backups if you lose or forget the password.*

Encryption in a backup plan

To enable encryption, specify the encryption settings when creating a backup plan. After a backup plan is applied, the encryption settings cannot be modified. To use different encryption settings, create a new backup plan.

To specify the encryption settings in a backup plan

1. On the backup plan panel, enable the **Encryption** switch.
2. Specify and confirm the encryption password.
3. Select one of the following encryption algorithms:
   - **AES 128** – the backups will be encrypted by using the Advanced Encryption Standard (AES) algorithm with a 128-bit key.
   - **AES 192** – the backups will be encrypted by using the AES algorithm with a 192-bit key.
   - **AES 256** – the backups will be encrypted by using the AES algorithm with a 256-bit key.
4. Click **OK**.

Encryption as a machine property

This option is intended for administrators who handle backups of multiple machines. If you need a unique encryption password for each machine or if you need to enforce encryption of backups regardless of the backup plan encryption settings, save the encryption settings on each machine individually. The backups will be encrypted using the AES algorithm with a 256-bit key.

Saving the encryption settings on a machine affects the backup plans in the following way:

- **Backup plans that are already applied to the machine.** If the encryption settings in a backup plan are different, the backups will fail.
- **Backup plans that will be applied to the machine later.** The encryption settings saved on a machine will override the encryption settings in a backup plan. Any backup will be encrypted, even if encryption is disabled in the backup plan settings.

This option can be used on a machine running Agent for VMware. However, be careful if you have more than one Agent for VMware connected to the same vCenter Server. It is mandatory to use the same encryption settings for all of the agents, because there is a type of load balancing among them.

After the encryption settings are saved, they can be changed or reset as described below.

Important *If a backup plan that runs on this machine has already created backups, changing the encryption settings will cause this plan to fail. To continue backing up, create a new plan.*

To save the encryption settings on a machine

1. Log on as an administrator (in Windows) or the root user (in Linux).

2. Run the following script:
   - In Windows: `<installation_path>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<encryption_password>`

     Here, `<installation_path>` is the backup agent installation path. By default, it is **%ProgramFiles%\Acronis**.
   - In Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<encryption_password>`

To reset the encryption settings on a machine

1. Log on as an administrator (in Windows) or root user (in Linux).
2. Run the following script:
   - In Windows: `<installation_path>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     Here, `<installation_path>` is the backup agent installation path. By default, it is **%ProgramFiles%\Acronis**.
   - In Linux: **/usr/sbin/acropsh -m manage_creds --reset**

How the encryption works

The AES cryptographic algorithm operates in the Cipher-block chaining (CBC) mode and uses a randomly generated key with a user-defined size of 128, 192 or 256 bits. The larger the key size, the longer it will take for the program to encrypt the backups and the more secure your data will be.

The encryption key is then encrypted with AES-256 using an SHA-256 hash of the password as a key. The password itself is not stored anywhere on the disk or in the backups; the password hash is used for verification purposes. With this two-level security, the backup data is protected from any unauthorized access, but recovering a lost password is not possible.

5.7 Conversion to a virtual machine

Conversion to a virtual machine is available only for disk-level backups. If a backup includes the system volume and contains all of the information necessary for the operating system to start, the resulting virtual machine can start on its own. Otherwise, you can add its virtual disks to another virtual machine.

Conversion methods

- **Regular conversion**

  There are two ways to configure a regular conversion:
  - **Make the conversion a part of a backup plan**
    (Section 5.7.2)

The conversion will be performed after each backup (if configured for the primary location) or after each replication (if configured for the second and further locations).

- **Create a separate conversion plan** (Section 9.1.4)

  This method enables you to specify a separate conversion schedule.

- **Recovery to a new virtual machine** (Section 6.3.2)
  This method enables you to choose disks for recovery and adjust the settings for each virtual disk. Use this method to perform the conversion once or occasionally, for example, to perform a physical-to-virtual migration (Section 14.5.1).

5.7.1 What you need to know about conversion [for SCS]

Supported virtual machine types

Conversion of a backup to a virtual machine can be done by the same agent that created the backup or by another agent.

To perform a conversion to VMware ESXi or Hyper-V, you need an ESXi or Hyper-V host and a backup agent (Agent for VMware or Agent for Hyper-V) that manages this host.

Conversion to VHDX files assumes that the files will be connected as virtual disks to a Hyper-V virtual machine.

The following table summarizes the virtual machine types that can be created by the agents:

VM type	Agent for VMware	Agent for Hyper-V	Agent for Windows	Agent for Linux
VMware ESXi	+	–	–	–
Microsoft Hyper-V	–	+	–	–
VMware Workstation	+	+	+	+
VHDX files	+	+	+	+

Limitations

- Agent for Windows, Agent for VMware (Windows), and Agent for Hyper-V cannot convert backups stored on NFS.
- Backups stored on NFS or on an SFTP server cannot be converted in a separate conversion plan (Section 9.1.4).
- Backups stored in Secure Zone can be converted only by the agent running on the same machine.
- Backups that contain Linux logical volumes (LVM) can be converted only if they were created by Agent for VMware or Agent for Hyper-V, and are directed to the same hypervisor. Cross-hypervisor conversion is not supported.
- When backups of a Windows machine are converted to VMware Workstation or VHDX files, the resulting virtual machine inherits the CPU type from the machine that performs the conversion. As a result, the corresponding CPU drivers are installed in the guest operating system. If started on a host with a different CPU type, the guest system displays a driver error. Update this driver manually.

Regular conversion to ESXi and Hyper-V vs. running a virtual machine from a backup

Both operations provide you with a virtual machine that can be started in seconds if the original machine fails.

Regular conversion takes CPU and memory resources. Files of the virtual machine constantly occupy space on the datastore (storage). This may be not practical if a production host is used for conversion. However, the virtual machine performance is limited only by the host resources.

In the second case, the resources are consumed only while the virtual machine is running. The datastore (storage) space is required only to keep changes to the virtual disks. However, the virtual machine may run slower, because the host does not access the virtual disks directly, but communicates with the agent that reads data from the backup. In addition, the virtual machine is temporary. Making the machine permanent is possible only for ESXi.

5.7.2 Conversion to a virtual machine in a backup plan

You can configure the conversion to a virtual machine from any backup or replication location that is present in a backup plan. The conversion will be performed after each backup or replication.

For information about prerequisites and limitations, please refer to "What you need to know about conversion" (Section 5.7.1).

To set up a conversion to a virtual machine in a backup plan

1. Decide from which backup location you want to perform the conversion.
2. On the backup plan panel, click **Convert to VM** under this location.
3. Enable the **Conversion** switch.
4. In **Convert to**, select the type of the target virtual machine. You can select one of the following:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **VHDX files**
5. Do one of the following:
   - For VMware ESXi and Hyper-V: click **Host**, select the target host, and then specify the new machine name template.
   - For other virtual machine types: in **Path**, specify where to save the virtual machine files and the file name template.

   The default name is **[Machine Name]_converted**.
6. [Optional] Click **Agent that will perform conversion**, and then select an agent.

   This may be the agent that performs the backup (by default) or an agent installed on another machine. If the latter is the case, the backups must be stored in a shared location such as a network folder, so that the other machine can access them.
7. [Optional] For VMware ESXi and Hyper-V, you can also do the following:
   - Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore (storage) for the virtual machine.
   - Change the disk provisioning mode. The default setting is **Thin** for VMware ESXi and **Dynamically expanding** for Hyper-V.
   - Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.
8. Click **Done**.

5.7.3 How regular conversion to VM works

The way the repeated conversions work depends on where you choose to create the virtual machine.

- **If you choose to save the virtual machine as a set of files:** each conversion re-creates the virtual machine from scratch.
- **If you choose to create the virtual machine on a virtualization server:** when converting an incremental or differential backup, the software updates the existing virtual machine instead of re-creating it. Such conversion is normally faster. It saves network traffic and CPU resource of the host that performs the conversion. If updating the virtual machine is not possible, the software re-creates it from scratch.

The following is a detailed description of both cases.

If you choose to save the virtual machine as a set of files

As a result of the first conversion, a new virtual machine will be created. Every subsequent conversion will re-create this machine from scratch. First, the old machine is temporarily renamed. Then, a new virtual machine is created that has the previous name of the old machine. If this operation succeeds, the old machine is deleted. If this operation fails, the new machine is deleted and the old machine is given its previous name. This way, the conversion always ends up with a single machine. However, extra storage space is required during conversion to store the old machine.

If you choose to create the virtual machine on a virtualization server

The first conversion creates a new virtual machine. Any subsequent conversion works as follows:

- If there has been a *full backup* since the last conversion, the virtual machine is re-created from scratch, as described earlier in this section.
- Otherwise, the existing virtual machine is updated to reflect changes since the last conversion. If updating is not possible (for example, if you deleted the intermediate snapshots, see below), the virtual machine is re-created from scratch.

Intermediate snapshots

To be able to update the virtual machine, the software stores a few intermediate snapshots of it. They are named **Backup…** and **Replica…** and should be kept. Unneeded snapshots are deleted automatically.

The latest **Replica…** snapshot corresponds to the result of the latest conversion. You can go to this snapshot if you want to return the machine to that state; for example, if you worked with the machine and now want to discard the changes made to it.

Other snapshots are for internal use by the software.

5.8 Replication

This section describes backup replication as a part of the backup plan. For information about creating a separate replication plan, refer to "Off-host data processing" (Section 9.1).

If you enable backup replication, each backup will be copied to another location immediately after creation. If earlier backups were not replicated (for example, the network connection was lost), the software also replicates all of the backups that appeared after the last successful replication.

Replicated backups do not depend on the backups remaining in the original location and vice versa. You can recover data from any backup, without access to other locations.

Usage examples

- **Reliable disaster recovery**

  Store your backups both on-site (for immediate recovery) and off-site (to secure the backups from local storage failure or a natural disaster).
- **Keeping only the latest recovery points**

  Delete older backups from a fast storage according to retention rules, in order to not overuse expensive storage space.

Supported locations

You can replicate a backup *from* any of these locations:

- A local folder
- A network folder
- Secure Zone
- An SFTP server

You can replicate a backup *to* any of these locations:

- A local folder
- A network folder
- An SFTP server
- A tape device

To enable replication of backups

1. On the backup plan panel, click **Add location**.

   The **Add location** control is shown only if replication is supported *from* the last selected location.
2. Specify the location where the backups will be replicated.
3. [Optional] In **How long to keep**, change the retention rules for the chosen location, as described in "Retention rules" (Section 5.5).
4. [Optional] In **Convert to VM**, specify the settings for conversion to a virtual machine, as described in "Conversion to a virtual machine" (Section 5.7).
5. [Optional] Repeat steps 1-4 for all locations where you want to replicate the backups. Up to five consecutive locations are supported, including the primary one.

5.9 Starting a backup manually

1. Select a machine that has at least one applied backup plan.
2. Click **Backup**.
3. If more than one backup plans are applied, select the backup plan.
4. Do one of the following:
   - To run an incremental backup, click **Run now**.
   - To run a full backup, click the arrow on the **Run now** button, and then select **Full**.
   - To run a differential backup, click the arrow on the **Run now** button, and then select **Differential**. This option is displayed only if the backup scheme is **Custom** or Grandfather-Father-Son (**GFS**).

The first backup created by a backup plan is always full.

The backup progress is shown in the **Status** column for the machine.

5.10 Backup options

To modify the backup options, click the gear icon next to the backup plan name, and then click **Backup options**.

Availability of the backup options

The set of available backup options depends on:

- The environment the agent operates in (Windows, Linux).
- The type of the data being backed up (disks, files, virtual machines, application data).
- The backup destination (a local or network folder).

The following table summarizes the availability of the backup options.

	File-level backup		**Virtual machines**		**SQL and Exchange**		
	Windows	Linux	Windows	Linux	ESXi	Hyper-V	Windows
Alerts (Section 5.10.1)	+	+	+	+	+	+	+
Backup consolidation (Section 5.10.2)	+	+	+	+	+	+	-
Backup file name (Section 5.10.3)	+	+	+	+	+	+	+
Backup format (Section 5.10.4)	+	+	+	+	+	+	+
Backup validation (Section 5.10.4)	+	+	+	+	+	+	+
Backup start conditions (section 5.10.6)	+	+	+	+	+	+	+
Changed block tracking (CBT) (Section 5.10.7)	+	-	-	-	+	+	-
Cluster backup mode (Section 5.10.8)	-	-	-	-	-	-	+
Compression level (Section 5.10.9)	+	+	+	+	+	+	+
Email notifications (Section 5.10.10)	+	+	+	+	+	+	+
Error handling (Section 5.10.11)							
Re-attempt, if an error occurs	+	+	+	+	+	+	+
Do not show messages and dialogs while processing (silent mode)	+	+	+	+	+	+	+
Ignore bad sectors	+	+	+	+	+	+	-
Re-attempt, if an error occurs during VM snapshot creation	-	-	-	-	+	+	-
Fast incremental/differential backup (Section 5.10.12)	+	+	-	-	-	-	-
File filters (Section 5.10.13)	+	+	+	+	+	+	-

	File-level backup		Virtual machines		SQL and Exchange		
	Windows	Linux	Windows	Linux	ESXi	Hyper-V	Windows
File-level backup snapshot Section 5.10.14)	-	-	+	+	-	-	-
Log truncation (Section 5.10.15)	-	-	-	-	+	+	SQL only
LVM snapshotting (Section 5.10.16)	-	+	-	-	-	-	-
Mount points (Section 5.10.17)	-	-	+	-	-	-	-
Multi-volume snapshot (Section 5.10.18)	+	+	+	+	-	-	-
Performance and backup window (Section 5.10.19)	+	+	+	+	+	+	+
Pre/Post commands (Section 5.10.20)	+	+	+	+	+	+	+
Pre/Post data capture commands (Section 5.10.21)	+	+	+	+	-	-	+
SAN hardware snapshots Section 5.10.22)	-	-	-	-	+	-	-
Scheduling (Section 5.10.23)							
Distribute start times within a time window	+	+	+	+	+	+	+
Limit the number of simultaneously running backups	-	-	-	-	+	+	-
Sector-by-sector backup (Section 5.10.24)	+	+	-	-	+	+	-
Splitting (Section 5.10.25)	+	+	+	+	+	+	+
Tape management (Section 5.10.26)	+	+	+	+	+	+	+
Task failure handling (Section 5.10.27)	+	+	+	+	+	+	+
Volume Shadow Copy Service (VSS) (Section 5.10.28)	+	-	+	-	-	+	+
Volume Shadow Copy Service (VSS) for virtual machines (Section 5.10.29)	-	-	-	-	+	+	-
Weekly backup (Section 5.10.30)	+	+	+	+	+	+	+
Windows event log (Section 5.10.31)	+	-	+	-	+	+	+

5.10.1 Alerts

No successful backups for a specified number of consecutive days

The preset is: **Disabled**.

This option determines whether to generate an alert if no successful backups were performed by the backup plan for a specified period of time. In addition to failed backups, the software counts backups that did not run on schedule (missed backups).

The alerts are generated on a per-machine basis and are displayed on the **Alerts** tab.

You can specify the number of consecutive days without backups after which the alert is generated.

5.10.2 Backup consolidation

This option defines whether to consolidate backups during cleanup or to delete entire backup chains.

The preset is: **Disabled**.

Consolidation is the process of combining two or more subsequent backups into a single backup.

If this option is enabled, a backup that should be deleted during cleanup is consolidated with the next dependent backup (incremental or differential).

Otherwise, the backup is retained until all dependent backups become subject to deletion. This helps avoid the potentially time-consuming consolidation, but requires extra space for storing backups whose deletion is postponed. The backups' age or number can exceed the values specified in the retention rules.

Important *Please be aware that consolidation is just a method of deletion, but not an alternative to deletion. The resulting backup will not contain data that was present in the deleted backup and was absent from the retained incremental or differential backup.*

This option is *not* effective if any of the following is true:

- The backup destination is a tape device.
- The backup scheme is set to **Always incremental (single-file)**.
- The backup format (p. 88) is set to **Version 12**.

Backups stored on tapes cannot be consolidated. Single-file backups (both version 11 and 12 formats) are always consolidated because their inner structure makes for fast and easy consolidation.

However, if version 12 format is used, and multiple backup chains are present (every chain being stored in a separate .tibx file), consolidation works only within the last chain. Any other chain is deleted as a whole, except for the first one, which is shrunk to the minimum size to keep the meta information (~12 KB). This meta information is required to ensure the data consistency during simultaneous read and write operations. The backups included in these chains disappear from the GUI as soon as the retention rule is applied, although they physically exist until the entire chain is deleted.

In all other cases, backups whose deletion is postponed are marked with the trash can icon () in the GUI. If you delete such a backup by clicking the X sign, consolidation will be performed. Backups stored on a tape disappear from the GUI only when the tape is overwritten or erased.

5.10.3 Backup file name

This option defines the names of the backup files created by the backup plan.

These names can be seen in a file manager when browsing the backup location.

What is a backup file?

Each backup plan creates one or more files in the backup location, depending on which backup scheme and which backup format (Section 5.10.4) are used. The following table lists the files that can be created per machine or mailbox.

	Always incremental (single-file)	**Other backup schemes**
Version 11 backup format	One .tib file and one .xml metadata file	Multiple .tib files and one .xml metadata file (traditional format)
Version 12 backup format	One .tibx file per backup chain (a full or differential backup, and all incremental backups that depend on it)	

All files have the same name, with or without the addition of a timestamp or a sequence number. You can define this name (referred to as the backup file name) when creating or editing a backup plan.

After you change a backup file name, the next backup will be a full backup, unless you specify a file name of an existing backup of the same machine. If the latter is the case, a full, incremental, or differential backup will be created according to the backup plan schedule.

Note that it is possible to set backup file names for locations that cannot be browsed by a file manager (such as a tape device). This makes sense if you want to see the custom names on the **Backups** tab.

Where can I see backup file names?

Select the **Backups** tab, and then select the group of backups.

- The default backup file name is shown on the **Details** panel.
- If you set a non-default backup file name, it will be shown directly on the **Backups** tab, in the **Name** column.

Limitations for backup file names

- A backup file name cannot end with a digit.

  In the default backup file name, to prevent the name from ending with a digit, the letter "A" is appended. When creating a custom name, always make sure that it does not end with a digit. When using variables, the name must not end with a variable, because a variable might end with a digit.
- A backup file name cannot contain the following symbols: **()&?*$<>":\|/#**, line endings (**\n**), and tabs (**\t**).

Default backup file name

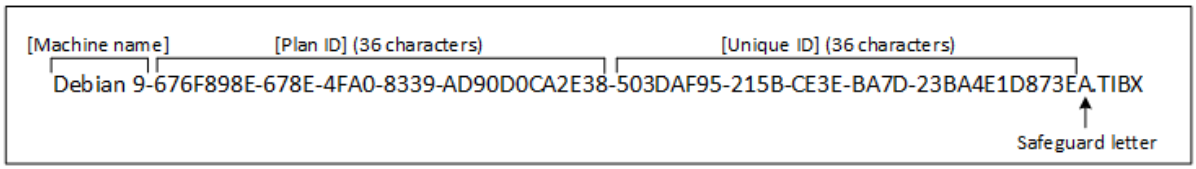
The default backup file name is **`[Machine Name]-[Plan ID]-[Unique ID]A`**.

The default backup file name for mailbox backup is **`[Mailbox ID]_mailbox_[Plan ID]A`**.

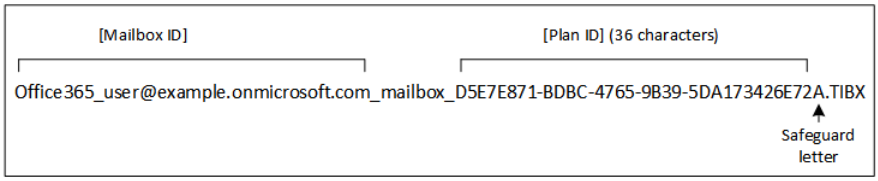
The name consists of the following variables:

- **[Machine Name]** This variable is replaced with the name of the machine (the same name that is shown in the backup console) for all types of backed up data.
- **[Plan ID]** This variable is replaced with a unique identifier of a backup plan. This value does not change if the plan is renamed.
- **[Unique ID]** This variable is replaced with a unique identifier of the selected machine or mailbox. This value does not change if the machine is renamed or the mailbox UPN is changed.
- **[Mailbox ID]** This variable is replaced with the mailbox UPN.
- **"A"** is a safeguard letter that is appended to prevent the name from ending with a digit.

The diagram below shows the default backup file name.



The diagram below shows the default backup file name for mailboxes.



Names without variables

If you change the backup file name to **MyBackup**, the backup files will look like the following examples. Both examples assume daily incremental backups scheduled at 14:40, starting from September 13, 2016.

For the **Version 12** format with the **Always incremental (single-file)** backup scheme:

```
MyBackup.tibx
```

For the **Version 12** format with other backup schemes:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

For the **Version 11** format with the **Always incremental (single-file)** backup scheme:

```
MyBackup.xml
MyBackup.tib
```

For the **Version 11** format with other backup schemes:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

Using variables

Besides the variables that are used by default, you can use the **[Plan name]** variable, which is replaced with the name of the backup plan.

If multiple machines or mailboxes are selected for backup, the backup file name must contain the **[Machine Name]**, the **[Mailbox ID]**, or the **[Unique ID]** variable.

Backup file name vs. simplified file naming

Using plain text and/or variables, you can construct the same file names as in earlier Acronis SCS Cyber Backup 12.5 Hardened Edition versions. However, simplified file names cannot be reconstructed—in version 12, a file name will have a time stamp unless a single-file format is used.

Usage examples

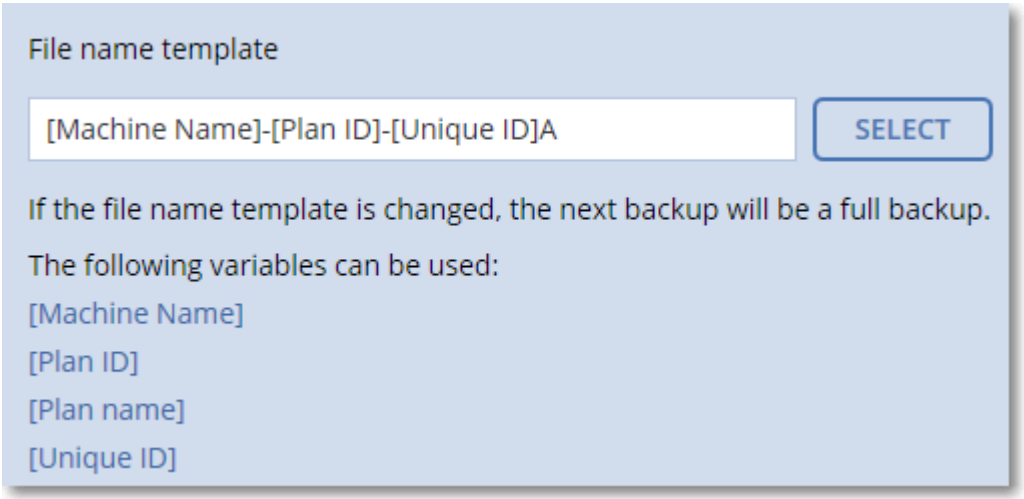
- **View user-friendly file names**

  You want to easily distinguish backups when browsing the backup location with a file manager.

- **Continue an existing sequence of backups**

  Let's assume a backup plan is applied to a single machine, and you have to remove this machine from the backup console or to uninstall the agent along with its configuration settings. After the machine is re-added or the agent is reinstalled, you can force the backup plan to continue backing up to the same backup or backup sequence. Just go this option, click **Select**, and select the required backup.

  The **Browse** button shows the backups in the location selected in the **Where to back up** section of the backup plan panel. It cannot browse anything outside this location.



5.10.4 Backup format

This option defines the format of the backups created by the backup plan. You can choose between the new format (**Version 12**) designed for faster backup and recovery, and the legacy format (**Version 11**) preserved for backward compatibility and special cases. After the backup plan is applied, this option cannot be modified.

This option is *not* effective for mailbox backups. Mailbox backups always have the new format.

The preset is: **Automatic selection**.

You can select one of the following:

- **Automatic selection**

  Version 12 will be used unless the backup plan appends backups to the ones created by earlier product versions.
- **Version 12**

  A new format recommended in most cases for fast backup and recovery. Each backup chain (a full or differential backup, and all incremental backups that depend on it) is saved to a single .tibx file.

  With this format, the retention rule **By total size of backups** is not effective.
- **Version 11**

  A legacy format to be used in a new backup plan that appends backups to the ones created by earlier product versions.

  Also, use this format (with any backup scheme except for **Always incremental (single-file)**) if you want full, incremental, and differential backups to be separate files.

Backup format and backup files

For backup locations that can be browsed with a file manager (such as local or network folders), the backup format determines the number of files and their extension. You can define the file names by using the backup file name (Section 5.10.3) option. The following table lists the files that can be created per machine or mailbox.

	Always incremental (single-file)	**Other backup schemes**
Version 11 backup format	One .tib file and one .xml metadata file	Multiple .tib files and one .xml metadata file (traditional format)
Version 12 backup format	One .tibx file per backup chain (a full or differential backup, and all incremental backups that depend on it)	

5.10.5 Backup validation

Validation is an operation that checks the possibility of data recovery from a backup. When this option is enabled, each backup created by the backup plan is validated immediately after creation.

The preset is: **Disabled**.

Validation calculates a checksum for every data block that can be recovered from the backup.

Validation is a time-consuming process, even for an incremental or differential backup, which are small in size. This is because the operation validates not only the data physically contained in the backup, but all of the data recoverable by selecting the backup. This requires access to previously created backups.

While the successful validation means a high probability of successful recovery, it does not check all factors that influence the recovery process. If you back up the operating system, we recommend performing a test recovery under the bootable media to a spare hard drive or running a virtual machine from the backup (Section 14.1) in the ESXi or Hyper-V environment.

5.10.6 Task start conditions

This option is effective in Windows and Linux operating systems.

This option determines the program behavior in case a task is about to start (the scheduled time comes or the event specified in the schedule occurs), but the condition (or any of multiple conditions) is not met. For more information about conditions refer to "Start conditions" (Section 5.4.2).

The preset is: **Wait until the conditions from the schedule are met.**

Wait until the conditions from the schedule are met

With this setting, the scheduler starts monitoring the conditions and launches the task as soon as the conditions are met. If the conditions are never met, the task will never start.

To handle the situation when the conditions are not met for too long and further delaying the task is becoming risky, you can set the time interval after which the task will run irrespective of the condition. Select the **Run the task anyway after** check box and specify the time interval. The task will start as soon as the conditions are met OR the maximum time delay lapses, depending on which comes first.

Skip the task execution

Delaying a task might be unacceptable, for example, when you need to execute a task strictly at the specified time. Then it makes sense to skip the task rather than wait for the conditions, especially if the tasks occur relatively often.

5.10.7 Changed block tracking (CBT)

This option is effective for disk-level backups of virtual machines and of physical machines running Windows. It is also effective for backups of Microsoft SQL Server databases and Microsoft Exchange Server databases.

The preset is: **Enabled**.

This option determines whether to use Changed Block Tracking (CBT) when performing an incremental or differential backup.

The CBT technology accelerates the backup process. Changes to the disk or database content are continuously tracked at the block level. When a backup starts, the changes can be immediately saved to the backup.

5.10.8 Cluster backup mode

Note *This functionality is not available in the Standard edition of Acronis SCS Cyber Backup 12.5 Hardened Edition.*

These options are effective for database-level backup of Microsoft SQL Server and Microsoft Exchange Server.

These options are effective only if the cluster itself (Microsoft SQL Server Always On Availability Groups (AAG) or Microsoft Exchange Server Database Availability Group (DAG)) is selected for backup, rather than the individual nodes or databases inside of it. If you select individual items inside the cluster, the backup will not be cluster-aware and only the selected copies of the items will be backed up.

Microsoft SQL Server

This option determines the backup mode for SQL Server Always On Availability Groups (AAG). For this option to be effective, Agent for SQL must be installed on all of the AAG nodes. For more information

about backing up Always On Availability Groups, refer to "Protecting Always On Availability Groups (AAG)" (Section 11.2.3).

The preset is: **Secondary replica if possible.**

You can choose one of the following:

- **Secondary replica if possible**

  If all secondary replicas are offline, the primary replica is backed up. Backing up the primary replica may slow down the SQL Server operation, but the data will be backed up in the most recent state.
- **Secondary replica**

  If all secondary replicas are offline, the backup will fail. Backing up secondary replicas does not affect the SQL server performance and allows you to extend the backup window. However, passive replicas may contain information that is not up-to-date, because such replicas are often set to be updated asynchronously (lagged).
- **Primary replica**

  If the primary replica is offline, the backup will fail. Backing up the primary replica may slow down the SQL Server operation, but the data will be backed up in the most recent state.

Regardless of the value of this option, to ensure the database consistency, the software skips databases that are *not* in the **SYNCHRONIZED** or **SYNCHRONIZING** states when the backup starts. If all databases are skipped, the backup fails.

Microsoft Exchange Server

This option determines the backup mode for Exchange Server Database Availability Groups (DAG). For this option to be effective, Agent for Exchange must be installed on all of the DAG nodes. For more information about backing up Database Availability Groups, refer to "Protecting Database Availability Groups (DAG)" (Section 11.2.4).

The preset is: **Passive copy if possible.**

You can choose one of the following:

- **Passive copy if possible**

  If all passive copies are offline, the active copy is backed up. Backing up the active copy may slow down the Exchange Server operation, but the data will be backed up in the most recent state.
- **Passive copy**

  If all passive copies are offline, the backup will fail. Backing up passive copies does not affect the Exchange Server performance and allows you to extend the backup window. However, passive copies may contain information that is not up-to-date, because such copies are often set to be updated asynchronously (lagged).
- **Active copy**

  If the active copy is offline, the backup will fail. Backing up the active copy may slow down the Exchange Server operation, but the data will be backed up in the most recent state.

Regardless of the value of this option, to ensure the database consistency, the software skips databases that are *not* in the **HEALTHY** or **ACTIVE** states when the backup starts. If all databases are skipped, the backup fails.

5.10.9 Compression level

The option defines the level of compression applied to the data being backed up. The available levels are: **None**, **Normal**, **High**, **Maximum**.

The preset is: **Normal**.

A higher compression level means that the backup process takes longer, but the resulting backup occupies less space. Currently, the High and Maximum levels work similarly.

The optimal data compression level depends on the type of data being backed up. For example, even maximum compression will not significantly reduce the backup size if the backup contains essentially compressed files, such as .jpg, .pdf or .mp3. However, formats such as .doc or .xls will be compressed well.

5.10.10 Email notifications

The option enables you to set up email notifications about events that occur during backup.

The preset is: **Use the system settings.**

You can either use the system settings or override them with custom values that will be specific for this plan only. The system settings are configured as described in "Email notifications" (Section 18.1).

Important *When the system settings are changed, all backup plans that use the system settings are affected.*

Before enabling this option, ensure that the **Email server** (Section 18.2) settings are configured.

To customize email notifications for a backup plan

1. Select **Customize the settings for this backup plan**.
2. In the **Recipients' email addresses** field, type the destination email address. You can enter several addresses separated by semicolons.
3. [Optional] In **Subject**, change the email notification subject.

   You can use the following variables:

   - **`[Alert]`** - alert summary.
   - **`[Device]`** - device name.
   - **`[Plan]`** - the name of the plan that generated the alert.
   - **`[ManagementServer]`** - the host name of the machine where the management server is installed.
   - **`[Unit]`** - the name of the unit to which the machine belongs.

   The default subject is **`[Alert]` Device: `[Device]` Plan: `[Plan]`**
4. Select the check boxes for the events that you want to receive notifications about. You can select from the list of all alerts that occur during backup, grouped by severity.

5.10.11 Error handling

These options enable you to specify how to handle errors that might occur during backup.

Re-attempt, if an error occurs

The preset is: **Enabled. Number of attempts: 30. Interval between attempts: 30 seconds.**

When a recoverable error occurs, the program re-attempts to perform the unsuccessful operation. You can set the time interval and the number of attempts. The attempts will be stopped as soon as the operation succeeds OR the specified number of attempts are performed, depending on which comes first.

For example, if the backup destination on the network becomes unavailable or not reachable, the program will attempt to reach the destination every 30 seconds, but no more than 30 times. The attempts will be stopped as soon as the connection is resumed OR the specified number of attempts is performed, depending on which comes first.

Do not show messages and dialogs while processing (silent mode)

The preset is: **Enabled**.

With the silent mode enabled, the program will automatically handle situations requiring user interaction (except for handling bad sectors, which is defined as a separate option). If an operation cannot continue without user interaction, it will fail. Details of the operation, including errors, if any, can be found in the operation log.

Ignore bad sectors

The preset is: **Disabled**.

When this option is disabled, each time the program comes across a bad sector, the backup activity will be assigned the **Interaction required** status. In order to back up the valid information on a rapidly dying disk, enable ignoring bad sectors. The rest of the data will be backed up and you will be able to mount the resulting disk backup and extract valid files to another disk.

Re-attempt, if an error occurs during VM snapshot creation

The preset is: **Enabled. Number of attempts: 3. Interval between attempts: 5 minutes.**

When taking a virtual machine snapshot fails, the program re-attempts to perform the unsuccessful operation. You can set the time interval and the number of attempts. The attempts will be stopped as soon as the operation succeeds OR the specified number of attempts are performed, depending on which comes first.

5.10.12 Fast incremental/differential backup

This option is effective for incremental and differential disk-level backup.

This option is not effective (always disabled) for volumes formatted with the JFS, ReiserFS3, ReiserFS4, ReFS, or XFS file systems.

The preset is: **Enabled**.

Incremental or differential backup captures only data changes. To speed up the backup process, the program determines whether a file has changed or not by the file size and the date/time when the file was last modified. Disabling this feature will make the program compare the entire file contents to those stored in the backup.

5.10.13 File filters

File filters define which files and folders to skip during the backup process.

File filters are available for both disk-level and file-level backup, unless stated otherwise.

To enable file filters

1. Select the data to back up.
2. Click the gear icon next to the backup plan name, and then click **Backup options**.
3. Select **File filters**.
4. Use any of the options described below.

Exclude files matching specific criteria

There are two options that function in an inverse manner.

- **Back up only files matching the following criteria**

  Example: If you select to back up the entire machine and specify **C:\File.exe** in the filter criteria, only this file will be backed up.

  Note *This filter is not effective for file-level backup if* ***Version 11*** *is selected in* ***Backup format*** *(Section 5.10.4).*

- **Do not back up files matching the following criteria**

  Example: If you select to back up the entire machine and specify **C:\File.exe** in the filter criteria, only this file will be skipped.

It is possible to use both options simultaneously. The latter option overrides the former, i.e. if you specify **C:\File.exe** in both fields, this file will be skipped during a backup.

Criteria

- **Full path**

  Specify the full path to the file or folder, starting with the drive letter (when backing up Windows) or the root directory (when backing up Linux).

  Both in Windows and Linux, you can use a forward slash in the file or folder path (as in **C:/Temp/File.tmp**). In Windows, you can also use the traditional backslash (as in **C:\Temp\File.tmp**).

- **Name**

  Specify the name of the file or folder, such as **Document.txt**. All files and folders with that name will be selected.

The criteria are *not* case-sensitive. For example, by specifying **C:\Temp**, you will also select **C:\TEMP**, **C:\temp**, and so on.

You can use one or more wildcard characters (*, **, and ?) in the criterion. These characters can be used both within the full path and in the file or folder name.

The asterisk (*) substitutes for zero or more characters in a file name. For example, the criterion **Doc*.txt** matches files such as **Doc.txt** and **Document.txt**

The double asterisk (**) substitutes for zero or more characters in a file name and path, including the slash character. For example, the criterion ****/Docs/**.txt** matches all txt files in all subfolders of all folders **Docs**.

The question mark (?) substitutes for exactly one character in a file name. For example, the criterion **Doc?.txt** matches files such as **Doc1.txt** and **Docs.txt**, but not the files **Doc.txt** or **Doc11.txt**

Exclude hidden files and folders

Select this check box to skip files and folders that have the **Hidden** attribute (for file systems that are supported by Windows) or that start with a period (.) (for file systems in Linux, such as Ext2 and Ext3). If a folder is hidden, all of its contents (including files that are not hidden) will be excluded.

Exclude system files and folders

This option is effective only for file systems that are supported by Windows. Select this check box to skip files and folders with the **System** attribute. If a folder has the **System** attribute, all of its contents (including files that do not have the **System** attribute) will be excluded.

Tip *You can view file or folder attributes in the file/folder properties or by using the attrib command. For more information, refer to the Help and Support Center in Windows.*

5.10.14 File-level backup snapshot

This option is effective only for file-level backup.

This option defines whether to back up files one by one or by taking an instant data snapshot.

Note *Files that are stored on network shares are always backed up one by one.*

The preset is:

- If only machines running Linux are selected for backup: **Do not create a snapshot.**
- Otherwise: **Create snapshot if it is possible.**

You can select one of the following:

- **Create a snapshot if it is possible**

  Back up files directly if taking a snapshot is not possible.
- **Always create a snapshot**

  The snapshot enables backing up of all files including files opened for exclusive access. The files will be backed up at the same point in time. Choose this setting only if these factors are critical, that is, backing up files without a snapshot does not make sense. If a snapshot cannot be taken, the backup will fail.
- **Do not create a snapshot**

  Always back up files directly. Trying to back up files that are opened for exclusive access will result in a read error. Files in the backup may be not time-consistent.

5.10.15 Log truncation

This option is effective for backup of Microsoft SQL Server databases and for disk-level backup with enabled Microsoft SQL Server application backup.

This option defines whether the SQL Server transaction logs are truncated after a successful backup.

The preset is: **Enabled**.

When this option is enabled, a database can be recovered only to a point in time of a backup created by this software. Disable this option if you back up transaction logs by using the native backup engine of Microsoft SQL Server. You will be able to apply the transaction logs after a recovery and thus recover a database to any point in time.

5.10.16 LVM snapshotting

This option is effective only for physical machines.

This option is effective for disk-level backup of volumes managed by Linux Logical Volume Manager (LVM). Such volumes are also called logical volumes.

This option defines how a snapshot of a logical volume is taken. The backup software can do this on its own or rely on Linux Logical Volume Manager (LVM).

The preset is: **By the backup software**.

- **By the backup software**. The snapshot data is kept mostly in RAM. The backup is faster and unallocated space on the volume group is not required. Therefore, we recommend changing the preset only if you are experiencing problems with backing up logical volumes.
- **By LVM**. The snapshot is stored on unallocated space of the volume group. If the unallocated space is missing, the snapshot will be taken by the backup software.

5.10.17 Mount points

This option is effective only in Windows for a file-level backup of a data source that includes mounted volumes or cluster shared volumes.

This option is effective only when you select for backup a folder that is higher in the folder hierarchy than the mount point. (A mount point is a folder on which an additional volume is logically attached.)

- If such folder (a parent folder) is selected for backup, and the **Mount points** option is enabled, all files located on the mounted volume will be included in the backup. If the **Mount points** option is disabled, the mount point in the backup will be empty.
  During recovery of a parent folder, the mount point content will or will not be recovered, depending on whether the **Mount points** option for recovery (Section 6.6.8) is enabled or disabled.
- If you select the mount point directly, or select any folder within the mounted volume, the selected folders will be considered as ordinary folders. They will be backed up regardless of the state of the **Mount points** option and recovered regardless of the state of the **Mount points** option for recovery (Section 6.6.8).

The preset is: **Disabled**.

Tip. *You can back up Hyper-V virtual machines residing on a cluster shared volume by backing up the required files or the entire volume with file-level backup. Just power off the virtual machines to be sure that they are backed up in a consistent state.*

Example

Let's assume that the **C:\Data1** folder is a mount point for the mounted volume. The volume contains folders **Folder1** and **Folder2**. You create a protection plan for file-level backup of your data.

If you select the check box for volume C and enable the **Mount points** option, the **C:\Data1** folder in your backup will contain **Folder1** and **Folder2**. When recovering the backed-up data, be aware of proper using the **Mount points** option for recovery (Section 6.6.8).

If you select the check box for volume C, and disable the **Mount points** option, the **C:\Data1** folder in your backup will be empty.

If you select the check box for the **Data1**, **Folder1** or **Folder2** folder, the checked folders will be included in the backup as ordinary folders, regardless of the state of the **Mount points** option.

5.10.18 Multi-volume snapshot

This option is effective for backups of physical machines running Windows or Linux.

This option applies to disk-level backup. This option also applies to file-level backup when the file-level backup is performed by taking a snapshot. (The "File-level backup snapshot" (Section 5.10.14) option determines whether a snapshot is taken during file-level backup).

This option determines whether to take snapshots of multiple volumes at the same time or one by one.

The preset is:

- If at least one machine running Windows is selected for backup: **Enabled**.
- If no machines are selected (this is the case when you start creating a backup plan from the **Plans** > **Backup** page): **Enabled**.
- Otherwise: **Disabled**.

When this option is enabled, snapshots of all volumes being backed up are created simultaneously. Use this option to create a time-consistent backup of data spanning multiple volumes; for instance, for an Oracle database.

When this option is disabled, the volumes' snapshots are taken one after the other. As a result, if the data spans several volumes, the resulting backup may be not consistent.

5.10.19 Performance and backup window

This option enables you to set one of three levels of backup performance (high, low, prohibited) for every hour within a week. This way, you can define a time window when backups are allowed to start and run. The high and low performance levels are configurable in terms of the process priority and output speed.

You can configure this option separately for each location specified in the backup plan. To configure this option for a replication location, click the gear icon next to the location name, and then click **Performance and backup window**.

This option is effective only for the backup and backup replication processes. Post-backup commands and other operations included in a backup plan (validation, conversion to a virtual machine) will run regardless of this option.

The preset is: **Disabled**.

When this option is disabled, backups are allowed to run at any time, with the following parameters (no matter if the parameters were changed against the preset value):

- CPU priority: **Low** (in Windows, corresponds to **Below normal**).
- Output speed: **Unlimited.**

When this option is enabled, scheduled backups are allowed or blocked according to the performance parameters specified for the current hour. At the beginning of an hour when backups are blocked, a backup process is automatically stopped and an alert is generated.

Even if scheduled backups are blocked, a backup can be started manually. It will use the performance parameters of the most recent hour when backups were allowed.

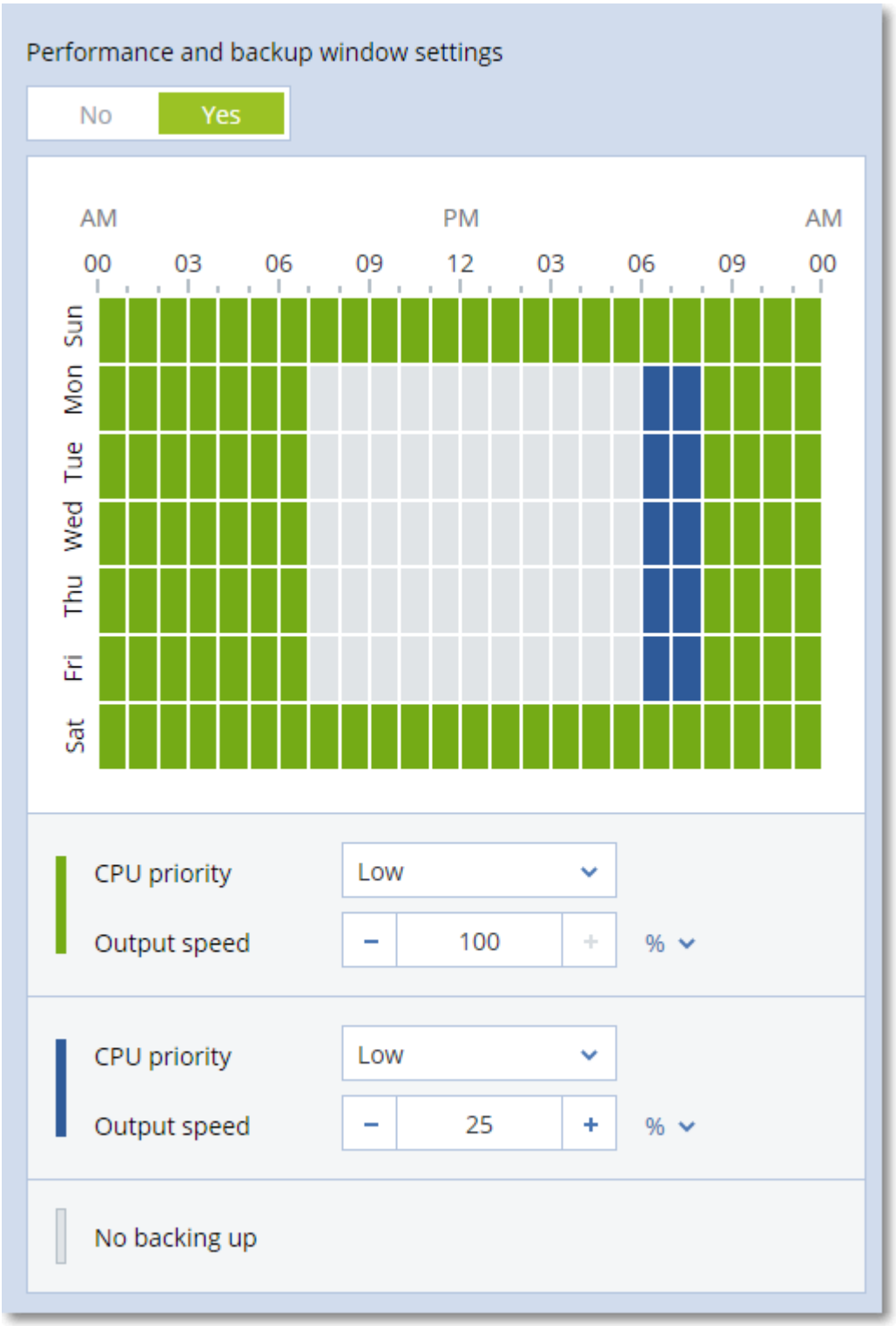
Backup window

Each rectangle represents an hour within a week day. Click a rectangle to cycle through the following states:

- **Green:** backup is allowed with the parameters specified in the green section below.

- **Blue:** backup is allowed with the parameters specified in the blue section below. This state is not available if the backup format is set to **Version 11**.
- **Gray:** backup is blocked.

You can click and drag to change the state of multiple rectangles simultaneously.



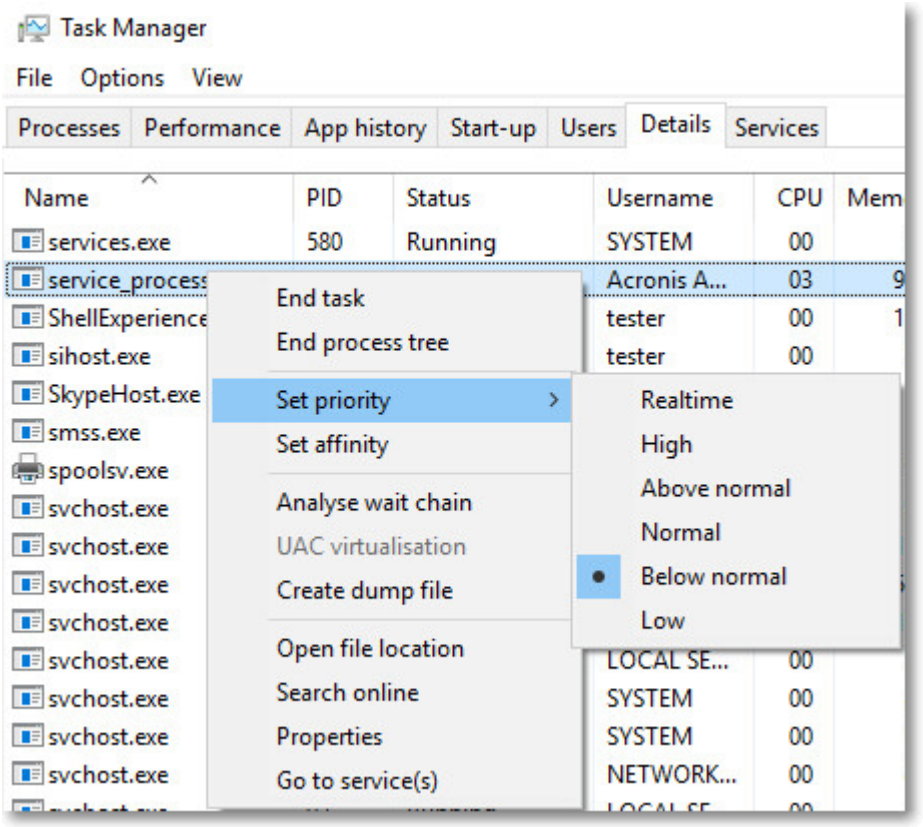
CPU priority

This parameter defines the priority of the backup process in the operating system.

The available settings are: **Low**, **Normal**, **High**.

The priority of a process running in a system determines the amount of CPU and system resources allocated to that process. Decreasing the backup priority will free more resources for other applications. Increasing the backup priority might speed up the backup process by requesting the operating system to allocate more resources like the CPU to the backup application. However, the resulting effect will depend on the overall CPU usage and other factors like disk in/out speed or network traffic.

This option sets the priority of the backup process (**service_process.exe)** in Windows and the niceness of the backup process (**service_process)** in Linux and OS X.



Output speed during backup

This parameter enables you to limit the hard drive writing speed (when backing up to a local folder) or the speed of transferring the backup data through the network (when backing up to a network share.

When this option is enabled, you can specify the maximum allowed output speed:

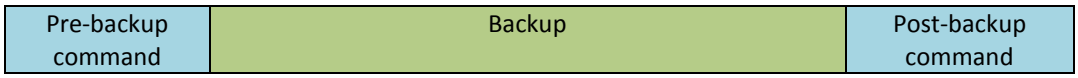
- As a percentage of the estimated writing speed of the destination hard disk (when backing up to a local folder) or of the estimated maximum speed of the network connection (when backing up to a network share).

  This setting works only if the agent is running in Windows.
- In KB/second (for all destinations).

5.10.20 Pre/Post commands

The option enables you to define the commands to be automatically executed before and after the backup procedure.

The following scheme illustrates when pre/post commands are executed.



Examples of how you can use the pre/post commands:

- Delete some temporary files from the disk before starting backup.
- Configure a third-party antivirus product to be started each time before the backup starts.
- Selectively copy backups to another location. This option may be useful because the replication configured in a backup plan copies *every* backup to subsequent locations.

The agent performs the replication *after* executing the post-backup command.

The program does not support interactive commands, i.e. commands that require user input (for example, "pause").

5.10.20.1 Pre-backup command

To specify a command/batch file to be executed before the backup process starts

1. Enable the **Execute a command before the backup** switch.
2. In the **Command...** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command's execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

Check box	**Selection**			
Fail the backup if the command execution fails*	Selected	Cleared	Selected	Cleared
Do not back up until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Perform the backup only after the command is successfully executed. Fail the backup if the command execution fails.	Perform the backup after the command is executed despite execution failure or success.	N/A	Perform the backup concurrently with the command execution and irrespective of the command execution result.

* A command is considered failed if its exit code is not equal to zero.

5.10.20.2 Post-backup command

To specify a command/executable file to be executed after the backup is completed

1. Enable the **Execute a command after the backup** switch.

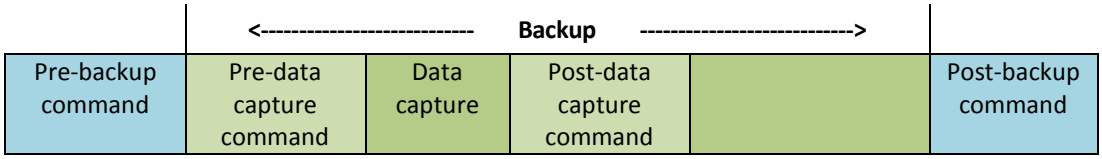
2. In the **Command...** field, type a command or browse to a batch file.
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field, specify the command execution arguments, if required.
5. Select the **Fail the backup if the command execution fails** check box if successful execution of the command is critical for you. The command is considered failed if its exit code is not equal to zero. If the command execution fails, the backup status will be set to **Error**.

   When the check box is not selected, the command execution result does not affect the backup failure or success. You can track the command execution result by exploring the **Activities** tab.
6. Click **Done**.

5.10.21 Pre/Post data capture commands

The option enables you to define the commands to be automatically executed before and after data capture (that is, taking the data snapshot). Data capture is performed at the beginning of the backup procedure.

The following scheme illustrates when the pre/post data capture commands are executed.



If the Volume Shadow Copy Service option (Section 5.10.28) is enabled, the commands' execution and the Microsoft VSS actions will be sequenced as follows:

"Before data capture" commands -> VSS Suspend -> Data capture -> VSS Resume -> "After data capture" commands.

By using the pre/post data capture commands, you can suspend and resume a database or application that is not compatible with VSS. Because the data capture takes seconds, the database or application idle time will be minimal.

5.10.21.1 Pre-data capture command

To specify a command/batch file to be executed before data capture

1. Enable the **Execute a command before the data capture** switch.
2. In the **Command...** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command's execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

Check box	**Selection**			
Fail the backup if the command execution fails*	Selected	Cleared	Selected	Cleared
Do not perform the data capture until the command	Selected	Selected	Cleared	Cleared

execution is complete				
Result				
	Preset Perform the data capture only after the command is successfully executed. Fail the backup if the command execution fails.	Perform the data capture after the command is executed despite execution failure or success.	N/A	Perform the data capture concurrently with the command and irrespective of the command execution result.

* A command is considered failed if its exit code is not equal to zero.

5.10.21.2 Post-data capture command

To specify a command/batch file to be executed after data capture

1. Enable the **Execute a command after the data capture** switch.
2. In the **Command...** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command's execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

Check box	**Selection**			
Fail the backup if the command execution fails*	Selected	Cleared	Selected	Cleared
Do not back up until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Continue the backup only after the command is successfully executed.	Continue the backup after the command is executed despite command execution failure or success.	N/A	Continue the backup concurrently with the command execution and irrespective of the command execution result.

* A command is considered failed if its exit code is not equal to zero.

5.10.22 SAN hardware snapshots

This option is effective for backups of VMware ESXi virtual machines.

The preset is: **Disabled**.

This option determines whether to use the SAN snapshots when performing a backup.

If this option is disabled, the virtual disk content will be read from a VMware snapshot. The snapshot will be kept for the whole duration of the backup.

If this option is enabled, the virtual disk content will be read from a SAN snapshot. A VMware snapshot will be created and kept briefly, to bring the virtual disks into a consistent state. If reading from a SAN snapshot is not possible, the backup will fail.

Prior to enabling this option, please check and carry out the requirements listed in "Using SAN hardware snapshots" (Section 14.2.3).

5.10.23 Scheduling

This option defines whether backups start as scheduled or with a delay, and how many virtual machines are backed up simultaneously.

The preset is: **Start all backups exactly as scheduled.**

You can select one of the following:

- **Start all backups exactly as scheduled**
  Backups of physical machines will start exactly as scheduled. Virtual machines will be backed up one by one.
- **Distribute start times within a time window**
  Backups of physical machines will start with a delay from the scheduled time. The delay value for each machine is selected randomly and ranges from zero to the maximum value you specify. You may want to use this setting when backing up multiple machines to a network location, to avoid excessive network load. The delay value for each machine is determined when the backup plan is applied to the machine and remains the same until you edit the backup plan and change the maximum delay value.
  Virtual machines will be backed up one by one.
- **Limit the number of simultaneously running backups by**
  This option is available only when a backup plan is applied to multiple virtual machines. This option defines how many virtual machines an agent can back up simultaneously when executing the given backup plan.
  If, according to the backup plan, an agent has to start backing up multiple machines at once, it will choose two machines. (To optimize the backup performance, the agent tries to match machines stored on different storages.) Once any of the two backups is completed, the agent chooses the third machine and so on.
  You can change the number of virtual machines for an agent to simultaneously back up. The maximum value is 10. However, if the agent executes multiple backup plans that overlap in time, the numbers specified in their options are added up. You can limit the total number of virtual machines (Section 14.5) that an agent can back up simultaneously, no matter how many backup plans are running.
  Backups of physical machines will start exactly as scheduled.

5.10.24 Sector-by-sector backup

The option is effective only for disk-level backup.

This option defines whether an exact copy of a disk or volume on a physical level is created.

The preset is: **Disabled**.

Move a tape back to the slot after each successful backup of each machine

The preset is: **Enabled**.

If you disable this option, a tape will remain in the drive after an operation using the tape is completed. Otherwise, the software will move the tape back to the slot where it was before the operation. If, according to the backup plan, other operations follow the backup (such as the backup validation or replication to another location), the tape will be moved back to the slot after completion of these operations.

If both this option and the **Eject tapes after each successful backup of each machine** option are enabled, the tape will be ejected.

Eject tapes after each successful backup of each machine

The preset is: **Disabled**.

When this check box is selected, the software will eject tapes after any successful backup of each machine. If, according to the backup plan, other operations follow the backup (such as the backup validation or replication to another location), the tapes will be ejected after completion of these operations.

Overwrite a tape in the stand-alone tape drive when creating a full backup

The preset is: **Disabled**.

The option applies only to stand-alone tape drives. When this option is enabled, a tape inserted into a drive will be overwritten every time a full backup is created.

Use the following tape devices and drives

This option enables you to specify tape devices and tape drives to be used by the backup plan.

A tape pool contains tapes from all tape devices attached to a machine. When you select a tape pool as a backup location, you indirectly select the machine to which the tape device(s) are attached. By default, backups can be written to tapes through any tape drive on any tape device attached to that machine. If some of the devices or drives are missing or not operational, the backup plan will use those that are available.

You can click **Only selected devices and drives**, and then choose tape devices and drives from the list. By selecting an entire device, you select all of its drives. This means that any of these drives can be used by the backup plan. If the selected device or drive is missing or is not operational, and no other devices are selected, the backup will fail.

By using this option, you can control backups performed by multiple agents to a large tape library with multiple drives. For example, a backup of a large file server or file share may not start if multiple agents back up their machines during the same backup window, because the agents occupy all of the drives. If you allow the agents to use, say, drives 2 and 3, drive 1 becomes reserved for the agent that backs up the share.

Use tape sets within the tape pool selected for backup

The preset is: **Disabled**.

Tapes within one pool can be grouped into so-called **tape sets**.

If you leave this option disabled, data will be backed up on all tapes belonging to a pool. If the option is enabled, you can separate backups according to the predefined or custom rules.

- **Use a separate tape set for each** (choose a rule: **Backup type**, **Device type**, **Device name**, **Day in month**, **Day of week**, **Month of year**, **Year**, **Date**)

  If this variant is selected, you can organize tape sets according to a predefined rule. For example, you can have separate tape sets for each day of the week or store backups of each machine on a separate tape set.

- **Specify a custom rule for tape sets**

  If this variant is selected, specify your own rule to organize tape sets. The rule can contain the following variables:

Variable syntax	Variable description	Available values
[Resource Name]	Backups of each machine will be stored on a separate tape set.	Names of the machines registered on the management server.
[Backup Type]	Full, incremental, and differential backups will be stored on separate tape sets.	**full**, **inc**, **diff**
[Resource Type]	Backups of machines of each type will be stored on a separate tape set.	**Server essentials**, **Server**, **Workstation**, **Physical machine**, **VMware Virtual Machine**, **Virtual-PC Virtual Machine**, **Virtual Server Virtual Machine**, **Hyper-V Virtual Machine**, **Parallels Virtual Machine**, **XEN Virtual Machine**, **KVM Virtual Machine**, **RHEV Virtual Machine**, **Parallels Cloud Virtual Machine**
[Day]	Backups created on each day of the month will be stored on a separate tape set.	**01**, **02**, **03**, ..., **31**
[Weekday]	Backups created on each day of the week will be stored on a separate tape set.	**Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**
[Month]	Backups created during each month of the year will be stored on a separate tape set.	**January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, **December**
[Year]	Backups created during each year will be stored on a separate tape set.	**2017**, **2018**, ...

  For example, if you specify the rule as **[Resource Name]-[Backup Type]**, you will have a separate tape set for each full, incremental, and differential backup of each machine to which the backup plan is applied.

You can also specify tape sets (Section 17.1.4.4) for individual tapes. In this case, the software will first write backups on tapes whose tape set value coincides with the value of the expression specified in the backup plan. Then, if necessary, other tapes from the same pool will be taken. After that, if the pool is replenishable, tapes from the **Free tapes** pool will be used.

For example, if you specify tape set **Monday** for Tape 1, **Tuesday** for Tape 2, etc. and specify **[Weekday]** in the backup options, the corresponding tape will be used on the respective day of the week.

5.10.27 Task failure handling

This option determines the program behavior when a scheduled execution of a backup plan fails. This option is not effective when a backup plan is started manually.

If this option is enabled, the program will try to execute the backup plan again. You can specify the number of attempts and the time interval between the attempts. The program stops trying as soon as an attempt completes successfully OR the specified number of attempts is performed, depending on which comes first.

The preset is: **Disabled**.

5.10.28 Volume Shadow Copy Service (VSS)

This option is effective only for Windows operating systems.

The option defines whether a Volume Shadow Copy Service (VSS) provider has to notify VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications; in particular, completion of all database transactions at the moment of taking the data snapshot by the backup software. Data consistency, in turn, ensures that the application will be recovered in the correct state and become operational immediately after recovery.

The preset is: **Enabled**. **Automatically select snapshot provider**.

You can select one of the following:

- **Automatically select snapshot provider**

  Automatically select among the hardware snapshot provider, software snapshot providers, and Microsoft Software Shadow Copy provider.
- **Use Microsoft Software Shadow Copy provider**

  We recommend choosing this option when backing up application servers (Microsoft Exchange Server, Microsoft SQL Server, or Active Directory).

Disable this option if your database is incompatible with VSS. Snapshots are taken faster, but data consistency of the applications whose transactions are not completed at the time of taking a snapshot cannot be guaranteed. You may use Pre/Post data capture commands (Section 5.10.21) to ensure that the data is backed up in a consistent state. For instance, specify pre-data capture commands that will suspend the database and flush all caches to ensure that all transactions are completed; and specify post-data capture commands that will resume the database operations after the snapshot is taken.

Note *If this option is enabled, files and folders that are specified in the* ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot*** *registry key are not backed up. In particular, offline Outlook Data Files (.ost) are not backed up because they are specified in the* ***OutlookOST*** *value of this key.*

Enable VSS full backup

If this option is enabled, logs of Microsoft Exchange Server and of other VSS-aware applications (except for Microsoft SQL Server) will be truncated after each successful full, incremental or differential disk-level backup.

The preset is: **Disabled**.

Leave this option disabled in the following cases:

- If you use Agent for Exchange or third-party software for backing up the Exchange Server data. This is because the log truncation will interfere with the consecutive transaction log backups.
- If you use third-party software for backing up the SQL Server data. The reason for this is that the third-party software will take the resulting disk-level backup for its "own" full backup. As a result, the next differential backup of the SQL Server data will fail. The backups will continue failing until the third-party software creates the next "own" full backup.
- If other VSS-aware applications are running on the machine and you need to keep their logs for any reason.

Enabling this option does not result in the truncation of Microsoft SQL Server logs. To truncate the SQL Server log after a backup, enable the Log truncation (Section 5.10.15) backup option.

5.10.29 Volume Shadow Copy Service (VSS) for virtual machines

This option defines whether quiesced snapshots of virtual machines are taken. To take a quiesced snapshot, the backup software applies VSS inside a virtual machine by using VMware Tools, or Hyper-V Integration Services.

The preset is: **Enabled**.

If this option is enabled, transactions of all VSS-aware applications running in a virtual machine are completed before taking snapshot. If a quiesced snapshot fails after the number of re-attempts specified in the "Error handling" (Section 5.10.11) option, and application backup is disabled, a non-quiesced snapshot is taken. If application backup is enabled, the backup fails.

If this option is disabled, a non-quiesced snapshot is taken. The virtual machine will be backed up in a crash-consistent state.

5.10.30 Weekly backup

This option determines which backups are considered "weekly" in retention rules and backup schemes. A "weekly" backup is the first backup created after a week starts.

The preset is: **Monday**.

5.10.31 Windows event log

This option is effective only in Windows operating systems.

This option defines whether the agents have to log events of the backup operations in the Application Event Log of Windows (to see this log, run eventvwr.exe or select **Control Panel** > **Administrative tools** > **Event Viewer**). You can filter the events to be logged.

The preset is: **Disabled**.

6 Recovery

6.1 Recovery cheat sheet

The following table summarizes the available recovery methods. Use the table to choose a recovery method that best fits your need.

What to recover	Recovery method
Physical machine (Windows or Linux)	Using the web interface (Section 6.3) Using bootable media (Section 6.3.4)
Virtual machine (VMware or Hyper-V)	Using the web interface (Section 6.3.3) Using bootable media (Section 6.3.4)
ESXi configuration	Using bootable media (Section 6.5)
Files/Folders	Using the web interface (Section 6.4.1) Using bootable media (Section 6.4.2) Extracting files from local backups (Section 6.4.3)
SQL databases	Using the web interface (Section 11.4.1)
Exchange databases	
Exchange mailboxes	
Oracle databases	Using Oracle Explorer tool (Section 12)

6.2 Creating bootable media

Bootable media is a CD, DVD, USB flash drive, or other removable media that enables you to run the agent without the help of an operating system. The main purpose of bootable media is to recover an operating system that cannot start.

We highly recommend that you create and test a bootable media as soon as you start using disk-level backup. Also, it is a good practice to re-create the media after each major update of the backup agent.

You can recover either Windows or Linux by using the same media.

To create bootable media in Windows or Linux

1. Download the bootable media ISO file. To download the file, click the account icon in the top-right corner > **Downloads** > **Bootable media**.
2. Do any of the following:
   - Burn a CD/DVD using the ISO file.
   - Create a bootable USB flash drive by using the ISO file and one of the free tools available online.

     Use `ISO to USB` or RUFUS if you need to boot an UEFI machine, `Win32DiskImager` for a BIOS machine. In Linux, using the `dd` utility makes sense.
   - Connect the ISO file as a CD/DVD drive to the virtual machine that you want to recover.

Alternatively, you can create bootable media by using Bootable Media Builder (Section 10.1).

6.3 Recovering a machine

6.3.1 Physical machine

This section describes recovery of physical machines by using the web interface.

Use bootable media instead of the web interface if you need to recover:

- Any operating system to bare metal or to an offline machine
- The structure of logical volumes (volumes created by Logical Volume Manager in Linux). The media enables you to recreate the logical volume structure automatically.

Recovery of an operating system requires a reboot. You can choose whether to restart the machine automatically or assign it the **Interaction required** status. The recovered operating system goes online automatically.

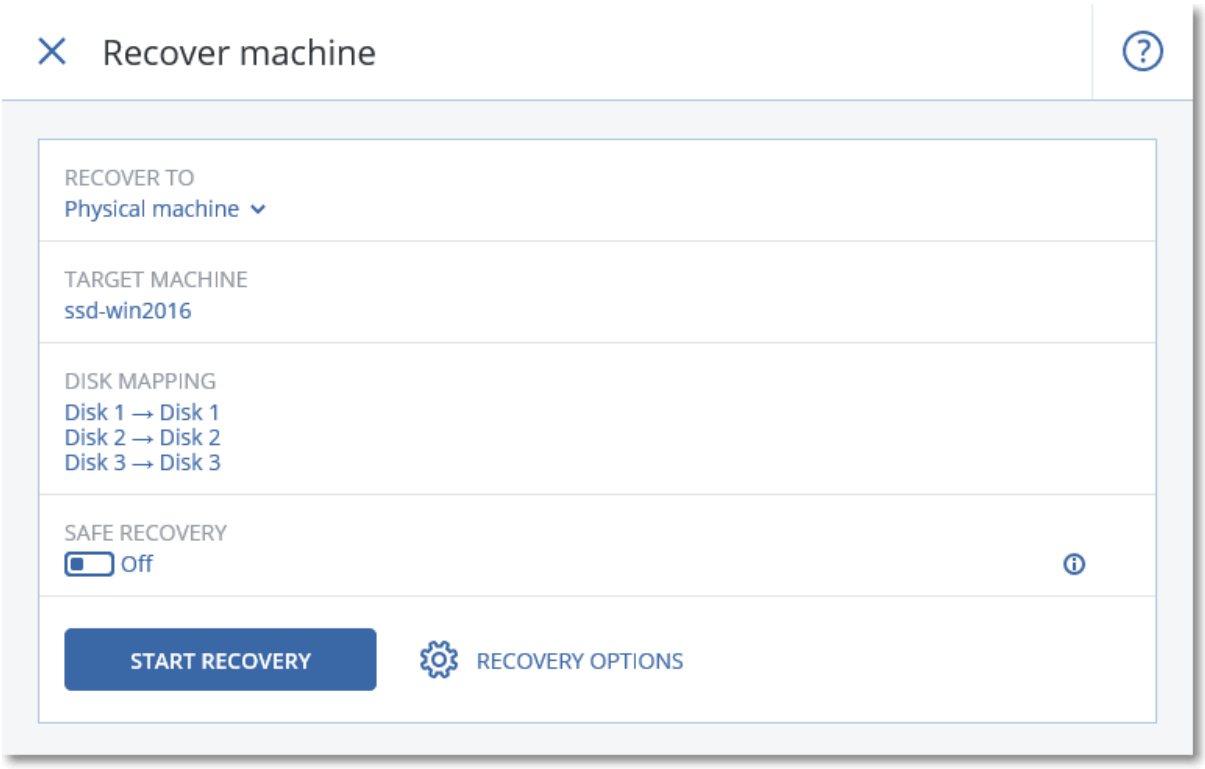
To recover a physical machine

1. Select the backed-up machine.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do any of the following:

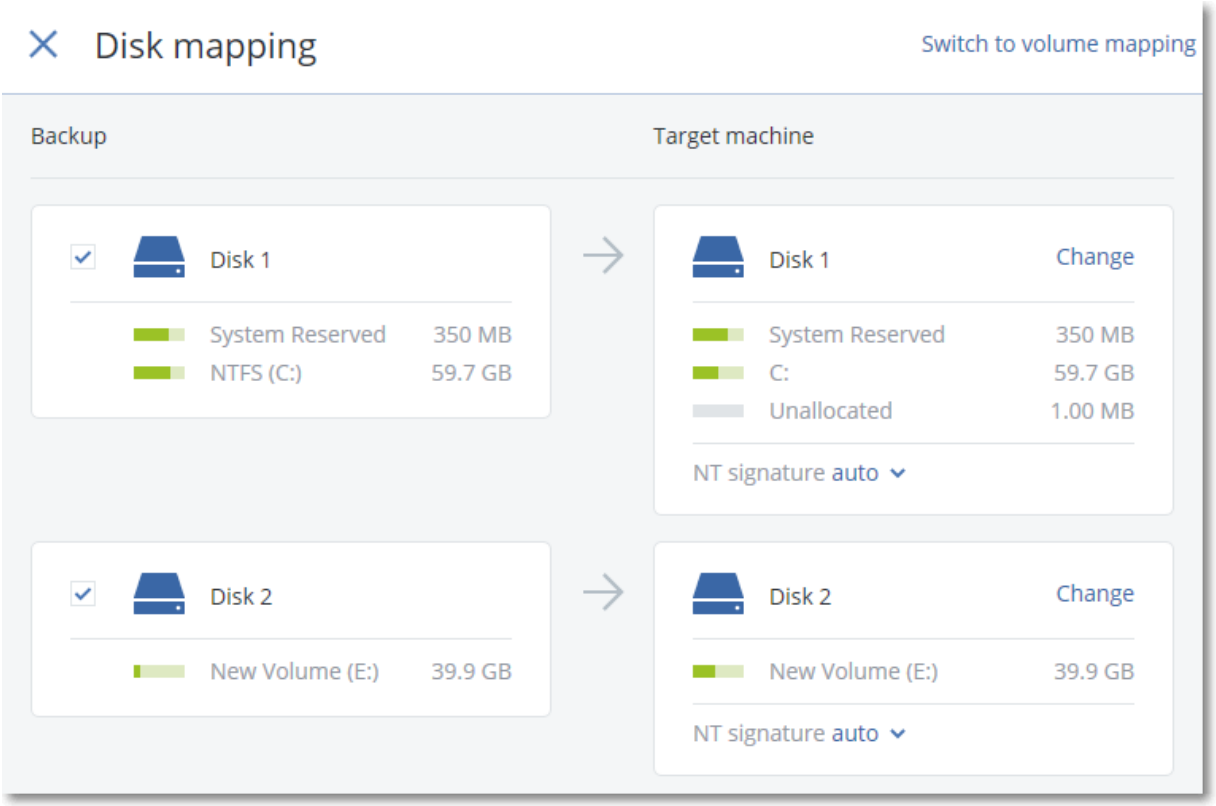
   - If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select a target machine that is online, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).
   - Recover the machine as described in "Recovering disks by using bootable media" (Section 6.3.4).
4. Click **Recover** > **Entire machine**.

   The software automatically maps the disks from the backup to the disks of the target machine. To recover to another physical machine, click **Target machine**, and then select a target machine that is online.



5. If you are unsatisfied with the mapping result or if the disk mapping fails, click **Disk mapping** to re-map the disks manually.

The mapping section also enables you to choose individual disks or volumes for recovery. You can switch between recovering disks and volumes by using the **Switch to...** link in the top-right corner.



6. Click **Start recovery**.
7. Confirm that you want to overwrite the disks with their backed-up versions. Choose whether to restart the machine automatically.

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

6.3.2 Physical machine to virtual

This section describes recovery of a physical machine as a virtual machine by using the web interface. This operation can be performed if at least one Agent for VMware or Agent for Hyper-V is installed and registered.

For more information about P2V migration, refer to "Machine migration" (Section 14.3). ***To recover a physical machine as a virtual machine***

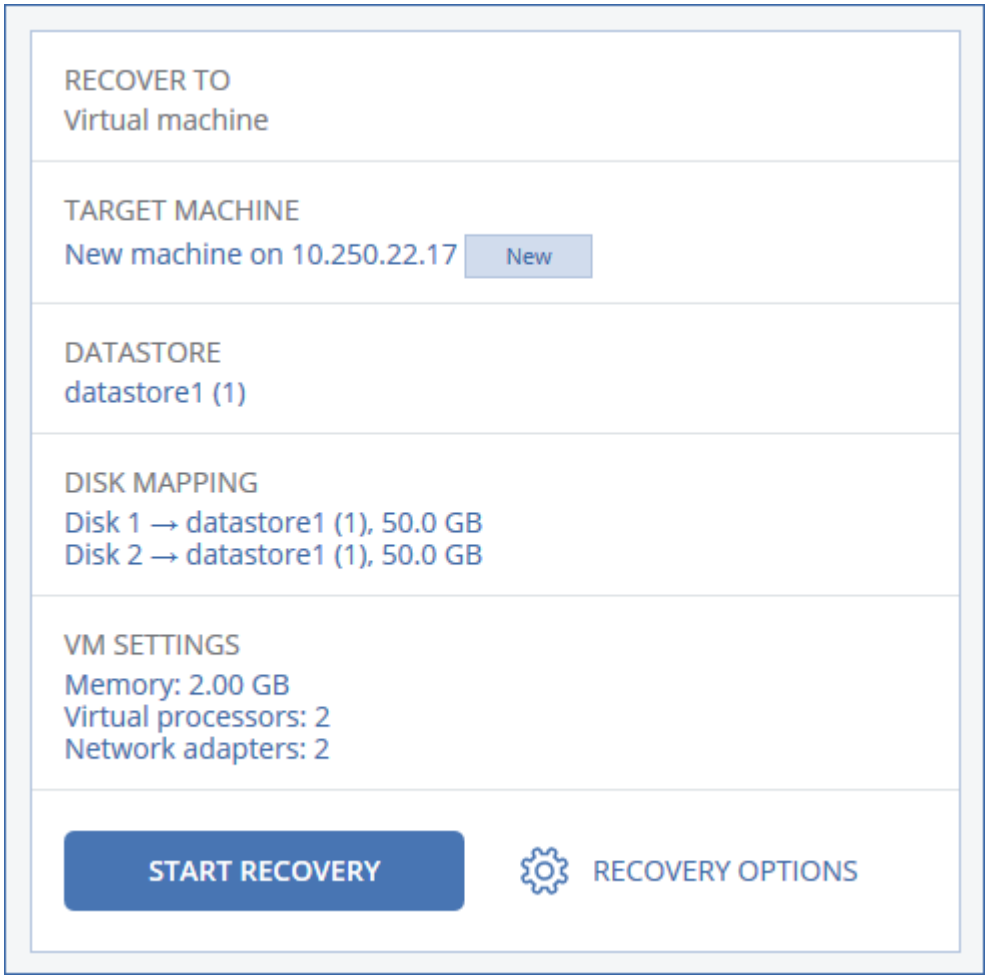
1. Select the backed-up machine.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do any of the following:

   - If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select a machine that is online, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).

- Recover the machine as described in "Recovering disks by using bootable media" (Section 6.3.4).

4. Click **Recover** > **Entire machine**.
5. In **Recover to**, select **Virtual machine**.
6. Click **Target machine**.
   a. Select the hypervisor (**VMware ESXi** or **Hyper-V**).
      At least one Agent for VMware or Agent for Hyper-V must be installed.
   b. Select whether to recover to a new or existing machine. The new machine option is preferable as it does not require the disk configuration of the target machine to exactly match the disk configuration in the backup.
   c. Select the host and specify the new machine name, or select an existing target machine.
   d. Click **OK**.
7. [Optional] When recovering to a new machine, you can also do the following:
   - Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore (storage) for the virtual machine.
   - Click **Disk mapping** to select the datastore (storage), interface, and provisioning mode for each virtual disk. The mapping section also enables you to choose individual disks for recovery.
   - Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.



8. Click **Start recovery**.
9. When recovering to an existing virtual machine, confirm that you want to overwrite the disks.

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

6.3.3 Virtual machine

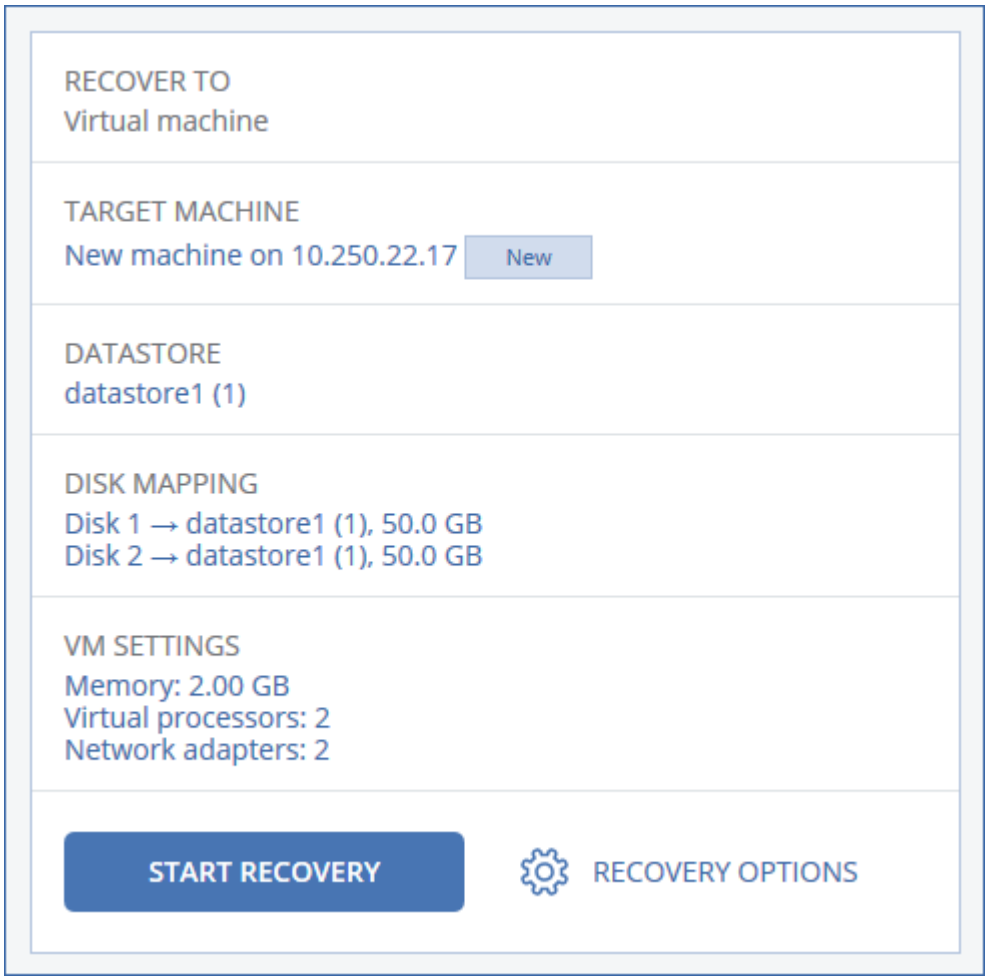
A virtual machine must be stopped during the recovery to this machine. The software stops the machine without a prompt. When the recovery is completed, you have to start the machine manually.

This behavior can be changed by using the VM power management recovery option (click **Recovery options** > **VM power management**).

To recover a virtual machine

1. Do one of the following:
   - Select a backed-up machine, click **Recovery**, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).
2. Click **Recover** > **Entire machine**.
3. If you want to recover to a physical machine, select **Physical machine** in **Recover to**. Otherwise, skip this step.
   Recovery to a physical machine is possible only if the disk configuration of the target machine exactly matches the disk configuration in the backup.
   If this is the case, continue to step 4 in "Physical machine" (Section 6.3.1). Otherwise, we recommend that you perform the V2P migration by using bootable media (Section 6.3.4).
4. The software automatically selects the original machine as the target machine.
   To recover to another virtual machine, click **Target machine**, and then do the following:
   a. Select the hypervisor (**VMware ESXi** or **Hyper-V**).
   b. Select whether to recover to a new or existing machine.
   c. Select the host and specify the new machine name, or select an existing target machine.
   d. Click **OK**.
5. [Optional] When recovering to a new machine, you can also do the following:
   - Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore (storage) for the virtual machine.
   - Click **Disk mapping** to select the datastore (storage), interface, and provisioning mode for each virtual disk. The mapping section also enables you to choose individual disks for recovery.

- Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.



6. Click **Start recovery**.
7. When recovering to an existing virtual machine, confirm that you want to overwrite the disks.

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

6.3.4 Recovering disks by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (Section 6.2).

To recover disks by using bootable media

1. Boot the target machine by using bootable media
2. Click **Manage this machine** locally or click **Rescue Bootable Media** twice, depending on the media type you are using
3. If a proxy server is enabled in your network, click **Tools** > **Proxy server**, and then specify the proxy server host name/IP address and port. Otherwise, skip this step.
4. On the welcome screen, click **Recover**.
5. Click Select data, and then click **Browse**.

6. Specify the backup location by browsing to the folder under **Local folders** or **Network folders**. Click **OK** to confirm your selection.

7. Select the backup from which you want to recover the data. If prompted, type the password for the backup.

8. In **Backup contents**, select the disks that you want to recover. Click **OK** to confirm your selection.

9. Under **Where to recover**, the software automatically maps the selected disks to the target disks. If the mapping is not successful or if you are unsatisfied with the mapping result, you can re-map disks manually.

Changing disk layout may affect the operating system bootability. Please use the original machine's disk layout unless you feel fully confident of success.

---

11. [For Linux only] If the backed-up machine had logical volumes (LVM) and you want to reproduce the original LVM structure:
    a. Ensure that the number of the target machine disks and each disk capacity are equal to or exceed those of the original machine, and then click **Apply RAID/LVM**.
    b. Review the volume structure, and then click **Apply RAID/LVM** to create it.
12. [Optional] Click **Recovery options** to specify additional settings.
13. Click **OK** to start the recovery.

6.3.5 Using Universal Restore

The most recent operating systems remain bootable when recovered to dissimilar hardware, including the VMware or Hyper-V platforms. If a recovered operating system does not boot, use the Universal Restore tool to update the drivers and modules that are critical for the operating system startup.

Universal Restore is applicable to Windows and Linux.

To apply Universal Restore

1. Boot the machine from the bootable media.
2. Click **Apply Universal Restore**.
3. If there are multiple operating systems on the machine, choose the one to apply Universal Restore to.
4. [For Windows only] Configure the additional settings (Section 6.3.5.1).
5. Click **OK**.

6.3.5.1 Universal Restore in Windows

Preparation

Prepare drivers

Before applying Universal Restore to a Windows operating system, make sure that you have the drivers for the new HDD controller and the chipset. These drivers are critical to start the operating system. Use the CD or DVD supplied by the hardware vendor or download the drivers from the vendor's website. The driver files should have the *.inf extension. If you download the drivers in the *.exe, *.cab or *.zip format, extract them using a third-party application.

The best practice is to store drivers for all the hardware used in your organization in a single repository sorted by device type or by the hardware configurations. You can keep a copy of the repository on a DVD or a flash drive; pick some drivers and add them to the bootable media; create the custom bootable media with the necessary drivers (and the necessary network configuration) for each of your servers. Or, you can simply specify the path to the repository every time Universal Restore is used.

Check access to the drivers in bootable environment

Make sure you have access to the device with drivers when working under bootable media. Use WinPE-based media if the device is available in Windows but Linux-based media does not detect it.

Universal Restore settings

Automatic driver search

Specify where the program will search for the Hardware Abstraction Layer (HAL), HDD controller driver and network adapter driver(s):

- If the drivers are on a vendor's disc or other removable media, turn on the **Search removable media**.
- If the drivers are located in a networked folder or on the bootable media, specify the path to the folder by clicking **Add folder**.

In addition, Universal Restore will search the Windows default driver storage folder. Its location is determined in the registry value **DevicePath**, which can be found in the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. This storage folder is usually WINDOWS/inf.

Universal Restore will perform the recursive search in all the sub-folders of the specified folder, find the most suitable HAL and HDD controller drivers of all those available, and install them into the system. Universal Restore also searches for the network adapter driver; the path to the found driver is then transmitted by Universal Restore to the operating system. If the hardware has multiple network interface cards, Universal Restore will try to configure all the cards' drivers.

Mass storage drivers to install anyway

You need this setting if:

- The hardware has a specific mass storage controller such as RAID (especially NVIDIA RAID) or a fibre channel adapter.
- You migrated a system to a virtual machine that uses a SCSI hard drive controller. Use SCSI drivers bundled with your virtualization software or download the latest drivers versions from the software manufacturer website.
- If the automatic drivers search does not help to boot the system.

Specify the appropriate drivers by clicking **Add driver**. The drivers defined here will be installed, with appropriate warnings, even if the program finds a better driver.

Universal Restore process

After you have specified the required settings, click **OK**.

If Universal Restore cannot find a compatible driver in the specified locations, it will display a prompt about the problem device. Do one of the following:

- Add the driver to any of the previously specified locations and click **Retry**.
- If you do not remember the location, click **Ignore** to continue the process. If the result is not satisfactory, reapply Universal Restore. When configuring the operation, specify the necessary driver.

Once Windows boots, it will initialize the standard procedure for installing new hardware. The network adapter driver will be installed silently if the driver has the Microsoft Windows signature. Otherwise, Windows will ask for confirmation on whether to install the unsigned driver.

After that, you will be able to configure the network connection and specify drivers for the video adapter, USB and other devices.

6.3.5.2 Universal Restore in Linux

Universal Restore can be applied to Linux operating systems with a kernel version of 2.6.8 or later.

When Universal Restore is applied to a Linux operating system, it updates a temporary file system known as the initial RAM disk (initrd). This ensures that the operating system can boot on the new hardware.

Universal Restore adds modules for the new hardware (including device drivers) to the initial RAM disk. As a rule, it finds the necessary modules in the **/lib/modules** directory. If Universal Restore cannot find a module it needs, it records the module's file name into the log.

Universal Restore may modify the configuration of the GRUB boot loader. This may be required, for example, to ensure the system bootability when the new machine has a different volume layout than the original machine.

Universal Restore never modifies the Linux kernel.

Reverting to the original initial RAM disk

You can revert to the original initial RAM disk if necessary.

The initial RAM disk is stored on the machine in a file. Before updating the initial RAM disk for the first time, Universal Restore saves a copy of it to the same directory. The name of the copy is the name of the file, followed by the **_acronis_backup.img** suffix. This copy will not be overwritten if you run Universal Restore more than once (for example, after you have added missing drivers).

To revert to the original initial RAM disk, do any of the following:

- Rename the copy accordingly. For example, run a command similar to the following:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img
initrd-2.6.16.60-0.21-default
```

- Specify the copy in the **initrd** line of the GRUB boot loader configuration.

6.4 Recovering files

6.4.1 Recovering files by using the web interface

1. Select the machine that originally contained the data that you want to recover.
2. Click **Recovery**.
3. Select the recovery point. Note that recovery points are filtered by location.
   If the selected machine is physical and it is offline, recovery points are not displayed. Do one of the following:
   - [Recommended] If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select a target machine that is online, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).
   - Use bootable media (Section 6.4.2).
4. Click **Recover** > **Files/folders**.
5. Browse to the required folder or use search to obtain the list of the required files and folders.
   You can use one or more wildcard characters (* and ?). For more details about using wildcards, refer to "File filters" (Section 5.10.13).
6. Select the files that you want to recover.
7. If you want to save the files as a .zip file, click **Download**, select the location to save the data to, and click **Save**. Otherwise, skip this step.
   Downloading is not available if your selection contains folders or the total size of the selected files exceeds 100 MB.
8. Click **Recover**.
   In **Recover to**, you see one of the following:
   - The machine that originally contained the files that you want to recover (if an agent is installed on this machine).
   - The machine where Agent for VMware or Agent for Hyper-V is installed (if the files originate from an ESXi or Hyper-V virtual machine).

   This is the target machine for the recovery. You can select another machine, if necessary.
9. In **Path**, select the recovery destination. You can select one of the following:
   - The original location (when recovering to the original machine)
   - A local folder on the target machine
   - A network folder that is accessible from the target machine.
10. Click **Start recovery**.
11. Select one of the file overwriting options:
    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**

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

6.4.2 Recovering files by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (Section 6.2).

To recover files by using bootable media

1. Boot the target machine by using the bootable media.
2. Click **Manage this machine locally** or click **Rescue Bootable Media** twice, depending on the media type you are using.
3. If a proxy server is enabled in your network, click **Tools** > **Proxy server**, and then specify the proxy server host name/IP address and port. Otherwise, skip this step.
4. On the welcome screen, click **Recover**.
5. Click **Select data**, and then click **Browse**.
6. Specify the backup location by browsing to the folder under **Local folders** or **Network folders**.

   Click **OK** to confirm your selection.
7. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
8. In **Backup contents**, select **Folders/files**.
9. Select the data that you want to recover. Click **OK** to confirm your selection.
10. Under **Where to recover**, specify a folder. Optionally, you can prohibit overwriting of newer versions of files or exclude some files from recovery.
11. [Optional] Click **Recovery options** to specify additional settings.
12. Click **OK** to start the recovery.

Note *Tape Location takes a lot of space and might not fit in RAM when you rescan and recover under Linux bootable media and WinPE bootable media. For Linux, you have to mount another location to save the data on a disk or share. See Acronis SCS Cyber Backup 12.5 Hardened Edition. Changing the TapeLocation Folder (KB 27445). For Windows PE, there is no workaround at the moment.*

6.4.3 Extracting files from local backups

You can browse the contents of backups and extract files that you need.

Requirements

- This functionality is available only in Windows by using File Explorer.
- A backup agent must be installed on the machine from which you browse a backup.
- The backed-up file system must be one of the following: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS, or HFS+.
- The backup must be stored in a local folder or on a network share (SMB/CIFS).

To extract files from a backup

1. Browse to the backup location by using File Explorer.
2. Double-click the backup file. The file names are based on the following template:

   `<machine name> - <backup plan GUID>`
3. If the backup is encrypted, enter the encryption password. Otherwise, skip this step.

   File Explorer displays the recovery points.
4. Double-click the recovery point.

   File Explorer displays the backed-up data.
5. Browse to the required folder.
6. Copy the required files to any folder on the file system.

6.5 Recovering ESXi configuration

To recover an ESXi configuration, you need Linux-based bootable media. For information about how to create bootable media, refer to "Creating bootable media" (Section 6.2).

If you are recovering an ESXi configuration to a non-original host and the original ESXi host is still connected to the vCenter Server, disconnect and remove this host from the vCenter Server to avoid unexpected issues during the recovery. If you want to keep the original host along with the recovered one, you can add it again after the recovery is complete.

The virtual machines running on the host are not included in an ESXi configuration backup. They can be backed up and recovered separately.

To recover an ESXi configuration

1. Boot the target machine by using the bootable media.
2. Click **Manage this machine locally**.
3. On the welcome screen, click **Recover**.
4. Click **Select data**, and then click **Browse**.
5. Specify the backup location:
   - Browse to the folder under **Local folders** or **Network folders**.

   Click **OK** to confirm your selection.
6. In **Show**, select **ESXi configurations**.
7. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
8. Click **OK**.
9. In **Disks to be used for new datastores**, do the following:
   - Under **Recover ESXi to**, select the disk where the host configuration will be recovered. If you are recovering the configuration to the original host, the original disk is selected by default.
   - [Optional] Under **Use for new datastore**, select the disks where new datastores will be created. Be careful because all data on the selected disks will be lost. If you want to preserve the virtual machines in the existing datastores, do not select any disks.
10. If any disks for new datastores are selected, select the datastore creation method in **How to create new datastores**: **Create one datastore per disk** or **Create one datastore on all selected HDDs**.
11. [Optional] In **Network mapping**, change the result of automatic mapping of the virtual switches present in the backup to the physical network adapters.
12. [Optional] Click **Recovery options** to specify additional settings.
13. Click **OK** to start the recovery.

6.6 Recovery options

To modify the recovery options, click **Recovery options** when configuring recovery.

Availability of the recovery options

The set of available recovery options depends on:

- The environment the agent that performs recovery operates in (Windows, Linux, or bootable media).
- The type of data being recovered (disks, files, virtual machines, application data).

The following table summarizes the availability of the recovery options.

	Disks			Files			Virtual machines	SQL and Exchange
	Windows	Linux	Bootable media	Windows	Linux	Bootable media	ESXi and Hyper-V	Windows
Backup validation (Section 6.6.1)	+	+	+	+	+	+	+	+
Boot mode (Section 6.6.2)	+	-	-	-	-	-	+	-
Date and time for files (Section 6.6.3)	-	-	-	+	+	+	-	-
Error handling (Section 6.6.4)	+	+	+	+	+	+	+	+
File exclusions (Section 6.6.5)	-	-	-	+	+	+	-	-
Flashback (Section 6.6.6)	+	+	+	-	-	-	+	-
Full path recovery (Section 6.6.7)	-	-	-	+	+	+	-	-
Mount points (Section 6.6.8)	-	-	-	+	-	-	-	-
Performance (Section 6.6.9)	+	+	-	+	+	-	+	+
Pre/post commands (Section 6.6.10)	+	+	-	+	+	-	+	+
SID changing (Section 6.6.11)	+	-	-	-	-	-	-	-
VM power management (Section 6.6.12)	-	-	-	-	-	-	+	-
Windows event log (Section 6.6.13)	+	-	-	+	-	-	Hyper-V only	+

6.6.1 Backup validation

This option defines whether to validate a backup to ensure that the backup is not corrupted, before data is recovered from it.

The preset is: **Disabled**.

Validation calculates a checksum for every data block saved in the backup.

Validation is a time-consuming process, even for an incremental or differential backup, which are small in size. This is because the operation validates not only the data physically contained in the

backup, but all of the data recoverable by selecting the backup. This requires access to previously created backups.

6.6.2 Boot mode

This option is effective when recovering a physical or a virtual machine from a disk-level backup that contains a Windows operating system.

This option enables you to select the boot mode (BIOS or UEFI) that Windows will use after the recovery. If the boot mode of the original machine is different from the selected boot mode, the software will:

- Initialize the disk to which you are recovering the system volume, according to the selected boot mode (MBR for BIOS, GPT for UEFI).
- Adjust the Windows operating system so that it can start using the selected boot mode.

The preset is: **As on the target machine.**

You can choose one of the following:

- **As on the target machine**

  The agent that is running on the target machine detects the boot mode currently used by Windows and makes the adjustments according to the detected boot mode.

  This is the safest value that automatically results in bootable system unless the limitations listed below apply. Since the **Boot mode** option is absent under bootable media, the agent on media always behaves as if this value is chosen.
- **As on the backed-up machine**

  The agent that is running on the target machine reads the boot mode from the backup and makes the adjustments according to this boot mode. This helps you recover a system on a different machine, even if this machine uses another boot mode, and then replace the disk in the backed-up machine.
- **BIOS**

  The agent that is running on the target machine makes the adjustments to use BIOS.
- **UEFI**

  The agent that is running on the target machine makes the adjustments to use UEFI.

Once a setting is changed, the disk mapping procedure will be repeated. This will take some time.

Recommendations

If you need to transfer Windows between UEFI and BIOS:

- Recover the entire disk where the system volume is located. If you recover only the system volume on top of an existing volume, the agent will not be able to initialize the target disk properly.
- Remember that BIOS does not allow using more than 2 TB of disk space.

Limitations

- Transferring between UEFI and BIOS is supported for:
  - 64-bit Windows operating systems starting with Windows Vista SP1
  - 64-bit Windows Server operating systems starting with Windows Server 2008 SP1
- Transferring between UEFI and BIOS is not supported if the backup is stored on a tape device.

When transferring a system between UEFI and BIOS is not supported, the agent behaves as if the **As on the backed-up machine** setting is chosen. If the target machine supports both UEFI and BIOS, you need to manually enable the boot mode corresponding to the original machine. Otherwise, the system will not boot.

6.6.3 Date and time for files

This option is effective only when recovering files.

This option defines whether to recover the files' date and time from the backup or assign the files the current date and time.

If this option is enabled, the files will be assigned the current date and time.

The preset is: **Enabled**.

6.6.4 Error handling

These options enable you to specify how to handle errors that might occur during recovery.

Re-attempt, if an error occurs

The preset is: **Enabled. Number of attempts: 30. Interval between attempts: 30 seconds.**

When a recoverable error occurs, the program re-attempts to perform the unsuccessful operation. You can set the time interval and the number of attempts. The attempts will be stopped as soon as the operation succeeds OR the specified number of attempts are performed, depending on which comes first.

Do not show messages and dialogs while processing (silent mode)

The preset is: **Disabled**.

With the silent mode enabled, the program will automatically handle situations requiring user interaction where possible. If an operation cannot continue without user interaction, it will fail. Details of the operation, including errors, if any, can be found in the operation log.

Save system information if a recovery with reboot fails

This option is effective for a disk or volume recovery to a physical machine running Windows or Linux.

The preset is: **Disabled**.

When this option is enabled, you can specify a folder on the local disk (including flash or HDD drives attached to the target machine) or on a network share where the log, system information, and crash dump files will be saved. This file will help the technical support personnel to identify the problem.

6.6.5 File exclusions

This option is effective only when recovering files.

The option defines which files and folders to skip during the recovery process and thus exclude from the list of recovered items.

Note Exclusions override the selection of data items to recover. For example, if you select to recover file MyFile.tmp and to exclude all .tmp files, file MyFile.tmp will not be recovered.

6.6.5.1 File Level Security

This option is effective when recovering files from disk and file level backups of NTFS-Formatted volumes

This option defines whether to recover NTFS permissions for files along with the files.

The preset is: **Enabled**.

You can choose whether to recover the permissions or let the files inherit the NTFS permissions form the folder to which they are recovered.

6.6.6 Flashback

This option is effective when recovering disks and volumes on physical and virtual machines.

If the option is enabled, only the differences between the data in the backup and the target disk data are recovered. This accelerates data recovery to the same disk as was backed up, especially if the volume layout of the disk has not changed. The data is compared at the block level.

For physical machines, comparing the data at the block level is a time-consuming operation. If the connection to the backup storage is fast, it will take less time to recover the entire disk than to calculate the data differences. Therefore, we recommend that you enable this option only if the connection to the backup storage is slow (for example, if the backup is stored on a remote network folder).

When recovering a physical machine, the preset is: **Disabled**.

When recovering a virtual machine, the preset is: **Enabled**.

6.6.7 Full path recovery

This option is effective only when recovering data from a file-level backup.

If this option is enabled, the full path to the file will be re-created in the target location.

The preset is: **Disabled**.

6.6.8 Mount points

This option is effective only in Windows for recovering data from a file-level backup.

Enable this option to recover files and folders that were stored on the mounted volumes and were backed up with the enabled Mount points (Section 5.10.17) option.

The preset is: **Disabled**.

This option is effective only when you select for recovery a folder that is higher in the folder hierarchy than the mount point. If you select for recovery folders within the mount point or the mount point itself, the selected items will be recovered regardless of the **Mount points** option value.

Note *Please be aware that if the volume is not mounted at the moment of recovery, the data will be recovered directly to the folder that has been the mount point at the time of backing up.*

6.6.9 Performance

This option defines the priority of the recovery process in the operating system.

The available settings are: **Low**, **Normal**, **High**.

The preset is: **Normal**.

The priority of a process running in a system determines the amount of CPU and system resources allocated to that process. Decreasing the recovery priority will free more resources for other

applications. Increasing the recovery priority might speed up the recovery process by requesting the operating system to allocate more resources to the application that will perform the recovery. However, the resulting effect will depend on the overall CPU usage and other factors like disk I/O speed or network traffic.

6.6.10 Pre/Post commands

The option enables you to define the commands to be automatically executed before and after the data recovery.

Example of how you can use the pre/post commands:

- Launch the **Checkdisk** command in order to find and fix logical file system errors, physical errors or bad sectors to be started before the recovery starts or after the recovery ends.

The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)

A post-recovery command will not be executed if the recovery proceeds with reboot.

6.6.10.1 Pre-recovery command

To specify a command/batch file to be executed before the recovery process starts

1. Enable the **Execute a command before the recovery** switch.
2. In the **Command...** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command's execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

Check box	**Selection**			
Fail the recovery if the command execution fails*	Selected	Cleared	Selected	Cleared
Do not recover until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Perform the recovery only after the command is successfully executed. Fail the recovery if the command execution failed.	Perform the recovery after the command is executed despite execution failure or success.	N/A	Perform the recovery concurrently with the command execution and irrespective of the command execution result.

* A command is considered failed if its exit code is not equal to zero.

6.6.10.2 Post-recovery command

To specify a command/executable file to be executed after the recovery is completed

1. Enable the **Execute a command after the recovery** switch.
2. In the **Command...** field, type a command or browse to a batch file.
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field, specify the command execution arguments, if required.
5. Select the **Fail the recovery if the command execution fails** check box if successful execution of the command is critical for you. The command is considered failed if its exit code is not equal to zero. If the command execution fails, the recovery status will be set to **Error**.

   When the check box is not selected, the command execution result does not affect the recovery failure or success. You can track the command execution result by exploring the **Activities** tab.
6. Click **Done**.

Note *A post-recovery command will not be executed if the recovery proceeds with reboot.*

6.6.11 SID changing

This option is effective when recovering Windows 8.1/Windows Server 2012 R2 or earlier.

This option is not effective when recovery to a virtual machine is performed by Agent for VMware or Agent for Hyper-V.

The preset is: **Disabled**.

The software can generate a unique security identifier (Computer SID) for the recovered operating system. You only need this option to ensure operability of third-party software that depends on Computer SID.

Microsoft does not officially support changing SID on a deployed or recovered system. So use this option at your own risk.

6.6.12 VM power management

These options are effective when recovery to a virtual machine is performed by Agent for VMware or Agent for Hyper-V.

Power off target virtual machines when starting recovery

The preset is: **Enabled**.

Recovery to an existing virtual machine is not possible if the machine is online, and so the machine is powered off automatically as soon as the recovery starts. Users will be disconnected from the machine and any unsaved data will be lost.

Clear the check box for this option if you prefer to power off virtual machines manually before the recovery.

Power on the target virtual machine when recovery is complete

The preset is: **Disabled**.

After a machine is recovered from a backup to another machine, there is a chance the existing machine's replica will appear on the network. To be on the safe side, power on the recovered virtual machine manually, after you take the necessary precautions.

6.6.13 Windows event log

This option is effective only in Windows operating systems.

This option defines whether the agents have to log events of the recovery operations in the Application Event Log of Windows (to see this log, run eventvwr.exe or select **Control Panel** > **Administrative tools** > **Event Viewer**). You can filter the events to be logged.

The preset is: **Disabled**.

7 Operations with backups

7.1 The Backups tab

The **Backups** tab shows backups of all machines ever registered on the management server. This includes offline machines and machines that are no longer registered.

Backups that are stored in a shared location (such as an SMB or NFS share) are visible to all users that have the read permission for the location.

Backup locations that are used in backup plans are automatically added to the **Backups** tab. To add a custom folder (for example, a detachable USB device) to the list of backup locations, click **Browse** and specify the folder path.

To select a recovery point by using the Backups tab

1. On the **Backups** tab, select the location where the backups are stored.

   The software displays all backups that your account is allowed to view in the selected location. The backups are combined in groups. The group names are based on the following template:

   `<machine name> - <backup plan name>`
2. Select a group from which you want to recover the data.
3. [Optional] Click **Change** next to **Machine to browse from**, and then select another machine. Some backups can only be browsed by specific agents. For example, you must select a machine running Agent for SQL to browse the backups of Microsoft SQL Server databases.

   Important *Please be aware that the **Machine to browse from** is a default destination for recovery from a physical machine backup. After you select a recovery point and click **Recover**, double check the **Target machine** setting to ensure that you want to recover to this specific machine. To change the recovery destination, specify another machine in **Machine to browse from**.*
4. Click **Show backups**.
5. Select the recovery point.

7.2 Mounting volumes from a backup

Mounting volumes from a disk-level backup lets you access the volumes as though they were physical disks.

Mounting volumes in the read/write mode enables you to modify the backup content; that is, save, move, create, delete files or folders, and run executables consisting of one file. In this mode, the software creates an incremental backup that contains the changes you make to the backup content. Please be aware that none of the subsequent backups will contain these changes.

Requirements

- This functionality is available only in Windows by using File Explorer.
- Agent for Windows must be installed on the machine that performs the mount operation.
- The backed-up file system must be supported by the Windows version that the machine is running.
- The backup must be stored in a local folder, on a network share (SMB/CIFS), or in the Secure Zone.

Usage scenarios

- **Sharing data**

  Mounted volumes can be easily shared over the network.
- **"Band aid" database recovery solution**

  Mount a volume that contains an SQL database from a recently failed machine. This will provide access to the database until the failed machine is recovered.
- **Offline virus clean**

  If a machine is infected, mount its backup, clean it with an antivirus program (or find the latest backup that is not infected), and then recover the machine from this backup.
- **Error check**

  If a recovery with volume resize has failed, the reason may be an error in the backed-up file system. Mount the backup in the read/write mode. Then, check the mounted volume for errors by using the **chkdsk /r** command. Once the errors are fixed and a new incremental backup is created, recover the system from this backup.

To mount a volume from a backup

1. Browse to the backup location by using File Explorer.
2. Double-click the backup file. By default, the file names are based on the following template:

   `<machine name> - <backup plan GUID>`
3. If the backup is encrypted, enter the encryption password. Otherwise, skip this step.

   File Explorer displays the recovery points.
4. Double-click the recovery point.

   File Explorer displays the backed-up volumes.

   Tip *Double-click a volume to browse its content. You can copy files and folders from the backup to any folder on the file system.*
5. Right-click a volume to mount, and then click one of the following:
   - **Mount**
   - **Mount in read-only mode**
6. If the backup is stored on a network share, provide access credentials. Otherwise, skip this step.

   The software mounts the selected volume. The first unused letter is assigned to the volume.

To unmount a volume

1. Browse to **Computer** (**This PC** in Windows 8.1 and later) by using File Explorer.
2. Right-click the mounted volume.

3. Click **Unmount**.
4. If the volume was mounted in the read/write mode, and its content was modified, select whether to create an incremental backup containing the changes. Otherwise, skip this step.

   The software unmounts the selected volume.

7.3 Exporting backups

The export operation creates a self-sufficient copy of a backup in the location you specify. The original backup remains untouched. Export enables you to separate a specific backup from a chain of incremental and differential backups for fast recovery, writing onto removable or detachable media or other purposes.

The result of an export operation is always a full backup. If you want to replicate the entire backup chain to a different location and preserve multiple recovery points, use a backup replication plan (Section 9.1.1).

The backup file name (Section 5.10.3) of the exported backup depends on the value of the backup format (section 5.10.4) option:

- For the **Version 12** format with any backup scheme, the backup file name is the same as that of the original backup, except for the sequence number. If multiple backups from the same backup chain are exported to the same location, a four-digit sequence number is appended to the file names of all backups except for the first one.
- For the **Version 11** format with the **Always incremental (single-file)** backup scheme, the backup file name exactly matches the backup file name of the original backup. If multiple backups from the same backup chain are exported to the same location, every export operation overwrites the previously exported backup.
- For the **Version 11** format with other backup schemes, the backup file name is the same as that of the original backup, except for the timestamp. The timestamps of the exported backups correspond to the time when the export is performed.

The exported backup inherits the encryption settings and password from the original backup. When exporting an encrypted backup, you must specify the password.

To export a backup

1. Select the backed-up machine.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do any of the following:
   - If the backup location is a shared storage (i.e. other agents can access it), click **Select machine**, select a target machine that is online, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).
4. Click the gear icon, and then click **Export**.
5. Select the agent that will perform the export.
6. If the backup is encrypted, provide the encryption password. Otherwise, skip this step.
7. Specify the export destination.
8. Click **Start**.

7.4 Deleting backups

To delete backups of a machine that is online and present in the backup console

1. On the **All devices** tab, select a machine whose backups you want to delete.
2. Click **Recovery**.
3. Select the location to delete the backups from.
4. Do one of the following:
   - To delete a single backup, select the backup to delete, click the gear icon, and then click **Delete**.
   - To delete all backups in the selected location, click **Delete all**.
5. Confirm your decision.

To delete backups of any machine

1. On the **Backups** tab, select the location from which you want to delete the backups.

   The software displays all backups that your account is allowed to view in the selected location. The backups are combined in groups. The group names are based on the following template:

   `<machine name> - <backup plan name>`
2. Select a group.
3. Do one of the following:
   - To delete a single backup, click **Show backups**, select the backup to delete, click the gear icon, and then click **Delete**.
   - To delete the selected group, click **Delete**.
4. Confirm your decision.

8 Operations with backup plans

For information about how to create a backup plan, refer to

"Backup" (Section 5). ***To edit a backup plan***

1. If you want to edit the backup plan for all machines to which it is applied, select one of these machines. Otherwise, select the machines for which you want to edit the backup plan.
2. Click **Backup**.
3. Select the backup plan that you want to edit.
4. Click the gear icon next to the backup plan name, and then click **Edit**.
5. To modify the plan parameters, click the corresponding section of the backup plan panel.
6. Click **Save changes**.
7. To change the backup plan for all machines to which it is applied, click **Apply the changes to this backup plan**. Otherwise, click **Create a new backup plan only for the selected devices**.

To revoke a backup plan from machines

1. Select the machines that you want to revoke the backup plan from.
2. Click **Backup**.
3. If several backup plans are applied to the machines, select the backup plan that you want to revoke.
4. Click the gear icon next to the backup plan name, and then click **Revoke**.

- To shift these operations outside of business hours, if setting up a dedicated agent is not in your plans

Unlike the backup and VM replication plans, which employ the time settings of machines running the agents, the off-host data processing plans run according to the time settings of the management server machine.

9.1.1 Backup replication

Supported locations

The following table summarizes backup locations supported by backup replication plans.

Backup location	Supported as a source	Supported as a target
Local folder	+	+
Network folder	+	+
NFS folder	–	–
Secure Zone	–	–
SFTP server	–	–
Tape device	–	+

Creating a backup replication plan

1. Click **Plans** > **Backup replication**.
2. Click **Create plan**.
   The software displays a new plan template.
3. [Optional] To modify the plan name, click the default name.
4. Click **Agent**, and then select the agent that will perform the replication.
   You can select any agent that has access to the source and target backup locations.
5. Click **Items to replicate**, and then select the backups that this plan will replicate.
   You can switch between selecting backups and selecting entire locations by using the **Locations** /**Backups** switch in the top-right corner.
   If the selected backups are encrypted, all of them must use the same encryption password. For backups that use different encryption passwords, create separate plans.
6. Click **Destination**, and then specify the target location.
7. [Optional] In **How to replicate**, select which backups to replicate. You can select one of the following:
   - **All backups** (default)
   - **Only full backups**
   - **Only the last backup**
8. [Optional] Click **Schedule**, and then change the schedule.
9. [Optional] Click **Retention rules**, and then specify the retention rules for the target location, as described in "Retention rules" (Section 5.5).
10. If the backups selected in **Items to replicate** are encrypted, enable the **Backup password** switch, and then provide the encryption password. Otherwise, skip this step.
11. [Optional] To modify the plan options, click the gear icon.
12. Click **Create**.

9.1.2 Validation

Validation is an operation that checks the possibility of data recovery from a backup.

Validation of a backup location validates all the backups stored in the location.

How it works

A validation plan offers two validation methods. If you select both methods, the operations will be performed consecutively.

- **Calculating a checksum for every data block saved in a backup**
  For more information about validation by calculating a checksum, refer to "Backup validation" (Section 5.10.5).
- **Running a virtual machine from a backup**
  This method works only for disk-level backups that contain an operating system. To use this method, you need an ESXi or Hyper-V host and a backup agent (Agent for VMware or Agent for Hyper-V) that manages this host.
  The agent runs a virtual machine from a backup, and then connects to VMware Tools or Hyper-V Heartbeat Service to ensure that the operating system has started successfully. If the connection fails, the agent attempts to connect every two minutes, a total of five times. If none of the attempts are successful, the validation fails.
  Regardless of the number of validation plans and validated backups, the agent that performs validation runs one virtual machine at a time. As soon as the validation result becomes clear, the agent deletes the virtual machine and runs the next one.

If the validation fails, you can drill down to the details on the **Activities** section of the **Overview** tab.

Supported locations

The following table summarizes backup locations supported by validation plans.

Backup location	Calculating a checksum	Running a VM
Local folder	+	+
Network folder	+	+
NFS folder	–	–
Secure Zone	–	–
SFTP server	–	–
Tape device	+	–

Creating a new validation plan

1. Click **Plans** > **Validation**.
2. Click **Create plan**.
   The software displays a new plan template.
3. [Optional] To modify the plan name, click the default name.
4. Click **Agent**, and then select the agent that will perform the validation.
   If you want to perform validation by running a virtual machine from a backup, select Agent for VMware or Agent for Hyper-V. Otherwise, select any agent that is registered on the management server and has access to the backup location.

5. Click **Items to validate**, and then select the backups that this plan will validate.

   You can switch between selecting backups and selecting entire locations by using the **Locations** / **Backups** switch in the top-right corner.

   If the selected backups are encrypted, all of them must use the same encryption password. For backups that use different encryption passwords, create separate plans.
6. [Optional] In **What to validate**, select which backups to validate. You can select one of the following:
   - **All backups**
   - **Only the last backup**
7. [Optional] Click **How to validate**, and then choose any of the following methods:
   - **Checksum verification**

     The software will calculate a checksum for every data block saved in a backup.
   - **Run as a virtual machine**

     The software will run a virtual machine from each backup.
8. If you chose **Run as a virtual machine**:
   a. Click **Target machine**, and then select the virtual machine type (ESXi or Hyper-V), the host and the machine name template.

      The default name is **[Machine Name]_validate**.
   b. Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore for the virtual machine.
   c. [Optional] Change the disk provisioning mode.

      The default setting is **Thin** for VMware ESXi and **Dynamically expanding** for Hyper-V.
   d. Do not disable the **VM heartbeat** switch if you need a correct validation result. This switch is designed for future releases.
   e. [Optional] Click **VM settings** to change the memory size and network connections of the virtual machine.

      By default, the virtual machine is *not* connected to a network and the virtual machine memory size equals that of the original machine.
9. [Optional] Click **Schedule**, and then change the schedule.
10. If the backups selected in **Items to validate** are encrypted, enable the **Backup password** switch, and then provide the encryption password. Otherwise, skip this step.
11. [Optional] To modify the plan options, click the gear icon.
12. Click **Create**.

9.1.3 Cleanup

Cleanup is an operation that deletes outdated backups according to the retention rules.

Supported locations

Cleanup plans support all backup locations, except for NFS folders, SFTP servers, and Secure Zone.

To create a new cleanup plan

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

   The software displays a new plan template.
3. [Optional] To modify the plan name, click the default name.

4. Click **Agent**, and then select the agent that will perform the cleanup.

   You can select any agent that has access to the backup location.
5. Click **Items to clean up**, and then select the backups which this plan will clean up.

   You can switch between selecting backups and selecting entire locations by using the **Locations** /**Backups** switch in the top-right corner.

   If the selected backups are encrypted, all of them must use the same encryption password. For backups that use different encryption passwords, create separate plans.
6. [Optional] Click **Schedule**, and then change the schedule.
7. [Optional] Click **Retention rules**, and then specify the retention rules, as described in "Retention rules" (Section 5.5).
8. If the backups selected in **Items to clean up** are encrypted, enable the **Backup password** switch, and then provide the encryption password. Otherwise, skip this step.
9. [Optional] To modify the plan options, click the gear icon.
10. Click **Create**.

9.1.4 Conversion to a virtual machine

You can create a separate plan for the conversion to a virtual machine and run this plan manually or on a schedule.

For information about prerequisites and limitations, please refer to "What you need to know about conversion" (Section 5.7.1).

To create a plan for conversion to a virtual machine

1. Click **Plans** > **Conversion to VM**.
2. Click **Create plan**.

   The software displays a new plan template.
3. [Optional] To modify the plan name, click the default name.
4. In **Convert to**, select the type of the target virtual machine. You can select one of the following:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **VHDX files**
5. Do one of the following:
   - For VMware ESXi and Hyper-V: click **Host**, select the target host, and then specify the new machine name template.
   - For other virtual machine types: in **Path**, specify where to save the virtual machine files and the file name template.

   The default name is **[Machine Name]_converted**.
6. Click **Agent**, and then select the agent that will perform the conversion.
7. Click **Items to convert**, and then select the backups that this plan will convert to virtual machines.

   You can switch between selecting backups and selecting entire locations by using the **Locations** / **Backups** switch in the top-right corner.

   If the selected backups are encrypted, all of them must use the same encryption password. For backups that use different encryption passwords, create separate plans.

8. [Only for VMware ESXi and Hyper-V] Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore (storage) for the virtual machine.
9. [Optional] For VMware ESXi and Hyper-V, you can also do the following:
   - Change the disk provisioning mode. The default setting is **Thin** for VMware ESXi and **Dynamically expanding** for Hyper-V.
   - Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.
10. [Optional] Click **Schedule**, and then change the schedule.
11. If the backups selected in **Items to convert** are encrypted, enable the **Backup password** switch, and then provide the encryption password. Otherwise, skip this step.
12. [Optional] To modify the plan options, click the gear icon.
13. Click **Create**.

10 Bootable media

10.1 Bootable Media Builder

Bootable Media Builder is a dedicated tool for creating bootable media.

Bootable Media Builder is installed by default when you install the management server. You can install the media builder separately on any machine running Windows or Linux. The supported operating systems are the same as for the corresponding agents.

Why use the media builder?

The bootable media that is available for downloading in the backup console can be used only for recovery. This media is based on a Linux kernel. Unlike Windows PE, it does not allow injecting custom drivers on the fly.

- The media builder enables you to create a customized Linux-based or WinPE-based bootable media with the backup functionality.
- Apart from creating physical media or its ISO, you can upload the media to Windows Deployment Services (WDS) and use network boot.
- Finally, you can write the media directly to a flash drive, without using third-party tools.

32- or 64-bit?

Bootable Media Builder can be installed from both 32-bit and 64-bit setup programs. The bitness of the media corresponds to the bitness of the setup program. However, you can create a 32-bit WinPE-based media by using the 64-bit media builder, if you download the 32-bit plugin.

Please remember that in most cases you need a 64-bit media to boot a machine that uses Unified Extensible Firmware Interface (UEFI).

10.1.1 Linux-based bootable media

To create a Linux-based bootable media

1. Start the Bootable Media Builder.

2. Specify the license key. The license will not get assigned or reassigned. It determines which functionality to enable for the created media. Without the license keys, you can create media only for recovery.
3. Select **Bootable media type: Default (Linux-based media)**.

   Select the way volumes and network resources will be handled—called the media style:

   - A media with Linux-style volume handling displays the volumes as, for example, hda1 and sdb2. It tries to reconstruct MD devices and logical (LVM) volumes before starting a recovery.
   - A media with Windows-style volume handling displays the volumes as, for example, C: and D:. It provides access to dynamic (LDM) volumes.
4. [Optional] Specify the parameters of the Linux kernel. Separate multiple parameters with spaces.

   For example, to be able to select a display mode for the bootable agent each time the media starts, type: **vga=ask**

   For a list of parameters, see Kernel parameters (Section 10.1.1.1).
5. Select the components to be placed on the media: the bootable agent and/or Universal Restore.

   Using a media with the bootable agent, you can perform backup, recovery, and disk management operations on any PC-compatible hardware, including bare metal.

   Universal Restore enables you to boot an operating system recovered to dissimilar hardware or to a virtual machine if the system bootability issues occur. The tool finds and installs drivers for devices that are critical for the operating system start, such as storage controllers, motherboard, or chipset.
6. [Optional] Specify the timeout interval for the boot menu plus the component that will automatically start on timeout.

   If not configured, the loader waits for someone to select whether to boot the operating system (if present) or the component.

   If you set, say, **10 sec.** for the bootable agent, the agent will launch 10 seconds after the menu is displayed. This enables unattended onsite operation when booting from WDS/RIS.
7. [Optional] If you want to automate the bootable agent operations, select the **Use the following script** check box. Then, select one of the scripts (Section 10.1.1.2) and specify the script parameters.
8. [Optional] Specify the remote logon settings: the user name and password to be specified in a command string if the **acrocmd** utility is running on a different machine. If you leave these boxes empty, the command does not need to contain credentials.

   These credentials are also required when you register the media on the management server from the backup console (Section 10.3).
9. [Optional] Select how to register the media on the management server on booting up. For more information about the registration settings, see "Management server" (Section 10.1.1.3).
10. [Optional] Specify network settings (Section 10.1.1.4): TCP/IP settings to be assigned to the machine network adapters.
11. [Optional] Specify a network port (Section 10.1.1.5): The TCP port that the bootable agent listens for incoming connection.
12. [Optional] If a proxy server is enabled in your network, specify its host name/IP address and port.
13. Select the type of media to create. You can:

    - Create CD, DVD, or other bootable media such as removable USB flash drives if the hardware BIOS allows for boot from such media.
    - Build an ISO image to burn it later on a blank disc or to connect it to a virtual machine.
    - Upload the selected components to Acronis PXE Server.
    - Upload the selected components to a WDS/RIS.

14. [Optional] Add Windows system drivers to be used by Universal Restore (Section 10.1.16). This window appears if Universal Restore is added to media and media other than WDS/RIS is selected.
15. If prompted, specify the host name/IP address and credentials for WDS/RIS, or a path to the media ISO file.
16. Check your settings in the summary screen and click **Proceed**.

10.1.1.1 Kernel parameters

This window lets you specify one or more parameters of the Linux kernel. They will be automatically applied when the bootable media starts.

These parameters are typically used when experiencing problems while working with the bootable media. Normally, you can leave this field empty.

You can also specify any of these parameters by pressing F11 while in the boot menu.

Parameters

When specifying multiple parameters, separate them with spaces.

acpi=off

Disables Advanced Configuration and Power Interface (ACPI). You may want to use this parameter when experiencing problems with a particular hardware configuration.

noapic

Disables Advanced Programmable Interrupt Controller (APIC). You may want to use this parameter when experiencing problems with a particular hardware configuration.

vga=ask

Prompts for the video mode to be used by the bootable media's graphical user interface. Without the **vga** parameter, the video mode is detected automatically.

vga=*mode_number*

Specifies the video mode to be used by the bootable media's graphical user interface. The mode number is given by *mode_number* in the hexadecimal format—for example: **vga=0x318**

Screen resolution and the number of colors corresponding to a mode number may be different on different machines. We recommend using the **vga=ask** parameter first to choose a value for *mode_number*.

quiet

Disables displaying of startup messages when the Linux kernel is loading, and starts the management console after the kernel is loaded.

This parameter is implicitly specified when creating the bootable media, but you can remove this parameter while in the boot menu.

Without this parameter, all startup messages will be displayed, followed by a command prompt. To start the management console from the command prompt, run the command: **/bin/product**

nousb

Disables loading of the USB (Universal Serial Bus) subsystem.

nousb2

Disables USB 2.0 support. USB 1.1 devices still work with this parameter. This parameter allows you to use some USB drives in the USB 1.1 mode if they do not work in the USB 2.0 mode.

nodma

Disables direct memory access (DMA) for all IDE hard disk drives. Prevents the kernel from freezing on some hardware.

nofw

Disables the FireWire (IEEE1394) interface support.

nopcmcia

Disables detection of PCMCIA hardware.

nomouse

Disables mouse support.

module_name=**off**

Disables the module whose name is given by *module_name*. For example, to disable the use of the SATA module, specify: **sata_sis=off**

pci=bios

Forces the use of PCI BIOS instead of accessing the hardware device directly. You may want to use this parameter if the machine has a non-standard PCI host bridge.

pci=nobios

Disables the use of PCI BIOS; only direct hardware access methods will be allowed. You may want to use this parameter when the bootable media fails to start, which may be caused by the BIOS.

pci=biosirq

Uses PCI BIOS calls to get the interrupt routing table. You may want to use this parameter if the kernel is unable to allocate interrupt requests (IRQs) or discover secondary PCI buses on the motherboard.

These calls might not work properly on some machines. But this may be the only way to get the interrupt routing table.

10.1.1.2 Scripts in bootable media

Note *This functionality is available only with the Acronis SCS Cyber Backup 12.5 Hardened Edition license.*

If you want the bootable media to perform a determined set of operations, you can specify a script while creating the media in Bootable Media Builder. Every time the media boots, it will run this script instead of displaying the user interface.

You can select one of the predefined scripts or create a custom script by following the scripting conventions.

Predefined scripts

Bootable Media Builder provides the following predefined scripts:

- Backup to and recovery from the bootable media (**entire_pc_local**)
- Backup to and recovery from a network share (**entire_pc_share**)

The scripts can be found on the machine where Bootable Media Builder is installed, in the following directories:

- In Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**

- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Backup to and recovery from the bootable media

This script will back up a machine to the bootable media or recover the machine from its most recent backup created by this script on the same media. On its start, the script will prompt the user to choose between backup, recovery, and starting the user interface.

In Bootable Media Builder, you can specify a password that the script will use to encrypt or access the backups.

Backup to and recovery from a network share

This script will back up a machine to a network share or recover the machine from its most recent backup located on a network share. On its start, the script will prompt the user to choose between backup, recovery, and starting the user interface.

In Bootable Media Builder, specify the following script parameters:

1. The network share path.
2. The user name and password for the network share.
3. [Optional] The backup file name. The default value is **AutoBackup**. If you want the script to append backups to an already existing backup, or to recover from a backup with a non-default name, change the default value to the file name of this backup.

   To find out the backup file name

   1. In the backup console, go to **Backups** > **Locations**.
   2. Select the network share (click **Add location** if the share is not listed).
   3. Select the backup.
   4. Click **Details**. The file name is displayed under **Backup file name**.
4. [Optional] A password that the script will use to encrypt or access the backups.

Custom scripts

Important *Creating custom scripts requires the knowledge of the Bash command language and JavaScript Object Notation (JSON). If you are not familiar with Bash, a good place to learn it is http://www.tldp.org/LDP/abs/html. The JSON specification is available at http://www.json.org.*

Files of a script

Your script must be located in the following directories on the machine where Bootable Media Builder is installed:

- In Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

The script must consist of at least three files:

- **<script_file>.sh** - a file with your Bash script. When creating the script, use only a limited set of shell commands, which you can find at https://busybox.net/downloads/BusyBox.html. Also, the following commands can be used:
  - **`acrocmd`** - the command-line utility for backup and recovery
  - **`product`** - the command that starts the bootable media user interface

This file and any additional files that the script includes (for example, by using the dot command) must be located in the **bin** subfolder. In the script, specify the additional file paths as **/ConfigurationFiles/bin/<some_file>**.

- **autostart** - a file for starting **<script_file>.sh**. The file contents must be as follows:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - a JSON file that contains the following:
  - The script name and description to be displayed in Bootable Media Builder.
  - The names of the script variables to be configured via Bootable Media Builder.
  - The parameters of controls that will be displayed in Bootable Media Builder for each variable.

Structure of autostart.json

Top-level object

Pair		Required	Description
Name	**Value type**		
displayName	string	Yes	The script name to be displayed in Bootable Media Builder.
description	string	No	The script description to be displayed in Bootable Media Builder.
timeout	number	No	A timeout (in seconds) for the boot menu before starting the script. If the pair is not specified, the timeout will be ten seconds.
variables	object	No	Any variables for **<script_file>.sh** that you want to configure via Bootable Media Builder. The value should be a set of the following pairs: the string identifier of a variable and the object of the variable (see the table below).

Variable object

Pair		Required	Description
Name	**Value type**		
displayName	string	Yes	The variable name used in **<script_file>.sh**.
type	string	Yes	The type of a control that is displayed in Bootable Media Builder. This control is used to configure the variable value. For all supported types, see the table below.
description	string	Yes	The control label that is displayed above the control in Bootable Media Builder.
default	string if **type** is **string**, **multiString**, **password**, or **enum** number if **type** is **number**, **spinner**, or **checkbox**	No	The default value for the control. If the pair is not specified, the default value will be an empty string or a zero, based on the control type. The default value for a check box can be **0** (the cleared state) or **1** (the selected state).

Pair		Required	Description
Name	**Value type**		
order	number (non-negative)	Yes	The control order in Bootable Media Builder. The higher the value, the lower the control is placed relative to other controls defined in **autostart.json**. The initial value must be **0**.
min (for **spinner** only)	number	No	The minimum value of the spin control in a spin box. If the pair is not specified, the value will be **0**.
max (for **spinner** only)	number	No	The maximum value of the spin control in a spin box. If the pair is not specified, the value will be **100**.
step (for **spinner** only)	number	No	The step value of the spin control in a spin box. If the pair is not specified, the value will be **1**.
items (for **enum** only)	array of strings	Yes	The values for a drop-down list.
required (for **string**, **multiString**, **password**, and **enum**)	number	No	Specifies if the control value can be empty (**0**) or not (**1**). If the pair is not specified, the control value can be empty.

Control type

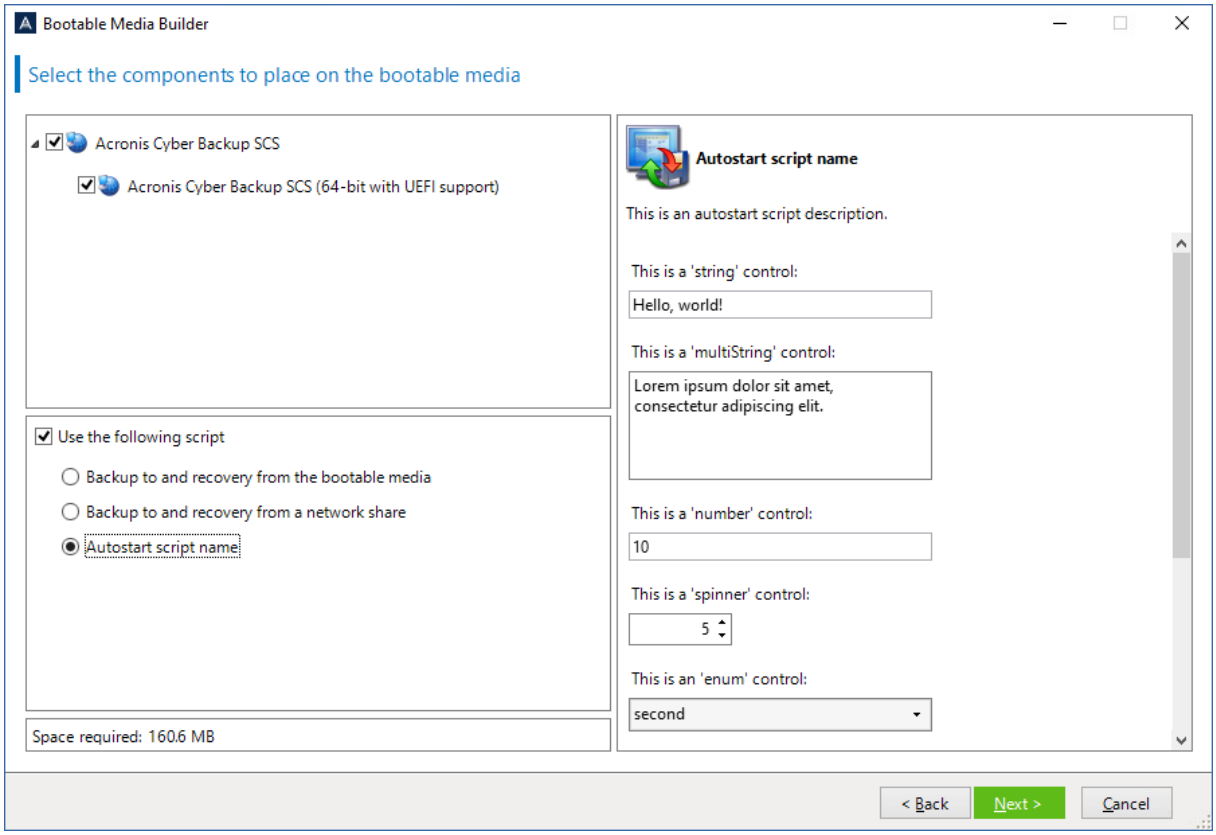
Name	Description
string	A single-line, unconstrained text box used to enter or edit short strings.
multiString	A multi-line, unconstrained text box used to enter or edit long strings.
password	A single-line, unconstrained text box used to enter passwords securely.
number	A single-line, numeric-only text box used to enter or edit numbers.
spinner	A single-line, numeric-only text box used to enter or edit numbers, with a spin control. Also, called a spin box.
enum	A standard drop-down list, with a fixed set of predetermined values.
checkbox	A check box with two states - the cleared state or the selected state.

The sample **autostart.json** below contains all possible types of controls that can be used to configure variables for **<script_file>.sh**.

```
{
   "displayName": "Autostart script name",
   "description": "This is an autostart script description.",
   "variables": {
      "var_string": {
         "displayName": "VAR_STRING",
         "type": "string", "order": 1,
         "description": "This is a 'string' control:", "default": "Hello,
         world!"
      },
      "var_multistring": {
         "displayName": "VAR_MULTISTRING",
```

```
            "type": "multiString", "order": 2,
            "description": "This is a 'multiString' control:",
            "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
        },
        "var_number": {
            "displayName": "VAR_NUMBER",
            "type": "number", "order": 3,
            "description": "This is a 'number' control:", "default": 10
        },
        "var_spinner": {
            "displayName": "VAR_SPINNER",
            "type": "spinner", "order": 4,
            "description": "This is a 'spinner' control:",
            "min": 1, "max": 10, "step": 1, "default": 5
        },
        "var_enum": {
            "displayName": "VAR_ENUM",
            "type": "enum", "order": 5,
            "description": "This is an 'enum' control:",
            "items": ["first", "second", "third"], "default": "second"
        },
        "var_password": {
            "displayName": "VAR_PASSWORD",
            "type": "password", "order": 6,
            "description": "This is a 'password' control:", "default": "qwe"
        },
        "var_checkbox": {
            "displayName": "VAR_CHECKBOX",
            "type": "checkbox", "order": 7,
            "description": "This is a 'checkbox' control", "default": 1
        }
    }
}
```

This is how it looks in Bootable Media Builder.



10.1.1.3 Management server

While creating bootable media, you have an option to pre-configure the media registration on the management server.

Registering the media enables you to manage the media via the backup console as if it was a registered machine. Besides the convenience of remote access, this grants an administrator the capability to trace all operations performed under bootable media. The operations are logged in **Activities**, so it is possible to see who and when started an operation.

If the registration was not pre-configured, it is still possible to register the media after booting the machine from it (Section 10.3).

To pre-configure registration on the management server

1. Select the **Register media on the management server** check box.
2. In **Server name or IP**, specify the host name or IP address of the machine where the management server is installed. You can use one of the following formats:
   - `http://<server>`. For example, `http://10.250.10.10` or `http://server1`
   - `<IP address>`. For example, `10.250.10.10`
   - `<host name>`. For example, `server1` or `server1.example.com`
3. In **Port**, specify the port that will be used to access the management server. The default value is 9877.
4. In **Display name**, specify the name that will be displayed for this machine in the backup console. If you leave this field empty, the display name will be set to one of the following:

- If the machine was previously registered on the management server, it will have the same name.
- Otherwise, either the fully qualified domain name (FQDN) or the IP address of the machine will be used.

5. Select which account will be used to register the media on the management server. The following options are available:
   - **Ask for user name and password at booting up**
     The credentials will have to be provided every time a machine is booted from the media. For successful registration, the account must be in the list of the management server administrators (**Settings** > **Administrators**). In the backup console, the media will be available under the organization or under a specific unit, according to the permissions given to the specified account.
     In the bootable media interface, it will be possible to change the user name and password by clicking **Tools** > **Register media on the management server**.
   - **Register under the following account**
     The machine will be registered automatically every time it is booted from the media.
     The account you specify must be in the list of the management server administrators (**Settings** > **Administrators**). In the backup console, the media will be available under the organization or under a specific unit, according to the permissions given to the specified account.
     In the bootable media interface, it will *not* be possible to change the registration parameters.
   - **Do not ask for user name and password**
     The machine will be registered anonymously, unless anonymous registration on the management server is disabled (Section 18.5).
     The **Activities** tab of the backup console will not show who used the media.
     In the backup console, the media will be available under the organization.
     In the bootable media interface, it will be possible to change the user name and password by clicking **Tools** > **Register media on the management server**.

10.1.1.4 Network settings

While creating bootable media, you have an option to pre-configure network connections that will be used by the bootable agent. The following parameters can be pre-configured:

- IP address
- Subnet mask
- Gateway
- DNS server
- WINS server.

Once the bootable agent starts on a machine, the configuration is applied to the machine's network interface card (NIC). If the settings have not been pre-configured, the agent uses DHCP auto configuration. You also have the ability to configure the network settings manually when the bootable agent is running on the machine.

Pre-configuring multiple network connections

You can pre-configure TCP/IP settings for up to ten network interface cards. To ensure that each NIC will be assigned the appropriate settings, create the media on the server for which the media is

customized. When you select an existing NIC in the wizard window, its settings are selected for saving on the media. The MAC address of each existing NIC is also saved on the media.

You can change the settings, except for the MAC address; or configure the settings for a non-existent NIC, if need be.

Once the bootable agent starts on the server, it retrieves the list of available NICs. This list is sorted by the slots the NICs occupy: the closest to the processor on top.

The bootable agent assigns each known NIC the appropriate settings, identifying the NICs by their MAC addresses. After the NICs with known MAC addresses are configured, the remaining NICs are assigned the settings that you have made for non-existent NICs, starting from the upper non-assigned NIC.

You can customize bootable media for any machine, and not only for the machine where the media is created. To do so, configure the NICs according to their slot order on that machine: NIC1 occupies the slot closest to the processor, NIC2 is in the next slot and so on. When the bootable agent starts on that machine, it will find no NICs with known MAC addresses and will configure the NICs in the same order as you did.

Example

The bootable agent could use one of the network adapters for communication with the management console through the production network. Automatic configuration could be done for this connection. Sizeable data for recovery could be transferred through the second NIC, included in the dedicated backup network by means of static TCP/IP settings.

10.1.1.5 Network port

While creating bootable media, you have an option to pre-configure the network port that the bootable agent listens to for an incoming connection from the **`acrocmd`** utility. The choice is available among:

- the default port
- the currently used port
- the new port (enter the port number)

If the port has not been pre-configured, the agent uses port 9876.

10.1.1.6 Drivers for Universal Restore

While creating bootable media, you have an option to add Windows drivers to the media. The drivers will be used by Universal Restore to boot up Windows that was migrated to dissimilar hardware.

You will be able to configure Universal Restore:

- to search the media for the drivers that best fit the target hardware
- to get the mass-storage drivers that you explicitly specify from the media. This is necessary when the target hardware has a specific mass storage controller (such as a SCSI, RAID, or Fiber Channel adapter) for the hard disk.

The drivers will be placed in the visible Drivers folder on the bootable media. The drivers are not loaded into the targetmachine RAM, therefore, the media must stay inserted or connected throughout the Universal Restore operation.

Adding drivers to bootable media is available when you are creating a removable media or its ISO or detachable media, such as a flash drive. Drivers cannot be uploaded on WDS/RIS.

The drivers can be added to the list only in groups, by adding the INF files or folders containing such files. Selecting individual drivers from the INF files is not possible, but the media builder shows the file content for your information.

To add drivers:

1. Click **Add** and browse to the INF file or a folder that contains INF files.
2. Select the INF file or the folder.
3. Click **OK**.

The drivers can be removed from the list only in groups, by removing INF files.

To remove drivers:

1. Select the INF file.
2. Click **Remove**.

10.1.2 WinPE-based bootable media

Bootable Media Builder provides two methods of integrating Acronis SCS Cyber Backup 12.5 Hardened Edition with WinPE:

- Creating the PE ISO with the plug-in from scratch.
- Adding the Acronis Plug-in to a WIM file for any future purpose (manual ISO building, adding other tools to the image and so on).

You can create WinRE-based PE images without any additional preparation, or create PE images after installing Windows Automated Installation Kit (AIK) (Section 10.1.2.1) or Windows Assessment and Deployment Kit (ADK) (Section 10.1.2.2).

WinRE-based PE images

Creating of WinRE-based images is supported for the following operation systems:

- Windows 7 (64-bit)
- Windows 8, 8.1, 10 (32-bit and 64-bit)
- Windows Server 2012, 2016, 2019, 2022 (64-bit)

PE images

After installing Windows Automated Installation Kit (AIK) or Windows Assessment and Deployment Kit (ADK), Bootable Media Builder supports WinPE distributions that are based on any the following kernels:

- Windows Vista (PE 2.0)
- Windows Vista SP1 and Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) with or without the supplement for Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE for Windows 10)

Bootable Media Builder supports both 32-bit and 64-bit WinPE distributions. The 32-bit WinPE distributions can also work on 64-bit hardware. However, you need a 64-bit distribution to boot a machine that uses Unified Extensible Firmware Interface (UEFI).

PE images based on WinPE 4 and later require approximately 1 GB of RAM to work.

10.1.2.1 Preparation: WinPE 2.x and 3.x

To be able to create or modify PE 2.x or 3.x images, install Bootable Media Builder on a machine where Windows Automated Installation Kit (AIK) is installed. If you do not have a machine with AIK, prepare it as follows.

To prepare a machine with AIK

1. Download and install Windows Automated Installation Kit.

   Automated Installation Kit (AIK) for Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en

   Automated Installation Kit (AIK) for Windows Vista SP1 and Windows Server 2008 (PE 2.1):

   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en

   Automated Installation Kit (AIK) for Windows 7 (PE 3.0):

   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en

   Automated Installation Kit (AIK) Supplement for Windows 7 SP1 (PE 3.1):

   http://www.microsoft.com/download/en/details.aspx?id=5188

   You can find system requirements for installation by following the above links.
2. [Optional] Burn the WAIK to DVD or copy to a flash drive.
3. Install the Microsoft .NET Framework from this kit (NETFXx86 or NETFXx64, depending on your hardware).
4. Install Microsoft Core XML (MSXML) 5.0 or 6.0 Parser from this kit.
5. Install Windows AIK from this kit.
6. Install Bootable Media Builder on the same machine.

It is recommended that you familiarize yourself with the help documentation supplied with Windows AIK. To access the documentation, select **Microsoft Windows AIK -> Documentation** from the start menu.

10.1.2.2 Preparation: WinPE 4.0 and later

To be able to create or modify PE 4 or later images, install Bootable Media Builder on a machine where Windows Assessment and Deployment Kit (ADK) is installed. If you do not have a machine with ADK, prepare it as follows.

To prepare a machine with ADK

1. Download the setup program of Assessment and Deployment Kit.

   Assessment and Deployment Kit (ADK) for Windows 8 (PE 4.0):
   http://www.microsoft.com/en-us/download/details.aspx?id=30652.

   Assessment and Deployment Kit (ADK) for Windows 8.1 (PE 5.0):
   http://www.microsoft.com/en-US/download/details.aspx?id=39982.

   Assessment and Deployment Kit (ADK) for Windows 10 (PE for Windows 10):
   https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx.

   You can find system requirements for installation by following the above links.

2. Install Assessment and Deployment Kit on the machine.
3. Install Bootable Media Builder on the same machine.

10.1.2.3 Adding Acronis Plug-in to WinPE

To add Acronis Plug-in to WinPE:

1. Start the Bootable Media Builder.
2. Specify the license keys. The license keys will not get assigned or reassigned. They determine which functionality to enable for the created media. Without the license keys, you can create media only for recovery.
3. Select **Bootable media type: Windows PE** or **Bootable media type: Windows PE (64-bit)**. A 64-bit media is required to boot a machine that uses Unified Extensible Firmware Interface (UEFI).

   If you have selected **Bootable media type: Windows PE**, do the following first:

   - Click **Download the Plug-in for WinPE (32-bit)**.
   - Save the plug-in to **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**.

   If you plan to recover an operating system to dissimilar hardware or to a virtual machine and want to ensure the system bootability, select the **Include the Universal Restore tool...** check box.
4. Select **Create WinPE automatically**.

   The software runs the appropriate script and proceeds to the next window.
5. Select whether to enable or disable the remote connection to a machine booted from the media. If enabled, enter a user name and password to be specified in a command line if the **acrocmd** utility is running on a different machine. If you leave these boxes empty, the remote connection via the command line interface will be disabled.
   These credentials are also required when you register the media on the management server from the backup console (Section 10.3).
6. Specify network settings (Section 10.1.1.4) for the machine network adapters or choose DHCP auto configuration.
7. [Optional] Select how to register the media on the management server on booting up. For more information about the registration settings, see "Management server" (Section 10.1.1.3).
8. [Optional] Specify the Windows drivers to be added to Windows PE.
   Once you boot a machine into Windows PE, the drivers can help you access the device where the backup is located. Add 32-bit drivers if you use a 32-bit WinPE distribution or 64-bit drivers if you use a 64-bit WinPE distribution.
   Also, you will be able to point to the added drivers when configuring Universal Restore for Windows. For using Universal Restore, add 32-bit or 64-bit drivers depending on whether you are planning to recover a 32-bit or a 64-bit Windows operating system.
   To add the drivers:

   - Click **Add** and specify the path to the necessary *.inf file for a corresponding SCSI, RAID, SATA controller, network adapter, tape drive or other device.
   - Repeat this procedure for each driver you want to be included in the resulting WinPE media.
9. Choose whether you want to create ISO or WIM image or upload the media on a server (WDS or RIS).
10. Specify the full path to the resulting image file including the file name, or specify the server and provide the user name and password to access it.
11. Check your settings in the summary screen and click **Proceed**.

12. Burn the .ISO to CD or DVD using a third-party tool or copy to a flash drive.

Once a machine boots into WinPE, the agent starts automatically.

To create a PE image (ISO file) from the resulting WIM file:

- Replace the default boot.wim file in your Windows PE folder with the newly created WIM file. For the above example, type:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Use the **Oscdimg** tool. For the above example, type:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
c:\winpe_x86\winpe_x86.iso
```

Do not copy and paste this example. Type the command manually, otherwise it will fail.

For more information on customizing Windows PE 2.x and 3.x, see the Windows Preinstallation Environment User's Guide (Winpe.chm). The information on customizing Windows PE 4.0 and later is available in the Microsoft TechNet Library.

10.2 Connecting to a machine booted from media

Once a machine boots from bootable media, the machine terminal displays a startup window with the IP address(es) obtained from DHCP or set according to the pre-configured values.

Configuring network settings

To change the network settings for a current session, click **Configure network** in the startup window. The **Network Settings** window that appears will allow you to configure network settings for each network interface card (NIC) of the machine.

Changes made during a session will be lost after the machine reboots.

Adding VLANs

In the **Network Settings** window, you can add virtual local area networks (VLANs). Use this functionality if you need access to a backup location that is included in a specific VLAN.

VLANs are mainly used to divide a local area network into segments. A NIC that is connected to an *access* port of the switch always has access to the VLAN specified in the port configuration. A NIC connected to a *trunk* port of the switch can access the VLANs allowed in the port configuration only if you specify the VLANs in the network settings.

To enable access to a VLAN via a trunk port

1. Click **Add VLAN**.
2. Select the NIC that provides access to the local area network that includes the required VLAN.
3. Specify the VLAN identifier.

After you click **OK**, a new entry appears in the list of network adapters.

If you need to remove a VLAN, click the required VLAN entry, and then click **Remove VLAN**.

Local connection

To operate directly on the machine booted from bootable media, click **Manage this machine locally** in the startup window.

Remote connection

To connect to the media remotely, register it on the management server, as described in "Registering media on the management server" (Section 10.3).

10.3 Registering media on the management server

Registering bootable media enables you to manage the media via the backup console as if it was a registered machine. This applies to all bootable media regardless of the boot method (physical media, Startup Recovery Manager, Acronis PXE Server, WDS, or RIS).

Registering the media is possible only if at least one Acronis SCS Cyber Backup 12.5 Hardened Edition license is added to the management server.

You can register the media from the media UI.

The registration parameters can be pre-configured in the Management server (Section 10.1.1.3) option of Bootable Media Builder. If all the registration parameters are pre-configured, the media will appear in the backup console automatically. If some of the parameters are pre-configured, some steps in the following procedures may be not available.

Registering the media from the media UI

The media can be downloaded or created by using Bootable Media Builder (Section 10.1).

To register media from the media UI

1. Boot the machine from the media.
2. Do one of the following:
   - In the startup window, under **Management server**, click **Edit**.
   - In the bootable media interface, click **Tools** > **Register media on the management server**.
3. In **Register at**, specify the host name or IP address of the machine where the management server is installed. You can use one of the following formats:
   - `http://<server>`. For example, **`http://10.250.10.10`** or **`http://server`**
   - `<IP address>`. For example, **`10.250.10.10`**
   - `<host name>`. For example, **`server`** or **`server.example.com`**
4. In **User name** and **Password**, provide the credentials of an account that is in the list of the management server administrators (**Settings** > **Administrators**). In the backup console, the media will be available under the organization or under a specific unit, according to the permissions given to the specified account.
5. In **Display name**, specify the name that will be displayed for this machine in the backup console. If you leave this field empty, the display name will be set to one of the following:
   - If the machine was previously registered on the management server, it will have the same name.
   - Otherwise, either the fully qualified domain name (FQDN) or the IP address of the machine will be used.
6. Click **OK**.

10.4 Configuring iSCSI and NDAS devices

This section describes how to configure Internet Small Computer System Interface (iSCSI) devices and Network Direct Attached Storage (NDAS) devices when working under bootable media. After

performing the steps below, you will be able to use these devices as if they were locally attached to the machine booted with bootable media.

An **iSCSI target server** (or **target portal**) is a server that hosts an iSCSI device. An **iSCSI target** is a component on the target server; this component shares the device and lists iSCSI initiators that are allowed access to the device. An **iSCSI initiator** is a component on a machine; this component provides interaction between the machine and an iSCSI target. When configuring access to an iSCSI device on a machine booted with bootable media, you need to specify the iSCSI target portal of the device and one of the iSCSI initiators listed in the target. If the target shares several devices, you will get access to all of them.

To add an iSCSI device in a Linux-based bootable media

1. Click **Tools** > **Configure iSCSI/NDAS devices**.
2. Click **Add host**.
3. Specify the IP address and port of the iSCSI target portal, and the name of any iSCSI initiator that is allowed access to the device.
4. If the host requires authentication, specify the user name and password for it.
5. Click **OK**.
6. Select the iSCSI target from the list, and then click **Connect**.
7. If CHAP authentication is enabled in the iSCSI target settings, you will be prompted for credentials to access the iSCSI target. Specify the same user name and target secret as in the iSCSI target settings. Click **OK**.
8. Click **Close** to close the window.

To add an iSCSI device in a PE-based bootable media

1. Click **Tools** > **Run the iSCSI Setup**.
2. Click the **Discovery** tab.
3. Under **Target Portals**, click **Add**, and then specify the IP address and port of the iSCSI target portal. Click **OK**.
4. Click the **General** tab, click **Change**, and then specify the name of any iSCSI initiator that is allowed access to the device.
5. Click the **Targets** tab, click **Refresh**, select the iSCSI target from the list, and then click **Connect**. Click **OK** to connect to the iSCSI target.
6. If CHAP authentication is enabled in the iSCSI target settings, you will see the **Authentication Failure** error. In this case, click **Connect**, click **Advanced**, select the **Enable CHAP log on** check box, and then specify the same user name and target secret as in the iSCSI target settings. Click **OK** to close the window, and then click **OK** to connect to the iSCSI target.
7. Click **OK** to close the window.

To add an NDAS device (only in a Linux-based bootable media)

1. Click **Tools** > **Configure iSCSI/NDAS devices**.
2. Click **NDAS devices**, and then click **Add device**.
3. Specify the 20-character device ID.
4. If you want to allow writing data onto the device, specify the five-character write key. Without this key, the device will be available in the read-only mode.
5. Click **OK**.
6. Click **Close** to close the window.

10.5 Startup Recovery Manager

Startup Recovery Manager is a bootable component residing on the system disk in Windows, or on the /boot partition in Linux and configured to start at boot time on pressing F11. It eliminates the need for a separate media or network connection to start the bootable rescue utility.

Startup Recovery Manager is especially useful for traveling users. If a failure occurs, reboot the machine, wait for the prompt "Press F11 for Acronis Startup Recovery Manager..." to appear, and then press F11. The program will start and you can perform recovery.

You can also back up using Startup Recovery Manager, while on the move.

On machines with the GRUB boot loader installed, you select the Startup Recovery Manager from the boot menu instead of pressing F11.

A machine booted with Startup Recovery Manager can be registered on the management server similarly to a machine booted from bootable media. To do this, click **Tools** > **Register media on the management server**, and then follow the step-by-step procedure described in "Registering media on the management server" (Section 10.3).

Activating Startup Recovery Manager

On a machine running Agent for Windows or Agent for Linux, Startup Recovery Manager can be activated by using the backup console.

To activate Startup Recovery Manager in the backup console

1. Select the machine that you want to activate Startup Recovery Manager on.
2. Click **Details**.
3. Enable the **Startup Recovery Manager** switch.
4. Wait while the software activates Startup Recovery Manager.

To activate Startup Recovery Manager on a machine without an agent

1. Boot the machine from bootable media.
2. Click **Tools** > **Activate Startup Recovery Manager**.
3. Wait while the software activates Startup Recovery Manager.

What happens when you activate Startup Recovery Manager

Activation enables the boot-time prompt "Press F11 for Acronis Startup Recovery Manager..." (if you do not have the GRUB boot loader) or adds the " Startup Recovery Manager" item to GRUB's menu (if you have GRUB).

The system disk (or, the /boot partition in Linux) should have at least 100 MB of free space to activate Startup Recovery Manager.

Unless you use the GRUB boot loader and it is installed in the Master Boot Record (MBR), Startup Recovery Manager activation overwrites the MBR with its own boot code. Thus, you may need to reactivate third-party boot loaders if they are installed.

Under Linux, when using a boot loader other than GRUB (such as LILO), consider installing it to a Linux root (or boot) partition boot record instead of the MBR before activating Startup Recovery Manager. Otherwise, reconfigure the boot loader manually after the activation.

Deactivating Startup Recovery Manager

Deactivation is performed similarly to activation.

Deactivation disables the boot time prompt "Press F11 for Acronis Startup Recovery Manager..." (or, the menu item in GRUB). If Startup Recovery Manager is not activated, you will need one of the following to recover the system when it fails to boot:

- boot the machine from a separate bootable media
- use network boot from a PXE server or Microsoft Remote Installation Services (RIS)

10.6 Acronis PXE Server

Acronis PXE Server allows for booting machines to Acronis bootable components through the network.

Network booting:

- eliminates the need to have a technician onsite to install the bootable media into the system that must be booted
- during group operations, reduces the time required for booting multiple machines as compared to using physical bootable media.

Bootable components are uploaded to Acronis PXE Server using Acronis Bootable Media Builder. To upload bootable components, start the Bootable Media Builder, and then follow the step-by-step instructions described in "Linux-based bootable media" (Section 10.1.1).

Booting multiple machines from the Acronis PXE Server makes sense if there is a Dynamic Host Control Protocol (DHCP) server on your network. Then the network interfaces of the booted machines will automatically obtain IP addresses.

Limitation:

Acronis PXE Server does not support UEFI boot loader.

10.6.1 Installing Acronis PXE Server

To install Acronis PXE Server

1. Log on as an administrator and start the Acronis SCS Cyber Backup 12.5 Hardened Edition setup program.
2. Click **Customize installation settings**.
3. Next to **What to install**, click **Change**.
4. Select the **PXE Server** check box. If you do not want to install other components on this machine, clear the corresponding check boxes. Click **Done** to continue.
5. [Optional] Change other installation settings.
6. Click **Install** to proceed with the installation.
7. After the installation completes, click **Close**.

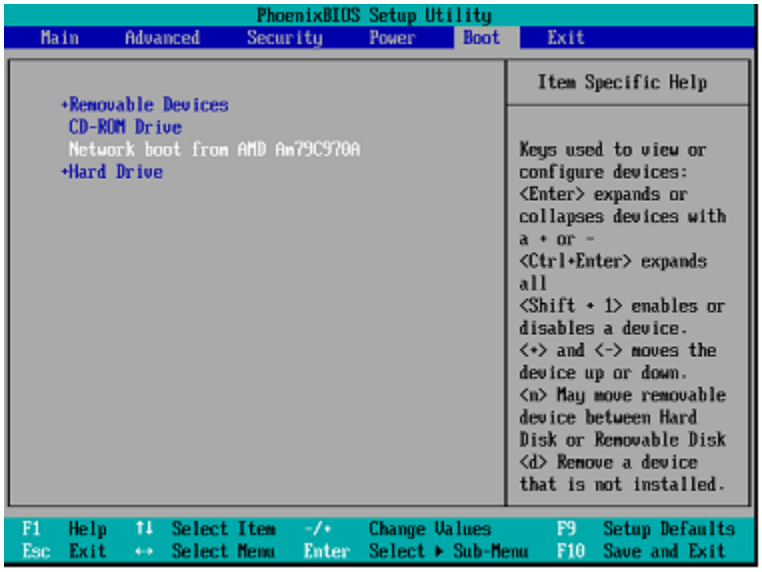
Acronis PXE Server runs as a service immediately after installation. Later on it will automatically launch at each system restart. You can stop and start Acronis PXE Server in the same way as other Windows services.

10.6.2 Setting up a machine to boot from PXE

For bare metal, it is enough that the machine's BIOS supports network booting.

On a machine that has an operating system on the hard disk, the BIOS must be configured so that the network interface card is either the first boot device, or at least prior to the Hard Drive device. The

example below shows one of reasonable BIOS configurations. If you don’t insert bootable media, the machine will boot from the network.



In some BIOS versions, you have to save changes to BIOS after enabling the network interface card so that the card appears in the list of boot devices.

If the hardware has multiple network interface cards, make sure that the card supported by the BIOS has the network cable plugged in.

10.6.3 Work across subnets

To enable the Acronis PXE Server to work in another subnet (across the switch), configure the switch to relay the PXE traffic. The PXE server IP addresses are configured on a per-interface basis using IP helper functionality in the same way as DHCP server addresses. For more information please refer to: https://support.microsoft.com/en-us/help/257579/pxe-clients-do-not-receive-an-ip-address-from-a-dhcp-server.

11 Protecting Microsoft applications

Protecting Microsoft SQL Server and Microsoft Exchange Server

There are two methods of protecting these applications:

- **Database backup**

  This is a file-level backup of the databases and the metadata associated with them. The databases can be recovered to a live application or as files.

- **Application-aware backup**

  This is a disk-level backup that also collects the applications' 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. This means that a single solution and a single backup plan can be used for both disaster recovery and data protection purposes.

For Microsoft Exchange Server, you can opt for **Mailbox backup**. This is a backup of individual mailboxes via the Exchange Web Services protocol. The mailboxes or mailbox items can be recovered

to a live Exchange Server. Mailbox backup is supported for Microsoft Exchange Server 2010 Service Pack 1 (SP1) and later.

Protecting Microsoft SharePoint

A Microsoft SharePoint farm consists of front-end servers that run SharePoint services, database servers that run Microsoft SQL Server, and (optionally) application servers that offload some SharePoint services from the front-end servers. Some front-end and application servers may be identical to each other.

To protect an entire SharePoint farm:

- Back up all of the database servers with application-aware backup.
- Back up all of the unique front-end servers and application servers with usual disk-level backup.

The backups of all servers should be done on the same schedule.

To protect only the content, you can back up the content databases separately.

Protecting a domain controller

A machine running Active Directory Domain Services can be protected by application-aware backup. If a domain contains more than one domain controller, and you recover one of them, a nonauthoritative restore is performed and a USN rollback will not occur after the recovery.

Recovering applications

The following table summarizes the available application recovery methods.

	From a database backup	From an application-aware backup	From a disk backup
Microsoft SQL Server	Databases to a live SQL Server instance (Section 11.5) Databases as files (section 11.5)	Entire machine (Section 6.3) Databases to a live SQL Server instance (Section 11.5) Databases as files (section 11.5)	Entire machine (Section 6.3.1)
Microsoft Exchange Server	Databases to a live Exchange (Section 11.6) Databases as files (Section 11.6) Granular recovery to a live Exchange (Section 11.7)*	Entire machine (Section 6.3.1) Databases to a live Exchange (Section 11.6) Databases as files (Section 11.6) Granular recovery to a live Exchange (Section 11.7)*	Entire machine (Section 6.3.1)
Microsoft SharePoint database servers	Databases to a live SQL Server instance (Section 11.5) Databases as files (Section 11.5) Granular recovery by using SharePoint Explorer	Entire machine (Section 6.3.1) Databases to a live SQL Server instance (Section 11.5) Databases as files (Section 11.5) Granular recovery by using SharePoint Explorer	Entire machine (Section 6.3.1)
Microsoft SharePoint front-end web servers	-	-	Entire machine (Section 6.3.1)
Active Directory Domain Services	-	Entire machine (Section 6.3.1)	-

* Granular recovery is also available from a mailbox backup.

11.1 Prerequisites

Before configuring the application backup, ensure that the requirements listed below are met.

To check the VSS writers state, use the **`vssadmin list writers`** command.

Common requirements

For Microsoft SQL Server, ensure that:

- At least one Microsoft SQL Server instance is started.
- The SQL writer for VSS is turned on.

For Microsoft Exchange Server, ensure that:

- The Microsoft Exchange Information Store service is started.
- Windows PowerShell is installed. For Exchange 2010 or later, the Windows PowerShell version must be at least 2.0.
- Microsoft .NET Framework is installed.

  For Exchange 2007, the Microsoft .NET Framework version must be at least 2.0.

  For Exchange 2010 or later, the Microsoft .NET Framework version must be at least 3.5.
- The Exchange writer for VSS is turned on.

Note *Agent for Exchange needs a temporary storage to operate. By default, the temporary files are located in* ***`%ProgramData%\Acronis\Temp`****. Ensure that you have at least as much free space on the volume where the* `%ProgramData%` *folder is located as 15 percent of an Exchange database size. Alternatively, you can change the location of the temporary files before creating Exchange backups as described in: https://kb.acronis.com/content/40040.*

On a domain controller, ensure that:

- The Active Directory writer for VSS is turned on.

When creating a protection plan, ensure that:

- For physical machines, the Volume Shadow Copy Service (VSS) (Section 5.10.28) backup option is enabled.
- For virtual machines, the Volume Shadow Copy Service (VSS) for virtual machines (Section 5.10.29) backup option is enabled.

Additional requirements for application-aware backups

When creating a protection plan, ensure that **Entire machine** is selected for backup. The **Sector-by-sector** backup option must be disabled in a protection plan, otherwise it will be impossible to perform a recovery of application data from such backups. If the plan is executed in the **Sector-by-sector** mode due to an automatic switch to this mode, then recovery of application data will also be impossible.

Requirements for ESXi virtual machines

If the application runs on a virtual machine that is backed up by Agent for VMware, ensure that:

- The virtual machine being backed up meets the requirements for application-consistent backup and restore listed in the article "Windows Backup Implementations" in the VMware documentation: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html
- VMware Tools is installed and up-to-date on the machine.

- User Account Control (UAC) is disabled on the machine. If you do not want to disable UAC, you must provide the credentials of a built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

Requirements for Hyper-V virtual machines

If the application runs on a virtual machine that is backed up by Agent for Hyper-V, ensure that:

- The guest operating system is Windows Server 2008 or later.
- For Hyper-V 2008 R2: the guest operating system is Windows Server 2008/2008 R2/2012.
- The virtual machine has no dynamic disks.
- The network connection exists between the Hyper-V host and the guest operating system. This is required to execute remote WMI queries inside the virtual machine.
- User Account Control (UAC) is disabled on the machine. If you do not want to disable UAC, you must provide the credentials of a built-in domain administrator (DOMAIN\Administrator) when enabling application backup.
- The virtual machine configuration matches the following criteria:
  - Hyper-V Integration Services is installed and up-to-date. The critical update is https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - In the virtual machine settings, the **Management** > **Integration Services** > **Backup (volume checkpoint)** option is enabled.
  - For Hyper-V 2012 and later: the virtual machine has no checkpoints.
  - For Hyper-V 2012 R2 and later: the virtual machine has a SCSI controller (check **Settings** > **Hardware**).

11.2 Database backup

Before backing up databases, ensure that the requirements listed in "Prerequisites" (Section 11.1) are met.

Select the databases as described below, and then specify other settings of the backup plan as appropriate (Section 5.1).

11.2.1 Selecting SQL databases

A backup of an SQL database contains the database files (.mdf, .ndf), log files (.ldf), and other associated files. The files are backed with the help of the SQL Writer service. The service must be running at the time that the Volume Shadow Copy Service (VSS) requests a backup or recovery.

The SQL transaction logs are truncated after each successful backup. SQL log truncation can be disabled in the backup plan options (Section 5.10.15).

To select SQL databases

1. Click **Devices** > **Microsoft SQL**.

   The software shows the tree of SQL Server Always On Availability Groups (AAG), machines running Microsoft SQL Server, SQL Server instances, and databases.
2. Browse to the data that you want to back up.

   Expand the tree nodes or double-click items in the list to the right of the tree.
3. Select the data that you want to back up. You can select AAGs, machines running SQL Server, SQL Server instances, or individual databases.

- If you select an AAG, all databases that are included into the selected AAG will be backed up. For more information about backing up AAGs, refer to "Protecting Always On Availability Groups (AAG)" (Section 11.2.3).
- If you select a machine running SQL Server, all databases that are attached to all SQL Server instances running on the selected machine will be backed up.
- If you select a SQL Server instance, all databases that are attached to the selected instance will be backed up.
- If you select databases directly, only the selected databases will be backed up.

4. Click **Backup**. If prompted, provide credentials to access the SQL Server data. The account must be a member of the **Backup Operators** or **Administrators** group on the machine and a member of the **sysadmin** role on each of the instances that you are going to back up.

11.2.2 Selecting Exchange Server data

The following table summarizes the Microsoft Exchange Server data that you can select for backup and the minimal user rights required to back up the data.

Exchange version	Data items	User rights
2007	Storage groups	Membership in the **Exchange Organization Administrators** role group
2010/2013/2016/2019	Databases, Database Availability Groups (DAG)	Membership in the **Server Management** role group.

A full backup contains all of the selected Exchange Server data.

An incremental backup contains the changed blocks of the database files, the checkpoint files, and a small number of the log files that are more recent than the corresponding database checkpoint. Because changes to the database files are included in the backup, there is no need to back up all the transaction log records since the previous backup. Only the log that is more recent than the checkpoint needs to be replayed after a recovery. This makes for faster recovery and ensures successful database backup, even with circular logging enabled.

The transaction log files are truncated after each successful backup.

To select Exchange Server data

1. Click **Devices** > **Microsoft Exchange**.
   The software shows the tree of Exchange Server Database Availability Groups (DAG), machines running Microsoft Exchange Server, and Exchange Server databases. If you configured Agent for Exchange as described in "Mailbox backup" (Section 11.4), mailboxes are also shown in this tree.
2. Browse to the data that you want to back up.
   Expand the tree nodes or double-click items in the list to the right of the tree.
3. Select the data that you want to back up.
   - If you select a DAG, one copy of each clustered database will be backed up. For more information about backing up DAGs, refer to "Protecting Database Availability Groups (DAG)" (Section 11.2.4).
   - If you select a machine running Microsoft Exchange Server, all databases that are mounted to the Exchange Server running on the selected machine will be backed up.
   - If you select databases directly, only the selected databases will be backed up.
   - If you configured Agent for Exchange as described in "Mailbox backup" (Section 11. 4), you can select mailboxes for backup (Section 11.4.1).

4. If prompted, provide the credentials to access the data.
5. Click **Protect**.

11.2.3 Protecting Always On Availability Groups (AAG)

Note *This functionality is not available in the Standard edition of Acronis SCS Cyber Backup 12.5 Hardened Edition.*

SQL Server high-availability solutions overview

The Windows Server Failover Clustering (WSFC) functionality enables you to configure a highly available SQL Server through redundancy at the instance level (Failover Cluster Instance, FCI) or at the database level (AlwaysOn Availability Group, AAG). You can also combine both methods.

In a Failover Cluster Instance, SQL databases are located on a shared storage. This storage can only be accessed from the active cluster node. If the active node fails, a failover occurs and a different node becomes active.

In an availability group, each database replica resides on a different node. If the primary replica becomes not available, a secondary replica residing on a different node is assigned the primary role.

Thus, the clusters are already serving as a disaster recovery solution themselves. However, there might be cases when the clusters cannot provide data protection: for example, in case of a database logical corruption, or when the entire cluster is down. Also cluster solutions do not protect from harmful content changes, as they usually immediately replicate to all cluster nodes.

Supported cluster configurations

This backup software supports *only* the Always On Availability Group (AAG) for SQL Server 2012 or later. Other cluster configurations, such as Failover Cluster Instances, database mirroring, and log shipping are *not* supported.

How many agents are required for cluster data backup and recovery?

For successful data backup and recovery of a cluster Agent for SQL has to be installed on each node of the WSFC cluster.

Backing up databases included in an AAG

1. Install Agent for SQL on each node of the WSFC cluster.

   Tip *After you install the agent on one of the nodes, the software displays the AAG and its nodes under* ***Devices*** *>* ***Microsoft SQL*** *>* ***Databases****. To install Agents for SQL on the rest of the nodes, select the AAG, click* ***Details****, and then click* ***Install agent*** *next to each of the nodes.*

2. Select the AAG to backup as described in "Selecting SQL databases" (Section 11.2.1).

   Important *You must select the AAG itself, rather than the individual nodes or databases inside of it. If you select individual items inside the AAG, the backup will not be cluster-aware and only the selected copies of the items will be backed up.*

3. Configure the "Cluster backup mode" (Section 5.10.8) backup option.

Recovery of databases included in an AAG

1. Select the databases that you want to recover, and then select the recovery point from which you want to recover the databases.

   When you select a clustered database under **Devices** > **Microsoft SQL** > **Databases**, and then click **Recover**, the software shows only the recovery points that correspond to the times when the selected copy of the database was backed up.

The easiest way to view all recovery points of a clustered database is to select the backup of the entire AAG on the Backups tab (Section 7.1). The names of AAG backups are based on the following template: `<AAG name> - <backup plan name>` and have a special icon.

2. To configure recovery, follow the steps described in "Recovering SQL databases" (Section 11.5), starting from step 5.

   The software automatically defines a cluster node to which the data will be recovered. The node's name is displayed in the **Recover to** field. You can manually change the target node.

   Important *A database that is included in an Always On Availability Group cannot be overwritten during a recovery because Microsoft SQL Server prohibits this. You need to exclude the target database from the AAG before the recovery. Or, just recover the database as a new non-AAG one. When the recovery is completed, you can reconstruct the original AAG configuration.*

11.2.4 Protecting Database Availability Groups (DAG)

Note *This functionality is not available in the Standard edition of Acronis SCS Cyber Backup 12.5 Hardened Edition.*

Exchange Server clusters overview

The main idea of Exchange clusters is to provide high database availability with fast failover and no data loss. Usually, it is achieved by having one or more copies of databases or storage groups on the members of the cluster (cluster nodes). If the cluster node hosting the active database copy or the active database copy itself fails, the other node hosting the passive copy automatically takes over the operations of the failed node and provides access to Exchange services with minimal downtime. Thus, the clusters are already serving as a disaster recovery solution themselves.

However, there might be cases when failover cluster solutions cannot provide data protection: for example, in case of a database logical corruption, or when a particular database in a cluster has no copy (replica), or when the entire cluster is down. Also cluster solutions do not protect from harmful content changes, as they usually immediately replicate to all cluster nodes.

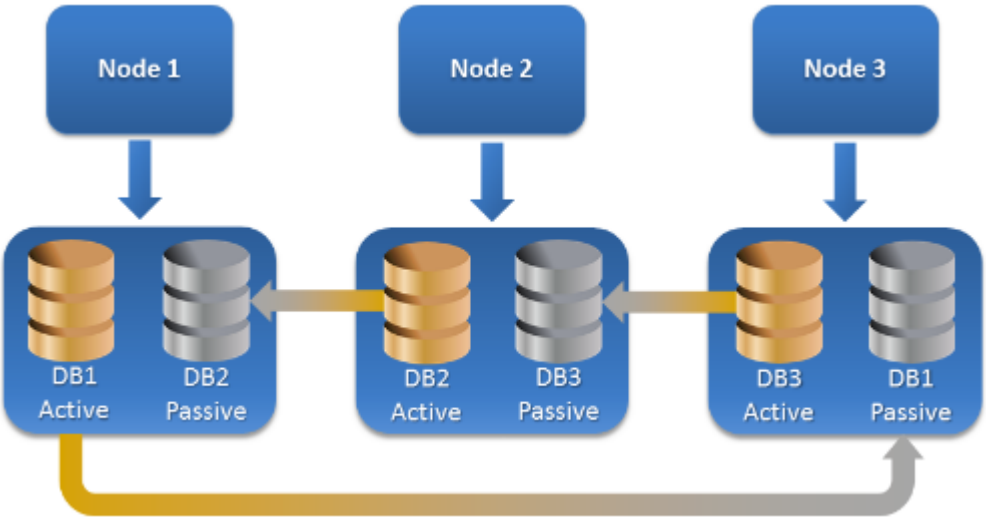
Cluster-aware backup

With cluster-aware backup, you back up only one copy of the clustered data. If the data changes its location within the cluster (due to a switchover or a failover), the software will track all relocations of this data and safely back it up.

Supported cluster configurations

Cluster-aware backup is supported *only* for Database Availability Group (DAG) in Exchange Server 2010 or later. Other cluster configurations, such as Single Copy Cluster (SCC) and Cluster Continuous Replication (CCR) for Exchange 2007, are *not* supported.

DAG is a group of up to 16 Exchange Mailbox servers. Any node can host a copy of mailbox database from any other node. Each node can host passive and active database copies. Up to 16 copies of each database can be created.



How many agents are required for cluster-aware backup and recovery?

For successful backup and recovery of clustered databases, Agent for Exchange has to be installed on each node of the Exchange cluster.

Tip *After you install the agent on one of the nodes, the backup console displays the DAG and its nodes under* ***Devices*** *>* ***Microsoft Exchange*** *>* ***Databases****. To install Agents for Exchange on the rest of the nodes, select the DAG, click* ***Details****, and then click* ***Install agent*** *next to each of the nodes.*

Backing up the Exchange cluster data

1. When creating a backup plan, select the DAG as described in "Selecting Exchange Server data" (Section 11.2.2).
2. Configure the "Cluster backup mode" (Section 5.10.8) backup option.
3. Specify other settings of the backup plan as appropriate (Section 5.1).

Important *For cluster-aware backup, ensure to select the DAG itself. If you select individual nodes or databases inside the DAG, only the selected items will be backed up and the* ***Cluster backup mode*** *option will be ignored.*

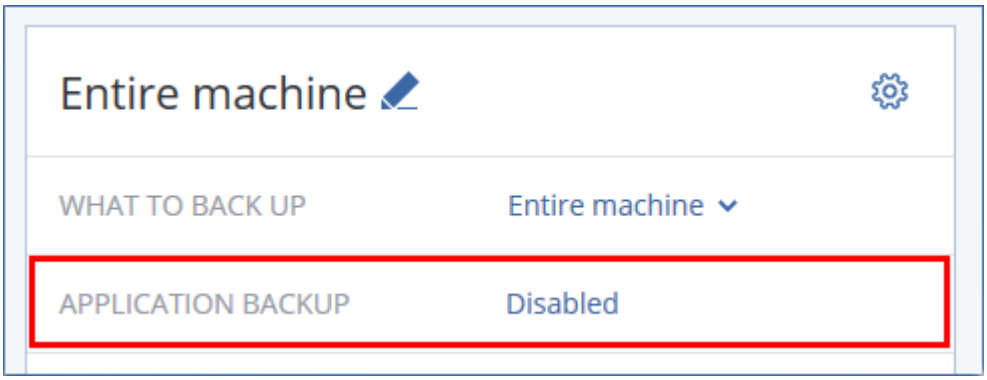
Recovering the Exchange cluster data

1. Select the recovery point for the database that you want to recover. Selecting an entire cluster for recovery is not possible.
   When you select a copy of a clustered database under **Devices** > **Microsoft Exchange** > **Databases** > `<cluster name>` > `<node name>` and click **Recover**, the software shows only the recovery points that correspond to the times when this copy was backed up.
   The easiest way to view all recovery points of a clustered database is to select its backup on the Backups tab (Section 7.1).
2. Follow the steps described in "Recovering Exchange databases", starting from step 5.
   The software automatically defines a cluster node to which the data will be recovered. The node's name is displayed in the **Recover to** field. You can manually change the target node.

11.3 Application-aware backup

Application-aware disk-level backup is available for physical machines and for ESXi virtual machines.

When you back up a machine running Microsoft SQL Server, Microsoft Exchange Server, or Active Directory Domain Services, enable **Application backup** for additional protection of these applications' data.



Why use application-aware backup?

By using application-aware backup, you ensure that:

1. The applications are backed up in a consistent state and thus will be available immediately after the machine is recovered.
2. You can recover the SQL and Exchange databases, mailboxes, and mailbox items without recovering the entire machine.
3. The SQL transaction logs are truncated after each successful backup. SQL log truncation can be disabled in the backup plan options (Section 5.10.15). The Exchange transaction logs are truncated on virtual machines only. You can enable the VSS full backup option (Section 5.10.28) if you want to truncate Exchange transaction logs on a physical machine.
4. If a domain contains more than one domain controller, and you recover one of them, a nonauthoritative restore is performed and a USN rollback will not occur after the recovery.

What do I need to use application-aware backup?

On a physical machine, Agent for SQL and/or Agent for Exchange must be installed, in addition to Agent for Windows.

On a virtual machine, no agent installation is required; it is presumed that the machine is backed up by Agent for VMware (Windows).

Agent for VMware (Virtual Appliance) can create application-aware backups, but cannot recover application data from them. To recover application data from backups created by this agent, you need Agent for VMware (Windows), Agent for SQL, or Agent for Exchange on a machine that has access to the location where the backups are stored. When configuring recovery of application data, select the recovery point on the **Backups** tab, and then select this machine in **Machine to browse from**.

Other requirements are listed in the "Prerequisites" (Section 11.1) and "Required user rights" (Section 11 3.1) sections.

11.3.1 Required user rights

An application-aware backup contains metadata of VSS-aware applications that are present on the disk. To access this metadata, the agent needs an account with the appropriate rights, which are listed below. You are prompted to specify this account when enabling application backup.

- For SQL Server:

  The account must be a member of the **Backup Operators** or **Administrators** group on the machine, and a member of the **sysadmin** role on each of the instances that you are going to back up.
- For Exchange Server:

  Exchange 2007: The account must be a member of the **Administrators** group on the machine, and a member of the **Exchange Organization Administrators** role group.

  Exchange 2010 and later: The account must be a member of the **Administrators** group on the machine, and a member of the **Organization Management** role group.
- For Active Directory:

  The account must be a domain administrator.

Additional requirement for virtual machines

If the application runs on a virtual machine that is backed up by Agent for VMware or Agent for Hyper-V, ensure that User Account Control (UAC) is disabled on the machine. If you do not want to disable UAC, you must provide the credentials of a built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

11.4 Mailbox backup

Mailbox backup is supported for Microsoft Exchange Server 2010 Service Pack 1 (SP1) and later.

Mailbox backup is available if at least one Agent for Exchange is registered on the management server. The agent must be installed on a machine that belongs to the same Active Directory forest as Microsoft Exchange Server.

Before backing up mailboxes, you must connect Agent for Exchange to the machine running the **Client Access** server role (CAS) of Microsoft Exchange Server. In Exchange 2016 and later, the CAS role is not available as a separate installation option. It is automatically installed as part of the Mailbox server role. Thus, you can connect the agent to any server running the **Mailbox role**.

To connect Agent for Exchange to CAS

1. Click **Devices** > **Add**.
2. Click **Microsoft Exchange Server**.
3. Click **Exchange mailboxes**.

   If no Agent for Exchange is registered on the management server, the software suggests that you install the agent. After the installation, repeat this procedure from step 1.
4. [Optional] If multiple Agents for Exchange are registered on the management server, click **Agent**, and then change the agent that will perform the backup.
5. In **Client Access server**, specify the fully qualified domain name (FQDN) of the machine where the **Client Access** role of Microsoft Exchange Server is enabled.

   In Exchange 2016 and later, the Client Access services are automatically installed as part of the Mailbox server role. Thus, you can specify any server running the **Mailbox role**. We refer to this server as CAS later in this section.

6. In **Authentication type**, select the authentication type that is used by the CAS. You can select **Kerberos** (default) or **Basic**.
7. [Only for basic authentication] Select which protocol will be used. You can select **HTTPS** (default) or **HTTP**.
8. [Only for basic authentication with the HTTPS protocol] If the CAS uses an SSL certificate that was obtained from a certification authority, and you want the software to check the certificate when connecting to the CAS, select the **Check SSL certificate** check box. Otherwise, skip this step.
9. Provide the credentials of an account that will be used to access the CAS. The requirements for this account are listed in "Required user rights" (Section 11.4.2).
10. Click **Add**.

As a result, the mailboxes appear under **Devices** > **Microsoft Exchange** > **Mailboxes**.

11.4.1 Selecting Exchange Server mailboxes

Select the mailboxes as described below, and then specify other settings of the backup plan as appropriate (Section 5.1).

To select Exchange mailboxes

1. Click **Devices** > **Microsoft Exchange**.

   The software shows the tree of Exchange databases and mailboxes.
2. Click **Mailboxes**, and then select the mailboxes that you want to back up.
3. Click **Backup**.

11.4.2 Required user rights

To access mailboxes, Agent for Exchange needs an account with the appropriate rights. You are prompted to specify this account when configuring various operations with mailboxes.

Membership of the account in the **Organization Management** role group enables access to any mailbox, including mailboxes that will be created in the future.

The minimum required user rights are as follows:

- The account must be a member of the **Server Management** and **Recipient Management** role groups.
- The account must have the **ApplicationImpersonation** management role enabled for all users or groups of users whose mailboxes the agent will access.

  For information about configuring the **ApplicationImpersonation** management role, refer to the following Microsoft knowledge base article: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

11.5 Recovering SQL databases

This section describes recovery from both database backups and application-aware backups.

You can recover SQL databases to a SQL Server instance, if Agent for SQL is installed on the machine running the instance. You will need to provide credentials for an account that is a member of the **Backup Operators** or **Administrators** group on the machine and a member of the **sysadmin** role on the target instance.

Alternatively, you can recover the databases as files. This can be useful if you need to extract data for data mining, audit, or further processing by third-party tools. You can attach the SQL database files to a SQL Server instance, as described in "Attaching SQL Server databases" (Section 11.5.2).

If you use only Agent for VMware, recovering databases as files is the only available recovery method.

System databases are basically recovered in the same way as user databases. The peculiarities of system database recovery are described in "Recovering system databases" (Section 11.5.1).

To recover SQL databases to a SQL Server instance

1. Do one of the following:
   - When recovering from an application-aware backup, under **Devices**, select the machine that originally contained the data that you want to recover.
   - When recovering from a database backup, click **Devices** > **Microsoft SQL**, and then select the databases that you want to recover.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do one of the following:
   - [Only when recovering from an application-aware backup] If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for SQL, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).

   The machine chosen for browsing in either of the above actions becomes a target machine for the SQL databases recovery.
4. Do one of the following:
   - When recovering from an application-aware backup, click **Recover** > **SQL databases**, select the databases that you want to recover, and then click **Recover**.
   - When recovering from a database backup, click **Recover** > **Databases to an instance**.
5. By default, the databases are recovered to the original ones. If the original database does not exist, it will be recreated. You can select another SQL Server instance (running on the same machine) to recover the databases to.

   To recover a database as a different one to the same instance:
   a. Click the database name.
   b. In **Recover to**, select **New database**.
   c. Specify the new database name.
   d. Specify the new database path and log path. The folder you specify must not contain the original database and log files.
6. [Optional] To change the database state after recovery, click the database name, and then choose one of the following states:
   - **Ready to use (RESTORE WITH RECOVERY)** (default)

     After the recovery completes, the database will be ready for use. Users will have full access to it. The software will roll back all uncommitted transactions of the recovered database that are stored in the transaction logs. You will not be able to recover additional transaction logs from the native Microsoft SQL backups.
   - **Non-operational (RESTORE WITH NORECOVERY)**

After the recovery completes, the database will be non-operational. Users will have no access to it. The software will keep all uncommitted transactions of the recovered database. You will be able to recover additional transaction logs from the native Microsoft SQL backups and thus reach the necessary recovery point.

- **Read-only (RESTORE WITH STANDBY)**

  After the recovery completes, users will have read-only access to the database. The software will undo any uncommitted transactions. However, it will save the undo actions in a temporary standby file so that the recovery effects can be reverted.

  This value is primarily used to detect the point in time when a SQL Server error occurred.

7. Click **Start recovery**.

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

To recover SQL databases as files

1. Do one of the following:
   - When recovering from an application-aware backup, under **Devices**, select the machine that originally contained the data that you want to recover.
   - When recovering from a database backup, click **Devices** > **Microsoft SQL**, and then select the databases that you want to recover.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do one of the following:
   - [Only when recovering from an application-aware backup] If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for SQL or Agent for VMware, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).

   The machine chosen for browsing in either of the above actions becomes a target machine for the SQL databases recovery.
4. Do one of the following:
   - When recovering from an application-aware backup, click **Recover** > **SQL databases**, select the databases that you want to recover, and then click **Recover as files**.
   - When recovering from a database backup, click **Recover** > **Databases as files**.
5. Click **Browse**, and then select a local or a network folder to save the files to.
6. Click **Start recovery**.

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

11.5.1 Recovering system databases

All system databases of an instance are recovered at once. When recovering system databases, the software automatically restarts the destination instance in the single-user mode. After the recovery completes, the software restarts the instance and recovers other databases (if any).

Other things to consider when recovering system databases:

- System databases can only be recovered to an instance of the same version as the original instance.
- System databases are always recovered in the "ready to use" state.

Recovering the master database

System databases include the **master** database. The **master** database records information about all databases of the instance. Hence, the **master** database in a backup contains information about databases which existed in the instance at the time of the backup. After recovering the **master** database, you may need to do the following:

- Databases that have appeared in the instance after the backup was done are not visible by the instance. To bring these databases back to production, attach them to the instance manually by using SQL Server Management Studio.
- Databases that have been deleted after the backup was done are displayed as offline in the instance. Delete these databases by using SQL Server Management Studio.

11.5.2 Attaching SQL Server databases

This section describes how to attach a database in SQL Server by using SQL Server Management Studio. Only one database can be attached at a time.

Attaching a database requires any of the following permissions: **CREATE DATABASE**, **CREATE ANY DATABASE**, or **ALTER ANY DATABASE**. Normally, these permissions are granted to the **sysadmin** role of the instance.

To attach a database

1. Run Microsoft SQL Server Management Studio.
2. Connect to the required SQL Server instance, and then expand the instance.
3. Right-click **Databases** and click **Attach**.
4. Click **Add**.
5. In the **Locate Database Files** dialog box, find and select the .mdf file of the database.
6. In the **Database Details** section, make sure that the rest of database files (.ndf and .ldf files) are found.

   Details. SQL Server database files may not be found automatically, if:

   - They are not in the default location, or they are not in the same folder as the primary database file (.mdf). Solution: Specify the path to the required files manually in the **Current File Path** column.
   - You have recovered an incomplete set of files that make up the database. Solution: Recover the missing SQL Server database files from the backup.
7. When all of the files are found, click **OK**.

11.6 Recovering Exchange databases

This section describes recovery from both database backups and application-aware backups.

You can recover Exchange Server data to a live Exchange Server. This may be the original Exchange Server or an Exchange Server of the same version running on the machine with the same fully qualified domain name (FQDN). Agent for Exchange must be installed on the target machine.

The following table summarizes the Exchange Server data that you can select for recovery and the minimal user rights required to recover the data.

Exchange version	Data items	User rights
2007	Storage groups	Membership in the **Exchange Organization Administrators** role group.
2010/2013/2016/2019	Databases	Membership in the **Server Management** role group.

Alternatively, you can recover the databases (storage groups) as files. The database files, along with transaction log files, will be extracted from the backup to a folder that you specify. This can be useful if you need to extract data for an audit or further processing by third-party tools, or when the recovery fails for some reason and you are looking for a workaround to mount the databases manually (Section 11.6.1).

If you use only Agent for VMware (Windows), recovering databases as files is the only available recovery method. Recovering databases by using Agent for VMware (Virtual Appliance) is not possible.

We will refer to both databases and storage groups as "databases" throughout the below procedures.

To recover Exchange databases to a live Exchange Server

1. Do one of the following:
   - When recovering from an application-aware backup, under **Devices**, select the machine that originally contained the data that you want to recover.
   - When recovering from a database backup, click **Devices** > **Microsoft Exchange** > **Databases**, and then select the databases that you want to recover.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do one of the following:
   - [Only when recovering from an application-aware backup] If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).

   The machine chosen for browsing in either of the above actions becomes a target machine for the Exchange data recovery.
4. Do one of the following:
   - When recovering from an application-aware backup, click **Recover** > **Exchange databases**, select the databases that you want to recover, and then click **Recover**.
   - When recovering from a database backup, click **Recover** > **Databases to an Exchange server**.
5. By default, the databases are recovered to the original ones. If the original database does not exist, it will be recreated.

   To recover a database as a different one:
   a. Click the database name.
   b. In **Recover to**, select **New database**.
   c. Specify the new database name.
   d. Specify the new database path and log path. The folder you specify must not contain the original database and log files.
6. Click **Start recovery**.

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

To recover Exchange databases as files

1. Do one of the following:
   - When recovering from an application-aware backup, under **Devices**, select the machine that originally contained the data that you want to recover.
   - When recovering from a database backup, click **Devices** > **Microsoft Exchange** > **Databases**, and then select the databases that you want to recover.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do one of the following:
   - [Only when recovering from an application-aware backup] If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange or Agent for VMware, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).

   The machine chosen for browsing in either of the above actions becomes a target machine for the Exchange data recovery.
4. Do one of the following:
   - When recovering from an application-aware backup, click **Recover** > **Exchange databases**, select the databases that you want to recover, and then click **Recover as files**.
   - When recovering from a database backup, click **Recover** > **Databases as files**.
5. Click **Browse**, and then select a local or a network folder to save the files to.
6. Click **Start recovery**.

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

11.6.1 Mounting Exchange Server databases

After recovering the database files, you can bring the databases online by mounting them. Mounting is performed by using Exchange Management Console, Exchange System Manager, or Exchange Management Shell.

The recovered databases will be in a Dirty Shutdown state. A database that is in a Dirty Shutdown state can be mounted by the system if it is recovered to its original location (that is, information about the original database is present in Active Directory). When recovering a database to an alternate location (such as a new database or as the recovery database), the database cannot be mounted until you bring it to a Clean Shutdown state by using the **`Eseutil /r <Enn>`** command. **`<Enn>`** specifies the log file prefix for the database (or storage group that contains the database) into which you need to apply the transaction log files.

The account you use to attach a database must be delegated an Exchange Server Administrator role and a local Administrators group for the target server.

For details about how to mount databases, see the following articles:

- Exchange 2010 or later: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

11.7 Recovering Exchange mailboxes and mailbox items

This section describes how to recover Exchange mailboxes and mailbox items from database backups, from application-aware backups, and from mailbox backups to a live Exchange Server.

The following items can be recovered:

- Mailboxes (except for archive mailboxes)
- Public folders
- Public folder items
- Email folders
- Email messages
- Calendar events
- Tasks
- Contacts
- Journal entries
- Notes

You can use search to locate the items.

Granular recovery can be performed to Microsoft Exchange Server 2010 Service Pack 1 (SP1) and later. The source backup may contain databases or mailboxes of any supported Exchange version.

Granular recovery can be performed by Agent for Exchange or Agent for VMware (Windows). The target Exchange Server and the machine running the agent must belong to the same Active Directory forest.

When a mailbox is recovered to an existing mailbox, the existing items with matching IDs are overwritten.

Recovery of mailbox items does not overwrite anything. Instead, the full path to a mailbox item is recreated in the target folder.

Requirements on user accounts

A mailbox being recovered from a backup must have an associated user account in Active Directory.

User mailboxes and their contents can be recovered only if their associated user accounts are *enabled*. Shared, room, and equipment mailboxes can be recovered only if their associated user accounts are *disabled*.

A mailbox that does not meet the above conditions is skipped during recovery.

If some mailboxes are skipped, the recovery will succeed with warnings. If all mailboxes are skipped, the recovery will fail.

11.7.1 Recovering mailboxes

To recover mailboxes from an application-aware backup or a database backup

1. Do one of the following:
   - When recovering from an application-aware backup: under **Devices**, select the machine that originally contained the data that you want to recover.

- When recovering from a database backup, click **Devices** > **Microsoft Exchange** > **Databases**, and then select the database that originally contained the data that you want to recover.

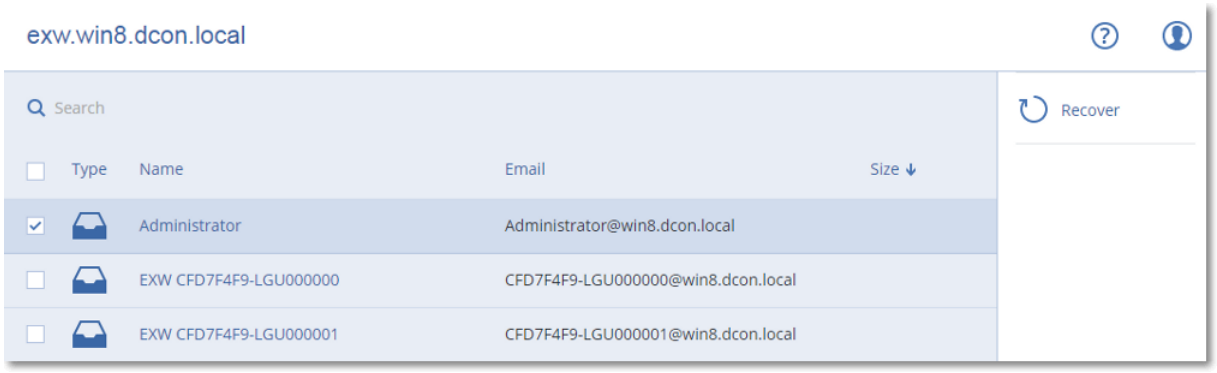
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Use other ways to recover:

   - [Only when recovering from an application-aware backup] If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange or Agent for VMware, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).

   The machine chosen for browsing in either of the above actions will perform the recovery instead of the original machine that is offline.
4. Click **Recover** > **Exchange mailboxes**.
5. Select the mailboxes that you want to recover.

   You can search mailboxes by name. Wildcards are not supported.



6. Click **Recover**.
7. Click **Target machine with Microsoft Exchange Server** to select or change the target machine.
   This step allows recovery to a machine that is not running Agent for Exchange.
   Specify the fully qualified domain name (FQDN) of the machine where the **Client Access** role of Microsoft Exchange Server is enabled. The machine must belong to the same Active Directory forest as the machine that performs the recovery.
   If prompted, provide the credentials of an account that will be used to access the machine. The requirements for this account are listed in "Required user rights" (Section 11.4.2).
8. [Optional] Click **Database to re-create any missing mailboxes** to change the automatically selected database.
9. Click **Start recovery**.

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

To recover a mailbox from a mailbox backup

1. Click **Devices** > **Microsoft Exchange** > **Mailboxes**.
2. Select the mailbox to recover, and then click **Recovery**.

   You can search mailboxes by name. Wildcards are not supported.

   If the mailbox was deleted, select it on the Backups tab (Section 7.1), and then click **Show backups**.
3. Select a recovery point. Note that recovery points are filtered by location.
4. Click **Recover** > **Mailbox**.
5. Perform steps 7-9 of the above procedure.

11.7.2 Recovering mailbox items

To recover mailbox items from an application-aware backup or a database backup

1. Do one of the following:
   - When recovering from an application-aware backup: under **Devices**, select the machine that originally contained the data that you want to recover.
   - When recovering from a database backup, click **Devices** > **Microsoft Exchange** > **Databases**, and then select the database that originally contained the data that you want to recover.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Use other ways to recover:
   - [Only when recovering from an application-aware backup] If the backup location is shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange or Agent for VMware, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).

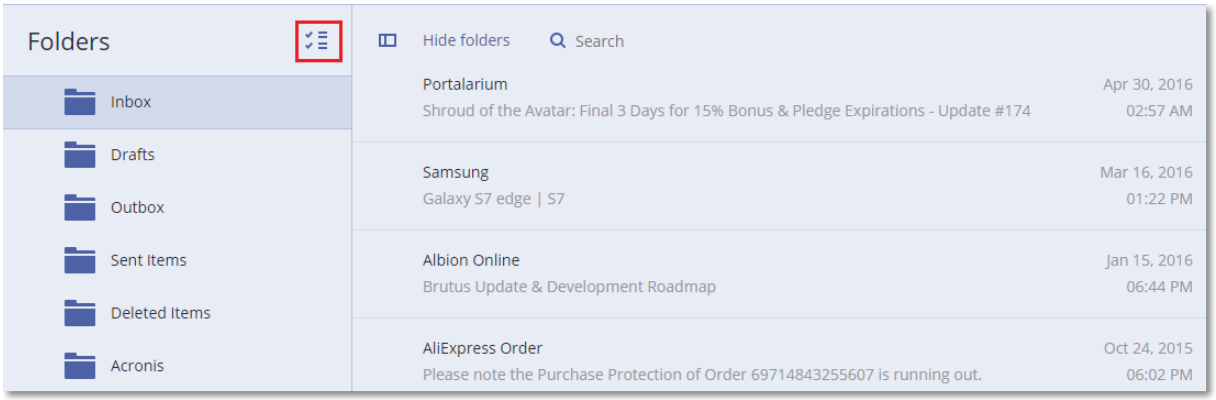
   The machine chosen for browsing in either of the above actions will perform the recovery instead of the original machine that is offline.
4. Click **Recover** > **Exchange mailboxes**.
5. Click the mailbox that originally contained the items that you want to recover.
6. Select the items that you want to recover.

   The following search options are available. Wildcards are not supported.
   - For email messages: search by subject, sender, recipient, and date.
   - For events: search by title and date.
   - For tasks: search by subject and date.
   - For contacts: search by name, email address, and phone number.

   When an email message is selected, you can click **Show content** to view its contents, including attachments.

   Tip *Click the name of an attached file to download it.*

   To be able to select folders, click the recover folders icon.



7. Click **Recover**.
8. Click **Target machine with Microsoft Exchange Server** to select or change the target machine. This step allows recovery to a machine that is not running Agent for Exchange.

   Specify the fully qualified domain name (FQDN) of the machine where the **Client Access** role of Microsoft Exchange Server is enabled. The machine must belong to the same Active Directory forest as the machine that performs the recovery.

If prompted, provide the credentials of an account that will be used to access the machine. The requirements for this account are listed in "Required user rights" (Section 11.4.2).

9. In **Target mailbox**, view, change, or specify the target mailbox.

   By default, the original mailbox is selected. If this mailbox does not exist or a non-original target machine is selected, you must specify the target mailbox.

10. [Only when recovering email messages] In **Target folder**, view or change the target folder in the target mailbox. By default, the **Recovered items** folder is selected.
11. Click **Start recovery**.

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

To recover a mailbox item from a mailbox backup

1. Click **Devices** > **Microsoft Exchange** > **Mailboxes**.
2. Select the mailbox that originally contained the items that you want to recover, and then click **Recovery**.

   You can search mailboxes by name. Wildcards are not supported.

   If the mailbox was deleted, select it on the Backups tab (Section 7.1), and then click **Show backups**.
3. Select a recovery point. Note that recovery points are filtered by location.
4. Click **Recover** > **Email messages**.
5. Select the items that you want to recover.

   The following search options are available. Wildcards are not supported.

   - For email messages: search by subject, sender, recipient, and date.
   - For events: search by title and date.
   - For tasks: search by subject and date.
   - For contacts: search by name, email address, and phone number.

   When an email message is selected, you can click **Show content** to view its contents, including attachments.

   Tip *Click the name of an attached file to download it.*

   When an email message is selected, you can click **Send as email** to send the message to an email address. The message is sent from your administrator account's email address.

   To be able to select folders, click the recover folders icon: 
6. Click **Recover**.
7. Perform steps 8-11 of the above procedure.

11.8 Changing the SQL Server or Exchange Server access credentials

You can change access credentials for SQL Server or Exchange Server without re-installing the agent.

To change the SQL Server or Exchange Server access credentials

1. Click **Devices**, and then click **Microsoft SQL** or **Microsoft Exchange**.
2. Select the Always On Availability Group, Database Availability Group, SQL Server instance, or Exchange Server for which you want to change the access credentials.
3. Click **Specify credentials**.
4. Specify the new access credentials, and then click **OK**.

To change the Exchange Server access credentials for mailbox backup

1. Click **Devices** > **Microsoft Exchange**, and then expand **Mailboxes**.
2. Select the Exchange Server for which you want to change the access credentials.
3. Click **Settings**.
4. Under **Exchange administrator account**, specify the new access credentials, and then click **Save**.

12 Protecting Oracle Database

Protection of Oracle Database is described in a separate document available at https://dl.acronisscs.com/u/pdf/AcronisBackup_12.5_OracleBackup_whitepaper.pdf

13 Active Protection

Active Protection protects a system from ransomware and cryptocurrency mining malware. Ransomware encrypts files and demands a ransom for the encryption key. Cryptomining malware performs mathematical calculations in the background, thus stealing the processing power and network traffic.

Active Protection is available for machines running Windows 7 and later, Windows Server 2008 R2 and later. Agent for Windows must be installed on the machine.

How it works

Active Protection monitors processes running on the protected machine. When a third-party process tries to encrypt files or mine cryptocurrency, Active Protection generates an alert and performs additional actions, if those are specified by the configuration.

In addition, Active Protection prevents unauthorized changes to the backup software's own processes, registry records, executable and configuration files, and backups located in local folders.

To identify malicious processes, Active Protection uses behavioral heuristics. Active Protection compares the chain of actions performed by a process with the chains of events recorded in the database of malicious behavior patterns. This approach enables Active Protection to detect new malware by its typical behavior.

Active Protection settings

To minimize resources consumed by the heuristic analysis, and to eliminate so-called false positives, when a trusted program is considered as ransomware, you can define the following settings:

- Trusted processes that are never considered ransomware. Processes signed by Microsoft are always trusted.
- Harmful processes that are always considered ransomware. These processes will not be able to start as long as Active Protection is enabled on the machine.
- Folders where file changes will not be monitored.

Specify the full path to the process executable, starting with the drive letter. For example: **`C:\Windows\Temp\er76s7sdkh.exe`**.

For specifying folders, you can use the wildcard characters * and ?. The asterisk (*) substitutes for zero or more characters. The question mark (?) substitutes for exactly one character. Environment variables, such as %AppData%, cannot be used.

Active Protection plan

All settings of Active Protection are contained in the Active Protection plan. This plan can be applied to multiple machines.

There can be only one Active Protection plan in an organization. If the organization has units, unit administrators are not allowed to apply, edit, or revoke the plan.

Applying the Active Protection plan

1. Select the machines for which you want to enable Active Protection.
2. Click **Active Protection**.
3. [Optional] Click **Edit** to modify the following settings:
   - In **Action on detection**, select the action that the software will perform when detecting a ransomware activity, and then click **Done**. You can select one of the following:
     - **Notify only** (default)
       The software will generate an alert about the process.
     - **Stop the process**
       The software will generate an alert and stop the process.
     - **Revert using cache**
       The software will generate an alert, stop the process, and revert the file changes by using the service cache.
   - In **Harmful processes**, specify harmful processes that will always be considered ransomware, and then click **Done**.
   - In **Trusted processes**, specify trusted processes that will never be considered ransomware, and then click **Done**. Processes signed by Microsoft are always trusted.
   - In **Folder exclusions**, specify a list of folders where file changes will not be monitored, and then click **Done**.
   - Disable the **Self-protection** switch.
     Self-protection prevents unauthorized changes to the software's own processes, registry records, executable and configuration files, and backups located in local folders. We do not recommend disabling this feature.
   - Change Protection options (Section 13.1).
4. If you modified the settings, click **Save changes**. The changes will be applied to all machines where Active Protection is enabled.
5. Click **Apply**.

13.1 Protection options

Backups

This option is effective when **Self-protection** is enabled in the Active Protection plan.

This option applies to files that have extensions .tibx, .tib, .tia, and are located in local folders.

This option lets you specify the processes that are allowed to modify the backup files, even though these files are protected by self-protection. This comes in handy, for example, if you delete backup files or move them to a different location by using a script.

The preset is: **Enabled**.

If this option is enabled, the backup files can be modified only by processes signed by the backup software vendor. This allows the software to apply retention rules and to delete backups when a user requests this from the web interface. Other processes, no matter suspicious or not, cannot modify the backups.

If this option is disabled, you can allow other processes to modify the backups. Specify the full path to the process executable, starting with the drive letter.

Cryptomining protection

This option defines whether Active Protection detects potential cryptomining malware.

The preset is: **Disabled**.

If a cryptomining activity is detected, the selected **Action on detection** is performed (except reverting files from cache, as there is nothing to revert).

Cryptomining malware degrades performance of useful applications, increases electricity bills, may cause system crashes and even hardware damage due to abuse. We recommend that you add cryptomining malware to the **Harmful processes** list to prevent it from running.

Mapped drives

This option defines whether Active Protection protects network folders that are mapped as local drives.

This option applies to folders shared via SMB or NFS.

The preset is: **Enabled**.

If a file was originally located on a mapped drive, it cannot be saved to the original location when extracted from the cache by the **Revert using cache** action. Instead, it will be saved to the folder specified in this option's settings. The default folder is **C:\ProgramData\Acronis\Restored Network Files**. If this folder does not exist, it will be created. If you want to change this path, be sure to specify a local folder. Network folders, including folders on mapped drives, are not supported.

14 Special operations with virtual machines

14.1 Running a virtual machine from a backup (Instant Restore)

Note *This functionality is available only with the Acronis SCS Cyber Backup 12.5 Hardened Edition Advanced license.*

You can run a virtual machine from a disk-level backup that contains an operating system. This operation, also known as instant recovery, 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.

We recommend running this temporary virtual machine for up to three days. Then, you can completely remove it or convert it to a regular virtual machine (finalize) without downtime.

As long as the temporary virtual machine exists, retention rules cannot be applied to the backup being used by that machine. Backups of the original machine can continue to run.

Usage examples

- **Disaster recovery**

  Instantly bring a copy of a failed machine online.
- **Testing a backup**

  Run the machine from the backup and ensure that the guest OS and applications are functioning properly.
- **Accessing application data**

  While the machine is running, use application's native management tools to access and extract the required data.

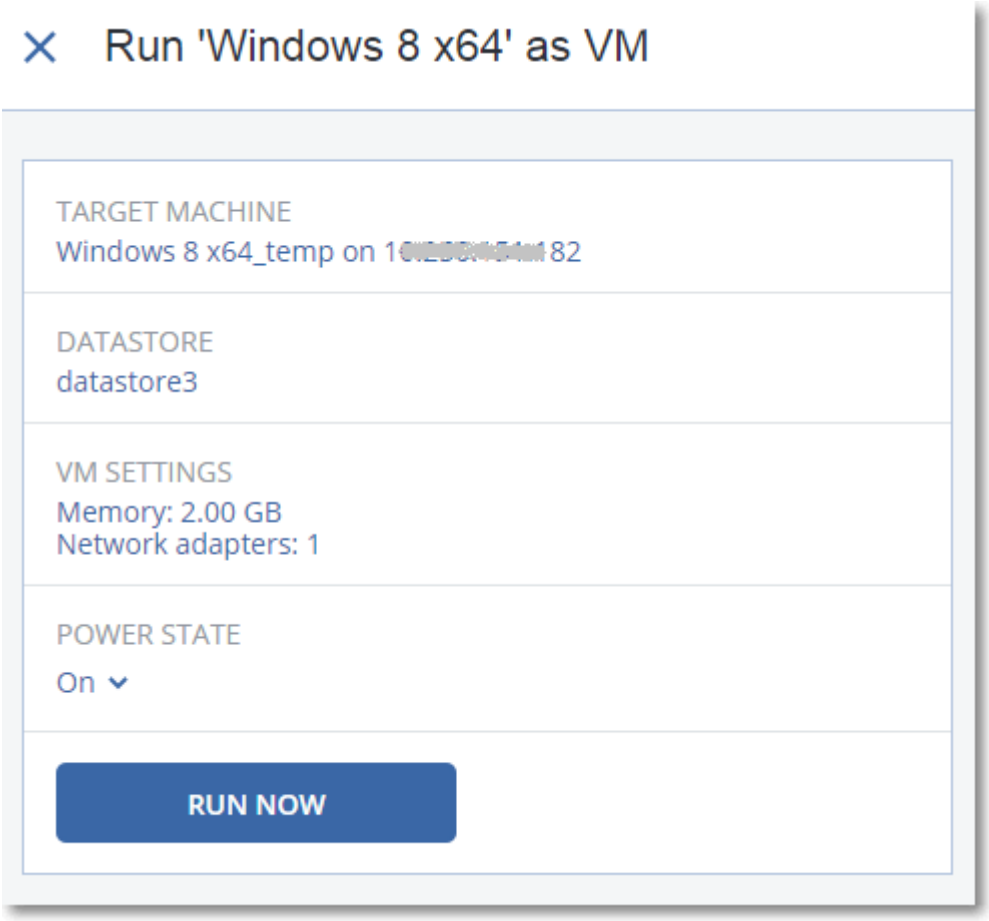
Prerequisites

- At least one Agent for VMware or Agent for Hyper-V must be registered in the backup service.
- The backup can be stored in a network folder, or in a local folder of the machine where Agent for VMware or Agent for Hyper-V is installed. If you select a network folder, it must be accessible from that machine. A virtual machine cannot be run from a backup stored on an SFTP server, a tape device, or in Secure Zone.
- The backup must contain an entire machine or all of the volumes that are required for the operating system to start.
- The backup must not contain Linux logical volumes (LVM).
- Backups of both physical and virtual machines can be used.

14.1.1 Running the machine

1. Do one of the following:
   - Select a backed-up machine, click **Recovery**, and then select a recovery point.
   - Select a recovery point on the Backups tab (Section 7.1).
2. Click **Run as VM**.

The software automatically selects the host and other required parameters.



3. [Optional] Click **Target machine**, and then change the virtual machine type (ESXi or Hyper-V), the host, or the virtual machine name.
4. [Optional] Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore for the virtual machine.
   Changes to the virtual disks accumulate while the machine is running. Ensure that the selected datastore has enough free space. If you are planning to preserve these changes by making the virtual machine permanent (Section 14.1.3), select a datastore that is suitable for running the machine in production.
5. [Optional] Click **VM settings** to change the memory size and network connections of the virtual machine.
6. [Optional] Select the VM power state (**On**/**Off**).
7. Click **Run now**.

As a result, the machine appears in the web interface with one of the following icons:  or 

. Such virtual machines cannot be selected for backup.

14.1.2 Deleting the machine

We do not recommend to delete a temporary virtual machine directly in vSphere/Hyper-V. This may lead to artifacts in the web interface. Also, the backup from which the machine was running may remain locked for a while (it cannot be deleted by retention rules).

To delete a virtual machine that is running from a backup

1. On the **All devices** tab, select a machine that is running from a backup.
2. Click **Delete**.

The machine is removed from the web interface. It is also removed from the vSphere or Hyper-V inventory and datastore (storage). All changes that occurred to the data while the machine was running are lost.

14.1.3 Finalizing the machine

While a virtual machine is running from a backup, the virtual disks' content is taken directly from that backup. Therefore, the machine will become inaccessible or even corrupted if the connection is lost to the backup location or to the backup agent.

For an ESXi machine, you have the option to make this machine permanent, i.e. recover all of its virtual disks, along with the changes that occurred while the machine was running, to the datastore that stores these changes. This process is named finalization.

Finalization is performed without downtime. The virtual machine will *not* be powered off during finalization.

To finalize a machine that is running from a backup

1. On the **All devices** tab, select a machine that is running from a backup.
2. Click **Finalize**.
3. [Optional] Specify a new name for the machine.
4. [Optional] Change the disk provisioning mode. The default setting is **Thin**.
5. Click **Finalize**.

The machine name changes immediately. The recovery progress is shown on the **Activities** tab. Once the recovery is completed, the machine icon changes to that of a regular virtual machine.

Finalization vs. regular recovery

The finalization process is slower than a regular recovery for the following reasons:

- During a finalization, the agent performs random access to different parts of the backup. When an entire machine is being recovered, the agent reads data from the backup sequentially.
- If the virtual machine is running during the finalization, the agent reads data from the backup more often, to maintain both processes simultaneously. During a regular recovery, the virtual machine is stopped.

14.2 Working in VMware vSphere

This section describes operations that are specific for VMware vSphere environments.

14.2.1 Replication of virtual machines

Replication is available only for VMware ESXi virtual machines.

Replication is the process of creating an exact copy (replica) of a virtual machine, and then maintaining the replica in sync with the original machine. By replicating a critical virtual machine, you will always have a copy of this machine in a ready-to-start state.

The replication can be started manually or on the schedule you specify. The first replication is full (copies the entire machine). All subsequent replications are incremental and are performed with Changed Block Tracking (Section 14.2.1.4), unless this option is disabled.

Replication vs. backing up

Unlike scheduled backups, a replica keeps only the latest state of the virtual machine. A replica consumes datastore space, while backups can be kept on a cheaper storage.

However, powering on a replica is much faster than a recovery and faster than running a virtual machine from a backup. When powered on, a replica works faster than a VM running from a backup and does not load the Agent for VMware.

Usage examples

- **Replicate virtual machines to a remote site.**
  Replication enables you to withstand partial or complete datacenter failures, by cloning the virtual machines from a primary site to a secondary site. The secondary site is usually located in a remote facility that is unlikely to be affected by environmental, infrastructure, or other factors that might cause the primary site failure.
- **Replicate virtual machines within a single site (from one host/datastore to another).**
  Onsite replication can be used for high availability and disaster recovery scenarios.

What you can do with a replica

- **Test a replica** (Section 14.2.1.2)
  The replica will be powered on for testing. Use vSphere Client or other tools to check if the replica works correctly. Replication is suspended while testing is in progress.
- **Failover to a replica** (Section 14.2.1.3)
  Failover is a transition of the workload from the original virtual machine to its replica. Replication is suspended while a failover is in progress.
- **Back up the replica**
  Both backup and replication require access to virtual disks, and thus impact the performance of the host where the virtual machine is running. If you want to have both a replica and backups of a virtual machine, but don't want to put additional load on the production host, replicate the machine to a different host, and set up backups of the replica.

Restrictions

The following types of virtual machines cannot be replicated:

- Fault-tolerant machines running on ESXi 5.5 and lower.
- Machines running from backups.
- Replicas of virtual machines.

14.2.1.1 Creating a replication plan

A replication plan must be created for each machine individually. It is not possible to apply an existing plan to other machines.

To create a replication plan

1. Select a virtual machine to replicate.
2. Click **Replication**.
   The software displays a new replication plan template.
3. [Optional] To modify the replication plan name, click the default name.
4. Click **Target machine**, and then do the following:
   a. Select whether to create a new replica or use an existing replica of the original machine.
   b. Select the ESXi host and specify the new replica name, or select an existing replica.
      The default name of a new replica is **[Original Machine Name]_replica**.
   c. Click **OK**.
5. [Only when replicating to a new machine] Click **Datastore**, and then select the datastore for the virtual machine.
6. [Optional] Click **Schedule** to change the replication schedule.
   By default, replication is performed on a daily basis, Monday to Friday. You can select the time to run the replication.
   If you want to change the replication frequency, move the slider, and then specify the schedule.
   You can also do the following:
   - Set a date range for when the schedule is effective. Select the **Run the plan within a date range** check box, and then specify the date range.
   - Disable the schedule. In this case, replication can be started manually.
7. [Optional] Click the gear icon to modify the replication options (Section 14.2.1.4).
8. Click **Apply**.
9. [Optional] To run the plan manually, click **Run now** on the plan panel.

As a result of running a replication plan, the virtual machine replica appears in the **All devices** list with the following icon: 

14.2.1.2 Testing a replica

To prepare a replica for testing

1. Select a replica to test.
2. Click **Test replica**.
3. Click **Start testing**.
4. Select whether to connect the powered-on replica to a network. By default, the replica will not be connected to a network.
5. [Optional] If you chose to connect the replica to the network, select the **Stop original virtual machine** check box to stop the original machine before powering on the replica.
6. Click **Start**.

To stop testing a replica

1. Select a replica for which testing is in progress.
2. Click **Test replica**.
3. Click **Stop testing**.
4. Confirm your decision.

14.2.1.3 Failing over to a replica

To failover a machine to a replica

1. Select a replica to failover to.
2. Click **Replica actions**.
3. Click **Failover**.
4. Select whether to connect the powered-on replica to a network. By default, the replica will be connected to the same network as the original machine.
5. [Optional] If you chose to connect the replica to the network, clear the **Stop original virtual machine** check box to keep the original machine online.
6. Click **Start**.

While the replica is in a failover state, you can choose one of the following actions:

- **Stop failover** (Section 14.2.1.3)
  Stop failover if the original machine was fixed. The replica will be powered off. Replication will be resumed.
- **Perform permanent failover to the replica** (Section 12.2.1.3)
  This instant operation removes the 'replica' flag from the virtual machine, so that replication to it is no longer possible. If you want to resume replication, edit the replication plan to select this machine as a source.
- **Failback** (Section 12.2.1.3)
  Perform failback if you failed over to the site that is not intended for continuous operations. The replica will be recovered to the original or a new virtual machine. Once the recovery to the original machine is complete, it is powered on and replication is resumed. If you choose to recover to a new machine, edit the replication plan to select this machine as a source.

Stopping failover

To stop a failover

1. Select a replica that is in the failover state.
2. Click **Replica actions**.
3. Click **Stop failover**.
4. Confirm your decision.

Performing a permanent failover

To perform a permanent failover

1. Select a replica that is in the failover state.
2. Click **Replica actions**.
3. Click **Permanent failover**.
4. [Optional] Change the name of the virtual machine.
5. [Optional] Select the **Stop original virtual machine** check box.
6. Click **Start**.

Failing back

To failback from a replica

1. Select a replica that is in the failover state.

2. Click **Replica actions**.
3. Click **Failback from replica**.
   The software automatically selects the original machine as the target machine.
4. [Optional] Click **Target machine**, and then do the following:
   a. Select whether to failback to a new or existing machine.
   b. Select the ESXi host and specify the new machine name, or select an existing machine.
   c. Click **OK**.
5. [Optional] When failing back to a new machine, you can also do the following:
   - Click **Datastore** to select the datastore for the virtual machine.
   - Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.
6. [Optional] Click **Recovery options** to modify the failback options (Section 14.2.1.5).
7. Click **Start recovery**.
8. Confirm your decision.

14.2.1.4 Replication options

To modify the replication options, click the gear icon next to the replication plan name, and then click **Replication options**.

Changed Block Tracking (CBT)

This option is similar to the backup option "Changed Block Tracking (CBT)" (Section 5.10.7).

Disk provisioning

This option defines the disk provisioning settings for the replica.

The preset is: **Thin provisioning**.

The following values are available: **Thin provisioning**, **Thick provisioning**, **Keep the original setting**.

Error handling

This option is similar to the backup option "Error handling" (Section 5.10.11).

Pre/Post commands

This option is similar to the backup option "Pre/Post commands" (Section 5.10.20).

Volume Shadow Copy Service VSS for virtual machines

This option is similar to the backup option "Volume Shadow Copy Service VSS for virtual machines" (Section 5.10.29).

14.2.1.5 Failback options

To modify the failback options, click **Recovery options** when configuring failback.

Error handling

This option is similar to the recovery option "Error handling" (Section 6.6.4).

Performance

This option is similar to the recovery option "Performance" (Section 6.6.9).

Pre/Post commands

This option is similar to the recovery option "Pre/Post commands" (Section 6.6.10).

VM power management

This option is similar to the recovery option "VM power management" (Section 6.6.12).

14.2.1.6 Seeding an initial replica

To speed up replication to a remote location and save network bandwidth, you can perform replica seeding.

Important *To perform replica seeding, Agent for VMware (Virtual Appliance) must be running on the target ESXi.*

To seed an initial replica

1. Do one of the following:
   - If the original virtual machine can be powered off, power it off, and then skip to step 4.
   - If the original virtual machine cannot be powered off, continue to the next step.
2. Create a replication plan (Section 14.2.1.1).
   When creating the plan, in **Target machine**, select **New replica** and the ESXi that hosts the original machine.
3. Run the plan once.
   A replica is created on the original ESXi.
4. Export the virtual machine (or the replica) files to an external hard drive.
   a. Connect the external hard drive to the machine where vSphere Client is running.
   b. Connect vSphere Client to the original vCenter\ESXi.
   c. Select the newly created replica in the inventory.
   d. Click **File** > **Export** > **Export OVF template**.
   e. In **Directory**, specify the folder on the external hard drive.
   f. Click **OK**.
5. Transfer the hard drive to the remote location.
6. Import the replica to the target ESXi.
   a. Connect the external hard drive to the machine where vSphere Client is running.
   b. Connect vSphere Client to the target vCenter\ESXi.
   c. Click **File** > **Deploy OVF template**.
   d. In **Deploy from a file or URL**, specify the template that you exported in step 4.
   e. Complete the import procedure.
7. Edit the replication plan that you created in step 2. In **Target machine**, select **Existing replica**, and then select the imported replica.

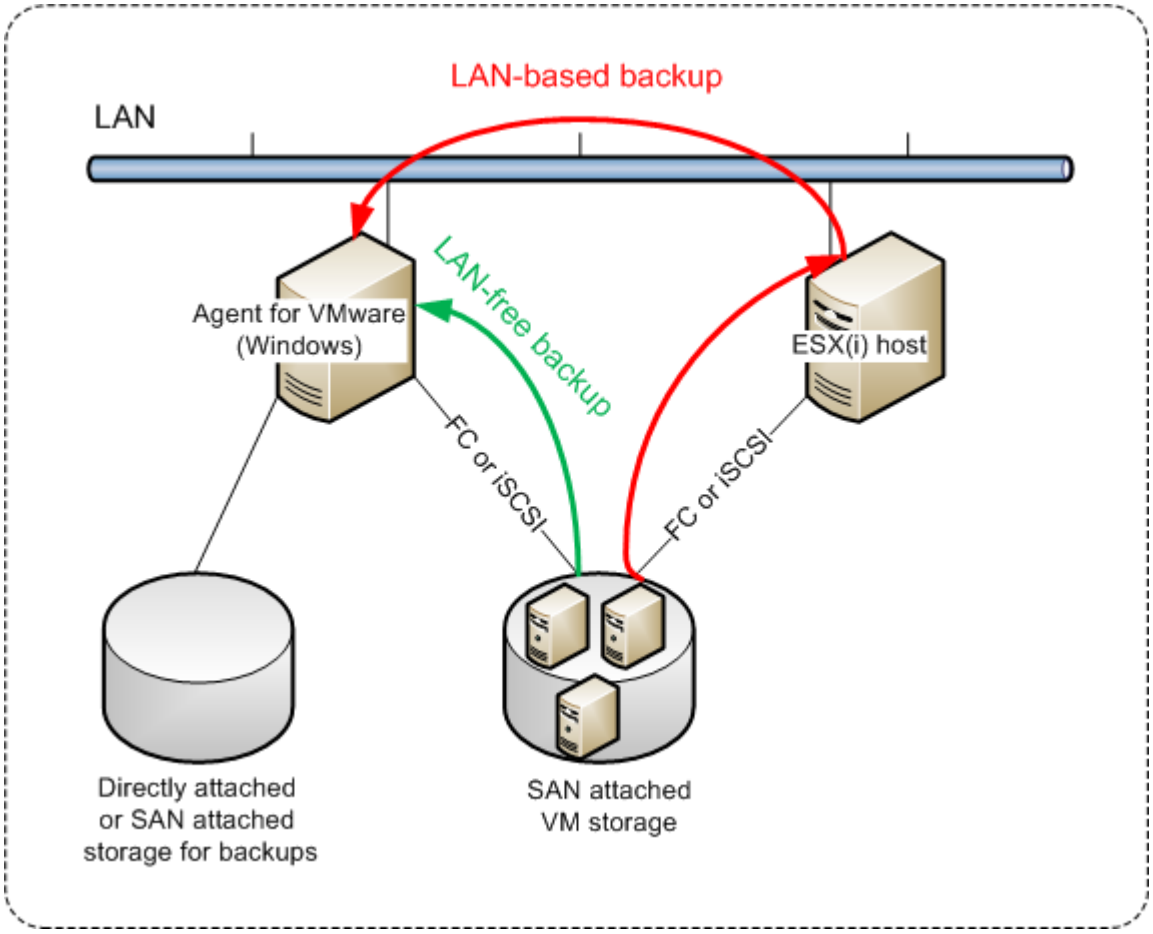
As a result, the software will continue updating the replica. All replications will be incremental.

14.2.2 LAN-free backup

If your production ESXi hosts are so heavily loaded that running the virtual appliances is not desirable, consider installing Agent for VMware (Windows) on a physical machine outside the ESXi infrastructure.

If your ESXi uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESXi host and LAN. This capability is called a LAN-free backup.

The diagram below illustrates a LAN-based and a LAN-free backup. LAN-free access to virtual machines is available if you have a fibre channel (FC) or iSCSI Storage Area Network. To completely eliminate transferring the backed-up data via LAN, store the backups on a local disk of the agent's machine or on a SAN attached storage.



To enable the agent to access a datastore directly

1. Install Agent for VMware on a Windows machine that has network access to the vCenter Server.
2. Connect the logical unit number (LUN) that hosts the datastore to the machine. Consider the following:
   - Use the same protocol (i.e. iSCSI or FC) that is used for the datastore connection to the ESXi.
   - The LUN *must not* be initialized and must appear as an "offline" disk in **Disk Management**. If Windows initializes the LUN, it may become corrupted and unreadable by VMware vSphere.

     To avoid LUN initialization, the **SAN Policy** is automatically set to **Offline All** during the Agent for VMware (Windows) installation.

As a result, the agent will use the SAN transport mode to access the virtual disks, i.e. it will read raw LUN sectors over iSCSI/FC without recognizing the VMFS file system (which Windows is not aware of).

Limitations

- In vSphere 6.0 and later, the agent cannot use the SAN transport mode if some of the VM disks are located on a VMware Virtual Volume (VVol) and some are not. Backups of such virtual machines will fail.
- Encrypted virtual machines, introduced in VMware vSphere 6.5, will be backed up via LAN, even if you configure the SAN transport mode for the agent. The agent will fall back on the NBD transport because VMware does not support SAN transport for backing up encrypted virtual disks.

Example

If you are using an iSCSI SAN, configure the iSCSI initiator on the machine running Windows where Agent for VMware is installed.

To configure the SAN policy

1. Log on as an administrator, open the command prompt, type **`diskpart`**, and then press **Enter**.
2. Type **`san`**, and then press **Enter**. Ensure that **SAN Policy : Offline All** is displayed.
3. If another value for SAN Policy is set:
   a. Type **`san policy=offlineall`**.
   b. Press **Enter**.
   c. To check that the setting has been applied correctly, perform step 2.
   d. Restart the machine.

To configure an iSCSI initiator

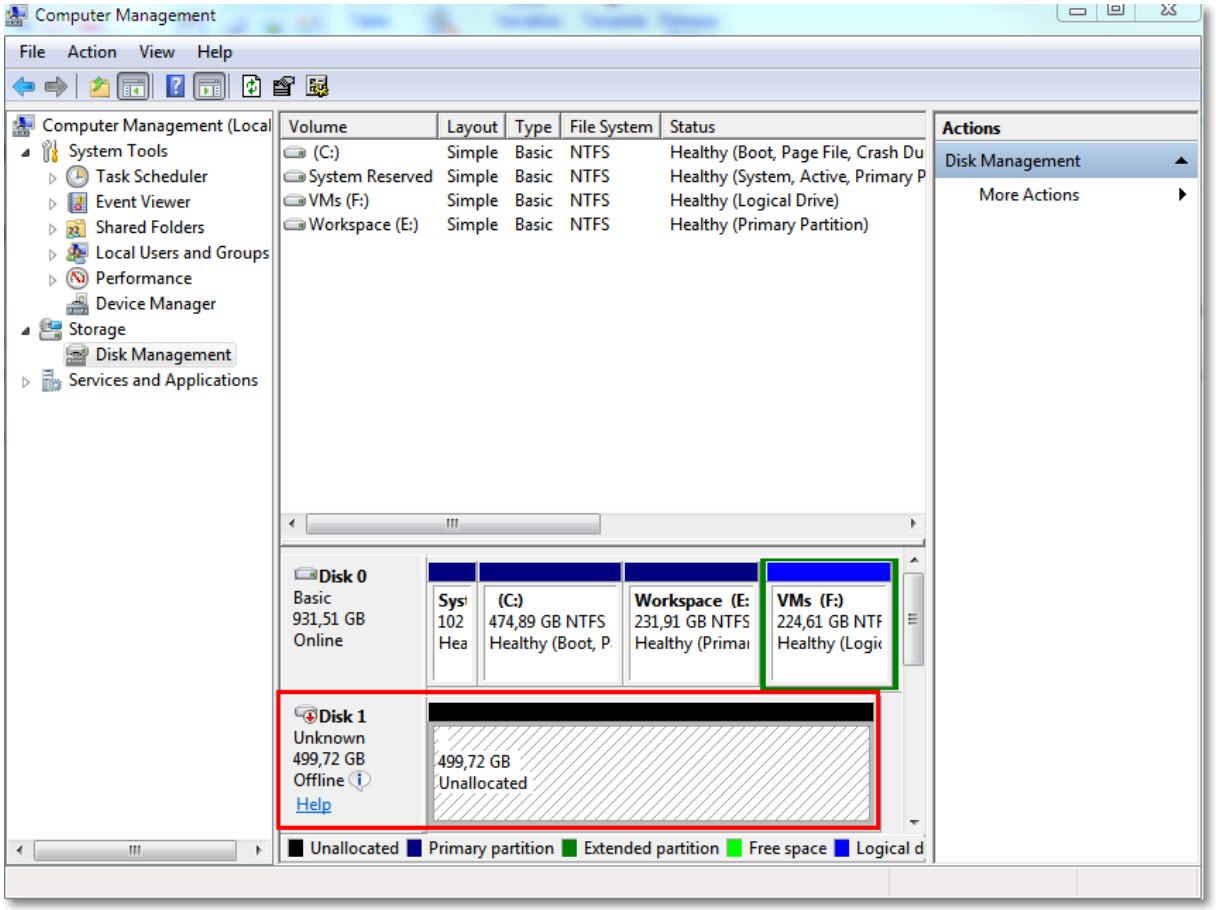
1. Go to **Control Panel** > **Administrative Tools** > **iSCSI Initiator**.

   Tip. *To find the **Administrative Tools** applet, you may need to change the **Control Panel** view to something other than **Home** or **Category**, or use search.*

2. If this is the first time that Microsoft iSCSI Initiator is launched, confirm that you want to start the Microsoft iSCSI Initiator service.
3. On the **Targets** tab, type the fully qualified domain name (FQDN) name or the IP address of the target SAN device, and then click **Quick Connect**.
4. Select the LUN that hosts the datastore, and then click **Connect**.

   If the LUN is not displayed, ensure that the zoning on the iSCSI target enables the machine running the agent to access the LUN. The machine must be added to the list of allowed iSCSI initiators on this target.
5. Click **OK**.

The ready SAN LUN should appear in **Disk Management** as shown in the screenshot below.



14.2.3 Using SAN hardware snapshots

If your VMware vSphere uses a storage area network (SAN) storage system as a datastore, you can enable Agent for VMware (Windows) to use SAN hardware snapshots when performing a backup.

Important *Only NetApp SAN storage is supported.*

Why use SAN hardware snapshots?

Agent for VMware needs a virtual machine snapshot in order to create a consistent backup. Because the agent reads the virtual disk content from the snapshot, the snapshot must be kept for the whole duration of the backup process.

By default, the agent uses native VMware snapshots created by the ESXi host. While the snapshot is kept, the virtual disk files are in the read-only state, and the host writes all changes done to the disks to separate delta files. Once the backup process is finished, the host deletes the snapshot, i.e. merges the delta files with the virtual disk files.

Both maintaining and deleting the snapshot affect the virtual machine performance. With large virtual disks and fast data changes, these operations take a long time during which the performance can degrade. In extreme cases, when several machines are backed up simultaneously, the growing delta files may nearly fill the datastore and cause all of the virtual machines to power off.

You can reduce the hypervisor resource utilization by offloading the snapshots to the SAN. In this case, the sequence of operations is as follows:

1. The ESXi takes a VMware snapshot in the beginning of the backup process, to bring the virtual disks to a consistent state.
2. The SAN creates a hardware snapshot of the volume or LUN that contains the virtual machine and its VMware snapshot. This operation typically takes a few seconds.
3. The ESXi deletes the VMware snapshot. Agent for VMware reads the virtual disk content from the SAN hardware snapshot.

Because the VMware snapshot is maintained only for a few seconds, the virtual machine performance degradation is minimized.

What do I need to use the SAN hardware snapshots?

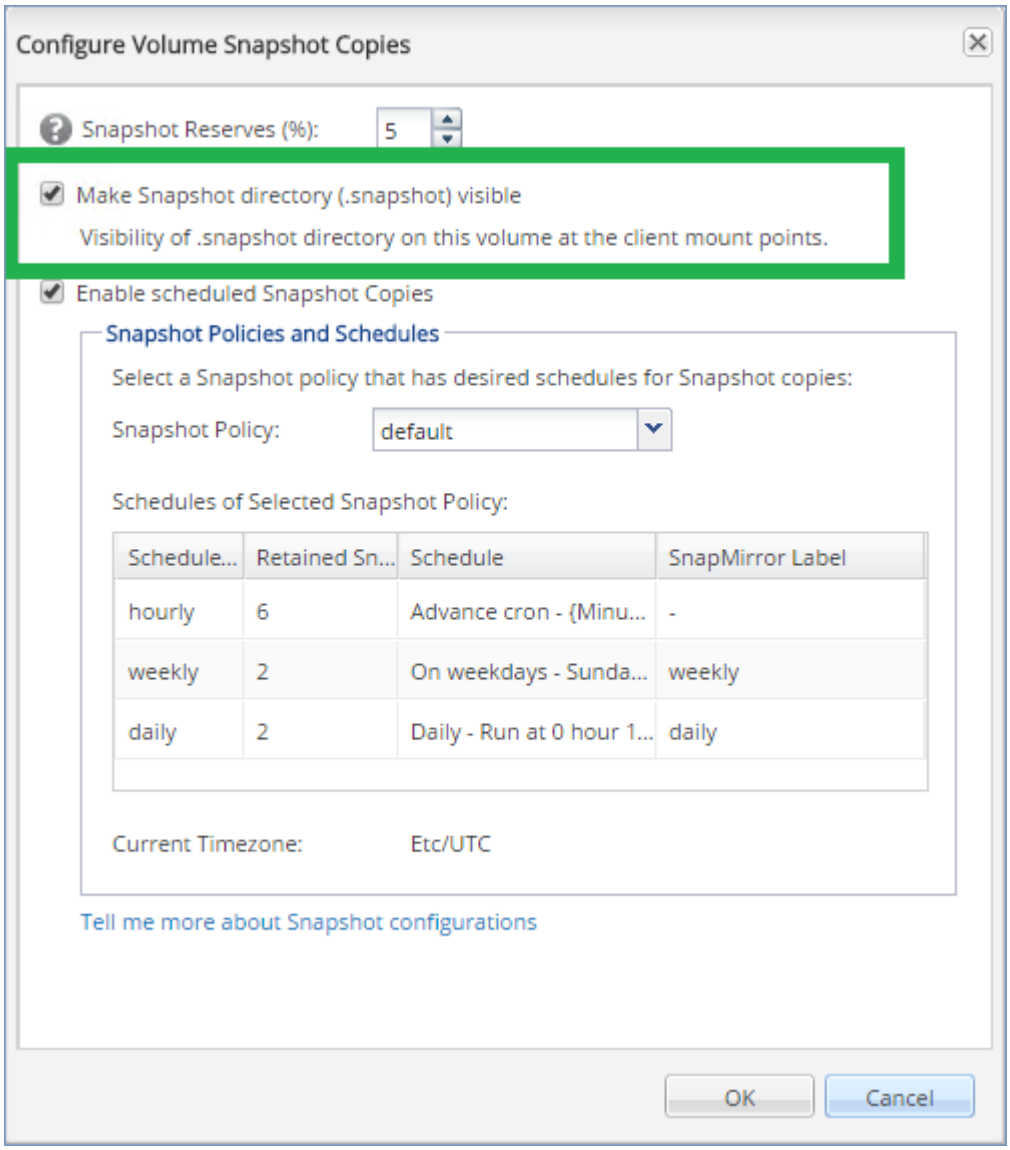
If you want to use the SAN hardware snapshots when backing up virtual machines, ensure that all of the following is true:

- The NetApp SAN storage meets the requirements described in "NetApp SAN storage requirements" (Section 14.2.3.1).
- The machine running Agent for VMware (Windows) is configured as described in "Configuring the machine running Agent for VMware" (Section 14.2.3.2).
- The SAN storage is registered on the management server (Section 13.2.3.3).
- [If there are Agents for VMware that did not take part in the above registration] The virtual machines that reside on the SAN storage are assigned to the SAN-enabled agents, as described in "Virtual machine binding" (Section 14.2.5).
- The "SAN hardware snapshots" (Section 5.10.22) backup option is enabled in the backup plan options.

14.2.3.1 NetApp SAN storage requirements

- The SAN storage must be used as an NFS or iSCSI datastore.
- The SAN must run Data ONTAP 8.1 or later in the **Clustered Data ONTAP (cDOT)** mode. The **7-mode** mode is not supported.

- In the NetApp OnCommand System Manager, the **Snapshot copies** > **Configure** > **Make Snapshot directory (.snapshot) visible** check box must be selected for the volume where the datastore is located.

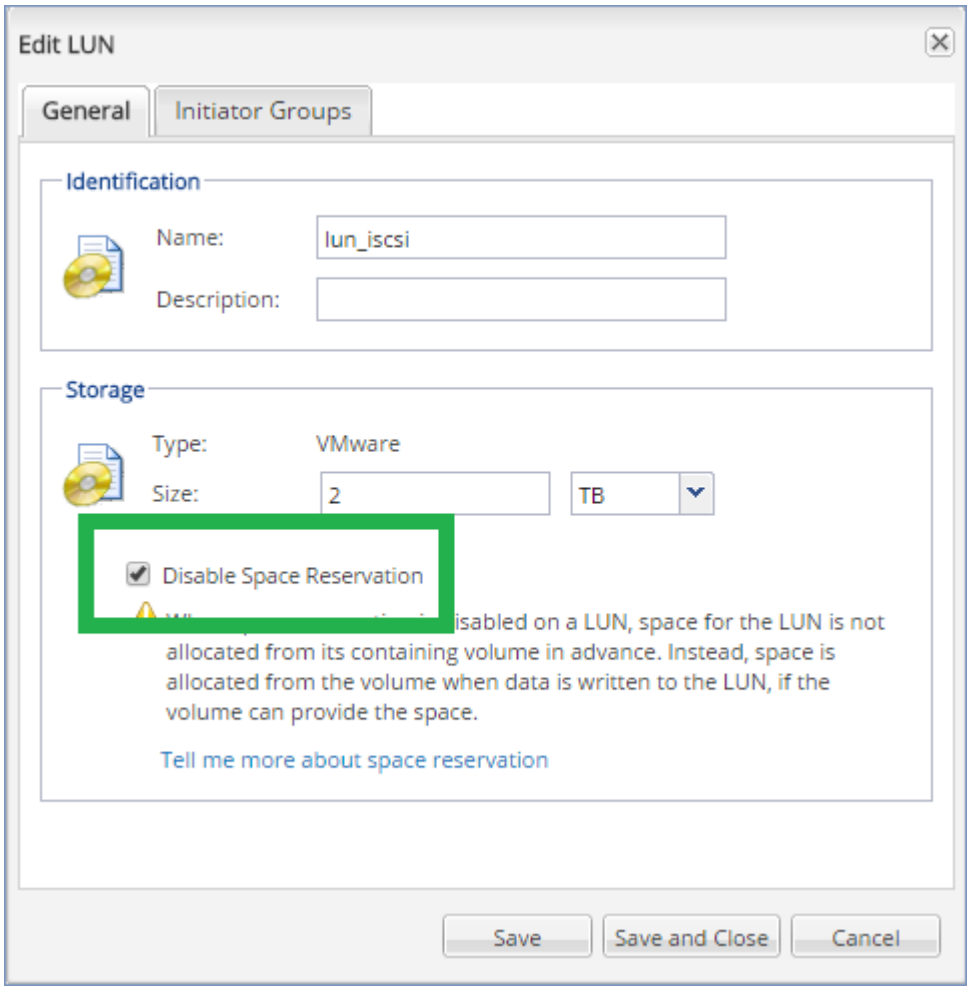


- [For NFS datastores] Access to NFS shares from Windows NFSv3 clients must be enabled on the Storage Virtual Machine (SVM) that was specified when creating the datastore. The access can be enabled by the following command:

```
vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
```

For more information, refer to the NetApp Best Practices document: https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices

- [For iSCSI datastores] In the NetApp OnCommand System Manager, the **Disable Space Reservation** check box must be selected for the iSCSI LUN where the datastore is located.



14.2.3.2 Configuring the machine running Agent for VMware

Depending on whether the SAN storage is used as an NFS or iSCSI datastore, refer to the corresponding section below.

Configuring iSCSI Initiator

Ensure that all of the following is true:

- Microsoft iSCSI Initiator is installed.
- The Microsoft iSCSI Initiator Service startup type is set to **Automatic** or **Manual**. This can be done in the **Services** snap-in.
- The iSCSI initiator is configured as described in the example section of "LAN-free backup" (Section 14.2.2).

Configuring NFS Client

Ensure that all of the following is true:

- Microsoft **Services for NFS** (in Windows Server 2008) or **Client for NFS** (in Windows Server 2012 and later) is installed.
- The NFS client is configured for anonymous access. This can be done as follows:

  a. Open Registry Editor.

b. Locate the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default

c. In this key, create a new **DWORD** value named **AnonymousUID** and set its value data to 0.

d. In the same key, create a new **DWORD** value named **AnonymousGID** and set its value data to 0.

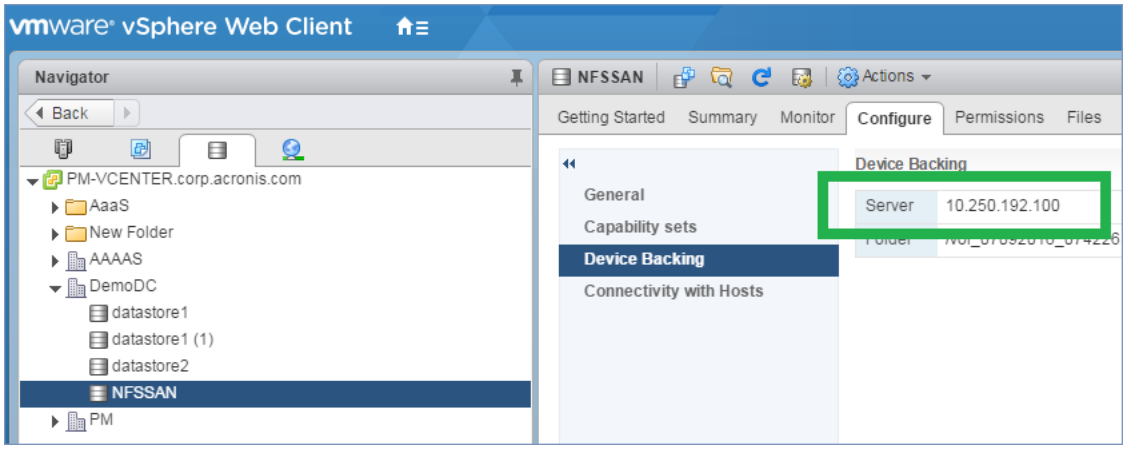
e. Restart the machine.

14.2.3.3 Registering SAN storage on the management server

1. Click **Settings** > **SAN storage**.
2. Click **Add storage**.
3. [Optional] In **Name**, change the storage name.

   This name will be displayed on the **SAN storage** tab.
4. In **Host name or IP address**, specify the NetApp Storage Virtual Machine (SVM, also known as a filer) that was specified when creating the datastore.

   To find the required information in VMware vSphere Web Client, select the datastore, and then click **Configure** > **Device backing**. The host name or IP address is displayed in the **Server** field.



5. In **User name** and **Password**, specify the SVM administrator credentials.

   Important *The specified account must be a local administrator on the SVM, rather than entire NetApp system management administrator.*

   You can specify an existing user or create a new one. To create a new user, in the NetApp OnCommand System Manager, navigate to **Configuration** > **Security** > **Users**, and then create a new user.
6. Select one or more Agent for VMware (Windows) which will be given the read permission for the SAN device.
7. Click **Add**.

14.2.4 Using a locally attached storage

You can attach an additional disk to Agent for VMware (Virtual Appliance) so the agent can back up to this locally attached storage. This approach eliminates the network traffic between the agent and the backup location.

A virtual appliance that is running on the same host or cluster with the backed-up virtual machines has direct access to the datastore(s) where the machines reside. This means the appliance can attach the backed-up disks by using the HotAdd transport, and therefore the backup traffic is directed from one local disk to another. If the datastore is connected as **Disk/LUN** rather than **NFS**, the backup will

be completely LAN-free. In the case of NFS datastore, there will be network traffic between the datastore and the host.

Using a locally attached storage presumes that the agent always backs up the same machines. If multiple agents work within the vSphere, and one or more of them use locally attached storages, you need to manually bind (Section 14.2.5) each agent to all machines it has to back up. Otherwise, if the machines are redistributed among the agents by the management server, a machine's backups may be dispersed over multiple storages.

You can add the storage to an already working agent or when deploying the agent from an OVF template (Section 1.10.3).

To attach a storage to an already working agent

1. In VMware vSphere inventory, right click the Agent for VMware (Virtual Appliance).
2. Add the disk by editing the settings of the virtual machine. The disk size must be at least 10 GB.

   Warning *Be careful when adding an already existing disk. Once the storage is created, all data previously contained on this disk will be lost.*
3. Go to the virtual appliance console. The **Create storage** link is available at the bottom of the screen. If it is not, click **Refresh**.
4. Click the **Create storage** link, select the disk and specify a label for it. The label length is limited to 16 characters, due to file system restrictions.

To select a locally attached storage as a backup destination

When creating a backup plan (Section 5), in **Where to back up**, select **Local folders**, and then type the letter corresponding to the locally attached storage, for example, **D:**.

14.2.5 Virtual machine binding

This section gives you an overview of how the management server organizes the operation of multiple agents within VMware vCenter.

The below distribution algorithm works for both virtual appliances and agents installed in Windows.

Distribution algorithm

The virtual machines are automatically evenly distributed between Agents for VMware. By evenly, we mean that each agent manages an equal number of machines. The amount of storage space occupied by a virtual machine is not counted.

However, when choosing an agent for a machine, the software tries to optimize the overall system performance. In particular, the software considers the agent and the virtual machine location. An agent hosted on the same host is preferred. If there is no agent on the same host, an agent from the same cluster is preferred.

Once a virtual machine is assigned to an agent, all backups of this machine are delegated to this agent.

Redistribution

Redistribution takes place each time the established balance breaks, or, more precisely, when a load imbalance among the agents reaches 20 percent. This may happen when a machine or an agent is added or removed, or a machine migrates to a different host or cluster, or if you manually bind a machine to an agent. If this happens, the management server redistributes the machines using the same algorithm.

For example, you realize that you need more agents to help with throughput and deploy an additional virtual appliance to the cluster. The management server will assign the most appropriate machines to the new agent. The old agents' load will reduce.

When you remove an agent from the management server, the machines assigned to the agent are distributed among the remaining agents. However, this will not happen if an agent gets corrupted or is deleted from manually from vSphere. Redistribution will start only after you remove such agent from the web interface.

Viewing the distribution result

You can view the result of the automatic distribution:

- in the **Agent** column for each virtual machine on the **All devices** section
- in the **Assigned virtual machines** section of the **Details** panel when an agent is selected in the **Settings** > **Agents** section

Manual binding

The Agent for VMware binding lets you exclude a virtual machine from this distribution process by specifying the agent that must always back up this machine. The overall balance will be maintained, but this particular machine can be passed to a different agent only if the original agent is removed.

To bind a machine with an agent

1. Select the machine.
2. Click **Details**.

   In the **Assigned agent** section, the software shows the agent that currently manages the selected machine.
3. Click **Change**.
4. Select **Manual**.
5. Select the agent to which you want to bind the machine.
6. Click **Save**.

To unbind a machine from an agent

1. Select the machine.
2. Click **Details**.

   In the **Assigned agent** section, the software shows the agent that currently manages the selected machine.
3. Click **Change**.
4. Select **Automatic**.
5. Click **Save**.

Disabling automatic assignment for an agent

You can disable the automatic assignment for Agent for VMware to exclude it from the distribution process by specifying the list of machines that this agent must back up. The overall balance will be maintained between other agents.

Automatic assignment cannot be disabled for an agent if there are no other registered agents, or if automatic assignment is disabled for all other agents.

To disable automatic assignment for an agent

1. Click **Settings** > **Agents**.
2. Select Agent for VMware for which you want to disable the automatic assignment.
3. Click **Details**.
4. Disable the **Automatic assignment** switch.

Usage examples

- Manual binding comes in handy if you want a particular (very large) machine to be backed up by Agent for VMware (Windows) via a fibre channel while other machines are backed up by virtual appliances.
- Manual binding is necessary if you are using SAN hardware snapshots (Section 14.2.3). Bind Agent for VMware (Windows) for which SAN hardware snapshots are configured with the machines that reside on the SAN datastore.
- It is necessary to bind VMs to an agent if the agent has a locally attached storage. (Section 14.2.4)
- Disabling the automatic assignment enables you to ensure that a particular machine is predictably backed up on the schedule you specify. The agent that only backs up one VM cannot be busy backing up other VMs when the scheduled time comes.
- Disabling the automatic assignment is useful if you have multiple ESXi hosts that are separated geographically. If you disable the automatic assignment, and then bind the VMs on each host to the agent running on the same host, you can ensure that the agent will never back up any machines running on the remote ESXi hosts, thus saving network traffic.

14.3 Machine migration

You can perform machine migration by recovering its backup to a non-orignal machine.

The following table summarizes the available migration options.

Backed-up machine type	Available recovery destinations		
	Physical machine	ESXi virtual machine	Hyper-V virtual machine
Physical machine	+	+	+
VMware ESXi virtual machine	+	+	+
Hyper-V virtual machine	+	+	+

For instructions on how to perform migration, refer to the following sections:

- Physical-to-virtual (P2V) - "Physical machine to virtual" (Section 6.3.1)
- Virtual-to-virtual (V2V) - "Virtual machine" (Section 6.3.3)
- Virtual-to-physical (V2P) - "Virtual machine" (Section 6.3.3) or "Recovering disks by using bootable media" (Section 6.3.4)

Although it is possible to perform V2P migration in the web interface, we recommend using bootable media in specific cases. Sometimes, you may want to use the media for migration to ESXi or Hyper-V.

The media enables you to do the following:

- Perform P2V and V2P migration of a Linux machine containing logical volumes (LVM). Use Agent for Linux or bootable media to create the backup and bootable media to recover.
- Provide drivers for specific hardware that is critical for the system bootability.

14.4 Limiting the total number of simultaneously backed-up virtual machine

The **Scheduling** (Section 5.10.23) backup option defines how many virtual machines an agent can back up simultaneously when executing the given backup plan.

When multiple backup plans overlap in time, the numbers specified in their backup options are added up. Even though the resulting total number is programmatically limited to 10, overlapping plans can affect the backup performance and overload both the host and the virtual machine storage.

You can further reduce the total number of virtual machines that an Agent for VMware or Agent for Hyper-V can back up simultaneously.

To limit the total number of virtual machines that Agent for VMware (Windows) or Agent for Hyper-V can back up

1. On the machine running the agent, create a new text document and open it in a text editor, such as Notepad.
2. Copy and paste the following lines into the file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Replace `00000001` with the hexadecimal value of the limit that you want to set. For example, `00000001` is 1 and `0000000A` is 10.
4. Save the document as **limit.reg**.
5. Run the file as an administrator.
6. Confirm that you want to edit the Windows registry.
7. Do the following to restart the agent:
   a. In the **Start** menu, click **Run**, and then type: **cmd**
   b. Click **OK**.
   c. Run the following commands:

```
net stop mms
net start mms
```

To limit the total number of virtual machines that Agent for VMware (Virtual Appliance) can back up

1. To start the command shell, press CTRL+SHIFT+F2 while in the virtual appliance UI.
2. Open the file **/etc/Acronis/MMS.config** in a text editor, such as **vi**.
3. Locate the following section:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Replace `10` with the decimal value of the limit that you want to set.
5. Save the file.
6. Execute the **`reboot`** command to restart the agent.

14.5 Managing virtualization environments

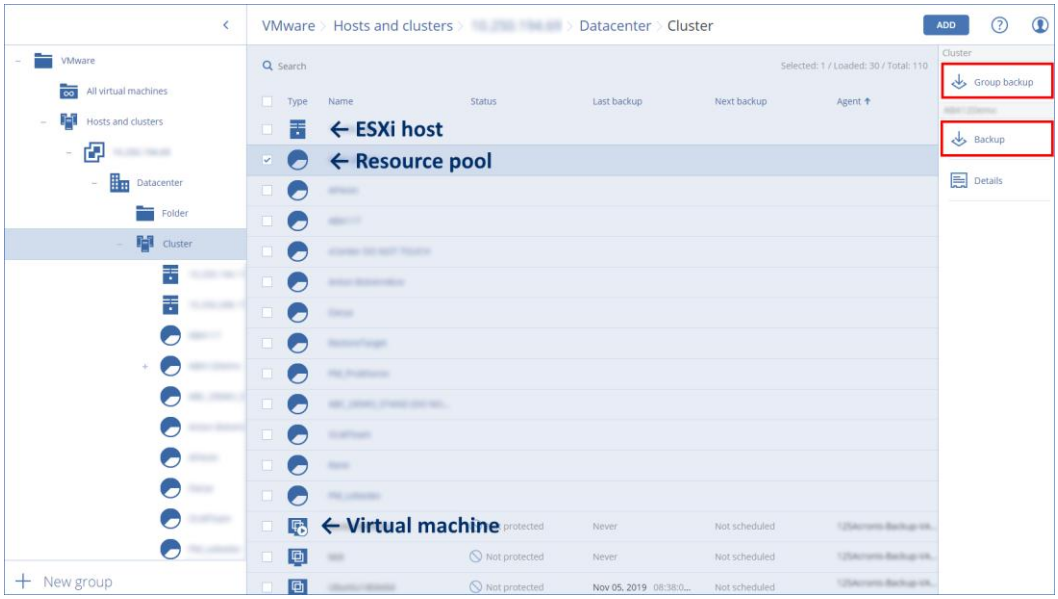
You can view the vSphere or Hyper-V in their native presentation. Once the corresponding agent is installed and registered, the **VMware** or **Hyper-V** tab appears under Devices.

In the **VMware** tab, you can back up the following vSphere infrastructure objects:

- Data center
- Folder
- Cluster
- ESXi host
- Resource pool

Each of these infrastructure objects work as a group object for virtual machines. When you apply a protection plan to any of these group objects, all virtual machines included in it, will be backed up. You can back up either the selected group machine by clicking **Protect**, or the parent group machines in which the selected group is included by clicking **Protect group**.

For example, you have selected the San Stefano cluster and then selected the resource pool inside it. If you click **Protect**, all virtual machines included in the selected resource pool will be backed up. If you click **Protect group**, all virtual machines included in the San Stefano cluster will be backed up.



You can change access credentials for the vCenter Server or stand-alone ESXi host without re-installing the agent.

To change the vCenter Server or ESXi host access credentials

1. Under **Devices**, click **VMware**.
2. Click **Hosts and Clusters**.
3. In the **Hosts and Clusters** list (to the right of the **Hosts and Clusters** tree), select the vCenter Server or stand-alone ESXi host that was specified during the Agent for VMware installation.
4. Click **Details**.
5. Under **Credentials**, click the user name.
6. Specify the new access credentials, and then click **OK**.

14.5.1 Agent for VMware - necessary privileges

This section describes the privileges required for operations with ESXi virtual machines and, additionally, for virtual appliance deployment.

To perform operations on all hosts and clusters managed by a vCenter Server, Agent for VMware needs the privileges on the vCenter Server. If you want the agent to operate on a specific ESXi host only, provide the agent with the same privileges on the host.

Specify the account with the necessary privileges during Agent for VMware installation or configuration. If you need to change the account at a later time, refer to the "Changing the vSphere access credentials" (Section 14.2.5) section.

		Operation				
Object	**Privilege**	**Back up a VM**	**Recover to a new VM**	**Recover to an existing VM**	**Run VM from backup**	**VA deployment**
Cryptographic operations (starting with vSphere 6.5)	**Add disk**	+*				
	Direct Access	+*				
Datastore	**Allocate space**		+	+	+	+
	Browse datastore				+	+
	Configure datastore	+	+	+	+	+
	Low level file operations				+	+
Global	**Licenses**	+	+	+	+	
	Disable methods	+	+	+		
	Enable methods	+	+	+		
Host > **Configuration**	**VM autostart configuration**					+
	Storage partition configuration				+	
Host > **Inventory**	**Modify cluster**					+
Host > **Local operations**	**Create VM**				+	+
	Delete VM				+	+
	Reconfigure VM				+	+
Network	**Assign network**		+	+	+	+
Resource	**Assign VM to resource pool**		+	+	+	+
vApp	**Add virtual machine**				+	
	Import					+
Virtual machine > **Configuration**	**Add existing disk**	+	+		+	
	Add new disk		+	+	+	+
	Add or remove device		+		+	+
	Advanced	+	+	+		+
	Change CPU count		+			

		Operation				
Object	**Privilege**	**Back up a VM**	**Recover to a new VM**	**Recover to an existing VM**	**Run VM from backup**	**VA deployment**
	Disk change tracking	+		+		
	Disk lease	+		+		
	Memory		+			
	Remove disk	+	+	+	+	
	Rename		+			
	Set annotation				+	
	Settings		+	+	+	
Virtual machine > **Guest Operations**	**Guest Operation Program Execution**	+**				+
	Guest Operation Queries	+**				+
	Guest Operation Modifications	+**				
Virtual machine > **Interaction**	**Acquire guest control ticket** (in vSphere 4.1 and 5.0)				+	+
	Configure CD media		+	+		
	Console interaction					+
	Guest operating system management by VIX API (in vSphere 5.1 and later)				+	+
	Power off			+	+	+
	Power on		+	+	+	+
Virtual machine > **Inventory**	**Create from existing**		+	+	+	
	Create new		+	+	+	+
	Move					+
	Register				+	
	Remove		+	+	+	+
	Unregister				+	
Virtual machine > **Provisioning**	**Allow disk access**		+	+	+	
	Allow read-only disk access	+		+		
	Allow virtual machine download	+	+	+	+	

		Operation				
Object	**Privilege**	**Back up a VM**	**Recover to a new VM**	**Recover to an existing VM**	**Run VM from backup**	**VA deployment**
Virtual machine > **State**	**Create snapshot**	+		+	+	+
	Remove snapshot	+		+	+	+

* This privilege is required for backing up encrypted machines only.

** This privilege is required for application-aware backups only.

15 Monitoring and reporting

The **Dashboard** section enables you to monitor the current state of your backup infrastructure. The **Reports** section enables you to generate on-demand and scheduled reports about the backup infrastructure. The **Reports** section is available only with an Advanced license.

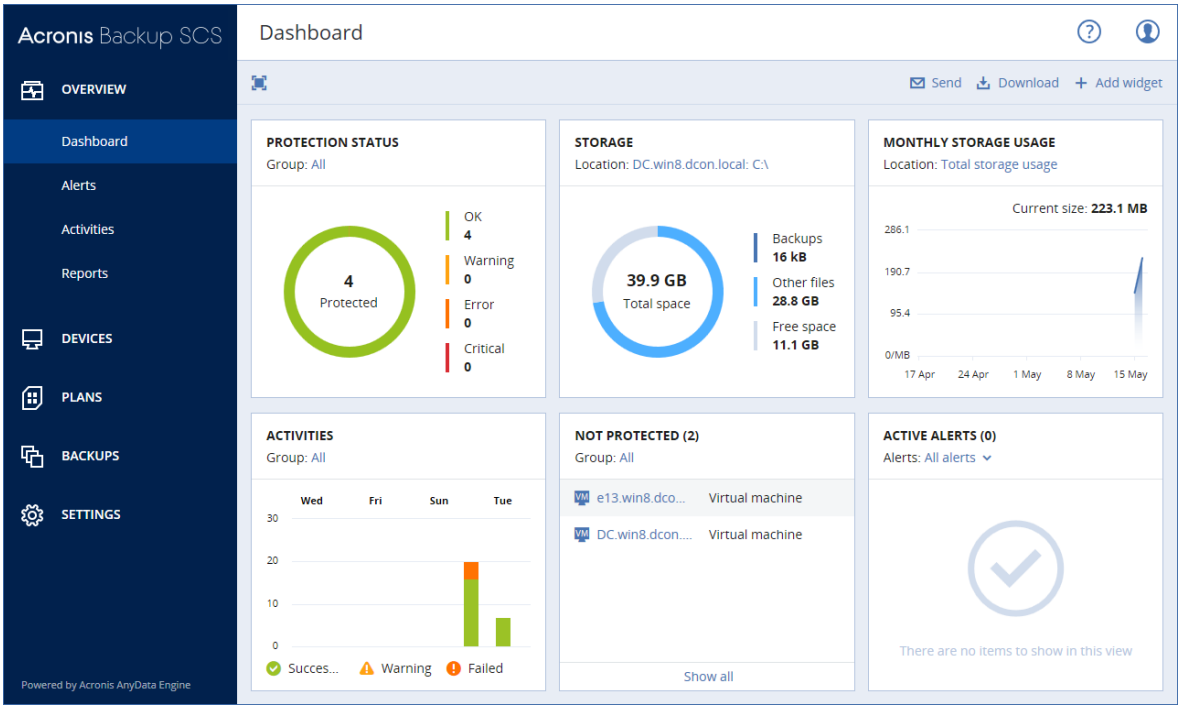
The **Dashboard** and **Reports** sections appear under the **Overview** tab only if the **Monitoring Service** component was installed with the management server (it is installed by default).

15.1 Dashboard

The **Dashboard** provides a number of customizable widgets that give an overview of your backup infrastructure. The widgets are updated in real time. You can choose from more than 20 widgets, presented as pie charts, tables, graphs, bar charts, and lists.

The following widgets are displayed by default:

- **Protection status**. Shows protection statuses for the selected device group.
- **Storage**. Shows total, free, and occupied space for the selected backup location.
- **Monthly storage usage**. Shows the monthly space usage trend for the selected backup location.
- **Activities**. Shows results of activities for the last seven days.
- **Not protected**. Shows devices without backup plans.
- **Active alerts**. Shows the five most recent active alerts.



Widgets have clickable elements that enable you to investigate and troubleshoot issues.

You can download the current state of the dashboard in the .pdf or .xlsx format, or send it via email. To send the dashboard via email, ensure that the **Email server** (Section 18.2) settings are configured.

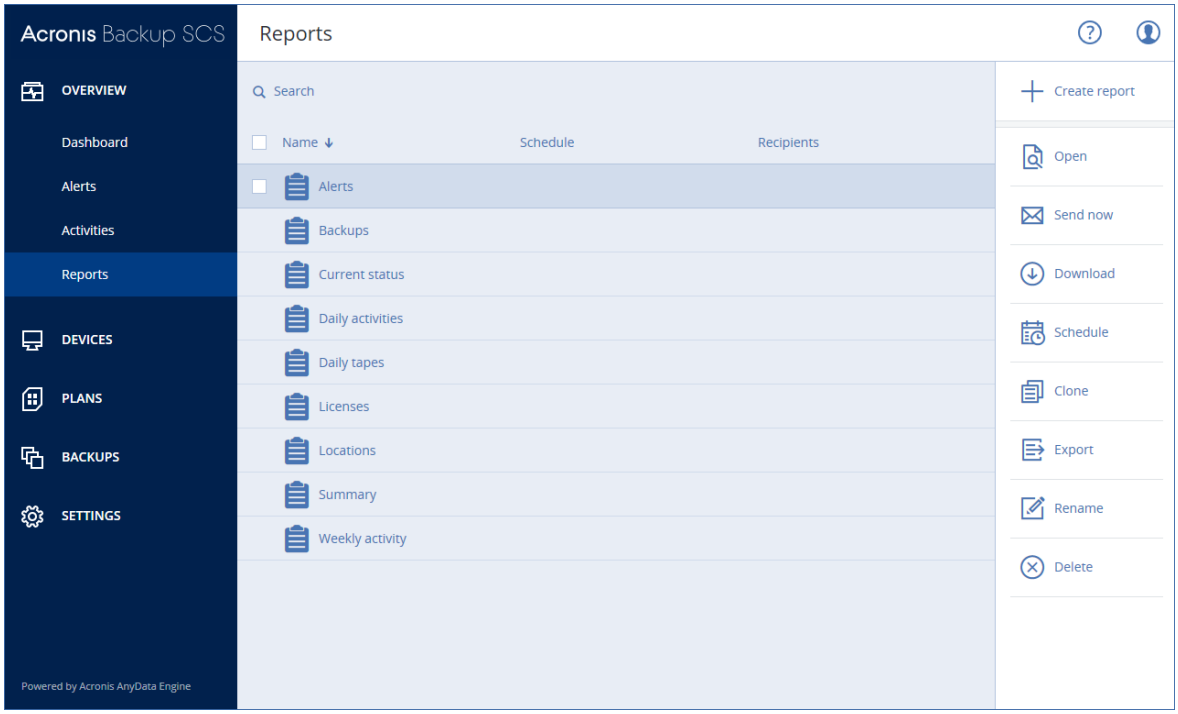
15.2 Reports

Note *This functionality is available only with the Acronis SCS Cyber Backup 12.5 Hardened Edition Advanced license.*

A report can include any set of the dashboard widgets. You can use predefined reports or create a custom report.

The reports can be sent via email or downloaded on a schedule. To send the reports via email, ensure that the **Email server** (Schedule 18.2) settings are configured.

If you want to process a report by using third-party software, schedule saving the report in the .xlsx format to a specific folder.



Basic operations with reports

Click **Overview** > **Reports**, select a report, and then do one of the following:

- To view a report, click **Open**.
- To send the report via email, click **Send now**, specify the email addresses, select the report format, and then click **Send**.
- To download the report, click **Download**.

Scheduling a report

1. Select a report, and then click **Schedule**.
2. Enable the **Send a scheduled report** switch.
3. Select whether to send the report via email, save it to a folder, or both. Depending on your choice, specify the email addresses, the folder path, or both.
4. Select the report format: .pdf, .xlsx, or both.
5. Select the reporting period: 1 day, 7 days, or 30 days.
6. Select the days and the time when the report will be sent or saved.
7. Click **Save**.

Exporting and importing the report structure

You can export and import the report structure (the set of widgets and the schedule settings) to a .json file. This may be useful in case of the management server re-installation or for copying the report structure to a different management server.

To export the report structure, select a report, and then click **Export**.

To import the report structure, click **Create report**, and then click **Import**.

Dumping the report data

You can save a dump of the report data to a .csv file. The dump includes all of the report data (without filtering) for a custom time range.

The software generates the data dump on the fly. If you specify a long period of time, this action may take a long time.

To dump the report data

1. Select a report, and then click **Open**.
2. Click the vertical ellipsis icon in the top-right corner, and then click **Dump data**.
3. In **Location**, specify the folder path for the .csv file.
4. In **Time range**, specify the time range.
5. Click **Save**.

15.3 Configuring the severity of alerts

An alert is a message that warns about actual or potential problems. You can use the alerts in various ways:

- The **Alerts** section of the **Overview** tab lets you quickly identify and solve the problems by monitoring the current alerts.
- Under **Devices**, the device status is derived from alerts. The **Status** column enables you to filter devices with problems.
- When configuring email notifications (Section 18.1), you can choose which alerts will trigger a notification.

An alert can have one of the following severities:

- **Critical**
- **Error**
- **Warning**

You can change the severity of an alert or disable an alert completely by using the alerts configuration file as described below. This operation requires restarting the management server.

Changing the severity of an alert does not affect already generated alerts.

Alerts configuration file

The configuration file is located on the machine running the management server.

- In Windows: `<installation_path>`**\AlertManager\alert_manager.yaml**

  Here, `<installation_path>` is the management server installation path. By default, it is **%ProgramFiles%\Acronis**.
- In Linux: **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

The file is structured as a YAML document. Each alert is an element in the **`alertTypes`** list.

The **`name`** key identifies the alert.

The **`severity`** key defines the alert severity. It must have one of the following values: **`critical`**, **`error`**, or **`warning`**.

The optional **enabled** key defines whether the alert is enabled or disabled. Its value must be either **true** or **false**. By default (without this key) all alerts are enabled.

To change the severity of an alert or disable an alert

1. On the machine where the management server is installed, open the **alert_manager.yaml** file in a text editor.
2. Locate the alert that you want to change or disable.
3. Do one of the following:
   - To change the alert severity, change the value of the **severity** key.
   - To disable the alert, add the **enabled** key, and then set its value to **false**.
4. Save the file.
5. Restart the management server service as described below.

To restart the management server service in Windows

1. In the **Start** menu, click **Run**, and then type: **cmd**
2. Click **OK**.
3. Run the following commands:

```
net stop acrmngsrv
net start acrmngsrv
```

To restart the management server service in Linux

1. Open **Terminal**.
2. Run the following command in any directory:

```
sudo service acronis_ams restart
```

16 Device groups

Device groups are designed for convenient management of a large number of registered devices.

You can apply a backup plan to a group. Once a new device appears in the group, the device becomes protected by the plan. If a device is removed from the group, the device will no longer be protected by the plan. A plan that is applied to a group cannot be revoked from a member of the group, only from the group itself.

Only devices 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.

A single device can be a member of more than one group.

Built-in groups

Once a device is registered, it appears in one of the built-in root groups on the **Devices** tab.

Root groups *cannot* be edited or deleted. You *cannot* apply plans to root groups.

Some of the root groups contain built-in sub-root groups. These groups *cannot* be edited or deleted. However, you *can* apply plans to sub-root built-in groups.

Custom groups

Protecting all devices in a built-in group with a single backup plan may not be satisfactory because of the different roles of the machines. The backed-up data is specific for each department; some data has to be backed up frequently, other data is backed up twice a year. Therefore, you may want to create various backup plans applicable to different sets of machines. In this case, consider creating custom groups.

A custom group can contain one or more nested groups. Any custom group can be edited or deleted. There are the following types of custom groups:

- **Static groups**

  Static groups contain the machines that were manually added to them. The static group content never changes unless you explicitly add or delete a machine.

  Example: You create a custom group for the accounting department and manually add the accountants' machines to this group. Once you apply a backup plan to the group, the accountants' machines become protected. If a new accountant is hired, you will have to add the new machine to the group manually.

- **Dynamic groups**

  Dynamic groups contain the machines added automatically according to the search criteria specified when creating a group. The dynamic group content changes automatically. A machine remains in the group while it meets the specified criteria.

  Example 1: The host names of the machines that belong to the accounting department contain the word "accounting". You specify the partial machine name as the group membership criterion and apply a backup plan to the group. If a new accountant is hired, the new machine will be added to the group as soon as it is registered, and thus will be protected automatically.

  Example 2: The accounting department forms a separate Active Directory organizational unit (OU). You specify the accounting OU as the group membership criterion and apply a backup plan to the group. If a new accountant is hired, the new machine will be added to the group as soon as it is registered and added to the OU (regardless of which comes first), and thus will be protected automatically.

16.1 Creating a static group

1. Click **Devices**, and then select the built-in group which contains the devices for which you want to create a static group.
2. Click the gear icon next to the group in which you want to create a group.
3. Click **New group**.
4. Specify the group name, and then click **OK**.

   The new group appears in the groups tree.

16.2 Adding devices to static groups

1. Click **Devices**, and then select one or more devices that you want to add to a group.
2. Click **Add to group**.

   The software displays a tree of groups to which the selected device can be added.
3. If you want to create a new group, do the following. Otherwise, skip this step.
   a. Select the group in which you want to create a group.
   b. Click **New group**.

Criterion	Meaning	Search query examples
osType	Operating system type. Possible values: ▪ **'windows'** ▪ **'linux'**	**osType IN ('linux')**
osProductType	The operating system product type. Possible values: ▪ **'dc'** Stands for Domain Controller. ▪ **'server'** ▪ **'workstation'**	**osProductType = 'server'**
tenant	The name of the unit to which the device belongs.	**tenant = 'Unit 1'**
tenantId	The identifier of the unit to which device belongs. To get the unit ID, under **Devices**, select the device, click **Details** > **All properties**. The ID is shown in the **ownerId** field.	**tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'**
state	Device state. Possible values: ▪ **'idle'** ▪ **'interactionRequired'** ▪ **'canceling'** ▪ **'backup'** ▪ **'recover'** ▪ **'install'** ▪ **'reboot'** ▪ **'failback'** ▪ **'testReplica'** ▪ **'run_from_image'** ▪ **'finalize'** ▪ **'failover'** ▪ **'replication'** ▪ **'createAsz'** ▪ **'deleteAsz'** ▪ **'resizeAsz'**	**state = 'backup'**

Criterion	Meaning	Search query examples
protectedByPlan	Devices that are protected by a backup plan with a given ID. To get the plan ID, click **Plans** > **Backup**, select the plan, click on the diagram in the **Status** column, and then click on a status. A new search with the plan ID will be created.	**protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
okByPlan	Devices that are protected by a backup plan with a given ID and have an **OK** status.	**okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
errorByPlan	Devices that are protected by a backup plan with a given ID and have an **Error** status.	**errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
warningByPlan	Devices that are protected by a backup plan with a given ID and have a **Warning** status.	**warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
runningByPlan	Devices that are protected by a backup plan with a given ID and have a **Running** status.	**runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
interactionByPlan	Devices that are protected by a backup plan with a given ID and have an **Interaction Required** status.	**interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
ou	Machines that belong to the specified Active Directory organizational unit.	**ou IN ('RnD', 'Computers')**
id	Device ID. To get the device ID, under **Devices**, select the device, click **Details** > **All properties**. The ID is shown in the **id** field.	**id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
lastBackupTime	The date and time of the last successful backup. The format is `'YYYY-MM-DD HH:MM'`.	**lastBackupTime > '2016-03-11'** **lastBackupTime <= '2016-03-11 00:15'** **lastBackupTime is null**
lastBackupTryTime	The time of the last backup attempt. The format is `'YYYY-MM-DD HH:MM'`.	**lastBackupTryTime >= '2016-03-11'**
nextBackupTime	The time of the next backup. The format is `'YYYY-MM-DD HH:MM'`.	**nextBackupTime >= '2016-03-11'**
agentVersion	Version of the installed backup agent.	**agentVersion LIKE '12.0.*'**
hostId	Internal ID of the backup agent. To get the backup agent ID, under **Devices**, select the machine, click **Details** > **All properties**. Use the **"id"** value of the **agent** property.	**hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**

Operators

The following table summarizes the available operators.

Operator	Meaning	Examples
AND	Logical conjunction operator.	`name like 'ru-00' AND tenant = 'Unit 1'`
OR	Logical disjunction operator.	`state = 'backup' OR state = 'interactionRequired'`
NOT	Logical negation operator.	`NOT(osProductType = 'workstation')`

`LIKE 'wildcard pattern'`	This operator is used to test if an expression matches the wildcard pattern. This operator is case-insensitive.
	The following wildcard operators can be used:
	▪ * or % The asterisk and the percent sign represent zero, one, or multiple characters
	▪ _ The underscore represents a single character
		`name LIKE 'ru-00'`
		`name LIKE '*ru-00'`
		`name LIKE '*ru-00*'`
		`name LIKE 'ru-00_'`

`IN (<value1>,... <valueN>)`	This operator is used to test if an expression matches any value in a list of values. This operator is case-sensitive.	`osType IN ('windows', 'linux')`
`RANGE(<starting_value>, <ending_value>)`	This operator is used to test if an expression is within a range of values (inclusive).	`ip RANGE('10.250.176.1','10.250.176.50')`

16.4 Applying a backup plan to a group

1. Click **Devices**, and then select the built-in group that contains the group to which you want to apply a backup plan.
   The software displays the list of child groups.
2. Select the group to which you want to apply a backup plan.
3. Click **Group backup**.
   The software displays the list of backup plans that can be applied to the group.
4. Do one of the following:
   - Expand an existing backup plan, and then click **Apply**.
   - Click **Create new**, and then create a new backup plan as described in "Backup" (Section 5).

17 Advanced storage options

Note *This functionality is available only with the Acronis SCS Cyber Backup 12.5 Hardened Edition Advanced license.*

17.1 Tape devices

The following sections describe in detail how to use tape devices for storing backups.

17.1.1 What is a tape device?

A **tape device** is a generic term that means a tape library or a stand-alone tape drive.

A **tape library** (robotic library) is a high-capacity storage device that contains:

- one or more tape drives
- multiple (up to several thousand) slots to hold tapes
- one or more changers (robotic mechanisms) intended to move the tapes between the slots and the tape drives.

It may also contain other components such as barcode readers or barcode printers.

An **autoloader** is a particular case of tape libraries. It contains one drive, several slots, a changer and a barcode reader (optional).

A **stand-alone tape drive** (also called **streamer**) contains one slot and can hold only one tape at a time.

17.1.2 Overview of tape support

Backup agents can back up data to a tape device directly. Fully automatic operation of the tape device is ensured.

17.1.2.1 Compatibility with RSM and third-party software

Coexistence with third-party software

It is not possible to work with tapes on a machine where third-party software with proprietary tape management tools is installed. To use tapes on such a machine, you need to uninstall or deactivate the third-party tape management software.

Interaction with Windows Removable Storage Manager (RSM)

Backup agents do not use RSM. When detecting a tape device (Section 17.1.4.1), they disable the device from RSM (unless it is being used by other software). As long as you want to work with the tape device, make sure that neither a user nor third-party software enables the device in RSM. If the tape device was enabled in RSM, repeat the tape device detection.

17.1.2.2 Supported hardware

Acronis SCS Cyber Backup 12.5 Hardened Edition supports external SCSI devices. These are devices connected to Fibre Channel or using the SCSI, iSCSI, Serial Attached SCSI (SAS) interfaces. Also, Acronis SCS Cyber Backup 12.5 Hardened Edition supports USB-connected tape devices.

In Windows, Acronis SCS Cyber Backup 12.5 Hardened Edition can back up to a tape device even if the drivers for the device's changer are not installed. Such a tape device is shown in **Device Manager** as **Unknown Medium Changer**. However, drivers for the device's drives must be installed. In Linux and under bootable media, backing up to a tape device without drivers is not possible.

Recognition of IDE or SATA connected devices is not guaranteed. It depends on whether proper drivers have been installed in the operating system.

17.1.2.3 Tape management database

The information about all tape devices attached to a machine is stored in the tape management database. The default database path is as follows:

DefaultBlockSize

This is the block size (in bytes) used when writing to tapes.

Possible values: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

If the value is 0 or if the parameter is absent, the block size is determined as follows:

- In Windows, the value is taken from the tape device driver.
- In Linux, the value is **64 KB**.

Registry key (on a machine running Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize

Line in /etc/Acronis/BackupAndRecovery.config (on a machine running Linux):

```
    <value name=DefaultBlockSize" type="Dword">
        "value"
    </value>
```

If the specified value is not accepted by the tape drive, the software divides it by two until the applicable value is reached or until the value reaches 32 bytes. If the applicable value is not found, the software multiplies the specified value by two until the applicable value is reached or until the value reaches 1 MB. If no value is accepted by the drive, the backup will fail.

WriteCacheSize

This is the buffer size (in bytes) used when writing to tapes.

Possible values: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, but not less than the **DefaultBlockSize** parameter value.

If the value is 0 or if the parameter is absent, the buffer size is **1 MB**. If the operating system does not support this value, the software divides it by two until the applicable value is found or until the **DefaultBlockSize** parameter value is reached. If the value supported by the operating system is not found, the backup fails.

Registry key (on a machine running Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

Line in /etc/Acronis/BackupAndRecovery.config (on a machine running Linux):

```
    <value name="WriteCacheSize" type="Dword">
        "value"
    </value>
```

If you specify a non-zero value that is not supported by the operating system, the backup will fail.

17.1.2.5 Tape-related backup options

You can configure the **Tape management** (Section 5.10.26) backup options to determine:

- Whether to enable file recovery from disk-level backups stored on tapes.
- Whether to return tapes back to slots after backup plan completion.
- Whether to eject tapes after backup completion.
- Whether to use a free tape for each full backup.
- Whether to overwrite a tape when creating a full backup (for stand-alone tape drives only).

- Whether to use tape sets to differentiate tapes used, for example, for backups created on different days of week or for backups of different machine types.

17.1.2.6 Parallel operations

Acronis SCS Cyber Backup 12.5 Hardened Edition can simultaneously perform operations with various components of a tape device. During an operation that uses a drive (backing up, recovering, rescanning (Section 17.1.4.4), or erasing (Section 17.1.4.4), you can launch an operation that uses a changer (moving (Section 17.1.4.3) a tape to another slot or ejecting (Section 17.1.4.4) a tape) and vice versa. If your tape library has more than one drive, you can also launch an operation that uses one of the drives during an operation with another drive. For example, several machines can back up or recover simultaneously using different drives of the same tape library.

The operation of detecting the new tape devices (Section 17.1.4.1) can be performed simultaneously with any other operation. During inventorying (Section 17.1.4.4), no other operation is available except for detecting the new tape devices.

Operations that cannot be performed in parallel are queued.

17.1.2.7 Limitations

The limitations of tape device usage are the following:

1. Tape devices are not supported when a machine is booted from 32-bit Linux-based bootable media.
2. You cannot back up Microsoft Exchange mailboxes to tapes.
3. You cannot create application-aware backups of physical and virtual machines.
4. The consolidation of backups located on tapes is not possible. As a result, the **Always incremental** backup scheme is unavailable when you back up to tapes.
5. The deduplication of backups located on tapes is not possible.
6. The software cannot automatically overwrite a tape that contains at least one non-deleted backup or if there are dependent backups on other tapes.
7. You cannot recover under an operating system from a backup stored on tapes if the recovery requires the operating system reboot. Use bootable media to perform such recovery.
8. You can validate (Section 9.1.2) any backup stored on tapes, but you cannot select for validation an entire tape-based location or tape device.
9. The software cannot simultaneously write one backup to multiple tapes or multiple backups through the same drive to the same tape.
10. Devices that use the Network Data Management Protocol (NDMP) are not supported.
11. Barcode printers are not supported.
12. Linear Tape File System (LTFS) formatted tapes are not supported.

17.1.3 Getting started with a tape device

17.1.3.1 Backing up a machine to a locally attached tape device

Prerequisites

- The tape device is attached to the machine in accordance with the manufacturer's instructions.
- The backup agent is installed on the machine.

Before backing up

1. Load tapes to the tape device.
2. Log in to the backup console.
3. In **Settings** > **Tape management**, expand the machine node, and then click **Tape devices**.
4. Ensure that the attached tape device is displayed. If it is not, click **Detect devices**.
5. Perform the tape inventory:
   a. Click the tape device name.
   b. Click **Inventory** to detect the loaded tapes. Keep **Full inventory** turned on. Do not turn on **Move unrecognized or imported tapes to the 'Free tapes' pool**. Click **Start inventorying now**.
   Result. The loaded tapes have been moved to proper pools as specified in the "Inventorying" (Section 17.1.4.4) section.

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

   c. If the loaded tapes were sent to the **Unrecognized tapes** or **Imported tapes** pool and you want to use them for backing up, move (Section 17.1.4.4) such tapes to the **Free tapes** pool manually.

   *Tapes sent to the **Imported tapes** pool contain backups written by Acronis software . Before moving such tapes to the **Free tapes** pool, ensure that you do not need these backups.*

Backing up

Create a backup plan as described in the "Backup" (Section 5) section. When specifying the backup location, select **Tape pool 'Acronis'**.

Results

- To access the location where backups will be created, click **Backups** > **Tape pool 'Acronis'**.
- Tapes with the backups will be moved to the **Acronis** pool.

17.1.3.2 Recovering under an operating system from a tape device

To recover under an operating system from a tape device:

1. Log in to the backup console.
2. Click **Devices**, and then select the backed-up machine.
3. Click **Recovery**.
4. Select a recovery point. Note that recovery points are filtered by location.
5. The software shows you the list of tapes required for the recovery. The missing tapes are grayed out. If your tape device has empty slots, load these tapes into the device.
6. Configure (Section 6.3) other recovery settings.
7. Click **Start recovery** to start the recovery operation.
8. If any of the required tapes are not loaded for some reason, the software will show you a message with the identifier of the needed tape. Do the following:
   a. Load the tape.
   b. Perform the fast inventorying (Section 17.1.4.4).
   c. Click **Overview** > **Activities**, and then click the recovery activity with the **Interaction required** status.
   d. Click **Show details**, and then click **Retry** to continue the recovery.

What if I do not see backups stored on tapes?

It may mean that the database with the contents of tapes is lost or corrupted for some reason.

To restore the database, do the following:

1. Perform the fast inventorying (Section 17.1.4.4).

   During the inventorying, do not *turn on* ***Move unrecognized and imported tapes to the 'Free tapes' pool****. If the switch is turned on, you may lose all your backups.*

2. Rescan (Section 17.1.4.4) the **Unrecognized tapes** pool. As a result, you will get the contents of the loaded tape(s).
3. If any of the detected backups continue on other tapes that have not been rescanned yet, load these tapes as prompted and rescan them.

17.1.3.3 Recovering under bootable media from a locally attached tape device

To recover under bootable media from a locally attached tape device:

1. Load the tape(s) required for the recovery into the tape device.
2. Boot the machine from the bootable media.
3. Click **Manage this machine locally** or click **Rescue Bootable Media** twice, depending on the media type you are using.
4. If the tape device is connected by using the iSCSI interface, configure the device as described in "Configuring iSCSI and NDAS devices" (Section 10.4).
5. Click **Tape management**.
6. Click **Inventory**.
7. In **Objects to be inventoried**, select the tape device.
8. Click **Start** to start the inventorying.
9. After the inventorying completes, click **Close**.
10. Click **Actions** > **Recover**.
11. Click **Select data**, and then click **Browse**.
12. Expand **Tape devices**, and then select the necessary device. The system prompts to confirm the rescanning. Click **Yes**.
13. Select the **Unrecognized tapes** pool.
14. Select the tapes to be rescanned. To select all the tapes of the pool, select the check box next to the **Tape name** column header.
15. If the tapes contain a password-protected backup, select the corresponding check box, and then specify the password for the backup in the **Password** box. If you do not specify a password, or the password is incorrect, the backup will not be detected. Please keep this in mind in case you see no backups after the rescanning.
    Tip. If the tapes contain several backups protected by various passwords, you need to repeat the rescanning several times specifying each password in turn.
16. Click **Start** to start the rescanning. As a result, you will get the contents of the loaded tape(s).
17. If any of the detected backups continue on other tapes that have not been rescanned yet, load these tapes as prompted and rescan them.
18. After the rescanning completes, click **OK**.
19. In the **Archive view**, select the backup whose data is to be recovered, and then select the data you want to recover. After you click **OK**, the **Recover data** page will show you the list of tapes

required for the recovery. The missing tapes are grayed out. If your tape device has empty slots, load these tapes into the device.

20. Configure other recovery settings.
21. Click **OK** to start the recovery.
22. If any of the required tapes are not loaded for some reason, the software will show you a message with the identifier of the needed tape. Do the following:
    a. Load the tape.
    b. Perform the fast inventorying (Section 17.1.4.4).
    c. Click **Overview** > **Activities**, and then click the recovery activity with the **Interaction required** status.
    d. Click **Show details**, and then click **Retry** to continue the recovery.

17.1.4 Tape management

17.1.4.1 Detecting tape devices

When detecting tape devices, the backup software finds tape devices attached to the machine and places information about them in the tape management database. Detected tape devices are disabled from RSM.

Usually, a tape device is detected automatically as soon as it is attached to a machine with the product installed. However you may need to detect tapes devices in the following cases:

- After you have attached or re-attached a tape device.
- After you have installed or reinstalled the backup software on the machine to which a tape device is attached.

To detect the tape devices

1. Click **Settings** > **Tape management**.
2. Select the machine to which the tape device is attached.
3. Click **Detect devices**. You will see the connected tape devices, their drives and slots.

17.1.4.2 Tape pools

The backup software uses tape pools that are logical groups of tapes. The software contains the following predefined tape pools: **Unrecognized tapes**, **Imported tapes**, **Free tapes**, and **Acronis**. Also, you can create your own custom pools.

The **Acronis** pool and custom pools are also used as backup locations.

Predefined pools

Unrecognized tapes

The pool contains tapes that were written by third-party applications. To write to such tapes, you need to move (Section 17.1.4.4) them to the **Free tapes** pool explicitly. You cannot move tapes from this pool to any other pool, except for the **Free tapes** pool.

Imported tapes

The pool contains tapes that were written by Acronis SCS Cyber Backup 12.5 Hardened Edition in a tape device attached to another agent. To write to such tapes, you need to move them to the **Free tapes** pool explicitly. You cannot move tapes from this pool to any other pool, except for the **Free tapes** pool.

Free tapes

The pool contains free (empty) tapes. You can manually move tapes to this pool from other pools.

When you move a tape to the **Free tapes** pool, the software marks it as empty. If the tape contains backups, they are marked with the  icon. When the software starts overwriting the tape, the data related to the backups will be removed from the database.

Acronis

The pool is used for backing up by default, when you do not want to create your own pools. Usually it applies to one tape drive with a small number of tapes.

Custom pools

You need to create several pools if you want to separate backups of different data. For example, you may want to create custom pools in order to separate:

- backups from different departments of your company
- backups from different machines
- backups of system volumes and users' data.

17.1.4.3 Operations with pools

Creating a pool

To create a pool:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Click **Create pool**.
4. Specify the pool name.
5. [Optional] Clear the **Take tapes from the 'Free tapes' pool automatically...** check box. If cleared, only tapes that are included into the new pool at a certain moment will be used for backing up.
6. Click **Create**.

Editing a pool

You can edit parameters of the **Acronis** pool or your own custom pool.

To edit a pool:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Select the required pool, and then click **Edit pool**.
4. You can change the pool name or settings. For more information about pool settings, see the "Creating a pool" (Section 17.1.4.3) section.
5. Click **Save** to save the changes.

Deleting a pool

You can delete only custom pools. Predefined tape pools (**Unrecognized tapes**, **Imported tapes**, **Free tapes**, and **Acronis**) cannot be deleted.

Note *After a pool is deleted, do not forget to edit backup plans that have the pool as the backup location. Otherwise, these backup plans will fail.*

To delete a pool:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Select the required pool and click **Delete**.
4. Select the pool to which the tapes of the pool being deleted will be moved after the deletion.
5. Click **OK** to delete the pool.

17.1.4.4 Operations with tapes

Moving to another slot

Use this operation in the following situations:

- You need to take several tapes out of a tape device simultaneously.
- Your tape device does not have a mail slot and the tapes to be taken out are located in slots of non-detachable magazine(s).

You need to move tapes to slots of one slot magazine and then take the magazine out manually.

To move a tape to another slot:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Click the pool that contains the necessary tape, and then select the required tape.
4. Click **Move to slot**.
5. Select a new slot to move the selected tape to.
6. Click **Move** to start the operation.

Moving to another pool

The operation allows you to move one or several tapes from one pool to another.

When you move a tape to the **Free tapes** pool, the software marks it as empty. If the tape contains backups, they are marked with the  icon. When the software starts overwriting the tape, the data related to the backups will be removed from the database.

Notes about specific types of tape

- You cannot move write-protected and once-recorded WORM (Write-Once-Read-Many) tapes to the **Free tapes** pool.
- Cleaning tapes are always displayed in the **Unrecognized tapes** pool; you cannot move them to any other pool.

To move tapes to another pool:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Click the pool that contains the necessary tapes, and then select the required tapes.
4. Click **Move to pool**.
5. [Optional] Click **Create new pool** if you want to create another pool for the selected tapes. Perform actions described in the "Creating a pool" (Section 17.1.4.3) section.
6. Select the pool to move the tapes to.
7. Click **Move** to save the changes.

Inventorying

The inventorying operation detects tapes loaded into a tape device and assigns names to those that have none.

Inventorying methods

There are two methods of inventorying.

Fast inventorying

The agent scans tapes for barcodes. Using barcodes, the software can quickly return a tape to the pool where it was before.

Select this method to recognize tapes used by the same tape device attached to the same machine. Other tapes will be sent to the **Unrecognized tapes** pool.

If your tape library contains no barcode reader, all tapes will be sent to the **Unrecognized tapes** pool. To recognize your tapes, perform full inventorying or combine fast and full inventorying as described later in this section.

Full inventorying

The agent reads earlier written tags and analyzes other information about the contents of the loaded tapes. Select this method to recognize empty tapes and tapes written by the same software on any tape device and any machine.

The following table shows pools to which tapes are sent as a result of the full inventorying.

Tape was used by...	**Tape is read by...**	**Tape is sent to pool...**
Agent	the same Agent	where the tape was before
	another Agent	**Imported tapes**
third-party backup application	Agent	**Unrecognized tapes**

Tapes of certain types are sent to specific pools:

Tape type	**Tape is sent to pool...**
Empty tape	**Free tapes**

Empty write-protected tape	**Unrecognized tapes**
Cleaning tape	**Unrecognized tapes**

The fast inventorying can be applied to entire tape devices. The full inventorying can be applied to entire tape devices, individual drives, or slots. For stand-alone tape drives, the full inventorying is always performed, even if the fast inventorying is selected.

Combination of fast and full inventorying

Full inventorying of an entire tape device may take a long time. If you need to inventory only a few tapes, proceed as follows:

1. Perform the fast inventorying of the tape device.
2. Click the **Unrecognized tapes** pool. Find the tapes you want to inventory and note which slots they occupy.
3. Perform the full inventorying of these slots.

What to do after inventorying

If you want to back up to tapes that were placed in the **Unrecognized tapes** or **Imported tapes** pool, move (Section 17.1.4.3) them to the **Free tapes** pool, and then to the **Acronis** pool or a custom pool. If the pool to which you want to back up is replenishable, you may leave the tapes in the **Free tapes** pool.

If you want to recover from a tape that was placed in the **Unrecognized tapes** or **Imported tapes** pool, you need to rescan (Section 17.1.4.4) it. The tape will be moved to the pool you have selected during the rescanning, and the backups stored on the tape will appear in the location.

Sequence of actions

1. Click **Settings** > **Tape management**.
2. Select the machine to which the tape device is attached, and then select the tape device that you want to inventory.
3. Click **Inventory**.
4. [Optional] To select the fast inventorying, turn off **Full inventory**.
5. [Optional] Turn on **Move unrecognized and imported tapes to the 'Free tapes' pool**.

   Warning. *Only enable this switch if you are absolutely sure that the data stored on your tapes can be overwritten.*
6. Click **Start inventorying now** to start inventory.

Rescanning

The information about the contents of tapes is stored in a dedicated database. The rescanning operation reads the contents of tapes and updates the database if the information in it mismatches the data stored on tapes. The backups detected as a result of the operation are placed in the specified pool.

Within one operation, you can rescan tapes of one pool. Only online tapes can be selected for the operation.

Run the rescanning:

- If information about a tape in the database is out of date (for example, a tape contents were modified by another agent).
- To obtain access to backups stored on tapes when working under bootable media.

- If you have mistakenly removed (Section 17.1.4.4) the information about a tape from the database. When you rescan a removed tape, the backups stored on it reappear in the database and become available for data recovery.
- If backups were deleted from a tape either manually or through retention rules but you want them to become accessible for data recovery. Before rescanning such a tape, eject (Section 17.1.4.4) it, remove (Section 17.1.4.4) the information about it from the database, and then insert the tape into the tape device again.

To rescan tapes:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape devices** under this machine.
3. Select the tape device you loaded the tapes to.
4. Perform the fast inventorying (Section 17.1.4.4).

   ***Note** During the inventorying, do* not *enable the **Move unrecognized and imported tapes to the 'Free tapes' pool** switch.*
5. Select the **Unrecognized tapes** pool. This is the pool to which most of the tapes are sent as a result of the fast inventorying. Rescanning any other pool is also possible.
6. [Optional] To rescan only individual tapes, select them.
7. Click **Rescan**.
8. Select the pool where the newly detected backups will be placed.
9. If necessary, select the **Enable file recovery from disk backups stored on tapes** check box. **Details**. If the check box is selected, the software will create special supplementary files on a hard disk of the machine where the tape device is attached. File recovery from disk backups is possible as long as these supplementary files are intact. Be sure to select the check box if the tapes contain application-aware backups (Section 11.3). Otherwise, you will not be able to recover the application data from these backups.
10. If the tapes contain password-protected backups, select the corresponding check box, and then specify the password for the backups. If you do not specify a password, or the password is incorrect, the backups will not be detected. Please keep this in mind in case you see no backups after the rescanning.
    Tip. If the tapes contain backups protected by various passwords, you need to repeat the rescanning several times specifying each password in turn.
11. Click **Start rescan** to start the rescanning.

Result. The selected tapes are moved to the selected pool. The backups stored on the tapes can be found in this pool. A backup spread over several tapes will not appear in the pool until all of these tapes are rescanned.

Renaming

When a new tape is detected by the software, it is automatically assigned a name in the following format: **Tape XXX**, where **XXX** is a unique number. Tapes are numbered sequentially. The renaming operation allows you to manually change the name of a tape.

To rename tapes:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.

3. Click the pool that contains the necessary tape, and then select the required tape.
4. Click **Rename**.
5. Type the new name of the selected tape.
6. Click **Rename** to save the changes.

Erasing

Erasing a tape physically deletes all backups stored on the tape and removes the information about these backups from the database. However the information about the tape itself remains in the database.

After erasing, a tape located in the **Unrecognized tapes** or **Imported tapes** pool is moved to the **Free tapes** pool. A tape located in any other pool is not moved.

To erase tapes:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Click the pool that contains the necessary tapes, and then select the required tapes.
4. Click **Erase**. The system prompts to confirm the operation.
5. Select the erasing method: fast or full.
6. Click **Erase** to start the operation.

   Details. You cannot cancel the erasing operation.

Ejecting

For successful ejecting of a tape from a tape library, the tape library must have the mail slot and the slot must not be locked by a user or by other software.

To eject tapes:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Click the pool that contains the necessary tapes, and then select the required tapes.
4. Click **Eject**. The software will prompt you to provide the tape description. We recommend that you describe the physical location where the tapes will be kept. During recovery, the software will display this description so you could easily find the tapes.
5. Click **Eject** to start the operation.

After a tape is ejected either manually or automatically (Section 5.10.26), it is recommended to write its name on the tape.

Removing

The removal operation deletes the information about the backups stored on the selected tape and about the tape itself from the database.

You can only remove an offline (ejected (Section 17.1.4.4)) tape.

To remove a tape:

1. Click **Settings** > **Tape management**.

2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Click the pool that contains the necessary tape, and then select the required tape.
4. Click **Remove**. The system prompts to confirm the operation.
5. Click **Remove** to remove the tape.

What to do if I removed a tape by mistake?

Unlike an erased (Section 17.1.4.3) tape, the data from a removed tape is not physically deleted. Hence, you can make backups stored on such tape available again. To do so:

1. Load the tape into your tape device.
2. Perform the fast inventorying (Section 17.1.4.4) to detect the tape

Notes' *During the inventorying, do not enable the Move unrecognized and imported tapes to the 'Free tapes' pool switch.*

3. Perform the rescanning (Section 17.1.4.4) to match the data stored on tapes with the database.

Specifying a tape set

The operation allows you to specify a tape set for tapes.

A **tape set** is a group of tapes within one pool.

Unlike specifying tape sets in the backup options (Section 5.10.26), where you can use variables, here you can specify only a string value.

Perform this operation if you want the software to back up to *specific* tapes according to a certain rule (for example, if you want to store Monday's backups on Tape 1, Tuesday's backups on Tape 2, etc). Specify a certain tape set for each of the required tapes, and then specify the same tape set or use proper variables in the backup options.

For the above example, specify tape set **`Monday`** for Tape 1, **`Tuesday`** for Tape 2, etc. In the backup options, specify **`[Weekday]`**. In this case, a proper tape will be used on the respective day of the week.

To specify a tape set for one or several tapes:

1. Click **Settings** > **Tape management**.
2. Select the machine to which your tape device is attached, and then click **Tape pools** under this machine.
3. Click the pool that contains the necessary tapes, and then select the required tapes.
4. Click **Tape set**.
5. Type the tape set name. If another tape set is already specified for the selected tapes, it will be replaced. If you want to exclude the tapes from the tape set without specifying another one, delete the existing tape set name.
6. Click **Save** to save the changes.

18 System settings

To access these settings, click **Settings** > **System settings**.

The **System settings** section is visible only to organization administrators (Section 19.1).

18.1 Email notifications

You can configure the global settings that are common for all email notifications sent from the management server.

In default backup options (Section 18.4), you can override these settings exclusively for the events that occur during backup. In this case, the global settings will be effective for operations other than backup.

When creating a backup plan (Section 5.10.10), you can choose which settings will be used: the global settings or the settings specified in the default backup options. You can also override them with custom values that will be specific for the plan only.

Important *When the global email notification settings are changed, all backup plans that use the global settings are affected.*

Before configuring these settings, ensure that the **Email server** (Section 18.2) settings are configured. ***To configure global email notification settings***

1. Click **Settings** > **System settings** > **Email notifications**.
2. In the **Recipients' email addresses** field, type the destination email address. You can enter several addresses separated by semicolons.
3. [Optional] In **Subject**, change the email notification subject.

   You can use the following variables:

   - **`[Alert]`** - alert summary.
   - **`[Device]`** - device name.
   - **`[Plan]`** - the name of the plan that generated the alert.
   - **`[ManagementServer]`** - the host name of the machine where the management server is installed.
   - **`[Unit]`** - the name of the unit to which the machine belongs.

   The default subject is **`[Alert]` Device: `[Device]` Plan: `[Plan]`**
4. [Optional] Select the **Daily recap about active alerts** check box, and then do the following:
   a. Specify the time when the recap will be sent.
   b. [Optional] Select the **Do not send the 'No active alerts' messages** check box.
5. Select the check boxes for the events that you want to receive notifications about. You can select from the list of all possible alerts, grouped by severity.
6. Click **Save**.

18.2 Email server

You can specify an email server that will be used to send email notifications from the management server.

To specify the email server

1. Click **Settings** > **System settings** > **Email server**.
2. In **Email service**, select **Custom.**
3. Specify the following settings:
   - In **SMTP server**, enter the name of the outgoing mail server (SMTP).
   - In **SMTP port**, set the port of the outgoing mail server. By default, the port is set to 25.

- Select whether to use SSL or TLS encryption. Select **None** to disable encryption.
- If the SMTP server requires authentication, select the **SMTP server requires authentication** check box, and then specify the credentials of an account that will be used to send messages. If you are not sure whether the SMTP server requires authentication, contact your network administrator or your email service provider for assistance.

4. In **Sender**, type the name of the sender. This name will be shown in the **From** field of the email notifications. If you leave this field empty, the messages will contain the account specified in step 3 or 4.
5. [Optional] Click **Send test message** to check whether the email notifications work correctly with the specified settings. Enter an email address to send the test message to.

18.3 Security

Log out inactive users after

This option lets you specify a timeout for automatic logout due to user inactivity. When one minute is left in the set timeout, the software prompts the user to stay logged in. Otherwise, the user will be logged out and all unsaved changes will be lost.

The preset is: **Enabled. Timeout: 10 minutes.**

Show notification about the last login of the current user

This option enables displaying the date and time of the user's last successful login, the number of authentication failures since the last successful login, and the IP address of the last successful login. This information is shown at the bottom of the screen every time the user logs in.

The preset is: **Disabled**.

Warn about local or domain password expiration

This option enables displaying when the password for user's access to Acronis SCS Cyber Backup 12.5 Hardened Edition Management Server will expire. This is the local or domain password with which the user logs on to the machine where the management server is installed. The time before password expiration is shown at the bottom of the screen and in the account menu in the top-right corner.

The preset is: **Disabled**.

18.4 Default backup options

The default values of backup options (Section 5.10) are common for all backup plans on the management server. An organization administrator can change a default option value against the pre-defined one. The new value will be used by default in all backup plans created after the change takes place.

When creating a backup plan, a user can override a default value with a custom value that will be specific for this plan only.

To change a default option value

1. Sign in to the backup console as an organization administrator.
2. Click **Settings** > **System settings**.
3. Expand the **Default backup options** section.
4. Select the option, and then make the necessary changes.
5. Click **Save**.

18.5 Configuring anonymous registration

During a local installation of an agent (Section 1.8.1), the setup program suggests the option to register the machine on the management server anonymously; in other words, to connect without authentication. Anonymous registration also happens if incorrect credentials for the management server are specified in the Agent for VMware (Virtual Appliance) GUI. Anonymous registration lets a management server administrator delegate the agent installation to users.

It is possible to disable anonymous registration on the management server so that the valid user name and password of a management server administrator are always required for a device registration. If a user opts for anonymous registration, the registration will fail. Registration of bootable media pre-configured with the **Do not ask for user name and password** option also will be rejected. During unattended installation, you will need to provide a registration token in the transform file (.mst) or as the **`msiexec`** command parameter.

To disable anonymous registration on the management server

1. Log in to the machine where the management server is installed.
2. Open the following configuration file in a text editor:
   - In Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - In Linux: **/var/lib/Acronis/ApiGateway/api_gateway.json**
3. Locate the following section:

   ```
   "auth": {
     "anonymous_role": {
       "enabled": true
     }
   },
   ```

   If you updated the management server from build 11010 or earlier, this section is absent. Copy and paste it to the beginning of the file right after the opening brace **`{`**.
4. Change **`true`** to **`false`**.
5. Save the **api_gateway.json** file.

   Important *Please be careful and do not accidentally delete any commas, brackets, and quotation marks in the configuration file.*

6. Restart Acronis Service Manager Service as described in "Changing the SSL certificate settings" (Section 3.2)

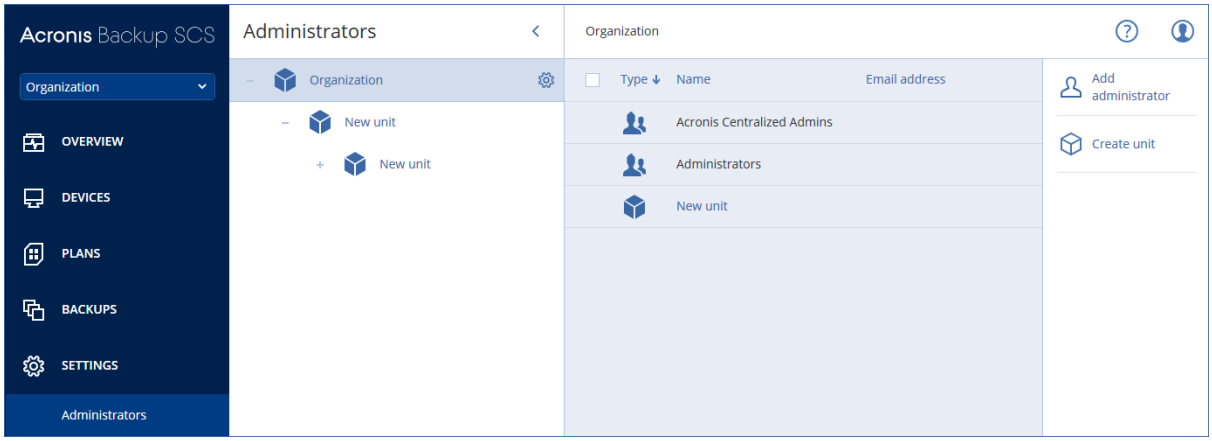
19 Administering user accounts and organization units

The functionality described in this section is available only to organization administrators

(Section 19.1). To access these settings, click **Settings** > **Administrators**.

19.1 Administrators and units

The **Administrators** panel shows the **Organization** group with the tree of units (if any) and the list of administrators of the unit that is selected in the tree.



Who are the management server administrators?

Any account that is able to sign in to the backup console is a management server administrator.

Organization administrators are the top-level administrators. *Unit administrators* are administrators of the child groups (units).

In the backup console, each administrator has a view scoped to their area of control. An administrator can view and manage anything on or below their level in the hierarchy.

Who are the default administrators?

In Windows

When the management server is being installed on a machine, the following happens:

- The **Acronis Centralized Admins** user group is created on the machine.

  On a domain controller, the group is named *DCNAME* **$ Acronis Centralized Admins**; here, *DCNAME* stands for the NetBIOS name of the domain controller.
- All members of the **Administrators** group are added to the **Acronis Centralized Admins** group. If the machine is in a domain but is not a domain controller, local (non-domain) users are then excluded. On a domain controller, there are no non-domain users.
- The **Acronis Centralized Admins** and the **Administrators** groups are added to the management server as **organization administrators**. If the machine is in a domain but is not a domain controller, the **Administrators** group is not added, so that local (non-domain) users do not become organization administrators.

You can delete the **Administrators** group from the list of the organization administrators. However, the **Acronis Centralized Admins** group cannot be deleted. In the unlikely case that all organization administrators have been deleted, you can add an account to the **Acronis Centralized Admins** group in Windows, and then log in to the backup console by using this account.

In Linux

When the management server is being installed on a machine, the **root** user is added to the management server as an **organization administrator**.

You can add other Linux users to the list of management server administrators as described later, and then delete the **root** user from this list. In the unlikely case that all organization administrators have been deleted, you can restart the **acronis_asm** service. As a result, the **root** user will be automatically re-added as an organization administrator.

Who can be an administrator?

If the management server is installed on a Windows machine that is included in an Active Directory domain, any local or domain user or user group can be added to the management server administrators. Otherwise, only local users and groups can be added.

For information about how to add an administrator to the management server, refer to "Adding administrators" (Section 19.2).

Units and unit administrators

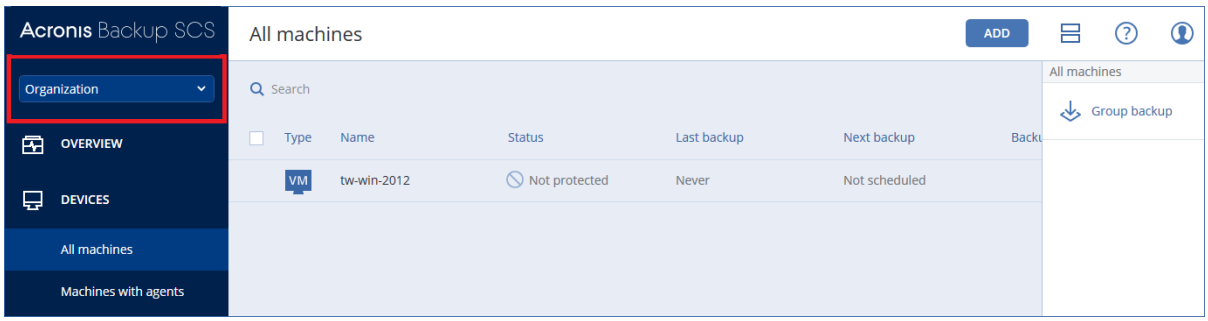
The **Organization** group is automatically created when you install the management server. With the Acronis SCS Cyber Backup 12.5 Hardened Edition Advanced license, you can create child groups called units, which typically correspond to units or departments of the organization, and add administrators to the units.

This way, you can delegate backup management to other people whose access permissions will be strictly limited to the corresponding units.

For information about how to create a unit, refer to "Creating units" (Section 19.3)

What if an account is added to multiple units?

An account can be added as a **unit administrator** to any number of units. For such an account, as well as for organization administrators, the unit selector is shown in the backup console. By using this selector, the administrator can view and manage each unit separately.



An account that has permissions for all units does not have permissions for the organization. Organization administrators must be added to the **Organization** group explicitly.

How to populate units with machines

When an administrator adds a machine via the web interface (Section 1.7), the machine is added to the unit managed by the administrator. If the administrator manages multiple units, the machine is added to the unit chosen in the unit selector. Therefore, the administrator must choose the unit prior to clicking **Add**.

When installing agents locally (Section 1.8), an administrator provides their credentials. The machine is added to the unit managed by the administrator. If the administrator manages multiple units, the installer prompts to choose a unit to which the machine will be added.

19.2 Adding administrators

To add administrators

1. Click **Settings** > **Administrators**.

   The software displays the list of the management server administrators and the tree of units (if any).
2. Select **Organization** or select the unit where you want to add an administrator.
3. Click **Add administrator**.
4. In **Domain**, select the domain that contains the user accounts that you want to add. If the management server is not included in an Active Directory domain or is installed in Linux, only local users can be added.
5. Search for the user name or the user group name.
6. Click "+" next to the name of the user or group.
7. Repeat steps 4-6 for all users or groups that you want to add.
8. When finished, click **Done**.
9. [Only in Linux] Add the user names to the Acronis Linux Pluggable Authentication Module (PAM) as described below.

To add user names to the Acronis Linux PAM

1. On the machine running the management server, as the root user, open the file **/etc/security/acronisagent.conf** with a text editor.
2. In this file, type the user names that you added as the management server administrators, one per line.
3. Save and close the file.

19.3 Creating units

1. Click **Settings** > **Administrators**.
2. The software displays the list of the management server administrators and the tree of units (if any).
3. Select **Organization** or select the parent unit for the new unit.
4. Click **Create unit**.
5. Specify a name for the new unit, and then click **Create**.

20 Command-line reference

Command-line reference is a separate document available at https://dl.acronisscs.com/support/documentation/AcronisBackup_12.5_Command_Line_Reference

21 Troubleshooting

This section describes how to save an agent log to a .zip file. If a backup fails for an unclear reason, this file will help the Acronis personnel to identify the problem.

To collect logs

1. Do one of the following:

- Under **Devices**, select the machine that you want to collect the logs from, and then click **Activities**.
- Under **Settings** > **Agents**, select the machine that you want to collect the logs from, and then click **Details**.

2. Click **Collect system information**.
3. If prompted by your web browser, specify where to save the file.

Copyright Statement

22 Glossary

B

Backup set

A group of backups to which an individual retention rule can be applied.

For the **Custom** backup scheme, the backup sets correspond to the backup methods (**Full**, **Differential**, and **Incremental**).

In all other cases, the backup sets are **Monthly**, **Daily**, **Weekly**, and **Hourly**.

- A monthly backup is the first backup created after a month starts.
- A weekly backup is the first backup created on the day of the week selected in the **Weekly backup** option (click the gear icon, then **Backup options** > **Weekly backup**).

  If a weekly backup is the first backup created after a month starts, this backup is considered monthly. In this case, a weekly backup will be created on the selected day of the next week.
- A daily backup is the first backup created after a day starts, unless this backup falls within the definition of a monthly or weekly backup.
- An hourly backup is the first backup created after an hour starts, unless this backup falls within the definition of a monthly, weekly, or daily backup.

D

Differential backup

A differential backup stores changes to the data against the latest full backup (**Glossary**). You need access to the corresponding full backup to recover the data from a differential backup.

F

Full backup

A self-sufficient backup containing all data chosen for backup. You do not need access to any other backup to recover the data from a full backup.

I

Incremental backup

A backup that stores changes to the data against the latest backup. You need access to other backups to recover data from an incremental backup.

S

Single-file backup format

A new backup format, in which the initial full and subsequent incremental backups are saved to a single .tib file, instead of a chain of files. This format leverages the speed of the incremental backup method, while avoiding its main disadvantage–difficult deletion of outdated backups. The software

marks the blocks used by outdated backups as "free" and writes new backups to these blocks. This results in extremely fast cleanup, with minimal resource consumption.

The single-file backup format is not available when backing up to locations that do not support random-access reads and writes, for example, SFTP servers.