

Acronis

acronis.com

Acronis Cyber Protect 15

Update 6



User Guide

REVISION: 3/5/2024

Table of contents

Acronis Cyber Protect 15 editions	17
Supported Cyber Protect features by operating system	17
Licensing	21
License types	21
Licensing in Acronis Cyber Protect 15 Update 3 and later	21
Types of management servers	22
Acronis account, local and cloud consoles	23
Managing licenses	25
Licensing in Acronis Cyber Protect 15 Update 2 and earlier	40
Adding license keys to a management server	41
Managing subscription licenses	41
Managing perpetual licenses	42
Installation	44
Installation overview	44
On-premises deployment	44
Cloud deployment	45
Components	47
Agents	47
Other components	50
Using Acronis Cyber Protect with other security solutions in your environment	52
Limitations	52
Software requirements	52
Supported web browsers	52
Supported operating systems and environments	53
Supported Microsoft SQL Server versions	61
Supported Microsoft Exchange Server versions	61
Supported Microsoft SharePoint versions	61
Supported Oracle Database versions	62
Supported SAP HANA versions	62
Supported virtualization platforms	62
Linux packages	70
Compatibility with encryption software	74
Compatibility with Dell EMC Data Domain storages	75
System requirements	76
Supported file systems	78

Network connection diagram for Acronis Cyber Protect	81
Network connection diagram - Cyber Protect processes	82
On-premises deployment	85
Installing the management server	85
Required user rights for the service logon account	88
Database for Scan Service	93
Adding machines from the Cyber Protect web console	108
Installing agents locally	117
Unattended installation or uninstallation	121
Common parameters	123
Management server installation parameters	126
Agent installation parameters	127
Storage node installation parameters	128
Catalog service installation parameters	128
Registering and unregistering machines manually	135
Checking for software updates	140
Migrating the management server	141
Cloud deployment	146
Activating the account	146
Preparation	146
Configuring proxy server settings	149
Installing agents	153
Unattended installation or uninstallation	157
Basic parameters	159
Registration parameters	160
Additional parameters	161
Basic parameters	165
Registration parameters	166
Additional parameters	166
Information parameters	167
Parameters for legacy features	168
Registering and unregistering machines manually	171
Deploying Agent for oVirt (Virtual Appliance)	174
Deploying Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance)	175
Autodiscovery of machines	175
Prerequisites	175
How autodiscovery works	175

Autodiscovery and manual discovery	177
Managing discovered machines	181
Troubleshooting	181
Deploying Agent for VMware (Virtual Appliance) from an OVF template	183
Before you start	183
Deploying the OVF template	184
Configuring the virtual appliance	184
Deploying Agent for Scale Computing HC3 (Virtual Appliance)	186
Before you start	186
Deploying the virtual appliance	187
Configuring the virtual appliance	187
Agent for Scale Computing HC3 – required roles	192
Deploying agents through Group Policy	192
Prerequisites	192
Step 1: Generating a registration token	193
Step 2: Creating the .mst transform and extracting the installation package	193
Step 3: Setting up the Group Policy objects	193
Updating virtual appliances	194
On-premises deployments	194
Cloud deployment	195
Updating agents	195
Updating agents on BitLocker-protected workloads	196
Upgrading to Acronis Cyber Protect 15	197
Uninstalling the product	197
In Windows	198
In Linux	198
In macOS	198
Removing Agent for VMware (Virtual Appliance)	198
Removing machines from the Cyber Protect web console	199
Accessing the Cyber Protect web console	200
On-premises deployment	200
In Windows	200
In Linux	201
Cloud deployment	201
Changing the language	201
Configuring a web browser for Integrated Windows Authentication	201
Adding the console to the list of local intranet sites	202

Adding the console to the list of trusted sites	204
Allowing only HTTPS connections to the web console	207
Adding a custom message to the web console	208
Prerequisites	208
SSL certificate settings	211
Using a self-signed certificate	211
Using a certificate issued by a trusted certificate authority	212
Cyber Protect web console view	216
Protection plan and modules	218
Creating a protection plan	218
Resolving plan conflicts	220
Applying several plans to a device	220
Resolving plan conflicts	220
Operations with protection plans	221
Backup	223
Backup module cheat sheet	225
Limitations	230
Selecting data to back up	231
Selecting entire machine	231
Selecting disks/volumes	231
Selecting files/folders	234
Selecting ESXi configuration	236
Continuous data protection (CDP)	237
Selecting a destination	242
Supported locations	243
Advanced storage options	244
About Secure Zone	245
About Acronis Cyber Infrastructure	248
Schedule	249
When backing up to cloud storage	250
When backing up to other locations	250
Additional scheduling options	251
Schedule by events	252
Start conditions	255
Retention rules	261
What else you need to know	262
Encryption	262

Encryption in a protection plan	263
Encryption as a machine property	263
How the encryption works	264
Notarization	264
How to use notarization	265
How it works	265
Conversion to a virtual machine	265
Conversion methods	266
What you need to know about conversion	266
Conversion to a virtual machine in a protection plan	267
How regular conversion to VM works	268
Replication	269
Usage examples	270
Supported locations	270
Considerations for users with the Advanced license	271
Starting a backup manually	272
Backup options	272
Availability of the backup options	272
Alerts	275
Backup consolidation	276
Backup file name	276
Backup format	280
Backup validation	282
Changed block tracking (CBT)	282
Cluster backup mode	283
Compression level	284
Email notifications	284
Error handling	285
Fast incremental/differential backup	286
File filters	287
File-level backup snapshot	289
Forensic data	289
Log truncation	297
LVM snapshotting	297
Mount points	298
Multi-volume snapshot	299
One-click recovery	299

Performance and backup window	300
Physical Data Shipping	304
Pre/Post commands	305
Pre/Post data capture commands	306
SAN hardware snapshots	309
Scheduling	309
Sector-by-sector backup	310
Splitting	310
Tape management	310
Task failure handling	315
Task start conditions	315
Volume Shadow Copy Service (VSS)	316
Volume Shadow Copy Service (VSS) for virtual machines	317
Weekly backup	317
Windows event log	318
Recovery	319
Recovery cheat sheet	319
Safe recovery	320
How it works	320
Creating bootable media	321
Recovering a machine	322
Recovering a physical machine	322
Recovering a physical machine to a virtual machine	324
Recovering a virtual machine	326
Recovery with restart	328
Recovering disks and volumes by using bootable media	329
Using Universal Restore	331
Recovering files	333
Recovering files by using the web interface	333
Downloading files from the cloud storage	335
Verifying file authenticity with Notary Service	335
Signing a file with ASign	336
Recovering files by using bootable media	337
Extracting files from local backups	338
Recovering system state	338
Recovering ESXi configuration	338
Recovery options	339

Availability of the recovery options	339
Backup validation	341
Boot mode	342
Date and time for files	343
Error handling	343
File exclusions	344
File-level security	344
Flashback	344
Full path recovery	345
Mount points	345
Performance	345
Pre/Post commands	345
Tape management	347
SID changing	347
VM power management	348
Windows event log	348
Power on after recovery	348
Disaster recovery	349
Operations with backups	350
The Backup storage tab	350
Mounting volumes from a backup	351
Requirements	351
Usage scenarios	351
Validating backups	352
Exporting backups	353
Deleting backups	354
The Plans tab	355
Off-host data processing	355
Backup scanning plans	356
Backup replication	356
Validation	357
Cleanup	359
Conversion to a virtual machine	360
Bootable media	362
Bootable media	362
Create a bootable media or download a ready-made one?	362
Linux-based or WinPE-based bootable media?	364

Linux-based	364
WinPE-based	364
Bootable Media Builder	364
Why use the media builder?	365
32- or 64-bit?	365
Linux-based bootable media	366
Top-level object	374
Variable object	374
Control type	376
WinPE-based bootable media	381
Connecting to a machine booted from media	387
Configuring network settings	387
Local connection	388
Remote connection	388
Registering media on the management server	388
Registering the media from the media UI	388
Local operations with bootable media	389
Setting up a display mode	390
Backup with bootable media on-premises	390
Recovery with bootable media on-premises	399
Disk management with bootable media	406
Simple Volume	422
Spanned Volume	422
Striped Volume	422
Mirrored Volume	423
Mirrored-Striped Volume	423
RAID-5	423
Remote operations with bootable media	430
Configuring iSCSI devices	432
Startup Recovery Manager	433
Activating Startup Recovery Manager	434
Deactivating Startup Recovery Manager	434
Acronis PXE Server	434
Installing Acronis PXE Server	435
Setting up a machine to boot from PXE	435
Work across subnets	436
Protecting mobile devices	437

Supported mobile devices	437
What you can back up	437
What you need to know	437
Where to get the backup app	438
How to start backing up your data	438
How to recover data to a mobile device	439
How to review data via the Cyber Protect web console	439
Protecting Microsoft applications	441
Protecting Microsoft SQL Server and Microsoft Exchange Server	441
Protecting Microsoft SharePoint	441
Protecting a domain controller	441
Recovering applications	442
Prerequisites	442
Common requirements	443
Additional requirements for application-aware backups	443
Database backup	444
Selecting SQL databases	444
Selecting Exchange Server data	445
Protecting Always On Availability Groups (AAG)	446
Protecting Database Availability Groups (DAG)	448
Application-aware backup	450
Why use application-aware backup?	450
What do I need to use application-aware backup?	450
Required user rights for application-aware backup	451
Mailbox backup	452
Selecting Exchange Server mailboxes	453
Required user rights	453
Recovering SQL databases	453
Recovering system databases	456
Attaching SQL Server databases	456
Recovering Exchange databases	457
Mounting Exchange Server databases	459
Recovering Exchange mailboxes and mailbox items	459
Recovery to an Exchange Server	460
Recovery to Microsoft 365	460
Recovering mailboxes	461
Recovering mailbox items	462

Copying Microsoft Exchange Server libraries	465
Changing the SQL Server or Exchange Server access credentials	465
Protecting Microsoft 365 mailboxes	467
Why back up Microsoft 365 mailboxes?	467
Recovery	467
Limitations	468
Adding a Microsoft 365 organization	468
Obtaining application ID and application secret	468
Changing the Microsoft 365 access credentials	470
Selecting mailboxes	470
Recovering mailboxes and mailbox items	470
Recovering mailboxes	470
Recovering mailbox items	471
Protecting Google Workspace data	473
Protecting Oracle Database	474
Special operations with virtual machines	475
Running a virtual machine from a backup (Instant Restore)	475
Usage examples	475
Prerequisites	475
Running the machine	476
Deleting the machine	477
Finalizing the machine	477
Working in VMware vSphere	478
Replication of virtual machines	478
LAN-free backup	484
Using SAN hardware snapshots	487
Using a locally attached storage	492
Virtual machine binding	492
Support for VM migration	495
Managing virtualization environments	495
Viewing backup status in vSphere Client	496
Agent for VMware – necessary privileges	497
Backing up clustered Hyper-V machines	501
High Availability of a recovered machine	501
Limiting the total number of simultaneously backed-up virtual machines	502
Machine migration	504
Windows Azure and Amazon EC2 virtual machines	505

Network requirements	506
Protecting SAP HANA	507
Antimalware and web protection	508
Antivirus & Antimalware protection	508
Real-time protection scan	508
On-demand malware scan	509
Antivirus & Antimalware protection settings	509
Active Protection	516
Windows Defender Antivirus	516
Schedule scan	517
Default actions	517
Real-time protection	518
Advanced	518
Exclusions	519
Microsoft Security Essentials	519
URL filtering	519
How it works	520
URL filtering settings	522
Quarantine	528
How do files get into the quarantine folder?	528
Managing quarantined files	528
Quarantine location on machines	528
Corporate whitelist	529
Automatic adding to the whitelist	529
Manual adding to the whitelist	529
Adding quarantined files to the whitelist	529
Whitelist settings	529
Viewing details about items in the whitelist	530
Antimalware scan of backups	530
Limitations	531
Protection of collaboration and communication applications	532
Vulnerability assessment and patch management	533
Vulnerability assessment	533
Supported Microsoft and third-party products	534
Supported Linux products	535
Vulnerability assessment settings	535
Vulnerability assessment for Windows machines	537

Vulnerability assessment for Linux machines	537
Managing found vulnerabilities	538
Patch management	539
How it works	539
Patch management settings	540
Managing list of patches	543
Automatic patch approval	544
Manual patch approval	547
On-demand patch installation	547
Patch lifetime in the list	548
Smart protection	549
Threat feed	549
How it works	549
Deleting all alerts	551
Data protection map	551
How it works	551
Managing the detected unprotected files	552
Data protection map settings	552
Remote desktop access	555
Remote access (RDP and HTML5 clients)	555
How it works	556
How to connect to a remote machine	558
Sharing a remote connection	558
Remote wipe	560
Device groups	561
Built-in groups	561
Custom groups	561
Creating a static group	562
Adding devices to static groups	562
Creating a dynamic group	562
Search query	563
Operators	572
Applying a protection plan to a group	573
Monitoring and reporting	574
The Overview dashboard	574
Cyber Protection	575
Protection status	576

Disk health monitoring	576
Data protection map	580
Vulnerability assessment widgets	581
Patch installation widgets	581
Backup scanning details	582
Recently affected	582
No recent backups	582
The Activities tab	584
Reports	586
Configuring the severity of alerts	589
Alerts configuration file	589
Advanced storage options	591
Tape devices	591
What is a tape device?	591
Overview of tape support	591
Getting started with a tape device	597
Tape management	602
Storage nodes	612
Installing a storage node and a catalog service	612
Adding a managed location	614
Deduplication	616
Location encryption	618
Cataloging	619
System settings	622
Email notifications	622
Email server	623
Security	623
Log out inactive users after	624
Show notification about the last login of the current user	624
Warn about local or domain password expiration	624
Updates	624
Default backup options	624
Protection settings	626
Updating the protection definitions	626
Agents with the Updater role	626
Scheduling the updates	627
Changing the download location	628

Cache storage options	629
Source of the latest protection definitions	629
Remote connection	629
Updating the protection definitions in an air-gapped environment	630
Downloading the definitions to an online management server	630
Transferring the definitions to an HTTP server	632
Configuring the source of definitions on the air-gapped management server	632
Administering user accounts and organization units	634
On-premises deployment	634
Units and administrative accounts	634
Adding administrative accounts	637
Creating units	638
Cloud deployment	638
Quotas	638
Notifications	640
Reports	641
Command-line reference	642
Troubleshooting	643
Glossary	644
Index	646

Copyright statement

© Acronis International GmbH, 2003-2024. All rights reserved.

All trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at <https://kb.acronis.com/content/7696>

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Acronis Cyber Protect 15 editions

Acronis Cyber Protect 15 is available in the following editions:

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

For detailed information about the features included in each edition, refer to [Acronis Cyber Protect 15 Editions Comparison including Cloud deployment](#).

All editions of Acronis Cyber Protect 15 are licensed by the number of protected workloads and their type (workstation, server, and virtual host). Cyber Protect editions are only available with subscription licenses. Cyber Backup editions are available both with subscription and perpetual licenses. For more information about the available options, refer to "Licensing" (p. 21).

Perpetual license keys for version 15 cannot be used with backup agents from Acronis Cyber Backup 12.5. However, these agents will continue working with their old license keys, even when their management server is upgraded to version 15.

Backup subscription licenses can be used with version 12.5 agents, even when the agents are upgraded to version 15. Cyber Protect subscription licenses can be used only by version 15 agents.

Version 12.5 backup agents that are registered on a version 15 management server cannot perform off-host data processing operations, such as backup replication, backup validation, cleanup, or conversion to a virtual machine.

Note

The features vary between different editions. Some of the features described in this documentation may be unavailable with your license. For detailed information about the features included in each edition, refer to [Acronis Cyber Protect 15 Editions Comparison including Cloud deployment](#).

Supported Cyber Protect features by operating system

The Cyber Protect features are supported on the following operating systems:

- Windows: Windows 7 and later, Windows Server 2008 R2 and later.
Windows Defender Antivirus management is supported on Windows 8.1 and later.
- Linux: CentOS 7.x, CentOS 8.0, VirtuoZZo 7.x, Acronis Cyber Infrastructure 3.x.
Other Linux distributions and versions might also support the Cyber Protect features, but have not been tested.
- macOS: 10.13.x and later (only Antivirus & Antimalware protection is supported).

Important

The Cyber Protect features are only supported for machines on which a protection agent is installed. For virtual machines protected in agentless mode, for example by Agent for Hyper-V, Agent for VMware, or Agent for Scale Computing, only backup is supported.

Cyber Protect features	Windows	Linux	macOS
Forensic backup	Yes	No	No
Continuous data protection (CDP)			
CDP for files and folders	Yes	No	No
CDP for changed files via application tracking	Yes	No	No
Autodiscovery and remote installation			
Network-based discovery	Yes	No	No
Active Directory-based discovery	Yes	No	No
Template-based discovery (importing machines from a file)	Yes	No	No
Manual adding of devices	Yes	No	No
Acronis Anti-malware protection			
Ransomware detection based on process behavior (AI-based)	Yes	No	No
Cryptomining processes detection	Yes	No	No
Real-time antimalware protection	Yes	No	Yes
Automatic recovery of affected files from the local cache	Yes	No	No
Self-protection for Acronis backup files	Yes	No	No
Self-protection for Acronis software	Yes	No	No
Static analysis for portable executable files	Yes	No	Yes*
External drives protection (HDD, flash drives, SD cards)	Yes	No	No
Network folder protection	Yes	No	No

Server-side protection	Yes	No	No
Protection of Zoom, WebEx, Microsoft Teams, and other remote work protection	Yes	No	No
On-demand antimalware scanning	Yes	No	Yes
Scan archive files	Yes	No	Yes
File/folder exclusions	Yes	No	Yes**
Processes exclusions	Yes	No	No
Corporate-wide whitelist	Yes	No	Yes
Behavior detection	Yes	No	No
Quarantine	Yes	No	Yes
URL filtering (http/https)	Yes	No	No
Windows Defender Antivirus management	Yes	No	No
Microsoft Security Essentials management	Yes	No	No
Vulnerability assessment			
Vulnerability assessment of operating system and its native applications	Yes	Yes***	No
Vulnerability assessment for third-party applications	Yes	No	No
Patch management			
Patch auto-approval	Yes	No	No
Manual patch installation	Yes	No	No
Automatic patch installation scheduling	Yes	No	No
Fail-safe patching: backup of machine before installing patches as part of a protection plan	Yes	No	No
Cancellation of a machine restart if a backup is running	Yes	No	No
Data protection map			
Scanning machines to find unprotected files	Yes	No	No

Unprotected locations overview	Yes	No	No
Protective action in Data protection map	Yes	No	No
Disk health			
AI-based HDD and SSD health control	Yes	No	No
Smart protection plans based on Acronis Cyber Protection Operations Center (CPOC) alerts			
Threat feed	Yes	No	No
Remediation wizard	Yes	No	No
Backup scanning			
Scanning of encrypted backups	Yes	No	No
Scanning of disk backups in the local storage, network shares, and Acronis Cloud Storage	Yes	No	No
Safe recovery			
Antimalware scanning with Acronis Antivirus & Antimalware protection during the recovery process	Yes	No	No
Remote desktop			
Connection via HTML5 based client	Yes	No	No
Connection via native Windows RDP client	Yes	No	No
Remote wipe	Yes****	No	No
Cyber Protect Monitor	Yes	No	Yes

* On macOS, static analysis for portable executable files is only supported for scheduled scans.

** On macOS, you can only use exclusions to specify files and folders that will not be scanned by real-time protection or scheduled scans.

*** The vulnerability assessment depends on the availability of official security advisories for specific distribution, for example <https://lists.centos.org/pipermail/centos-announce>, <https://lists.centos.org/pipermail/centos-cr-announce>, and others.

**** Remote wipe is only available for machines running Windows 10 or later.

Licensing

To protect a workload by using Acronis Cyber Protect, you need a license. A license is not required for installing Acronis Cyber Protect.

License types

Acronis Cyber Protect is available with subscription licenses. Within the validity period, which starts from the date of purchase, unlimited updates and free technical support are available. After the validity period ends, the existing protection plans stop working and new protection plans cannot be created.

Renewals for the legacy perpetual licenses are available. Some features, such as cloud deployment or cloud-to-cloud backups are not available with a perpetual license.

A trial license is also available. It provides you access to all product features for 30 days from the license activation.

For more details about the different licensing options, refer to [Acronis Cyber Protect 15: licensing and upgrade/downgrade FAQ](#) in our knowledge base. The Acronis licensing policy is available at <https://www.acronis.com/company/licensing.html>.

Important

Acronis Cyber Protect 15 Update 3 introduced a new licensing model. It requires license registration and activation of the on-premises management servers.

Licensing in Acronis Cyber Protect 15 Update 3 and later

In Acronis Cyber Protect 15 Update 3 and later, no license keys are added in the local console of the management server (<https://<IP address of your management server>:<port>>).

Instead, you add the licenses to your account in Acronis Customer Portal (<https://account.acronis.com>), and then you manage your licenses in Acronis Cyber Protect cloud console (<https://cloud.acronis.com>).

License management of offline management servers requires operations both in the local and cloud consoles.

To learn more about the local and cloud consoles, refer to "Acronis account, local and cloud consoles" (p. 23).

To start using a management server with Acronis Cyber Protect 15 Update 3 and later

1. Add one or more licenses to your account in Acronis Customer Portal (<https://account.acronis.com>).
Licenses that you purchased online are automatically added to this account.
2. [For the on-premises deployment mode] Activate your management server.
3. Allocate a license to the management server.

Types of management servers

Depending on your deployment mode, you can use the following types of management servers:

- Cloud management server
- On-premises management server
 - Online management server
 - Offline management server

You can have more than one management server in your Acronis account. You can also use a mixed deployment mode with a cloud management server and on-premises management server.

If you use multiple management servers, you can split a license quota between them. For more information on how to do that, refer to "Transferring license quota to another management server" (p. 33).

Cloud management server

With cloud deployment, you do not install and maintain a management server in your network. You use a management server that is already deployed in an Acronis data center and you only need to install protection agents for your workloads.

The cloud management server does not need activation. It is always online and the licensing information is automatically synchronized between the server and your Acronis account.

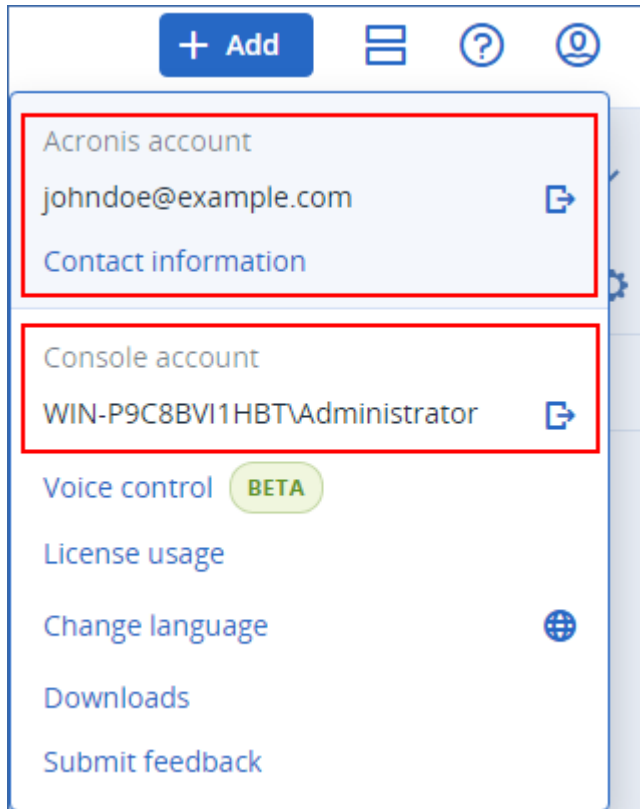
On-premises management server

With on-premises deployment, you install both the management server and the protection agents in your network. You can have an offline management server that is not connected to the Internet or an online management server that has access to the Internet.

On-premises management servers require activation. For more information about the activation, refer to "Activating a management server" (p. 27).

Note

Two different accounts are shown in the local console of an activated on-premises management server: the Acronis account, which is used to sync the licensing information; and the console account, which is used for accessing the local console itself.



Online on-premises management server

You activate an online management server via the Internet, by signing in to your Acronis account when you access the local console for the first time.

Offline on-premises management server

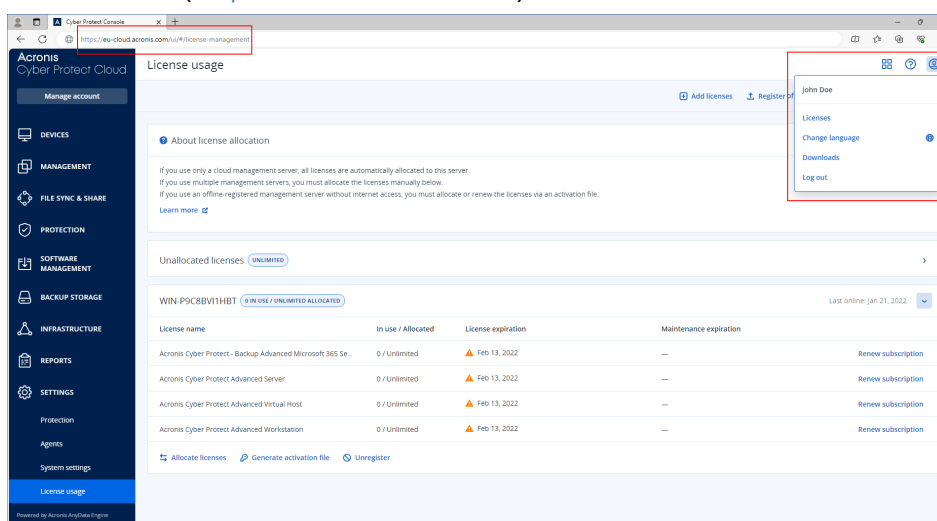
You activate an offline management server and sync its licensing information to your Acronis account manually, through a file.

Acronis account, local and cloud consoles

To use Acronis Cyber Protect and to manage your licenses and their usage, you need an Acronis account. All your licenses and management servers are registered to that account.

With this account, you access the following consoles:

- Cloud console (<https://cloud.acronis.com>)

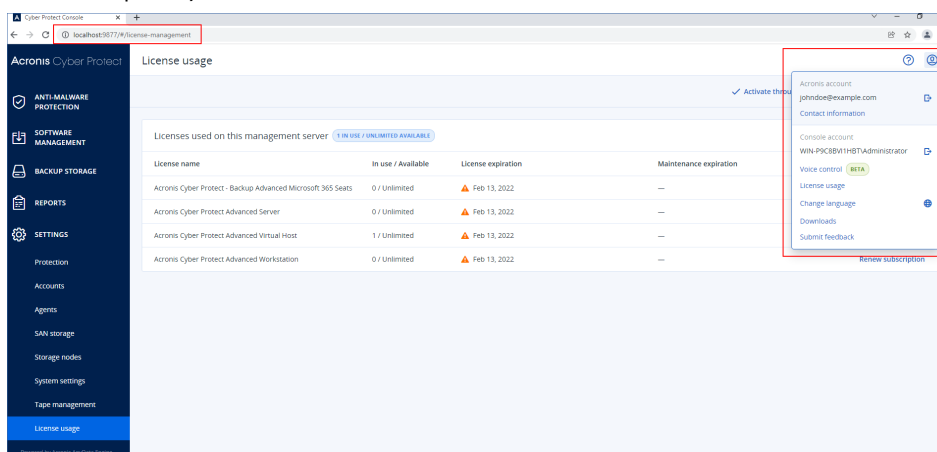


Note

After you log in to the cloud console, its URL changes and shows the exact data center to which your account belongs. For example, <https://eu-cloud.acronis.com> or <https://jp-cloud.acronis.com>.

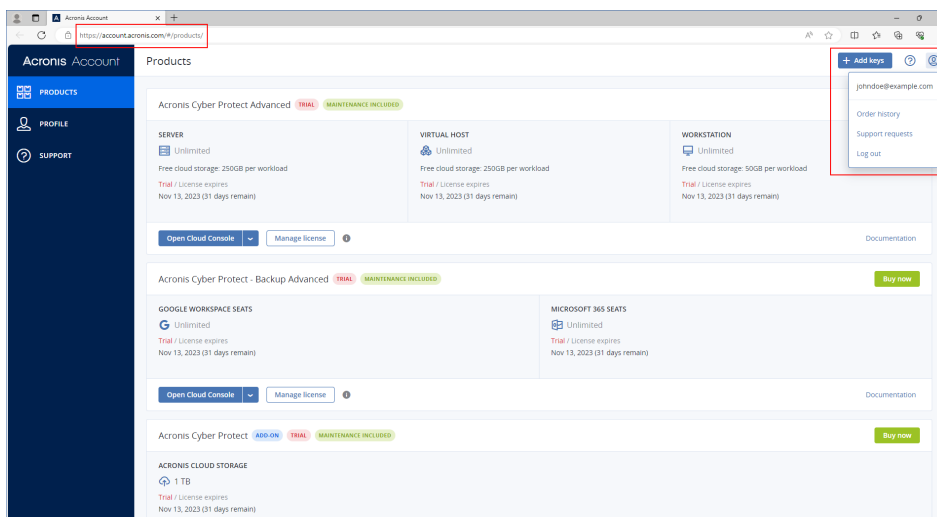
The cloud console is the main location where you manage your licenses. Here, on the **Settings** > **License usage** tab, you can allocate available licenses and license quota to a specific management server, reallocate license quotas to another management server, or finalize the registration of an offline management server.

- Local console of an on-premises management server (<https://<IP address of your management server>:<port>>)



Here, you can check the allocated licenses, their quota and usage, and their expiration date. You use the local console, along with the cloud console, when you activate an offline management server or allocate licenses to it.

- Acronis Customer Portal (<https://account.acronis.com>)



In Acronis Customer Portal, you can manage your purchased products, for example, by checking the expiration date of your subscriptions, adding new license keys, registering license renewals, or requesting an upgrade. You can also contact the Support team, download the product installation files, and access the product documentation.

Managing licenses

The table below summarizes the available operations and shows where to perform them.

Operation	Location
Adding licenses to your account	You add licenses in Acronis Customer Portal (https://account.acronis.com). Licenses that you purchased online are automatically added there.
Activating a management server	<p>You activate a management server by registering it in your account.</p> <p>You activate online management servers in their local console (<a href="https://<IP address of your management server>:<port>">https://<IP address of your management server>:<port>), by signing in to your Acronis account.</p> <p>The activation of an offline management server requires operations both in the local and the cloud consoles.</p>
Allocating licenses to a management server Modifying an existing license allocation	<p>On online management servers, you allocate licenses by using the cloud console (https://cloud.acronis.com). The allocated licenses are automatically synced to the management server.</p> <p>On offline management servers, you allocate licenses through an activation file. This procedure requires that you use both the local console of the management server (<a href="https://<IP address of your management server>:<port>">https://<IP address of your management server>:<port>) and the cloud console (https://cloud.acronis.com).</p>
Assigning licenses to workloads	This operation is automatic.
Unregistering a	You unregister online management servers by using the cloud console

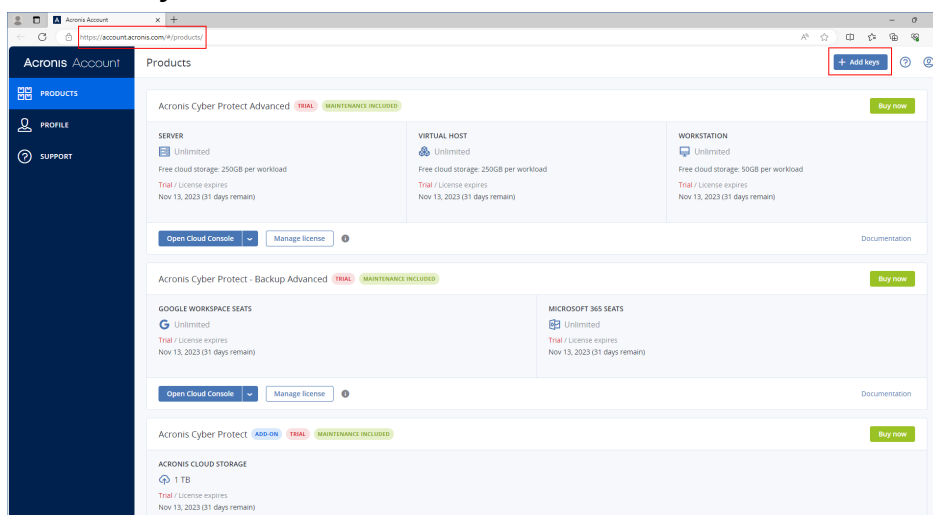
Operation	Location
management server from your account	<p>(https://cloud.acronis.com).</p> <p>You unregister offline management servers through a deactivation file. This procedure requires that you use both the local console of the offline management server (<a href="https://<IP address of your management server>:<port>">https://<IP address of your management server>:<port>) and the cloud console (https://cloud.acronis.com).</p> <p>To unregister an offline management server to which you do not have access, you use only the cloud console.</p>

Adding licenses to your Acronis account

To use a license, you must add it to your Acronis account. Licenses that you purchased online are automatically added to your account. You must manually add the licenses that you purchased offline.

To add a license in your Acronis account

1. Log in to Acronis Customer Portal (<https://account.acronis.com>) by using your Acronis account credentials.
2. In the navigation menu, click **Products**.
3. Click **Add keys**.



4. Enter one or more license keys, one per line, and then click **Add**.

Note

You can enter up to 100 license keys at a time.

The licenses are now added to your account and you can manage their usage in the cloud console (<https://cloud.acronis.com>).

Important

Before upgrading to Acronis Cyber Protect 15 Update 3, export your locally stored perpetual licenses to a file, and then add them to your Acronis account.

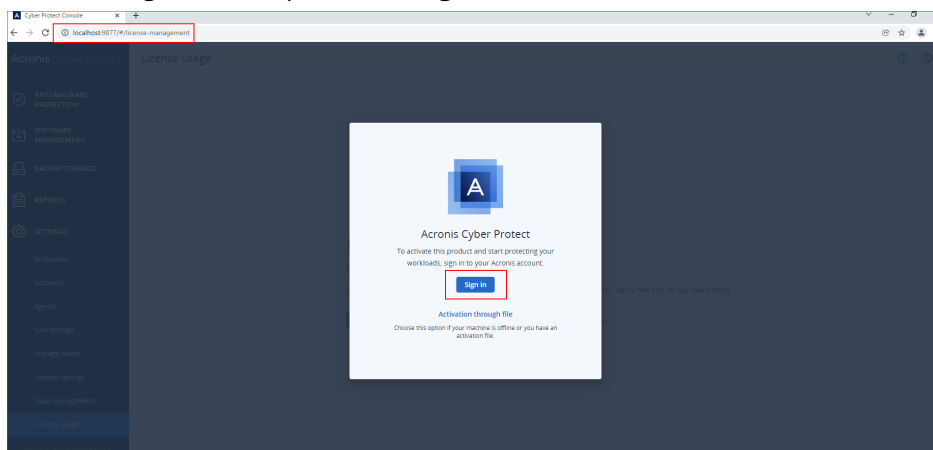
To check the license keys that you entered locally on a management server, go to `https://<IP address of your management server>:<port>/api/account_server/v2/licensing/legacy/license_keys`.

Activating a management server

You activate a management server by registering it in your Acronis account.

To activate an online management server

1. After installing Acronis Cyber Protect management server, open its local console (`https://<IP address of your management server>:<port>`).
2. In the dialog box that opens, click **Sign in**.



3. Sign in to your Acronis account.

As a result, the management server is automatically registered and activated.

To start protecting your workloads, allocate at least one license to this server. For more information on how to allocate a license, refer to "Allocating licenses to a management server" (p. 30).

Note

Online management servers require Internet access to sync the licensing information to your Acronis account. If such a server stays offline for more than 30 days, its protection plans will stop working and your workloads will become unprotected.

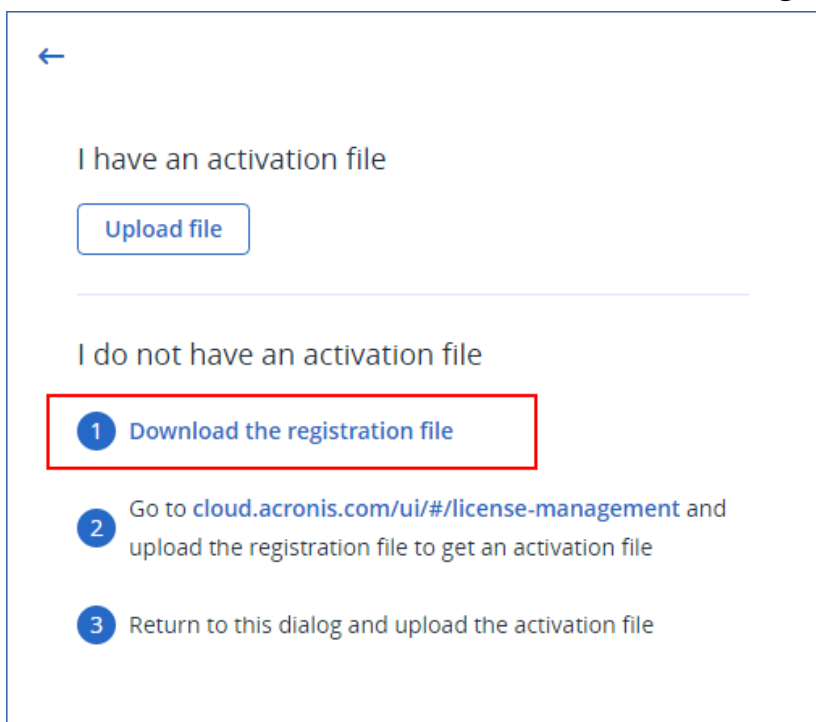
If you sign out from your Acronis account in the local console, the licensing information cannot be synced. If you do not sign in again within 30 days, the protection plans will stop working and your workloads will become unprotected.

To activate an offline management server

The activation of an offline management server requires operations both in the local and the cloud consoles.

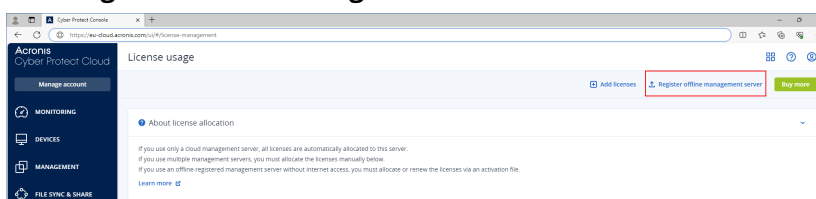
To access the cloud console, you need a second machine that is connected to the Internet.

1. After installing Acronis Cyber Protect management server, open its local console (<https://<IP address of your management server>:<port>>).
2. In the dialog box that opens, click **Activation through file**.
3. Under **I do not have an activation file**, click **Download the registration file**.



The registration file is downloaded to your machine.

4. On a machine with access to the Internet, log in to the cloud console (<https://cloud.acronis.com>), and then go to **Settings > License usage**.
5. Click **Register offline management server**.



6. In the dialog box that opens, click **Browse**, and then select the registration file that you downloaded from your offline management server.
 7. In the dialog box that opens, click **Download file**.
- An activation file is downloaded to your machine.

Important

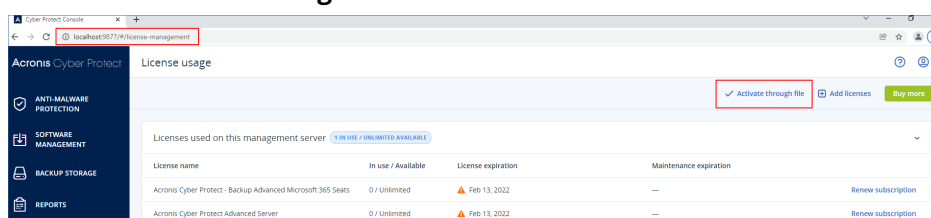
If this offline management server is the only management server in your environment, the licenses in your Acronis account will be automatically allocated to it. The activation file will contain this information, so no additional allocation is required.

If this is not the only management server in your environment, after the activation, you must allocate licenses by following the procedure in "Allocating licenses to a management server" (p. 30).

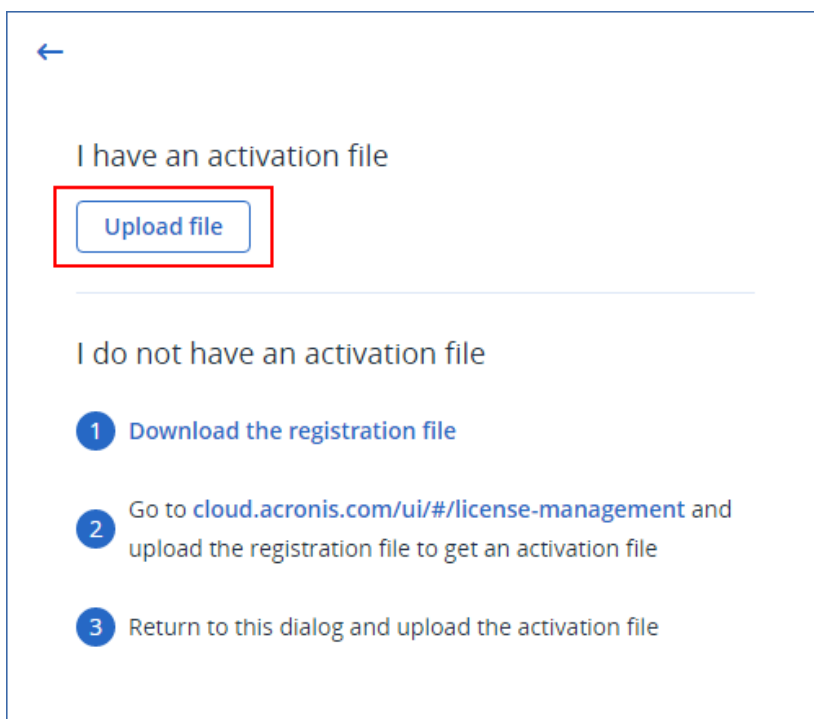
8. In the local console of the offline management server (<https://<IP address of your management server>:<port>>), go to the **Activation through file** dialog box.

Note

If the **Activation through file** dialog box is not open, navigate to **Settings > License usage**, and then click **Activate through file**.



9. Under **I have an activation file**, click **Upload file**, and then select the activation file that you downloaded from the cloud console.



As a result, the offline management server is registered in your Acronis account and activated.

Note

You might not be able to activate a management server that runs on a virtual machine which UUID is not unique. The UUID of a virtual machine might be duplicated when you clone it or convert it with VMware vCenter Converter, for example. If you face a similar issue, contact our Support team.

For more information on how to prevent UUID duplication on VMware virtual machines, refer to [Editing a virtual machine with a duplicate UUID.bios \(1002403\)](#).

Allocating licenses to a management server

To use a license, you must allocate its quota or a share of its quota to a management server. You can allocate more than one license to a management server. Also, you can split the license quota and allocate different shares of the quota to different management servers.

Note

If there is only one management server in your Acronis account, all your licenses are automatically allocated to this server. To learn how to reallocate licenses to another management server, refer to "Transferring license quota to another management server" (p. 33).

If you have more than one management server in your Acronis account, the new licenses are shown under **Unallocated licenses** in the cloud console (<https://cloud.acronis.com>). You need to allocate these licenses manually.

All operations with licenses are automatically synced to the online management servers. To sync an allocation change to an offline management server, create a new activation file, and then repeat the allocation procedure. To learn more about the different management servers, refer to "Types of management servers" (p. 22).

To allocate licenses to an online management server

1. In the cloud console (<https://cloud.acronis.com>), click **Settings > License usage**.
2. Navigate to the management server that you want to allocate a license to.
3. Click **Allocate licenses**.
4. In the dialog box that opens, specify the license and the license quota that you want to allocate to this server.
5. Click **Save**.

As a result, the licensing information is automatically synced to the management server and you can use the allocated license to protect your workloads.

To modify the allocation, repeat the procedure above.

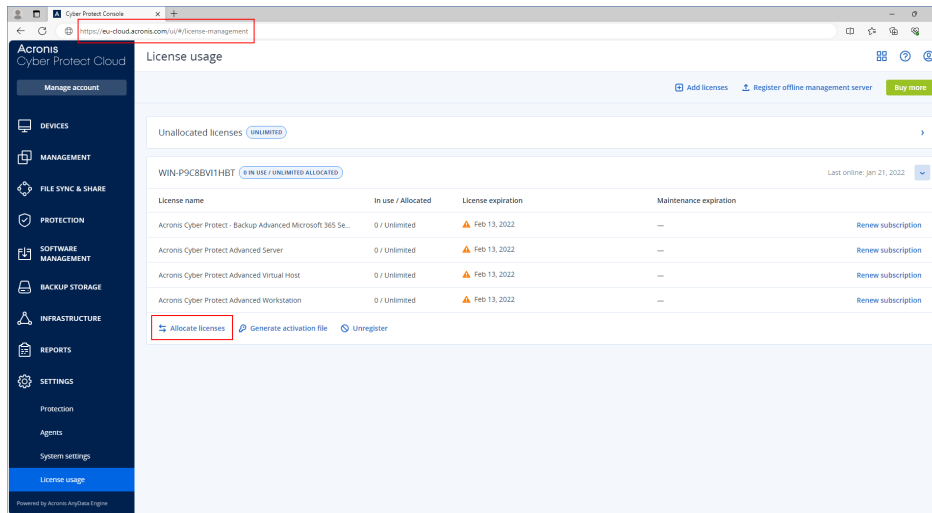
Important

If the modified license quota is smaller than the number of protection agents, the least-loaded agents will stop working. This selection is automatic. If it does not fit your needs, reassign the available licenses manually.

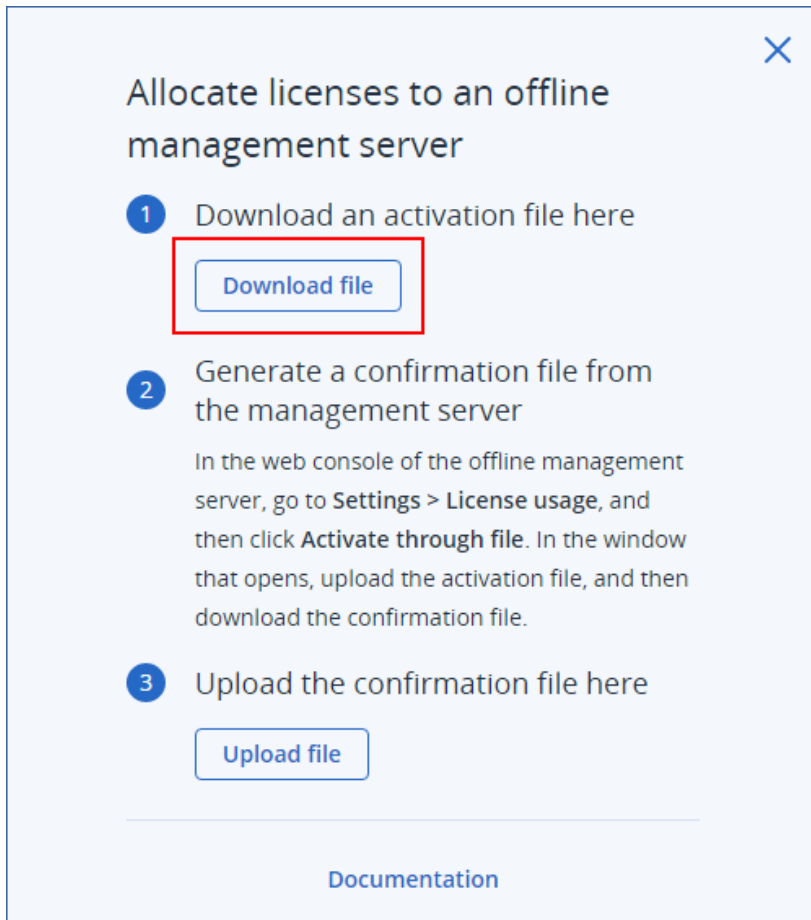
To allocate licenses to an offline management server

To allocate licenses to an offline management server, you need to use both the cloud and the local consoles. To access the cloud console, you need a second machine that is connected to the Internet.

1. On a machine with the Internet access, log in to the cloud console (<https://cloud.acronis.com>), and then click **Settings > License usage**.
2. Navigate to the management server that you want to allocate a license to.
3. Click **Allocate licenses**.



4. In the dialog box that opens, specify the license and the license quota that you want to allocate to this server.
5. Click **Save**.
6. In the **Allocate licenses to an offline management server** dialog box, click **Download file**.



The activation file is downloaded to your machine.

7. In the local console of the offline management server (<https://<IP address of your management server>:<port>>), navigate to **Settings > License usage**, and then click **Activate through file**.
8. In the dialog box that opens, under **I have an activation file**, click **Upload file**, and then select the activation file that you downloaded from the cloud console.

The screenshot shows a dialog box with a back arrow in the top left corner. It contains two main sections. The first section is titled "I have an activation file" and features a button labeled "Upload file", which is highlighted with a red rectangular border. The second section is titled "I do not have an activation file" and contains a three-step numbered list: 1. "Download the registration file", 2. "Go to cloud.acronis.com/ui/#/license-management and upload the registration file to get an activation file", and 3. "Return to this dialog and upload the activation file".

As a result, the licensing information is synced between your Acronis account and the offline management server.

To increase the allocated license quota, repeat the procedure above.

To decrease the allocated license quota, refer to "Decreasing the license quota allocated to an offline management server" (p. 34).

Transferring license quota to another management server

You can transfer a license quota from one management server to another. This option may be useful when the licenses allocated to a management server are not used by any workloads and you need more licenses for another management server.

Note

If there is only one management server in your Acronis account, all your licenses are automatically allocated to this server.

If you have more than one management server in your Acronis account, the new licenses are shown under **Unallocated licenses** in the cloud console (<https://cloud.acronis.com>). You need to allocate these licenses manually.

To transfer a license quota to another management server

1. Decrease the license quota that is allocated to the original management server by following the procedure in "Allocating licenses to a management server" (p. 30).

The released license quota appears in the **Unallocated licenses** section in the cloud console.

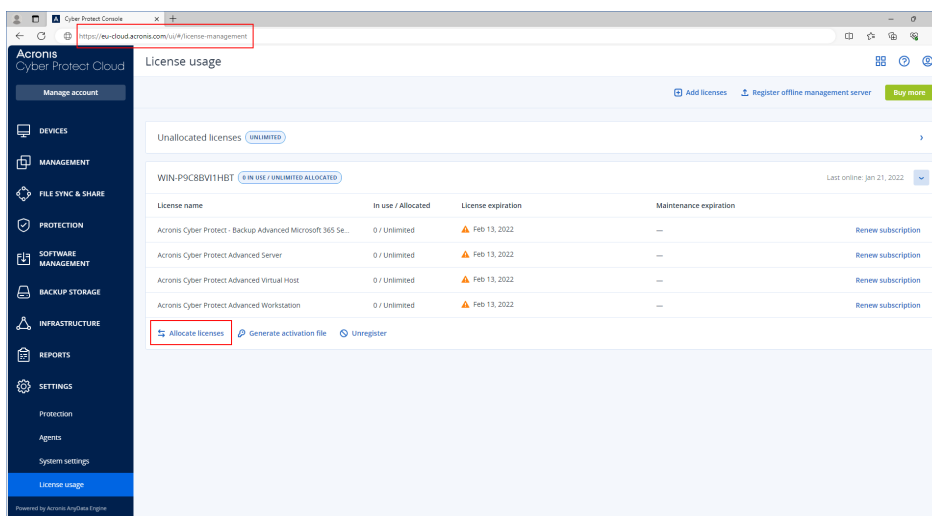
2. Allocate the license quota to the second management server by following the procedure in "Allocating licenses to a management server" (p. 30).

Decreasing the license quota allocated to an offline management server

To decrease the license quota allocated to an offline management server, you need to use both the cloud and the local consoles. To access the cloud console, you need a second machine that is connected to the Internet.

1. On a machine with access to the Internet, log in to the cloud console (<https://cloud.acronis.com>), and then click **Settings > License usage**.
2. Navigate to the management server that you want to allocate a license to, and then click

Allocate licenses.



3. In the dialog box that opens, modify the licenses and the license quota allocated to this server, and then click **Save**.


Allocate licenses to WIN-P9C8BVI1HBT

Licenses	Available	Allocated to server		
Acronis Cyber Protect - Backup Advanced Microsoft ...	Unlimited	—	0	+ <input type="checkbox"/> Unlimited
Acronis Cyber Protect Advanced Server	Unlimited	—	2	+ <input type="checkbox"/> Unlimited
Acronis Cyber Protect Advanced Virtual Host	Unlimited	—	1	+ <input type="checkbox"/> Unlimited
Acronis Cyber Protect Advanced Workstation	Unlimited	—	15	+ <input type="checkbox"/> Unlimited

Cancel
Save

The new allocation is now pending. To cancel it, click **Remove this allocation**.

4. In the **Allocate licenses to an offline management server** dialog box, click **Download file**.



Allocate licenses to an offline management server

- 1 Download an activation file here

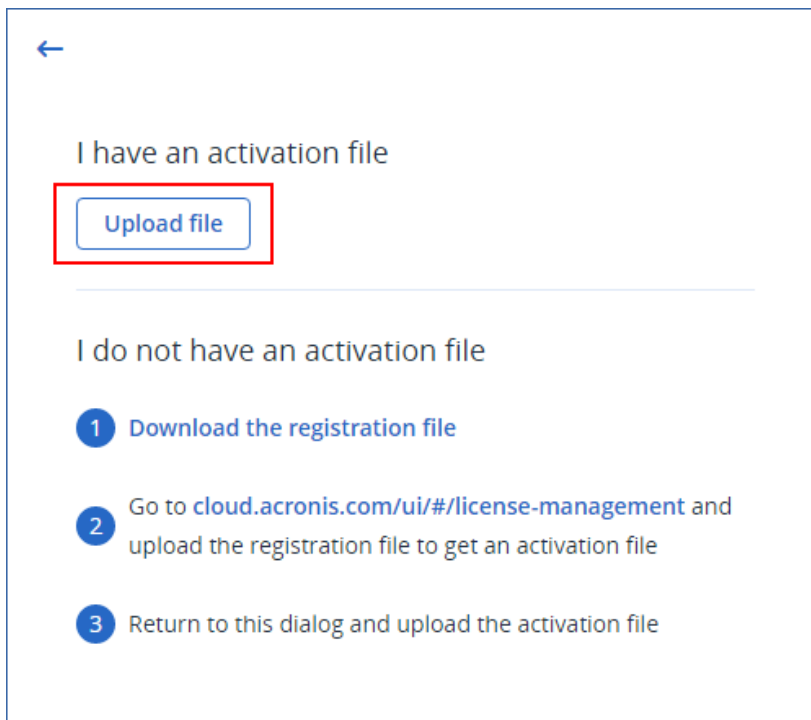
Download file
- 2 Generate a confirmation file from the management server
In the web console of the offline management server, go to **Settings > License usage**, and then click **Activate through file**. In the window that opens, upload the activation file, and then download the confirmation file.
- 3 Upload the confirmation file here

Upload file

[Documentation](#)

The activation file is downloaded to your machine.

5. In the local console of the offline management server (<https://<IP address of your management server>:<port>>), navigate to **Settings > License usage**, and then click **Activate through file**.
6. In the dialog box that opens, under **I have an activation file**, click **Upload file**, and then select the activation file that you downloaded from the cloud console.



A screenshot of a software dialog box. At the top left is a blue back arrow. Below it, the text "I have an activation file" is displayed. Underneath this text is a button labeled "Upload file", which is highlighted with a red rectangular border. A horizontal line separates this section from the section below. The lower section is titled "I do not have an activation file" and contains a three-step numbered list. Each step is preceded by a blue circle containing a white number. The steps are: 1. Download the registration file; 2. Go to cloud.acronis.com/ui/#/license-management and upload the registration file to get an activation file; 3. Return to this dialog and upload the activation file.

←

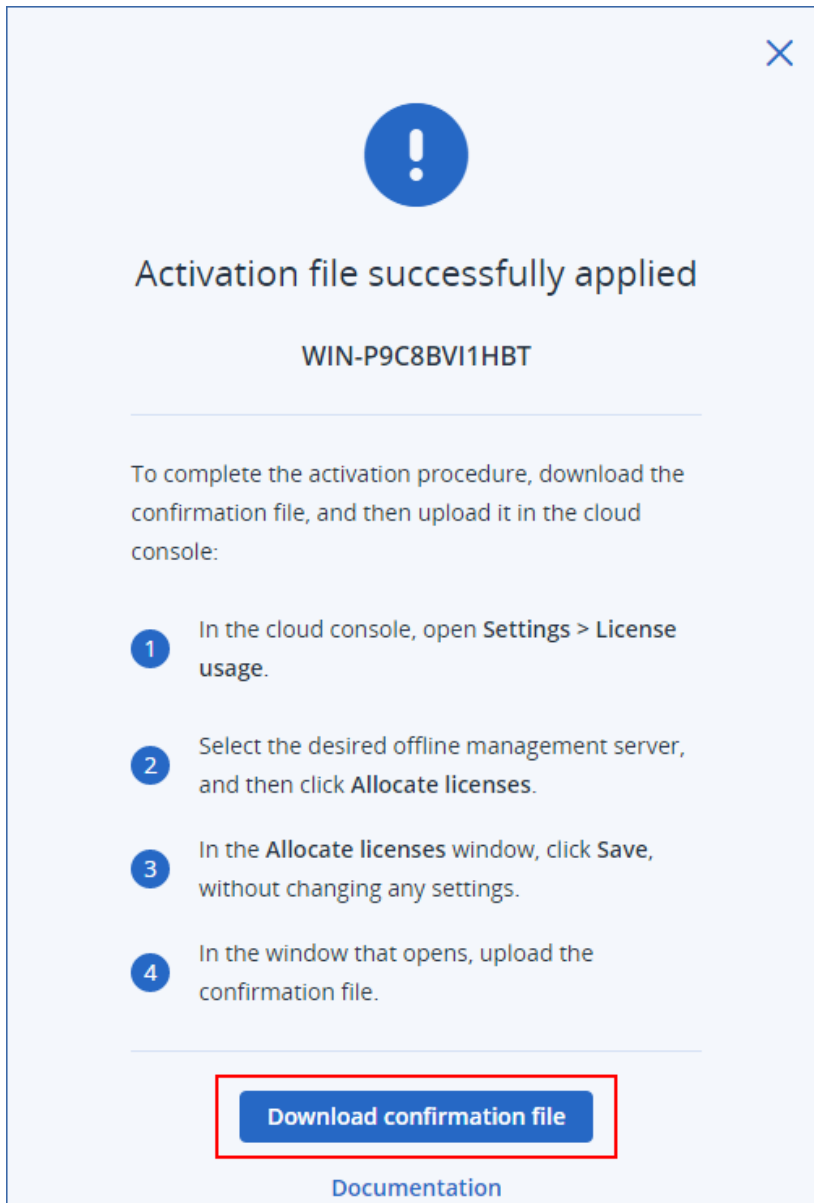
I have an activation file

Upload file

I do not have an activation file

- 1 Download the registration file
- 2 Go to cloud.acronis.com/ui/#/license-management and upload the registration file to get an activation file
- 3 Return to this dialog and upload the activation file

7. In the dialog box that opens, click **Download confirmation file**.



The confirmation file is downloaded to your machine.

8. In the cloud console (<https://cloud.acronis.com>), click **Settings > License usage**.
9. Navigate to the management server that you want to allocate a license to, and then click **Allocate licenses**.
10. In the dialog box that opens, click **Save**, without changing any settings.
11. In the **Allocate licenses to an offline management server** dialog box, click **Upload file**, and then select the confirmation file that you downloaded from your offline management server.

×

Allocate licenses to an offline management server

- 1 Download an activation file here
[Download file](#)
- 2 Generate a confirmation file from the management server
In the web console of the offline management server, go to **Settings > License usage**, and then click **Activate through file**. In the window that opens, upload the activation file, and then download the confirmation file.
- 3 Upload the confirmation file here
[Upload file](#)

[Documentation](#)

As a result, the licensing information is synced between your Acronis account and the offline management server.

Important

If the modified license quota is smaller than the number of protection agents, the least-loaded agents will stop working. This selection is automatic. If it does not fit your needs, reassign the available licenses manually.

Assignment of licenses to workloads

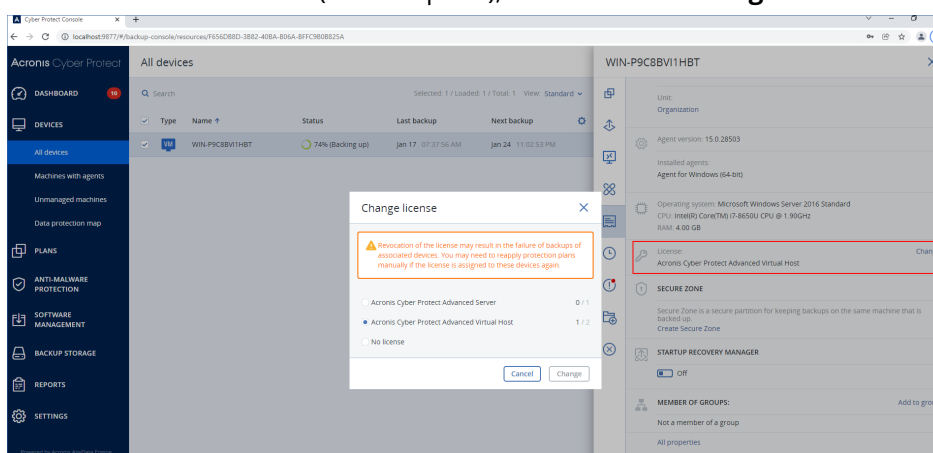
A management server distributes the allocated licenses between the workloads that are registered on this server.

The management server assigns a license to a workload the first time you apply a protection plan to this workload. If more than one license is allocated to the management server, it assigns the workload the most appropriate license, depending on the type of the workload, the operating system, and required level of protection.

To check the assigned license, in the web console of the management server, select the desired workload, and then click **Details**.

To reassign a license to a workload manually

1. In the web console of the management server, click **Devices**, and then select the desired workload.
2. Click **Details**.
3. [For on-premises management servers] Navigate to the **License** section, and then click **Change**.
4. [For cloud management servers] Navigate to the **Service quota** section, and then click **Change**.
5. Select the desired license (service quota), and then click **Change**.



Limitations

For offline management servers, current usage of the license quota is shown only in the local console. Offline management servers do not sync this data to your Acronis account and it is not available in the cloud console.

Known issues

In the cloud console, the license usage or assignment of the **Virtual Host** license might be incorrectly shown. For more information, refer to [this knowledge base article](#).

Unregistering a management server

To unregister an online management server

1. In the cloud console (<https://cloud.acronis.com>), click **Settings** > **License usage**.
2. Navigate to the desired management server, and then click **Unregister**.
3. The **Unregister management server** window is displayed.
4. Enter the email address associated to the account to confirm unregistration.
5. Click **Unregistration**.

As a result, all licenses that were allocated to the unregistered server are released and can be allocated to another management server in your account. In the local console of the unregistered management server, the licenses are reset to zero.

To unregister an offline management server

There are two different entry points to unregister an offline management server:

In local console:

1. In the local console, click **Unregister** on the line where the account is displayed. The **Unregister management server** window is displayed.
2. In the **Login** field, type the email address associated to the local administrator.
3. Click **Unregister**.
4. The **Unregistration is successful** pop up screen is displayed.
5. Click **Download unregistration file**.
6. In the cloud console, click **Unregister**. The **Unregister management server** window is displayed.
7. Click **Unregister offline management server**. The **Unregister offline management server** window is displayed.
8. Click **Browse**, and then select the unregistration file that you downloaded from the local console.
9. Click **Unregister**.

In cloud console:

1. On a machine with Internet access, log in to the cloud console (<https://cloud.acronis.com>), and then click **Settings > License usage**.
2. Navigate to the desired management server, and then click **Unregister**. The **Unregister management server** window is displayed.
3. Click **Unregister offline management server**. The **Unregister offline management server** window is displayed.
4. In the local console of the management server that you want to unregister (<https://<IP address of your management server>:<port>>), go to **Settings > License usage**, and then click **Unregister**. The unregistration file is downloaded to your machine.
5. In the cloud console, go back to the **Unregister offline management server** window.
6. Click **Browse**, and then select the unregistration file that you downloaded from the local console.
7. Click **Unregister**.
8. Alternatively, if you do not have access to the machine on which the management server is installed, click **I don't have access to the machine with the management server**.

Warning!

This machine will be permanently blocked and removed from your account. You will not be able to register the management server on it again.

As a result, all licenses that were allocated to the unregistered server are released and can be allocated to another management server in your account. In the local console of the unregistered management server, the licenses are reset to zero.

Licensing in Acronis Cyber Protect 15 Update 2 and earlier

To start using Acronis Cyber Protect version 15 Update 2 and earlier, you need to add at least one license key to the management server. A license is automatically assigned to a machine when a

protection plan is applied.

Licenses can also be assigned and revoked manually. Manual operations with licenses are available only to organization administrators. For more information about the administrators, refer to "Units and administrative accounts" (p. 634).

Adding license keys to a management server

In Acronis Cyber Protect 15 Update 2 and earlier, you add the license keys to the management server.

To add license keys to a management server

1. In the Cyber Protect web console, go to **Settings > Licenses**.
2. Click **Add keys**.
3. Enter one or more license keys, one key per line.
4. Click **Add**.
5. [When adding subscription license keys] To activate a subscription license, sign in to your Acronis account.
 - a. In the sign-in form, enter the credentials that you use for Acronis Customer Portal (<https://account.acronis.com>), and then click **Sign in**.
 - b. Confirm your account, and then click **Sync**.
 - c. After the operation completes, click **Done**.
6. In the **Add license keys** panel, click **Done**.

Note

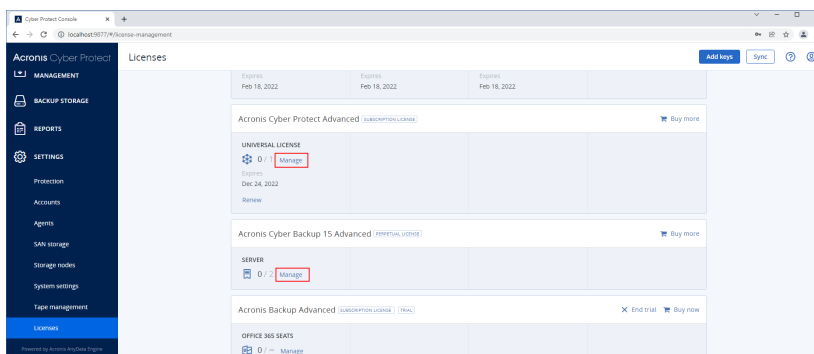
You can automatically import the subscription license keys that are registered in your Acronis account, instead of adding them to the management server again. To import the license keys, in the **Add license keys** panel, click **Sync with Acronis account**, and then sign in to your Acronis account.

Managing subscription licenses

Before assigning a license to a workload, you must add the license key to the management server. For more information on how to do it, refer to "Adding license keys to a management server" (p. 41).

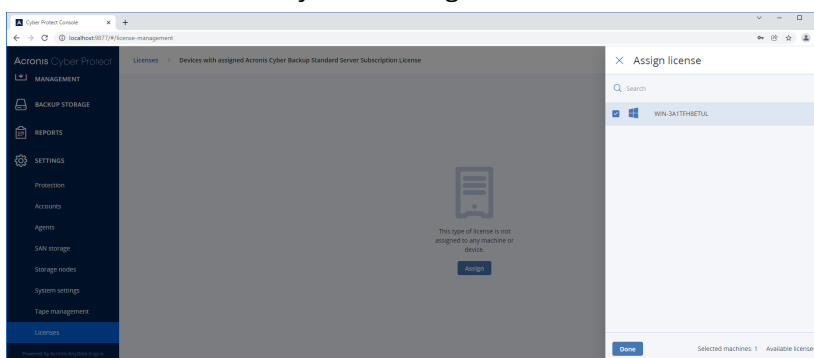
To assign a subscription license to a workload

1. In the Cyber Protect web console, go to **Settings > Licenses**.
2. Navigate to the desired license, and then click **Manage**.



3. Click **Assign**.

The workloads to which you can assign this license are shown.



4. Select a workload, and then click **Done**.

To revoke a subscription license from a workload

1. In the Cyber Protect web console, go to **Settings > Licenses**.
2. Navigate to the desired license, and then click **Manage**.
3. Select the workload from which you want to revoke the license.
4. Click **Revoke**.
5. Confirm your decision.

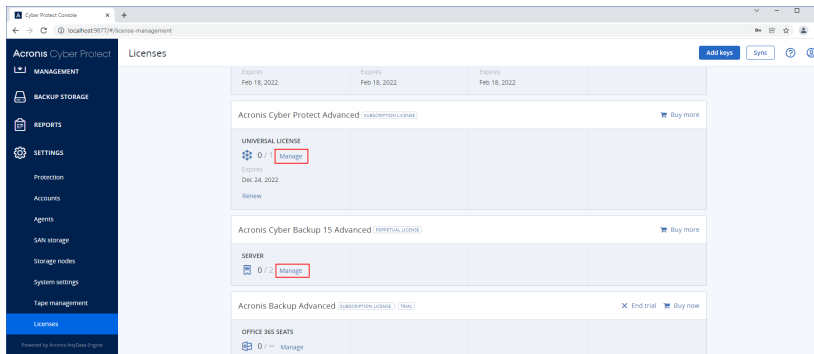
The revoked license is released and you can assign it to another workload.

Managing perpetual licenses

Before assigning a license to a workload, you must add the license key to the management server. For more information on how to do it, refer to "Adding license keys to a management server" (p. 41).

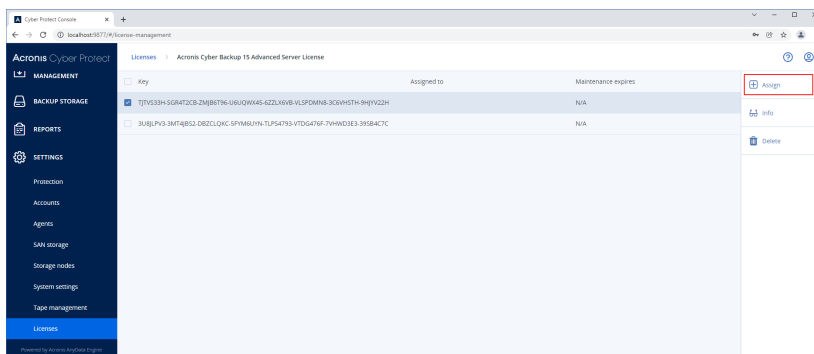
To assign a perpetual license to a workload

1. In the Cyber Protect web console, go to **Settings > Licenses**.
2. Navigate to the desired license, and then click **Manage**.



The license keys that correspond to the selected license are shown.

3. Select the license key that you want to assign to a workload.
4. Click **Assign**.



The workloads to which you can assign this license key are shown.

5. Select a workload, and then click **Done**.

To revoke a perpetual license from a workload

1. In the Cyber Protect web console, go to **Settings > Licenses**.
2. Select the desired license, and then click **Manage**.

The license keys that correspond to the selected license are shown. Check the workload to which this license key is assigned in the **Assigned to** column.

3. Select the license key that you want to revoke.
4. Click **Revoke**.
5. Confirm your decision.

The revoked license key remains in the license list and you can assign it to another workload.

Installation

Installation overview

Acronis Cyber Protect supports two methods of deployment: on-premises and cloud. The main difference between them is the location of the Acronis Cyber Protect management server.

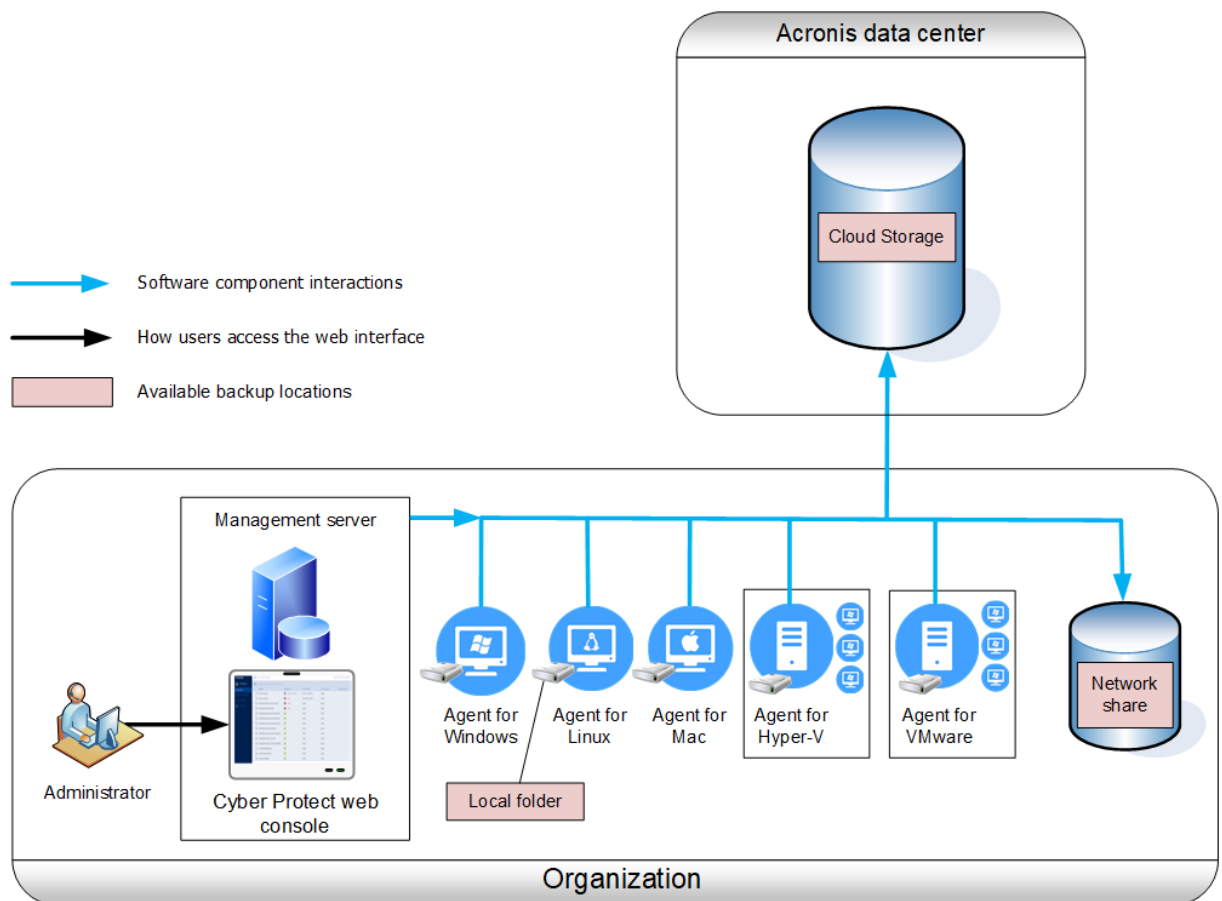
The management server is the central point for managing all of your backups. With the on-premises deployment, it is installed in your local network; with the cloud deployment, it is located in one of the Acronis data centers. The web interface to this server is named a Cyber Protect web console.

The management server is responsible for the communication with the protection agents and performs general plan management functions. Before every protection activity, agents refer to the management server to verify the prerequisites. Sometimes, the connection to the management server could be lost, which will prevent the deployment of new protection plans. However, if a protection plan has already been deployed to a machine, the agent continues the protection operations for 30 days after the communication with the management server is lost.

Both types of deployment require that a protection agent is installed on each machine that you want to back up. The supported types of storage are also the same. The cloud storage space is sold separately from the Acronis Cyber Protect licenses.

On-premises deployment

On-premises deployment means that all of the product components are installed in your local network. This is the only deployment method available with a perpetual license. Also, you have to use this method if your machines are not connected to the Internet.



Management server location

You can install the management server on a machine running either Windows or Linux.

Installation in Windows is recommended because you will be able to deploy agents to other machines from the management server. With the Advanced license, it is possible to create organizational units and add administrators to them. This way, you can delegate protection management to other people whose access permissions will be strictly limited to the corresponding units.

Installation in Linux is recommended in a Linux-only environment. You will need to install an agent locally on the machines that you want to back up.

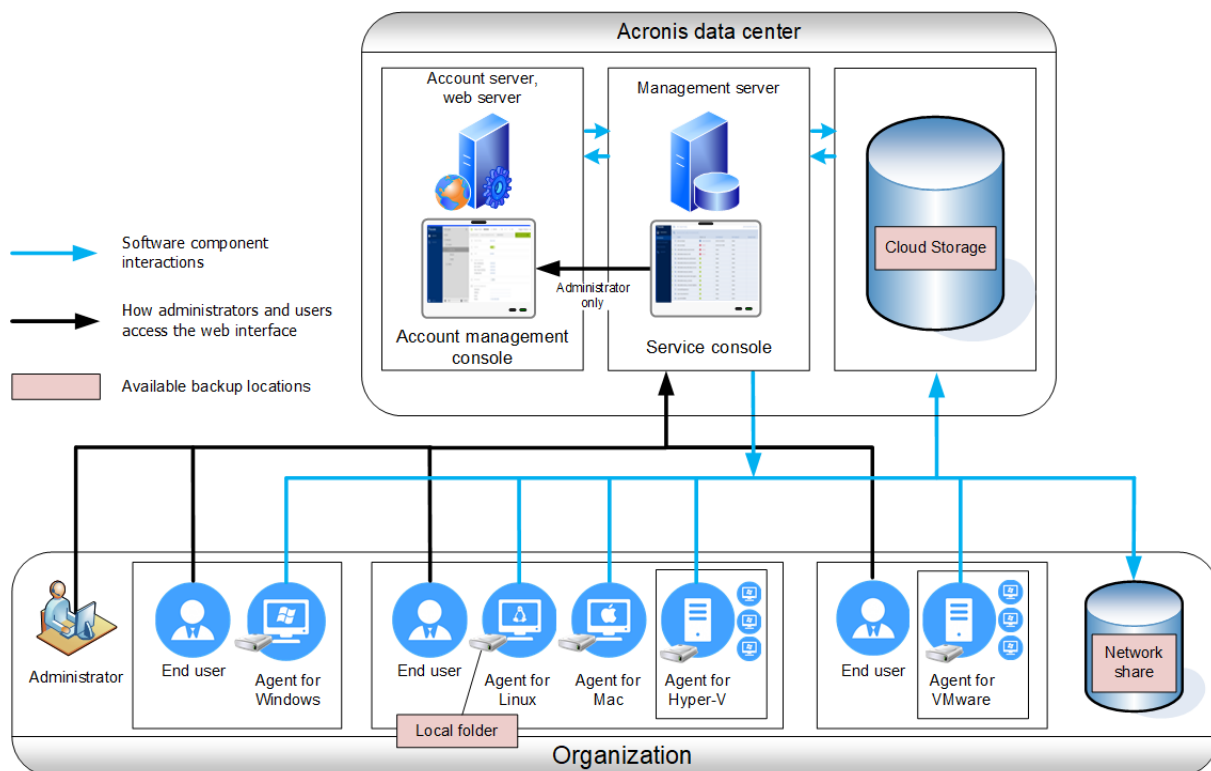
Cloud deployment

Cloud deployment means that the management server is located in one of the Acronis data centers. The benefit of this approach is that you do not need to maintain the management server in your local network. You can think of Acronis Cyber Protect as of a cyber protection service provided to you by Acronis.

Access to the account server enables you to create user accounts, set service usage quotas for them, and create groups of users (units) to reflect the structure of your organization. Every user can

access the Cyber Protect web console, download the required agent, and install it on their machines in minutes.

Administrator accounts can be created at the unit or organization level. Each account has a view scoped to their area of control. Users have access only to their own backups.



The following table summarizes differences between the on-premises and cloud deployments. Each column lists the features that are available only in the corresponding type of deployment.

On-premises deployment	Cloud deployment
<ul style="list-style-type: none"> • Perpetual licenses can be used • On-premises management server that can be used in air-gapped environments* • SFTP server as a backup location • Acronis Cyber Infrastructure as a backup location • Tape devices and Acronis Storage Nodes as backup locations** • Upgrade from previous versions of Acronis Cyber Protect, including Acronis Backup for VMware 	<ul style="list-style-type: none"> • Cloud-to-cloud backup of Microsoft 365 data, including protection of groups, public folders, OneDrive*** and SharePoint Online data • Cloud-to-cloud backup of Google Workspace data • Agent for Mac supports both x64 and ARM-based processors, such as Apple silicon M1 and M2 • Agent for Virtuozzo (backup of Virtuozzo virtual machines at the hypervisor level) • Agent for oVirt (backup of oVirt KVM virtual machines at the hypervisor level) • Agent for Virtuozzo Hybrid Infrastructure (backup of Virtuozzo Hybrid Infrastructure virtual machines at the hypervisor level) • Disaster recovery as a cloud service****

* For more information about activating the management server in an air-gapped environment, refer to "To activate an offline management server" (p. 27).

** The feature is not available in the Standard edition.

***The OneDrive root folder is excluded from backup operations by default. If you select to back up specific OneDrive files and folders, they will be backed up. Files that are not available on the device will have invalid contents in the archive.

**** The feature is available only with the Disaster Recovery add-on.

Components

Agents

Agents are applications that perform data backup, recovery, and other operations on the machines managed by Acronis Cyber Protect.

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.

Some agents can be installed only on machines with specific roles or applications, for example, Agent for Hyper-V is installed on machines running the Hyper-V role, Agent for SQL – on machines running SQL databases, Agent for Exchange – on machines running the Mailbox role of Microsoft Exchange Server, and Agent for Active Directory – on domain controllers.

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

What are you going to back up?	Which agent to install?	Where to install it?	Agent availability	
			On-premises	Cloud
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		+	+
Disks, volumes, and files on physical	Agent for Mac		+	+

machines running macOS				
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.	+	+ No mailbox backup
Microsoft 365 mailboxes	Agent for Office 365	On a Windows machine that is connected to the Internet.	+	+
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.	+	+
Hyper-V virtual machines	Agent for Hyper-V	On the Hyper-V host.	+	+
Scale Computing HC3 virtual machines	Agent for Scale Computing HC3	On the Scale Computing HC3 host.	+	+
Virtual machines hosted on Windows Azure	The same as for physical machines***	On the machine that will be backed up.	+	+
Virtual machines hosted on Amazon EC2			+	+
Citrix XenServer virtual machines			+****	+
Red Hat Virtualization (RHV/RHEV) virtual machines				
Kernel-based Virtual Machines (KVM)				
Oracle virtual machines				
Nutanix AHV virtual machines				
Mobile devices				
Mobile devices running Android	Mobile app for Android	On the mobile device that will be backed up.	-	+
Mobile devices running iOS	Mobile app for iOS		-	+

*During the installation, Agent for Exchange checks for enough free space on the machine where it will run. Free space equal to 15 percent of the biggest Exchange database is temporarily needed during a granular recovery.

**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"](#).

***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. Nevertheless, the machine is counted as virtual when you set quotas for the number of machines in a cloud deployment.

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

Other components

Component	Function	Where to install it?	Availability	
			On-premises	Cloud
Management Server	Management Server is the central point for managing all of your backups. With the on-premise deployment, it is installed in your local network. It manages the agents and 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.	+	-
Scan Service	Optional component that enables antimalware scan of backups in a cloud storage, or in a local or network folder. Scan Service requires Microsoft SQL Server or PostgreSQL database. It is not compatible with the default SQLite database that the management server uses.	On the Windows or Linux machine running the management server.	+	-
Bootable Media	Creates bootable	On a machine running	+	-

Builder	media.	Windows or Linux.		
Command-Line Tool	Supports the command-line interface with the acrocmbd utility. acrocmbd does not contain any tools that physically execute the commands. It only provides the command-line interface to Cyber Protect components - agents and the management server.	On a machine running Windows, Linux, or macOS.	+	+
Acronis Cyber Protect 15 Monitor	Provides graphical user interface for Agent for Windows and Agent for Mac. It shows information about the protection status of the machine on which the agent is installed, and allows its users to configure the backup encryption and proxy server settings. In Windows, Acronis Cyber Protect 15 Monitor requires that Agent for Windows is installed on the same machine.	On a machine running Windows or macOS.	+	+
Storage Node	Stores backups. It is required for cataloging and deduplication. Storage Node requires that Agent for Windows is installed on the same machine.	On a machine running Windows.	+	-
Catalog Service	Performs cataloging of backups on storage	On a machine running Windows.	+	-

	nodes.			
PXE Server	Enables booting machines into bootable media through the network.	On a machine running Windows.	+	-

Using Acronis Cyber Protect with other security solutions in your environment

You can use Acronis Cyber Protect with or without other security solutions, such as stand-alone antivirus software, in your environment.

Without another security solution, you can use Acronis Cyber Protect for complete cyber protection or for traditional backup and recovery, depending on your license and your needs. For more information about the features available with each license, refer to "[Acronis Cyber Protect 15 Editions Comparison including Cloud deployment](#)." You can adjust the scope of your [protection plans](#) by enabling only the modules that you need.

You can choose Acronis Cyber Protect for complete cyber protection, including protection against viruses and other malware, even if you already have another security solution in your environment. In this case, you need to disable or remove the other security solution, in order to avoid conflicts.

Alternatively, you might want to enhance your cyber protection without disabling or removing your current security solution. This is also possible – just ensure that you do not use the Antivirus and antimalware module in your protection plans. All other modules can be used freely.

Limitations

- [Antimalware scan of backups](#) requires that you install Scan Service when installing Cyber Protect Management Server.
- [Remote access via HTML5 client](#) is only available if Cyber Protect Management Server is installed on a machine running Linux.

Software requirements

Supported web browsers

The web interface supports the following web browsers:

- Google Chrome 29 or later
- Mozilla Firefox 23 or later
- Opera 16 or later

- Microsoft Edge 25 or later
- Safari 8 or later running in macOS or iOS

In other web browsers (including Safari browsers running in other operating systems), the user interface might be displayed incorrectly or some functions may be unavailable.

Supported operating systems and environments

Agents

Agent for Windows

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86).

Note

You can install the agent only on Windows XP machines with NTFS-formatted drives.

- Windows XP Professional SP2 (x86) – supported with a special version of Agent for Windows. For details and limitations of this support, refer to "Agent for Windows XP SP2" (p. 60).
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 and later – Standard and Enterprise editions (x86, x64)

Note

Acronis Cyber Protect requires the KB940349 update from Microsoft, which cannot be downloaded separately anymore. To ensure that the functionality originally provided by KB940349 is available on your machine, install all currently available updates for Windows Server 2003.

For more information on KB940349, refer to [this knowledge base article](#).

- Windows Small Business Server 2003/2003 R2
- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation, and Web editions (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – all editions (x86, x64)

Note

To use Acronis Cyber Protect with Windows 7, you must install the following updates from Microsoft:

- Windows 7 Extended Security Updates (ESU)
- KB4474419
- KB4490628

For more information on the required updates, refer to [this knowledge base article](#).

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation, and Web editions

- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server

Agent for SQL, Agent for Exchange (for database backup and application-aware backup), Agent for Active Directory

Each of these agents can be installed on a machine running any operating system listed above and a supported version of the respective application, with the following exception:

- Agent for SQL is not supported for on-premises deployment on Windows 7 Starter and Home editions (x86, x64)

Agent for Exchange (for mailbox backup)

This agent can be installed on a machine with or without Microsoft Exchange Server.

- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation, and Web editions (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – all editions
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation, and Web editions
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – Home, Pro, Education, and Enterprise editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server

Agent for Office 365

- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation, and Web editions (x64 only)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation, and Web editions
- Windows Home Server 2011
- Windows Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions (x64 only), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (x64 only)
- Windows 10 – Home, Pro, Education, and Enterprise editions (x64 only)
- Windows Server 2016 – all installation options (x64 only), except for Nano Server
- Windows Server 2019 – all installation options (x64 only), except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server

Agent for Oracle

- Windows Server 2008R2 – Standard, Enterprise, Datacenter, and Web editions (x86, x64)
- Windows Server 2012R2 – Standard, Enterprise, Datacenter, and Web editions (x86, x64)
- Linux – any kernel and distribution supported by Agent for Linux (listed below)

Agent for Linux

Note

The following Linux distributions and kernel versions have been specifically tested. However, even if your Linux distribution or kernel version is not listed below, it may still work correctly in all required scenarios, due to the specifics of the Linux operating systems.

If you encounter issues while using Acronis Cyber Protect with your combination of Linux distribution and kernel version, contact the Support team for further investigation.

Linux with kernel from 2.6.9 to 5.19 and glibc 2.3.4 or later, including the following x86 and x86_64 distributions:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

Important

Configurations with Btrfs are not supported for SUSE Linux Enterprise Server 12 and SUSE Linux Enterprise Server 15.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5* – both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

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`

If your Linux distribution does not support the D-Bus mechanism (for example, Red Hat Enterprise Linux 6.x or CentOS 6.x) Acronis Cyber Protect will use the default location for storing secure keys because the operating system does not provide D-Bus compatible location.

* Supported only with kernels from 4.18 to 5.19

Agent for Mac

Note

ARM-based processors, such as Apple silicon M1 and M2, are supported only with the cloud deployment. They are not supported with the on-premises deployment. For more information about the differences between the cloud and on-premises deployment, see "Installation overview" (p. 44).

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12

- macOS Ventura 13
- macOS Sonoma 14

Agent for VMware (Virtual Appliance)

This agent is delivered as a virtual appliance for running on an ESXi host.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Agent for VMware (Windows)

This agent is delivered as a Windows application for running in any operating system listed above for Agent for Windows with the following exceptions:

- 32-bit operating systems are not supported.
- Windows XP, Windows Server 2003/2003 R2, and Windows Small Business Server 2003/2003 R2 are not supported.

Agent for Hyper-V

- Windows Server 2008 (x64 only) with Hyper-V role, including Server Core installation mode
- Windows Server 2008 R2 with Hyper-V role, including Server Core installation mode
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 with Hyper-V role, including Server Core installation mode
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (x64 only) with Hyper-V
- Windows 10 – Pro, Education, and Enterprise editions with Hyper-V
- Windows Server 2016 with Hyper-V role – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 with Hyper-V role – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022 with Hyper-V – all installation options, except for Nano Server

Agent for Scale Computing HC3 (Virtual Appliance)

This agent is delivered as a virtual appliance that is deployed in the Scale Computing HC3 cluster via the Cyber Protect web console. There is no stand-alone installer for this agent.

Scale Computing Hypercore 8.8, 8.9, 9.0

Management Server (for on-premises deployment only)

In Windows

- Windows 7 – all editions (x86, x64)

Note

To use Acronis Cyber Protect with Windows 7, you must install the following updates from Microsoft:

- Windows 7 Extended Security Updates (ESU)
- KB4474419
- KB4490628

For more information on the required updates, refer to [this knowledge base article](#).

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, and Foundation editions
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server

In Linux

Note

The following Linux distributions and kernel versions have been specifically tested. However, even if your Linux distribution or kernel version is not listed below, it may still work correctly in all required scenarios, due to the specifics of the Linux operating systems.

If you encounter issues while using Acronis Cyber Protect with your combination of Linux distribution and kernel version, contact the Support team for further investigation.

Linux with kernel from 2.6.9 to 5.19 and glibc 2.3.4 or later, including the following x86_64 distributions.

x86 distributions are not supported.

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

Important

Configurations with Btrfs are not supported for SUSE Linux Enterprise Server 12 and SUSE Linux Enterprise Server 15.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

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`

If your Linux distribution does not support the D-Bus mechanism (for example, Red Hat Enterprise Linux 6.x or CentOS 6.x) Acronis Cyber Protect will use the default location for storing secure keys because the operating system does not provide D-Bus compatible location.

* Supported only with kernels from 4.18 to 5.19

Storage Node (for on-premises deployment only)

- Windows Server 2008 – Standard, Enterprise, Datacenter, and Foundation editions (x64 only)
- Windows Small Business Server 2008
- Windows 7 – all editions (x64 only)
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, and Foundation editions
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions (x64 only), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016

- Windows 10 – Home, Pro, Education, Enterprise, and IoT Enterprise editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server
- Windows Server 2022 – all installation options, except for Nano Server

Agent for Windows XP SP2

Agent for Windows XP SP2 supports only the 32-bit version of Windows XP SP2.

To protect machines running Windows XP SP1 (x64), Windows XP SP2 (x64), or Windows XP SP3 (x86), use the regular Agent for Windows.

Agent for Windows XP SP2 requires an Acronis Cyber Backup 12.5 license. Acronis Cyber Protect 15 license keys are not supported.

Installation

Agent for Windows XP SP2 requires at least 550 MB of disk space and 150 MB of RAM. While backing up, the agent typically consumes about 350 MB of memory. The peak consumption may reach 2 GB, depending on the amount of data being processed.

Agent for Windows XP SP2 can be installed only locally on the machine that you want to back up. To download the agent setup program, click the account icon in the top-right corner, and then click **Downloads > Agent for Windows XP SP2**.

Cyber Protect Monitor and Bootable Media Builder cannot be installed. To download the bootable media ISO file, click the account icon in the top-right corner > **Downloads > Bootable media**.

Update

Agent for Windows XP SP2 does not support the remote update functionality. To update the agent, download the new version of the setup program, and then repeat the installation.

If you updated Windows XP from SP2 to SP3, uninstall Agent for Windows XP SP2, and then install the regular Agent for Windows.

Limitations

- Only disk-level backup is available. Individual files can be recovered from a disk or volume backup.
- [Schedule by events](#) is not supported.
- [Conditions for protection plan execution](#) are not supported.
- Only the following backup destinations are supported:
 - Cloud storage
 - Local folder
 - Network folder
 - Secure Zone

- The **Version 12** backup format and the features that require the **Version 12** backup format are not supported. In particular, [physical data shipping](#) is not available. The **Performance and backup window** option, if enabled, applies only the green-level settings.
- Selection of individual disks/volumes for recovery and manual disk mapping during a recovery are not supported in the web interface. This functionality is available under bootable media.
- [Off-host data processing](#) is not supported.
- Agent for Windows XP SP2 cannot perform the following operations with backups:
 - [Converting backups to a virtual machine](#)
 - [Mounting volumes from a backup](#)
 - [Extracting files from a backup](#)
 - [Export](#) and manual validation of a backup.

You can perform these operations by using another agent.
- Backups created by Agent for Windows XP SP2 cannot be [run as a virtual machine](#).

Supported Microsoft SQL Server versions

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

The SQL Server Express editions of the above SQL server versions are supported as well.

Supported Microsoft Exchange Server versions

- Microsoft Exchange Server 2019 – all editions.
- Microsoft Exchange Server 2016 – all editions.
- Microsoft Exchange Server 2013 – all editions, Cumulative Update 1 (CU1) and later.
- Microsoft Exchange Server 2010 – all editions, all service packs. Mailbox backup and granular recovery from database backups are supported starting with Service Pack 1 (SP1).
- Microsoft Exchange Server 2007 – all editions, all service packs. Mailbox backup and granular recovery from database backups are not supported.

Supported Microsoft SharePoint versions

Acronis Cyber Protect 15 supports the following Microsoft SharePoint versions:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1

- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*In order to use SharePoint Explorer with these versions, you need a SharePoint recovery farm to attach the databases to.

The backups or databases from which you extract data must originate from the same SharePoint version as the one where SharePoint Explorer is installed.

Supported Oracle Database versions

- Oracle Database version 11g, all editions
- Oracle Database version 12c, all editions.

Only single-instance configurations are supported.

Supported SAP HANA versions

HANA 2.0 SPS 03 installed in RHEL 7.6 running on a physical machine or VMware ESXi virtual machine.

Because SAP HANA does not support recovery of multitenant database containers by using storage snapshots, this solution supports SAP HANA containers with only one tenant database.

Supported virtualization platforms

The following table summarizes how various virtualization platforms are supported.

Note

The following hypervisor vendors and versions supported via the **Backup from inside a guest OS** method have been specifically tested. However, even if you run a hypervisor from a vendor or hypervisor with a version that is not listed below, the **Backup from inside a guest OS** method may still work correctly in all required scenarios.

If you encounter issues while using Acronis Cyber Protect with your combination of hypervisor vendor and version, contact the Support team for further investigation.

VMware

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
VMware vSphere versions: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 VMware vSphere editions: VMware vSphere Essentials*	+	+

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
VMware vSphere Essentials Plus*		
VMware vSphere Standard*		
VMware vSphere Advanced		
VMware vSphere Enterprise		
VMware vSphere Enterprise Plus		
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual server)		
VMware Workstation		+
VMware ACE		
VMware Player		

* 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 limits the 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.

Note

Acronis officially supports any update within the supported major vSphere version.

For example, vSphere 8.0 support includes support for any update within this version, unless stated otherwise. For example, vSphere 8.0 Update 1 is also supported along with originally released vSphere 8.0.

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 and 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 protection plan. If you want to back up these disks or data on these disks, install an agent in the guest operating system.

- **In-guest iSCSI connection**

Agent for VMware does not back up LUN volumes connected by an iSCSI initiator that works within the guest operating system. Because the ESXi hypervisor is not aware of such volumes, the volumes are not included in hypervisor-level snapshots and are omitted from the backup without a warning. If you want to back up such volumes or data on such volumes, install an agent in the guest operating system.

- **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 protection plan](#).
- 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 7.0.

Microsoft

Hyper-V virtual machines running on a hyper-converged cluster with Storage Spaces Direct (S2D) are supported. Storage Spaces Direct is also supported as a backup storage.

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Windows Server 2008 (x64) with Hyper-V		
Windows Server 2008 R2 with Hyper-V		
Microsoft Hyper-V Server 2008/2008 R2		
Windows Server 2012/2012 R2 with Hyper-V	+	+
Microsoft Hyper-V Server 2012/2012 R2		
Windows 8, 8.1 (x64) with Hyper-V		
Windows 10 with Hyper-V		

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Windows Server 2016 with Hyper-V – all installation options, except for Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 with Hyper-V – all installation options, except for Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 with Hyper-V – all installation options, except for Nano Server		
Microsoft Virtual PC 2004 and 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+

Limitations

- **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 protection 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 Hyper-V does not back up LUN volumes connected by an iSCSI initiator that works within the guest operating system. Because the Hyper-V hypervisor is not aware of such volumes, the volumes are not included in hypervisor-level snapshots and are omitted from the backup without a warning. If you want to back up such volumes or data on such volumes, install an agent in the guest operating system.

- **VHD/VHDX file names with ampersand symbols**

On Hyper-V hosts running Windows Server 2016 or later, you cannot back up legacy virtual machines (version 5.0) originally created with Hyper-V 2012 R2 or older, if the names of their VHD/VHDX files contain the ampersand symbol (&).

To be able to back up such machines, in Hyper-V Manager, detach the corresponding virtual disk from the virtual machine, edit the VHD/VHDX file name by removing the ampersand symbol, and then attach the disk back to the virtual machine.

Scale Computing

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	+	+

Citrix

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6		Only fully virtualized (aka HVM) guests. Paravirtualized (aka PV) guests are not supported.

Red Hat and Linux

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		+
Red Hat Virtualization (managed by oVirt) 4.2, 4.3, 4.4 (only available with the cloud deployment)	+	+
Kernel-based Virtual Machines (KVM)		+
Kernel-based Virtual Machines (KVM) managed by oVirt 4.3 running on Red Hat Enterprise Linux 7.6, 7.7 or CentOS 7.6, 7.7 (only available with the cloud deployment and with an	+	+

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Advanced license)		
Kernel-based Virtual Machines (KVM) managed by oVirt 4.4 running on Red Hat Enterprise Linux 8.x or CentOS Stream 8.x (only available with the cloud deployment and with an Advanced license)	+	+
Kernel-based Virtual Machines (KVM) managed by oVirt 4.5 running on Red Hat Enterprise Linux 8.x or CentOS Stream 8.x (only available with the cloud deployment and with an Advanced license)	+	+

Limitations

Linux machines containing logical volumes (LVM)

The following operations are not supported for Linux machines with LVM that you back up in the agentless mode:

- You cannot select individual Linux LVM volumes as backup source—neither by direct selection nor by using policy rules. You can back up workloads with such volumes only by selecting **Entire machine** in **What to back up**.
- The file filters (Inclusions/Exclusions) are not applicable. Any configured inclusions or exclusions will be ignored. For more information about the file filters, see "File filters" (p. 287).

The following operations are not supported for Linux machines with LVM that you back up in the agent-based mode (that is, by Agent for Linux installed on the backed-up machine):

- Performing a machine migration by recovering its backup as a virtual machine (for example, by using Agent for VMware, Agent for Hyper-V, Agent for Virtuozzo, Agent for Virtuozzo Hybrid Infrastructure, or Agent for Scale Computing for P2V, V2P, or V2V migration). To recover data from such a backup, use bootable media.
For more information about the migrations scenarios, see "Machine migration" (p. 504).
- Running a virtual machine from a backup created by Agent for Linux or bootable media.

Parallels

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Parallels Workstation		+

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Parallels Server 4 Bare Metal		+

Oracle

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Oracle VM Server 3.0, 3.3, 3.4		Only fully virtualized (aka HVM) guests. Paravirtualized (aka PV) guests are not supported.
Oracle VM VirtualBox 4.x		+

Nutanix

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Nutanix Acropolis Hypervisor (AHV) 20160925.x through 20180425.x		+

Virtuozzo (only available with the cloud deployment)

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Virtual machines only. Containers are not supported.
Virtuozzo 7.0.13, 7.0.14	Ploop containers only. Virtual	Virtual machines only. Containers

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
	machines are not supported.	are not supported.
Virtuozzo Hybrid Server 7.5	+	Virtual machines only. Containers are not supported.

Limitations

Linux machines containing logical volumes (LVM)

The following operations are not supported for Linux machines with LVM that you back up in the agentless mode:

- You cannot select individual Linux LVM volumes as backup source—neither by direct selection nor by using policy rules. You can back up workloads with such volumes only by selecting **Entire machine** in **What to back up**.
- The file filters (Inclusions/Exclusions) are not applicable. Any configured inclusions or exclusions will be ignored. For more information about the file filters, see "File filters" (p. 287).

The following operations are not supported for Linux machines with LVM that you back up in the agent-based mode (that is, by Agent for Linux installed on the backed-up machine):

- Performing a machine migration by recovering its backup as a virtual machine (for example, by using Agent for VMware, Agent for Hyper-V, Agent for Virtuozzo, Agent for Virtuozzo Hybrid Infrastructure, or Agent for Scale Computing for P2V, V2P, or V2V migration). To recover data from such a backup, use bootable media.
For more information about the migrations scenarios, see "Machine migration" (p. 504).
- Running a virtual machine from a backup created by Agent for Linux or bootable media.

Virtuozzo Hybrid Infrastructure (only available with the cloud deployment)

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5	+	+

Limitations

Linux machines containing logical volumes (LVM)

The following operations are not supported for Linux machines with LVM that you back up in the agentless mode:

- You cannot select individual Linux LVM volumes as backup source—neither by direct selection nor by using policy rules. You can back up workloads with such volumes only by selecting **Entire machine** in **What to back up**.
- The file filters (Inclusions/Exclusions) are not applicable. Any configured inclusions or exclusions will be ignored. For more information about the file filters, see "File filters" (p. 287).

The following operations are not supported for Linux machines with LVM that you back up in the agent-based mode (that is, by Agent for Linux installed on the backed-up machine):

- Performing a machine migration by recovering its backup as a virtual machine (for example, by using Agent for VMware, Agent for Hyper-V, Agent for Virtuozzo, Agent for Virtuozzo Hybrid Infrastructure, or Agent for Scale Computing for P2V, V2P, or V2V migration). To recover data from such a backup, use bootable media.

For more information about the migrations scenarios, see "Machine migration" (p. 504).

- Running a virtual machine from a backup created by Agent for Linux or bootable media.

Amazon

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Amazon EC2 instances		+

Microsoft Azure

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

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: <pre>yum install perl</pre>
CentOS Fedora	kernel-devel gcc make elfutils-libelf-devel	The setup program will download and install the packages automatically.
	perl	Run the following command: <pre>yum install perl</pre>
Ubuntu Debian	linux-headers linux-image gcc make perl	Run the following commands: <pre>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</pre>
SUSE Linux OpenSUSE	kernel-source gcc make perl	<pre>sudo zypper install kernel-source sudo zypper install gcc sudo zypper install make sudo zypper install perl</pre>

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.

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
- CheckPoint Harmony Endpoint
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

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

Common installation rule

We strongly recommend that you install the encryption software before installing the protection 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.
2. Install the protection agent.
3. Create Secure Zone.
4. 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 and CheckPoint Harmony Endpoint

You can recover a system by using a recovery with restart or a bootable media.

Recovery with restart

To recover an encrypted system, follow the steps in "Recovering a physical machine" (p. 322).

Ensure that the requirements in "Recovery with restart" (p. 328) are met.

Note

For Bitlocker-encrypted volumes, recovery with restart is only available on UEFI-based machines running Windows 7 and later or Windows Server 2008 R2 and later. For CheckPoint-encrypted volumes, recovery with restart is only available on UEFI-based machines running Windows 10 and Windows 11.

Recovery with restart is not available on BIOS-based machines or machines running Linux or macOS.

Recovery with bootable media

1. Boot from the bootable media.
2. Recover the system.

Important

Backed-up data is recovered as non-encrypted.

3. Reboot the recovered system.
4. Turn on the encryption software.

If you only need to recover one partition of a multi-partitioned disk, perform the recovery 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 only by using the bootable media.

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>

Compatibility with Dell EMC Data Domain storages

With Acronis Cyber Protect, you can use Dell EMC Data Domain devices as backup storage. Retention lock (Governance mode) is supported.

If retention lock is enabled, you need to add the AR_RETENTION_LOCK_SUPPORT environment variable to the machine with the protection agent that uses this storage as a backup destination.

Note

Dell EMC Data Domain storages with enabled retention lock are not supported by Agent for Mac.

To add the variable in Windows

1. Log in as administrator to the machine with the protection agent.
2. In the **Control Panel**, go to **System and Security > System > Advanced system settings**.
3. On the **Advanced tab**, click **Environment Variables**.
4. In the **System variables** panel, click **New**.
5. In the **New System Variable** window, add the new variable as follows:
 - Variable name: AR_RETENTION_LOCK_SUPPORT
 - Variable value: 1
6. Click **OK**.
7. In the **Environment Variables** window, click **OK**.
8. Restart the machine.

To add the variable in Linux

1. Log in as administrator to the machine with the protection agent.
2. Go to the /sbin directory, and then open the acronis_mms file for editing.
3. Above the line export LD_LIBRARY_PATH, add the following line:

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. Save the acronis_mms file.
5. Restart the machine.

To add the variable in a virtual appliance

1. Log in as administrator to the virtual appliance machine.
2. Go to the /bin directory, and then open the autostart file for editing.
3. Under the line export LD_LIBRARY_PATH, add the following line:

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. Save the autostart file.
5. Restart the virtual appliance machine.

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	Disk space required for installation	Minimum memory consumption
Agent for Windows	850 MB	150 MB
Agent for Windows and one of the following agents: <ul style="list-style-type: none"> • Agent for SQL 	950 MB	170 MB

• Agent for Exchange		
Agent for Windows and one of the following agents: • Agent for VMware (Windows) • Agent for Hyper-V	1170 MB	180 MB
Agent for Office 365	500 MB	170 MB
Agent for Linux	2.0 GB	130 MB
Agent for Mac	500 MB	150 MB
For on-premises deployments only		
Management Server in Windows	1.7 GB	200 MB
Management Server in Linux	1.5 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	4.0 GB	340 MB
Storage Node and Agent for Windows • 64-bit platform only • To use deduplication, minimum 8 GB of RAM are required. For more information, see "Deduplication best practices" (p. 616).	1.1 GB	330 MB

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.

Backup operations, including deleting backups, require about 1 GB of RAM per 1 TB of backup size. The memory consumption may vary, depending on the amount and type of data being processed by the agents.

Note

The RAM usage might increase when backing up to extra large backup sets (4 TB and more).

On x64 systems, operations with bootable media and disk recovery with restart require at least 2 GB of memory.

A management server with one registered workload consumes 200 MB of memory. A workload is any type of protected resource – for example, a physical machine, a virtual machine, a mailbox, or a

database instance. Each additional workload adds about 2 MB. Thus, a server with 100 registered workloads consumes approximately 400 MB above the operating system and running applications.

The maximum number of registered workloads is 900-1000. This limitation originates from the management server's embedded SQLite database.

To overcome this limitation, specify an external Microsoft SQL Server instance when you install the management server. With an external SQL database, you can register up to 8000 workloads to the management server, without significant performance degradation. With 8000 registered workloads, the SQL Server instance will consume about 8 GB of RAM.

For better backup performance, manage the workloads by groups, with up to 500 workloads in each group.

Supported file systems

A protection 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	Mac bootable media	
FAT16/32	All agents	+	+	+	No limitations
NTFS		+	+	+	
ext2/ext3/ext4		+	+	-	

HFS+	Agent for Mac	-	-	+	
APFS		-	-	+	<ul style="list-style-type: none"> Supported starting with macOS High Sierra 10.13 Disk configuration should be re-created manually when recovering to a non-original machine or bare metal.
JFS	Agent for Linux	-	+	-	<ul style="list-style-type: none"> Files cannot be excluded from a disk backup Fast incremental/differential backup cannot be enabled
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	<ul style="list-style-type: none"> 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		+	+	+	<ul style="list-style-type: none"> Files cannot be excluded from a disk backup Fast incremental/differential backup cannot be enabled Volumes cannot be resized during a recovery Recovering files from a backup stored on a tape is not supported
Linux swap	Agent for Linux	-	+	-	No limitations
exFAT	All agents	+	+ Bootable media cannot be used for recovery if the backup <i>is stored on</i> exFAT	+	<ul style="list-style-type: none"> 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.

Data Deduplication

In Windows Server 2012 and later, you can enable the Data Deduplication feature for an NTFS volume. Data Deduplication reduces the used space on the volume by storing duplicate fragments of the volume's files only once.

You can back up and recover a data deduplication-enabled volume at a disk level, without limitations. File-level backup is supported, except when using Acronis VSS Provider. To recover files from a disk backup, either run a virtual machine from your backup, or [mount the backup](#) on a machine running Windows Server 2012 or later, and then copy the files from the mounted volume.

The Data Deduplication feature of Windows Server is unrelated to the Acronis Backup Deduplication feature.

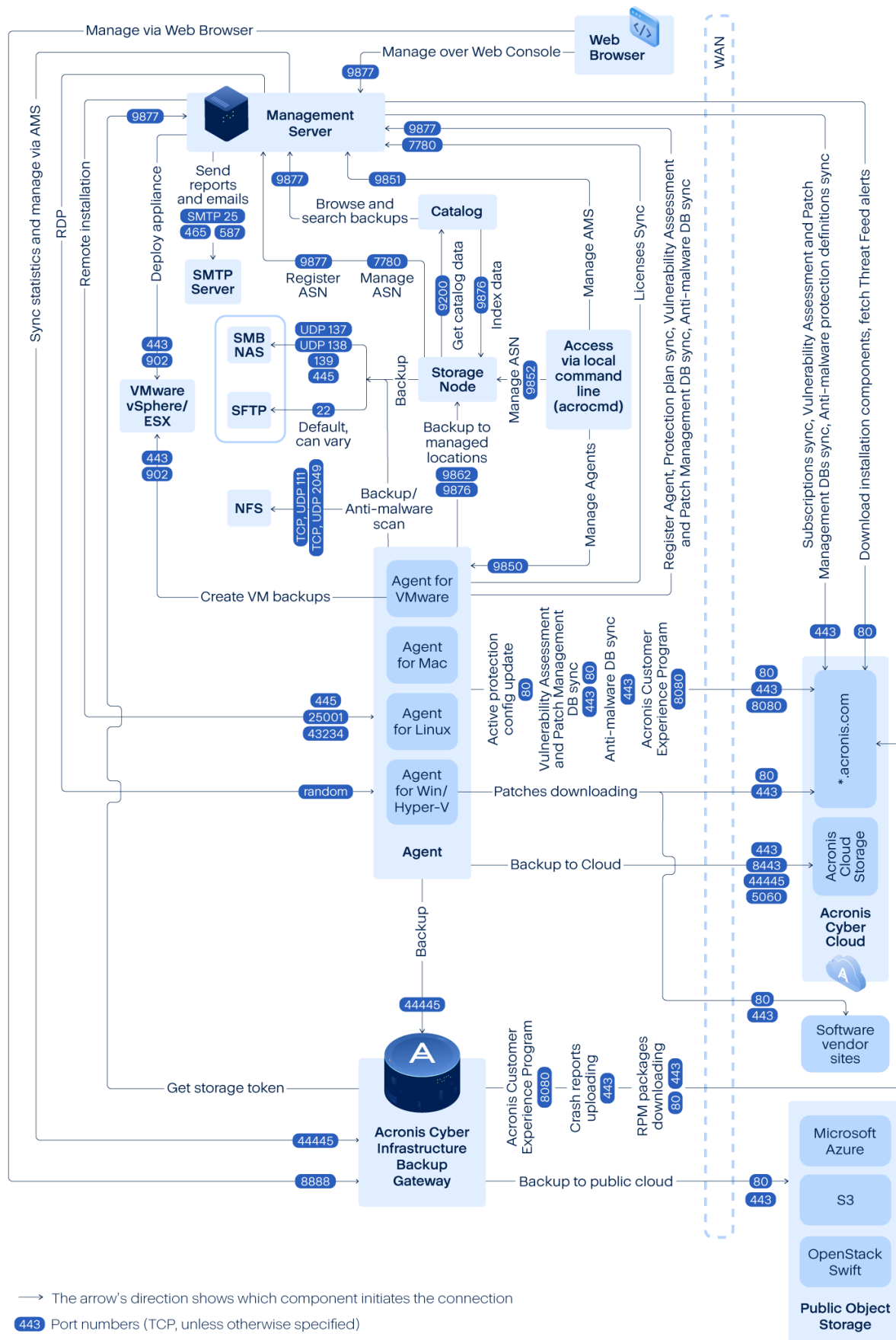
Network connection diagram for Acronis Cyber Protect

This topic contains the connection diagrams for Acronis Cyber Protect.

Visit our Knowledge Base for a list of ports, services, and processes that Acronis Cyber Protect uses:

- For Windows, see [Windows services and processes \(65663\)](#).
- For Linux, see [Linux components, services, and processes \(67276\)](#).

Network connection diagram - Cyber Protect processes



Important

The outgoing ports in the network diagram are dynamic. Some services can also use dynamic ports for inbound connections. When you troubleshoot network issues, ensure that the traffic through dynamic ports is allowed.

The dynamic ports are managed by the operating system and are assigned randomly. The default dynamic port range in Windows is 49152 – 65535. This range may vary according to the operating system and can be changed manually.

Management server is the central component of Acronis Cyber Protect. It exposes two TCP ports: 7780 and 9877. Port 9877, protected with TLS, is used to provide both the REST API and a web-based user interface. The REST API endpoints authenticate requests by using JWT tokens represented either as a separate HTTP header or encoded as an HTTP cookie. Port 7780 implements the ZeroMQ protocol with ZMTP CURVE authentication and encryption. Port 7780 is used by the agents and storage node to exchange management messages with the management server asynchronously. The management server also communicates with the cloud services to download updates over standard HTTP and HTTPS ports.

Storage node is the storage component of Acronis Cyber Protect. It exposes TCP port 9876. This port is used for sending and receiving backup data. Transport is protected with TLS and authentication is done using mutual TLS. The application-level protocol is Acronis proprietary. The storage node communicates to backend storage systems by using the appropriate protocols and authentication mechanisms.

Catalog is a supporting component of Acronis Cyber Protect. It indexes data on the storage node, accessing it on port 9876 and exposes the index on port 9200.

Backup gateway implements the next generation of Acronis proprietary data access protocol. The same component is used in Acronis Cyber Cloud, if the customer opts-in for cloud backup. TCP port 44445, [registered at IANA](#), is used by the gateway. Data protection is done via TLS and the authentication is done using mutual TLS. The backup gateway also may use port 8888 for the HTTPS-based management service.

Agent communicates with the management server, storage node, and backup gateway over the ports, as described above. The agent may also communicate with standards-based file services (SMB, NFS) when they are used as a backup destination. Standard ports and appropriate authentication protocols are used in this case. Agent for VMware uses the VMware vSphere API over the ports defined by VMware vSphere when such functionality is configured.

The vulnerability assessment for Linux is implemented via a CVSS service deployed in Acronis Cyber Cloud. Protection agents choose dynamically the closest data center via ping from the list <https://cloud.acronis.com/services.json>.

On-premises deployment

An on-premises deployment includes a number of software components, which are described in the "Components" (p. 47) section. For details about the interaction between these components and the required ports, refer to "Network connection diagram for Acronis Cyber Protect" (p. 81).

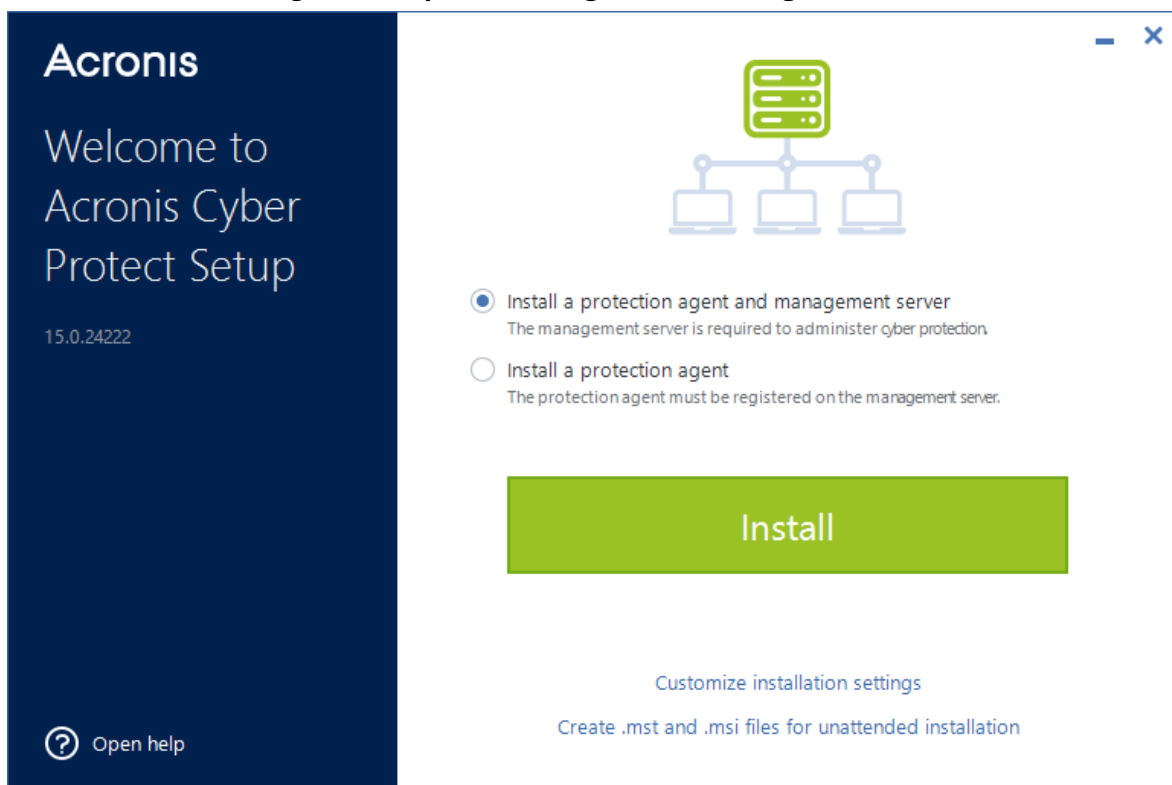
Installing the management server

Install the management server only on machines on which the sleep mode and hibernation are disabled.

Installation in Windows

To install the management server

1. Log on as an administrator and start the Acronis Cyber Protect setup program.
2. [Optional] To change the language of the setup program, click **Setup language**.
3. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
4. Leave the default setting **Install a protection agent and management server**.



5. Do any of the following:

- Click **Install**.

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
- 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
- Cyber Protect 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" (p. 86).
- 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" (p. 192).

6. Proceed with the installation.

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

To start using your management server, activate it by signing in to your Acronis account or through an activation file.

Customizing installation settings

This section describes settings that can be changed during the installation.

Components to install

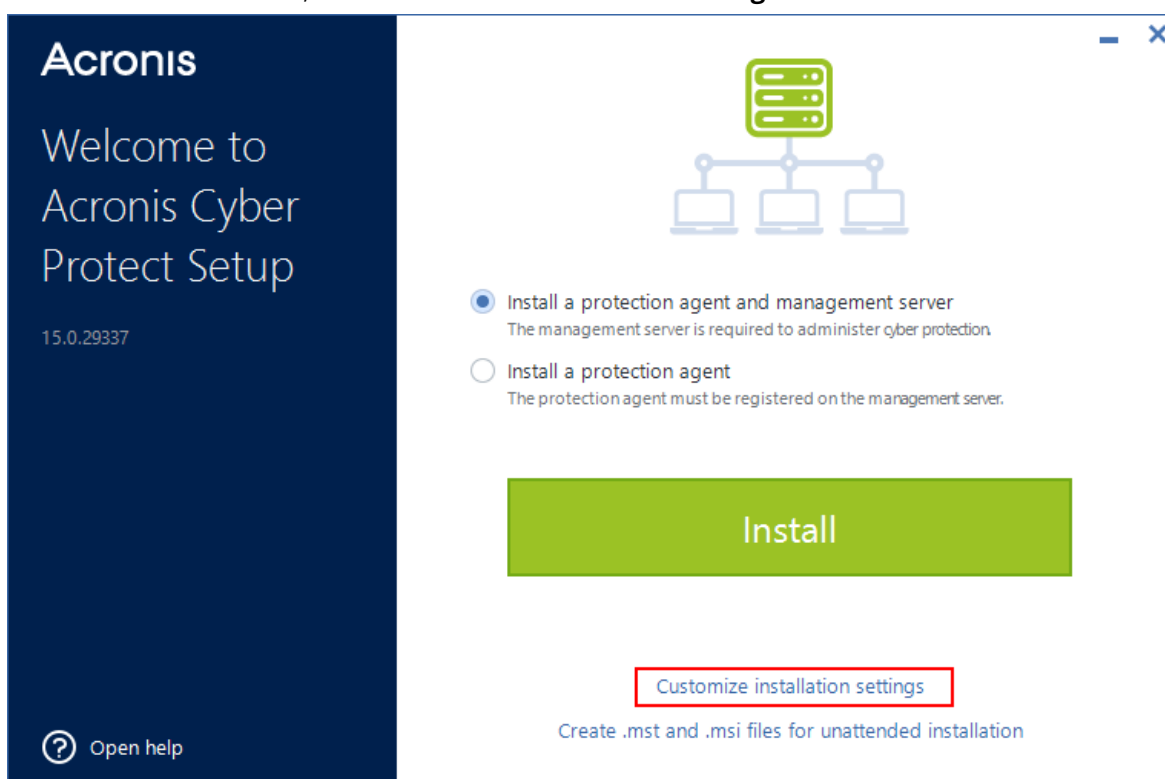
Depending on whether you install a management server and a protection agent, or a protection agent only, the following components are selected by default:

Management server and protection agent	Protection agent only
Management Server	Agent for Windows
Components for Remote Installation	Bootable Media Builder
Agent for Windows	Command-Line Tool
Bootable Media Builder	Cyber Protect Monitor
Command-Line Tool	
Cyber Protect Monitor	

For the full list of available components, refer to "Components" (p. 47).

To install optional components

1. In the installation wizard, click **Customize installation settings**.



2. In **What to install**, click **Change**.
3. Select the desired components, and then click **Done**.
4. If prompted, configure the settings for the selected components.
5. Click **Install**.

Service logon account

You can change the account under which the agent or the management service will run by using the **Logon account for the agent service** and **Logon account for the management server service** options, respectively.

You can choose one of the following options:

- **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 option is that the domain security policies do not affect the user rights of these accounts. By default, the agent runs under the **Local System** account.
- **Create a new account** (default for the management server service and the storage node service)
The account names are **Acronis Agent User**, **AMS User**, and **ASN User** for the agent, management server, and the storage node services, 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.

The user account that you specify when the setup program runs on a domain controller must be granted the Log on as a service right. This account must have already been used on the domain controller, in order for its profile folder to be created on that machine.

For more information about installing the agent on a read-only domain controller, refer to [this knowledge base article](#).

Also, selecting **Use the following account** allows you to use Windows authentication for Microsoft SQL Server if you configure the management server with a SQL database.

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

Required user rights for the service logon account

A protection agent runs as **Managed Machine Service** (MMS) on a Windows machine. The account under which the agent runs must have the following rights for the agent to work correctly:

1. The MMS user must be included in the **Backup Operators** and **Administrators** groups. On a domain controller, the user must be included in the **Domain Admins** group.
2. The MMS user must be granted the **Full Control** permission on folder %PROGRAMDATA%\Acronis (in Windows XP and Server 2003, %ALLUSERSPROFILE%\Application Data\Acronis) and on its subfolders.
3. The MMS user must be granted the **Full Control** permission on certain registry keys in the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis.
4. The MMS user must be assigned the following user rights in Windows:
 - **Log on as a service**
 - **Adjust memory quotas for a process**
 - **Replace a process level token**
 - **Modify firmware environment values**

The **ASN user** must have local administrator rights on the machine where Acronis Storage Node is installed.

To assign user rights in Windows

Note

This procedure uses the **Log on as service** user right as an example. The steps for the other user rights are the same.

1. Log in to the computer as administrator.
2. In **Control Panel**, open **Administrative Tools**. Alternatively, press Win+R on the keyboard, type **control admintools**, and then press Enter.
3. Open **Local Security Policy**.
4. Expand **Local Policies**, and then click **User Rights Assignment**.

5. In the right pane, right-click **Log on as a service**, and then select **Properties**.
6. Click **Add User or Group...** to add a new user.
7. In the **Select Users or Groups** window, find the user you want to add, and then click **OK**.
8. In the **Log on as a service Properties** window, click **OK** to save the changes.

Note

The user that you add to the **Log on as service** user right must not be listed in the **Deny log on as a service** policy in **Local Security Policy**.

Important

We do not recommend changing the logon account manually after the installation completes.

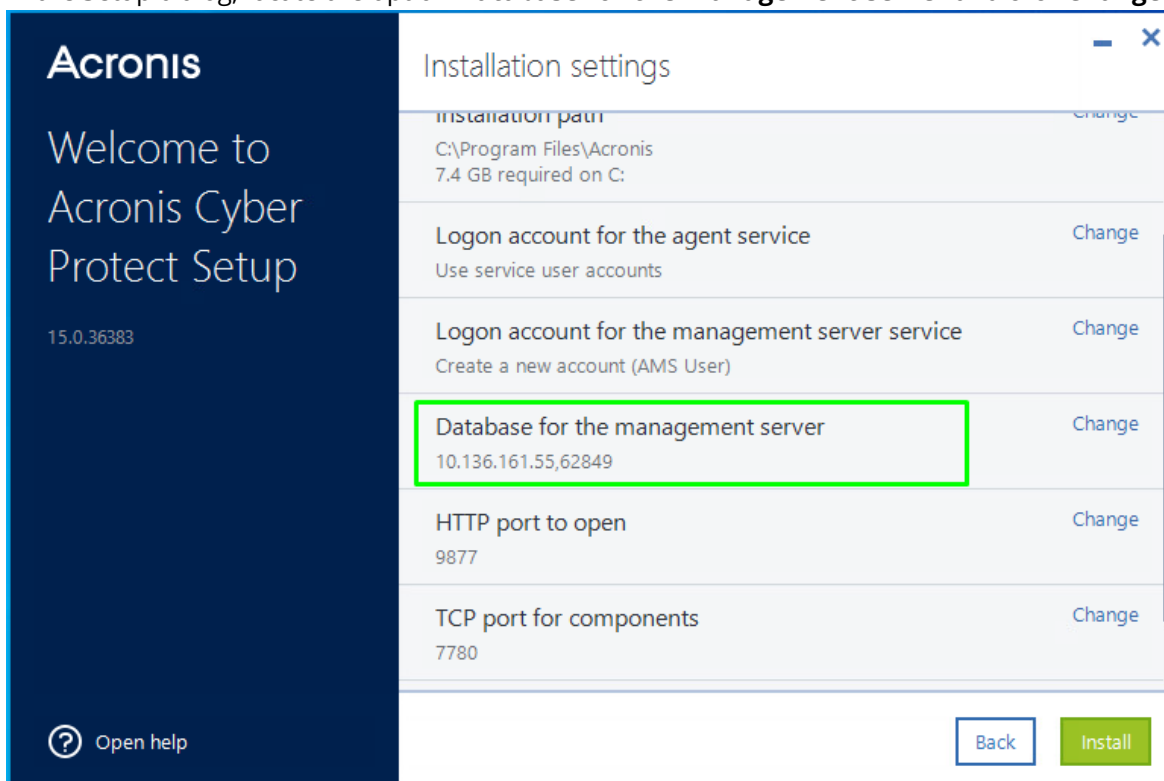
Database for the management server

You can configure the management server with the following databases:

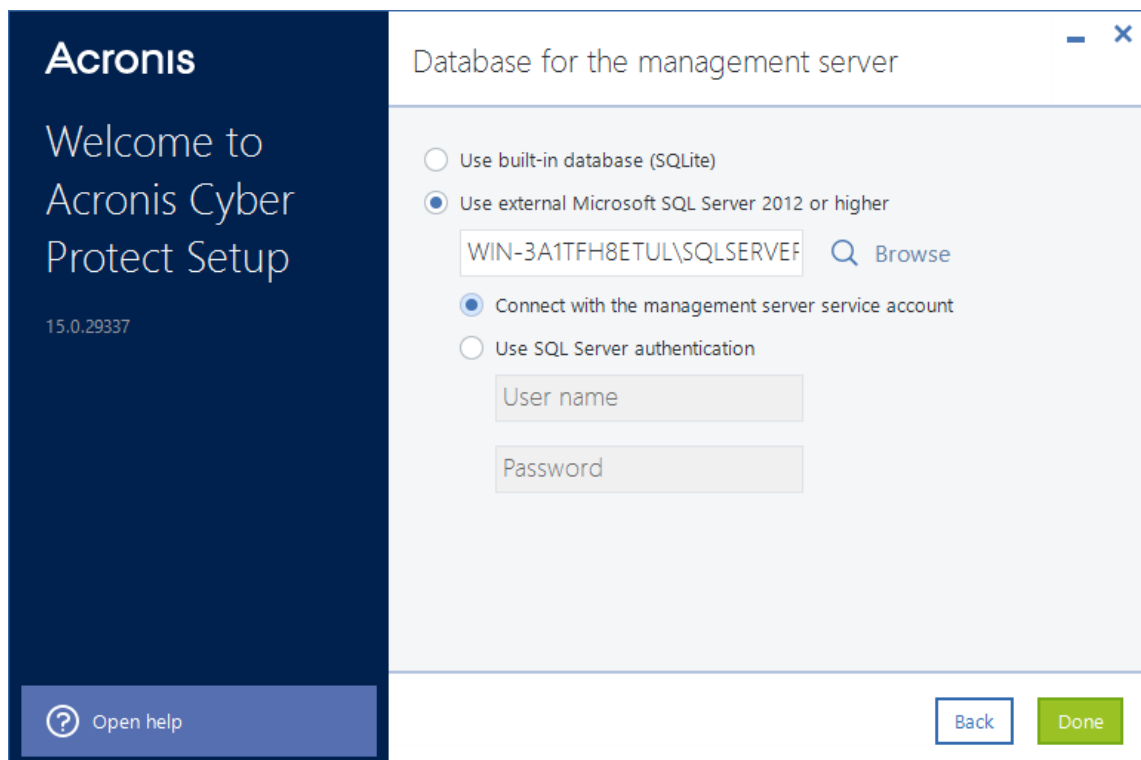
- **SQLite**
By default, the management server uses the built-in SQLite database. It allows registering approximately 900-1000 workloads on the management server. SQLite is not compatible with Scan Service.
- **Microsoft SQL**
Microsoft SQL allows registering up to 8000 workloads on the management server, without significant performance degradation. The same Microsoft SQL instance can be used by the management server, by the Scan Service, and by other programs.
The following MS SQL Server versions are supported:
 - Microsoft SQL Server 2019 (running in Windows)
 - Microsoft SQL Server 2017 (running in Windows)
 - Microsoft SQL Server 2016
 - Microsoft SQL Server 2014
 - Microsoft SQL Server 2012

To connect to an external SQL database

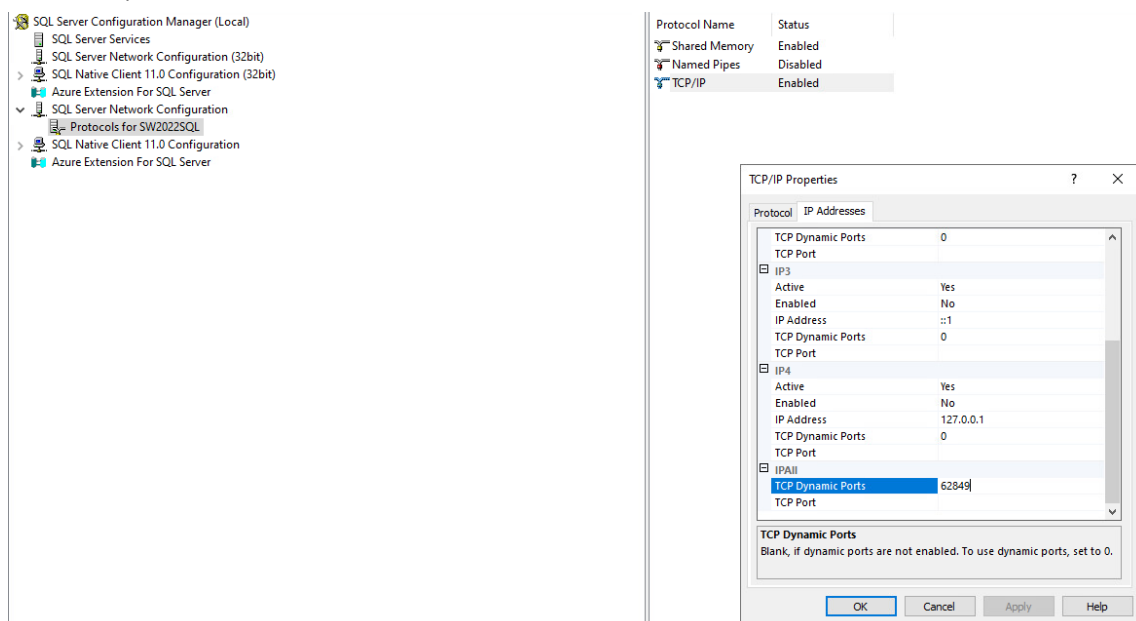
1. In the Setup dialog, locate the option **Database for the management server** and click **Change**.



2. Select **Use external Microsoft SQL Server 2012 or higher** and specify the domain name or address of the Microsoft SQL server.
 - If you are connecting to the default Microsoft SQL instance on the server (**MSSQLSERVER**), you can specify only the domain name of the machine where it runs. If the instance has a custom name, you must specify it by using the following format: <machine name\instance name>.



- If you enter IP address, enter the connection port number as well, using the format <ip_address, port>.



Important

Verify that the SQL Server Browser Service and the TCP/IP client protocol are enabled on the machine that runs the Microsoft SQL instance. For more information 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.

3. Select how to connect to the specified Microsoft SQL instance:

- Windows authentication (**Connect with the management server service account**)

You can use this method if you configured the **Logon account for the management server service** option in the Setup dialog with the **Use the following account** option enabled. The specified account must follow the format <MACHINE NAME>\Administrator and must have the **dbcreator** or **sysadmin** role in Microsoft SQL Server.

For more information about the logon account, refer to "Required user rights for the service logon account" (p. 88).

- SQL Server authentication (**Use SQL Server authentication**)

You can use this method independently of other configurations. The specified account must have the **dbcreator** or **sysadmin** role in Microsoft SQL Server.

Scan Service

Scan Service is an optional component that enables antimalware scan of backups in a cloud storage, or in a local or network folder. Scan Service requires that the management server is installed on the same machine.

Installing Scan Service provides access to the following functionality:

- Backup scanning plans
- Backup scanning details widget
- Corporate whitelist
- Safe recovery
- The **Status** column in the list of backups

You can install Scan Service during the installation of the management server or you can add Scan Service later, by modifying the existing installation. For more information about how to install optional components as Scan Service, refer to "To install optional components" (p. 86).

Important

Scan Service is not compatible with the default SQLite database that the management server uses.

You can configure Scan Service with a Microsoft SQL or a PostgreSQL database. For more information about how to choose one, refer to "Database for Scan Service" (p. 93).

Database for Scan Service

Scan Service is not compatible with SQLite, which is the default database for the management server.

If your management server uses SQLite, you can only configure Scan Service with a PostgreSQL database. PostgreSQL 9.6 and later are supported.

If your management server uses Microsoft SQL Server, you can configure Scan Service with the same database, without additional settings. You can also configure Scan Service with a PostgreSQL database.

To configure Scan Service with a PostgreSQL database

1. In the installation wizard, under **Database for the scan service**, click **Change**.
2. Select **PostgreSQL Server database**.
3. Specify the PostgreSQL instance host name, or IP address and port.
4. Specify the credentials of a user who has the **CREATEDB** privilege or who is a superuser.

Note

The SCRAM-SHA-256 authentication method in PostgreSQL 10 and later is not supported.

5. Click **Done**.

Ports

You can customize 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 completes will require re-registering 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.

Proxy server

You can choose whether the protection agents use an HTTP proxy server when backing up to and recovering from the cloud storage.

Additionally, you use the same proxy server for communication between the different Acronis Cyber Protect components.

To use a proxy server, specify its host name or IP address, and the port number. If the proxy server requires authentication, specify the access credentials.

Note

Updating the protection definitions (antivirus and antimalware definitions, advanced detection definitions, vulnerability assessment and patch management definitions) is not possible when using a proxy server.

Installation in Linux

Preparation

1. If you want to install Agent for Linux along with the management server, ensure that the necessary [Linux packages](#) are installed on the machine.
2. Choose the database to be used by the management server.

Limitation

Management servers that run on Linux machines do not support remote installation of protection agents, which is used, for example, in the autodiscovery procedure. For more information about a possible workaround, refer to our knowledge base: <https://kb.acronis.com/content/69553>.

Installation

To install the management server, you need at least 4 GB of free disk space.

To install the management server

1. As the root user, navigate to the directory with the installation file, make the file executable, and then run it.

```
chmod +x <installation file name>
```

```
./<installation file name>
```

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 Cyber Protect web console will open in your default web browser.

To start using your management server, activate it by signing in to your Acronis account or through an activation file.

Installation in a Docker container

To install the management server in a Docker container, first install Docker Engine in your environment.

For more information, see <https://docs.docker.com/engine/install/>.

Installing the management server

Prerequisites

To install the management server in a Docker container, you need the following files:

- [AB_AMS_prepare_env_ams.sh](#).
- The Docker image of the management sever.
 - To obtain the image file, contact your Acronis sales representative.
 - The procedure below uses `acronisbackup15ams_29098.image` as an example.

To install the management server in a Docker container

Note

To run the commands in this procedure, use `sudo` or run them under the root account.

1. Load the Docker image for the management server.

Input template

```
docker load -i /<path>/<image file>
```

Input example

```
sudo docker load -i ./acronisbackup15ams_29098.image
```

2. Open the `AB_AMS_prepare_env_ams.sh` file for editing and ensure that the script uses the correct image name and build number.

In this example, `acronisbackup15ams:29098`.

```
1 #! /bin/bash
2
3 DOCKER_IMAGE=acronisbackup15ams:29098
```

3. If necessary, edit the script, and then save the `AB_AMS_prepare_env_ams.sh` file.
4. Assign the execute permission to the `AB_AMS_prepare_env_ams.sh` file, and then run it.

Input template

```
chmod +x /<path>/AB_AMS_prepare_env_ams.sh
```

```
/<path>/AB_AMS_prepare_env_ams.sh
```

Input example

```
sudo chmod +x ./AB_AMS_prepare_env_ams.sh
```

```
sudo ./AB_AMS_prepare_env_ams.sh
```

Output example

```
[root@centos7x64-UEFI ~]# docker load -i acronisbackup15ams_29098.image.1
d6bb3538baeb: Loading layer [=====>]
3.584kB/3.584kB
7119294a5178: Loading layer [=====>]
2.041GB/2.041GB
Loaded image: acronisbackup15ams:29098

[root@centos7x64-UEFI ~]# ./AB_AMS_prepare_env_ams.sh
=== Check docker swarm exist ===
OK
=== Check docker volume exist: AcronisAMS_var_log ===
[]
Error: No such volume: AcronisAMS_var_log
Try to fix.
Creating docker volume: AcronisAMS_var_log
AcronisAMS_var_log
OK
=== Check docker volume exist: AcronisAMS_opt_acronis ===
[]
Error: No such volume: AcronisAMS_opt_acronis
Try to fix.
Creating docker volume: AcronisAMS_opt_acronis
AcronisAMS_opt_acronis
OK
=== Check docker volume exist: AcronisAMS_etc ===
[]
Error: No such volume: AcronisAMS_etc
Try to fix.
Creating docker volume: AcronisAMS_etc
AcronisAMS_etc
OK
=== Check docker volume exist: AcronisAMS_usr_sbin ===
[]
Error: No such volume: AcronisAMS_usr_sbin
Try to fix.
Creating docker volume: AcronisAMS_usr_sbin
AcronisAMS_usr_sbin
OK
=== Check docker volume exist: AcronisAMS_var_lib_acronis ===
[]
```



```

Error: No such volume: AcronisAMS_var_lib_acronis
Try to fix.
Creating docker volume: AcronisAMS_var_lib_acronis
AcronisAMS_var_lib_acronis
OK
=== Check docker volume exist: AcronisAMS_usr_lib_acronis ===
[]
Error: No such volume: AcronisAMS_usr_lib_acronis
Try to fix.
Creating docker volume: AcronisAMS_usr_lib_acronis
AcronisAMS_usr_lib_acronis
OK
Copying files from container: /etc/* -> docker volume "etc"
Copying files: /var/log/* -> docker volume "var_log"
Copying files: /usr/sbin/* -> docker volume "usr_sbin"
+ FILE_VERS=/var/lib/Acronis/BackupAndRecovery_version.txt
+ prepare_mode=no
+ getopts ph flag
+ case "${flag}" in
+ prepare_mode=yes
+ getopts ph flag
+ '[' -f /var/lib/Acronis/BackupAndRecovery_version.txt ']'
+ '[' '!' -f /var/lib/Acronis/BackupAndRecovery_version.txt ']'
+ /tmp/AcronisBackup.x86_64 -a --id=AcronisCentralizedManagementServer
Initializing...Done
Warning
The following issues have been detected in the system configuration:

* The following devices from '/proc/partitions' are missing from '/dev' and will be
created automatically:
sda(8,0)
sda1(8,1)
sda2(8,2)
sda3(8,3)
sdb(8,16)

Installing the required package 'java-1.8.0-openjdk-headless'...Trying to install the
required packages by using YUM.
Done
Stopping services...Done
Installing Acronis Cyber Protect Packages
MonitoringServer-15.0.29098-1
WebConsole-15.0.29098-1
AcronisCentralizedManagementServer-15.0.29098-1
Upgrading services...
Starting services...Done
Upgrading services stage after-start...
Congratulations!
Acronis Cyber Protect has been successfully installed in the system.

Warning: A firewall has been detected in the system.

```

Please configure the firewall to allow connections to Acronis Cyber Protect.

```
+ [[ yes == \y\e\s ]]
+ echo 'prepare_mode=yes: exit 0 from container'
prepare_mode=yes: exit 0 from container
+ echo 'sleep 60'
sleep 60
+ sleep 60
+ exit 0
Docker secret ams_masterkey already created
```

Command to run docker service for ams:

```
docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/var/lib/Acronis/CredStore/masterkey.local" --secret="ams_
masterkey" "acronisbackup15ams:29098"
```

5. Run the Docker service to create the container with Acronis Management Server.

Input template

```
docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/var/lib/Acronis/CredStore/masterkey.local" --secret="ams_
masterkey" "<image:build>"
```

Input example

```
sudo docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/var/lib/Acronis/CredStore/masterkey.local" --secret="ams_
masterkey" "acronisbackup15ams:29098"
```

Note

At the end of this command, you must use an image name and build number that depend on the image file.

In the example above, these are `acronisbackup15ams:29098`. To check them for your image, run the `docker images` command, and see the `REPOSITORY` and `TAG` columns.

Input example

```
sudo docker images
```

Output example

#	REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
#	acronisbackup15ams	29098	9f473ae338b7	4 weeks ago	2.14GB

6. Enter the container, and then set the password for the root user.

- a. Check the container ID.

Input example

```
sudo docker service ps -a
```

Output example

#	CONTAINER ID	IMAGE	COMMAND	CREATED
	STATUS	PORTS	NAMES	
#	bfb9d14d4879	acronisbackup15ams:29098	"/bin/bash -c'/opt/..."	2 minutes ago
	Up 2 minutes	7780/tcp, 9877/tcp	ams.1.ko7xklvta28rasyukn6kic1ka	

- b. Enter the container.

Input template

```
docker exec -it <container ID> bash
```

Input example

```
sudo docker exec -it bfb9d14d4879 bash
```

- c. Set the password for the root user.

Input template

```
echo root:<your_new_root_password> | chpasswd
```

Input example

```
sudo echo root:MyPassword | chpasswd
```

7. Log in as the root user to the Cyber Protect console at http://ip_docker_host:9877.

Updating the management server

The update procedures and prerequisites depend on the version of the management server that you use.

Build 26981 or earlier

Acronis Cyber Protect version 15 Update 2 was released as build 26981 on 7 May 2021.

You can update the management server to build 29486 (released on 19 April 2022) or later.

Prerequisites

To update the management server in a Docker container, you need the following files:

- [AB_AMS_migrate_data_to_volumes.sh](#).
- [AB_AMS_prepare_env_ams.sh](#).
- The Docker image of the new version of the management sever.
To obtain the image file, contact your Acronis sales representative.
The procedure below uses `acronisbackup15ams_29098.image` as an example.

To update the management server in a Docker container

Note

To run the commands in this procedure, use `sudo` or run them under the `root` account.

1. Check the loaded Docker images.

Input example

```
sudo docker images
```

Output example

#	REPOSITORY				TAG	IMAGE
ID	CREATED	SIZE				
#	acronisbackup12.5ams				27009	
26b7ba78400f	9 months ago	3.18GB				

2. Stop the AMS service. You can use the service name or service ID in this command.

Input example

```
sudo docker service rm ams
```

3. Assign execute permission to the `AB_AMS_migrate_data_to_volumes.sh` file, and then run it to migrate the data of the management server to docker volumes.

Input template

```
chmod +x /<path>/AB_AMS_migrate_data_to_volumes.sh
```

```
/<path>/AB_AMS_migrate_data_to_volumes.sh -i <image:build>
```

Input example

```
sudo chmod +x ./AB_AMS_migrate_data_to_volumes.sh
```

```
sudo ./AB_AMS_migrate_data_to_volumes.sh -i acronisbackup12.5ams:27009
```

4. Load the Docker image with the newer version of Acronis Management Server.

Input template

```
docker load -i /<path>/<image file>
```

Input example

```
sudo docker load -i ./acronisbackup15ams_29098.image
```

Output example

# REPOSITORY			TAG	IMAGE
ID	CREATED	SIZE		
# acronisbackup12.5ams			27009	
26b7ba78400f	9 months ago	3.18GB		
# acronisbackup15ams			29098	
5d20f7d3155f	26 hours ago	2.38GB		

5. Open the AB_AMS_prepare_env_ams.sh file for editing and ensure that the script uses the correct image name and build number.

In this example, acronisbackup15ams:29098.

```
1 #! /bin/bash
2
3 DOCKER_IMAGE=acronisbackup15ams:29098
```

6. If necessary, edit the script, and then save the AB_AMS_prepare_env_ams.sh file.
7. Assign the execute permission to the AB_AMS_prepare_env_ams.sh file, and then run it.

Input template

```
chmod +x /<path>/AB_AMS_prepare_env_ams.sh
```

```
/<path>/AB_AMS_prepare_env_ams.sh
```

Input example

```
sudo chmod +x ./AB_AMS_prepare_env_ams.sh
```

```
sudo ./AB_AMS_prepare_env_ams.sh
```

8. Run the Docker service to create the container with Acronis Management Server.

Input template

```
docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/opt/CredStore/masterkey.local" --secret="ams_masterkey"
"<image:build>"
```

Input example

```
sudo docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/opt/CredStore/masterkey.local" --secret="ams_masterkey"
"acronisbackup15ams:29098"
```

Note

At the end of this command, you must use an image name and build number that depend on the image file.

In the example above, these are acronisbackup15ams:29098. To check them for your image, run the `docker images` command, and see the `REPOSITORY` and `TAG` columns.

Input example

```
sudo docker images
```

Output example

#	REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
#	acronisbackup15ams	29098	9f473ae338b7	4 weeks ago	2.14GB

9. Enter the container, and then set the password for the root user.

- a. Check the container ID.

Input example

```
sudo docker service ps -a
```

Output example

#	CONTAINER ID	IMAGE	COMMAND	CREATED
	STATUS	PORTS	NAMES	
#	bfb9d14d4879	acronisbackup15ams:29098	"/bin/bash -c'/opt/..."	2 minutes ago
	Up 2 minutes	7780/tcp, 9877/tcp	ams.1.ko7xklvta28rasyukn6kic1ka	

- b. Enter the container.

Input template

```
docker exec -it <container ID> bash
```

Input example

```
sudo docker exec -it bfb9d14d4879 bash
```

- c. Set the password for the root user.

Input template

```
echo root:<your_new_root_password> | chpasswd
```

Input example

```
sudo echo root:MyPassword | chpasswd
```

10. Log in as the root user to the Cyber Protect console at http://ip_docker_host:9877.

Build 29240 or later

Acronis Cyber Protect version 15 Update 4 was released as build 29240 on 7 March 2022.

Prerequisites

To update the management server in a Docker container, you need the following files:

- [AB_AMS_prepare_env_ams.sh](#).
- The Docker image of the new version of the management sever.

To obtain the image file, contact your Acronis sales representative.

The procedure below uses `acronisbackup15ams_29098.image` as an example.

To update the management server in a Docker container

Note

To run the commands in this procedure, use `sudo` or run them under the root account.

1. Check the loaded Docker images.

Input example

```
sudo docker images
```

Output example

# REPOSITORY	CREATED	SIZE	TAG	IMAGE ID
# acronisbackup15ams			29094	
26b7ba78400f	9 months ago	3.18GB		

- Stop the AMS service. You can use the service name or service ID in this command.

Input example

```
sudo docker service rm ams
```

- Load the Docker image with the newer version of Acronis Management Server.

Input template

```
docker load -i /<path>/<image file>
```

Input example

```
sudo docker load -i ./acronisbackup15ams_29098.image
```

Output example

# REPOSITORY	ID	CREATED	SIZE	TAG	IMAGE
# acronisbackup15ams				29094	
26b7ba78400f		9 months ago	3.18GB		
# acronisbackup15ams				29098	
5d20f7d3155f		26 hours ago	2.38GB		

- Open the AB_AMS_prepare_env_ams.sh file for editing and ensure that the script uses the correct image name and build number.

In this example, acronisbackup15ams:29098.

```
1 #! /bin/bash
2
3 DOCKER_IMAGE=acronisbackup15ams:29098
```

- If necessary, edit the script, and then save the AB_AMS_prepare_env_ams.sh file.
- Assign the execute permission to the AB_AMS_prepare_env_ams.sh file, and then run it.

Input template

```
chmod +x /<path>/AB_AMS_prepare_env_ams.sh
```

```
/<path>/AB_AMS_prepare_env_ams.sh
```

Input example

```
sudo chmod +x ./AB_AMS_prepare_env_ams.sh
```



```
sudo ./AB_AMS_prepare_env_ams.sh
```

7. Run the Docker service to create the container with Acronis Management Server.

Input template

```
docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/opt/CredStore/masterkey.local" --secret="ams_masterkey"
"<image:build>"
```

Input example

```
sudo docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/opt/CredStore/masterkey.local" --secret="ams_masterkey"
"acronisbackup15ams:29098"
```

Note

At the end of this command, you must use an image name and build number that depend on the image file.

In the example above, these are acronisbackup15ams:29098. To check them for your image, run the `docker images` command, and see the `REPOSITORY` and `TAG` columns.

Input example

```
sudo docker images
```

Output example

#	REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
#	acronisbackup15ams	29098	9f473ae338b7	4 weeks ago	2.14GB

8. Enter the container, and then set the password for the root user.

- a. Check the container ID.

Input example

```
sudo docker service ps -a
```

Output example

#	CONTAINER ID	IMAGE	COMMAND	CREATED
	STATUS	PORTS	NAMES	
#	bfb9d14d4879	acronisbackup15ams:29098	"/bin/bash -c'/opt/..."	2 minutes ago
	Up 2 minutes	7780/tcp, 9877/tcp	ams.1.ko7xklvta28rasyukn6kic1ka	

- b. Enter the container.

Input template

```
docker exec -it <container ID> bash
```

Input example

```
sudo docker exec -it bfb9d14d4879 bash
```

- c. Set the password for the root user.

Input template

```
echo root:<your_new_root_password> | chpasswd
```

Input example

```
sudo echo root:MyPassword | chpasswd
```

9. Log in as the root user to the Cyber Protect console at http://ip_docker_host:9877.

Acronis Cyber Protect appliance

With Acronis Cyber Protect appliance, you can easily obtain a virtual machine with the following software:

- CentOS
- Acronis Cyber Protect components:
 - Management Server
 - Agent for Linux
 - Agent for VMware (Linux)

The appliance is provided as a .zip archive. The archive contains the .ovf and .iso files. You can deploy the .ovf file to an ESXi host or use the .iso file to boot an existing virtual machine. The archive also contains the .vmdk file that should be placed in the same directory with .ovf.

Note

VMware Host Client (a web client used to manage standalone ESXi 6.0+) does not allow deploying OVF templates with an ISO image inside. If this is your case, create a virtual machine that meets the requirements below, and then use the .iso file to install the software.

Requirements for the virtual appliance are as follows:

- Minimum system requirements:
 - 2 CPUs
 - 6 GB RAM
 - One 10 GB virtual disk (40 GB recommended)
- In VMware virtual machine settings, click **Options** tab > **General** > **Configuration Parameters**, and then ensure that the `disk.EnableUUID` parameter value is `true`.

Limitation

Management servers that run on Linux machines, including Acronis Cyber Protect appliance, do not support remote installation of protection agents, which is used, for example, in the autodiscovery procedure. For more information about a possible workaround, refer to our knowledge base: <https://kb.acronis.com/content/69553>.

Installing the software

1. Do one of the following:
 - Deploy the appliance from `.ovf`. After the deployment has completed, power on the resulting machine.
 - Boot an existing virtual machine from the `.iso`.
2. Select **Install or update Acronis Cyber Protect**, and then press **Enter**. Wait for the initial setup window to appear.
3. [Optional] To change the installation settings, select **Change settings**, and then press **Enter**. You can specify the following settings:
 - The host name of the appliance (by default, `AcronisAppliance-
<random part>`).
 - The password for the "root" account that will be used to log in to the Cyber Protect web console (by default, **not specified**).
If you leave the default value, after Acronis Cyber Protect is installed, you will be prompted to specify the password. Without this password, you will not be able to log in to the Cyber Protect web console and the Cockpit web console.
 - Network settings of a network interface card:
 - **Use DHCP** (by default)
 - **Set static IP address**
 If the machine has several network interface cards, the software selects one of them randomly and applies these settings to it.
4. Select **Install with the current settings**.

As a result, CentOS and Acronis Cyber Protect will be installed on the machine.

Further actions

After the installation is completed, the software displays the links to the Cyber Protect web console and the Cockpit web console. Connect to the Cyber Protect web console to start using Acronis Cyber Protect: add more devices, create backups plans, and so on.

To add ESXi virtual machines, click **Add > VMware ESXi**, and then specify the address and credentials for the vCenter Server or stand-alone ESXi host.

There are no Acronis Cyber Protect settings that are configured in the Cockpit web console. The console is provided for convenience and troubleshooting.

Updating the software

1. Download and unpack the .zip archive with the new appliance version.
2. Boot the machine from the .iso unpacked in the previous step.
 - a. Save the .iso to your vSphere datastore.
 - b. Connect the .iso to the machine's CD/DVD drive.
 - c. Restart the machine.
 - d. [Only during the first update] Press **F2**, and then change the boot order so that CD/DVD drive comes first.
3. Select **Install or update Acronis Cyber Protect** , and then press **Enter**.
4. Select **Update**, and then press **Enter**.
5. Once the update is completed, disconnect the .iso from the machine's CD/DVD drive.

As a result, Acronis Cyber Protect will be updated. If the CentOS version in the .iso file is also newer than the version on the disk, the operating system will be updated before updating Acronis Cyber Protect.

Adding machines from the Cyber Protect web console

You can add a machine in one of the following ways:

- By downloading the setup program and running it locally on the target machine.
- By remotely installing a protection agent on the target machine.

Limitations

- Remote installation is only available with a management server running on a Windows machine. Target machines must also be running Windows.
- Remote installation is not supported on machines running Windows XP.
- Remote installation is not supported on domain controllers. To learn how to install a protection agent on a domain controller, refer to "Installation in Windows" (p. 117). Ensure that you customize the installation settings by selecting **Use the following account** under **Logon account for the agent service**. To learn more about this option, refer to "Required user rights for the service logon account" (p. 88).

Adding a machine running Windows

You can add a Windows machine by installing a protection agent remotely, in the Cyber Protect web console, or by downloading and running the setup program locally.

To install an agent remotely

Important

Before starting the installation, ensure that the prerequisites for remote installation are met and that there is at least one agent in your environment that can be used as deployment agent. For more information, refer to "Prerequisites for remote installation" (p. 110) and "Deployment agent" (p. 111).

1. In the Cyber Protect web console, go to **Devices > All devices**.
2. Click **Add**.
3. [To install Agent for Windows] Click **Windows**.
4. [To install another supported agent] Click the button that corresponds to the application that you want to protect.

The following agents are available:

- 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, go to step 9.

- Agent for Active Directory + Agent for Windows
- Agent for Office 365

5. In the pane that opens, select the deployment agent.
6. Specify the host name or IP address of the target machine, and the credentials of an account with administrative rights for that machine.

We recommend that you use the built-in Administrator account. To use another account, add that account to the Administrators group and modify the registry of the target machine as described in the following article: <https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows>.

7. Select the name or the IP address of the management server that the agent will use to access that server.

By default, the server name is selected. You may need to select the IP address instead if your management server has more than one network interface or if you are facing DNS issues that cause the agent registration to fail.

8. Click **Install**.
9. [If you selected **Microsoft Exchange Server > Exchange mailboxes** in step 4] Specify the machine where the **Client Access** server role (CAS) of Microsoft Exchange Server is enabled. For more information, refer to "Mailbox backup" (p. 452).

To download and install an agent locally

1. In the Cyber Protect web console, click the account icon in the upper-right corner, and then click **Downloads**.

2. Click the name of the Windows installer that you need.
The setup program is downloaded to your machine.
3. Run the setup program on the machine that you want to protect. For more information, refer to "Installation in Windows" (p. 117).

Prerequisites for remote installation

- For successful installation on a remote machine running Windows 7 or later, the option **Control panel > Folder options > View > Use Sharing Wizard** must be *disabled* on that machine.
- For successful installation on a remote machine that is *not* a member of an Active Directory domain, User Account Control (UAC) must be *disabled* on that machine. For more information on how to disable it, refer to "To disable UAC" (p. 111).
- By default, the credentials of the built-in Administrator account are required for remote installation on any Windows machine. To perform remote installation by using the credentials of another administrator account, User Account Control (UAC) remote restrictions must be *disabled*. For more information on how to disable them, refer to "To disable UAC remote restrictions" (p. 111).
- File and Printer Sharing must be *enabled* on the remote machine. To access this option:
 - [On a machine running Windows 2003 Server] Go to **Control panel > Windows Firewall > Exceptions > File and Printer Sharing**.
 - [On a machine running Windows Server 2008, Windows 7, or later] Go to **Control panel > Windows Firewall > Network and Sharing Center > Change advanced sharing settings**.
- Acronis Cyber Protect uses TCP ports **445**, **25001**, and **43234** for remote installation. Port **445** is automatically opened when you enable File and Printer Sharing. Ports 43234 and 25001 are automatically opened through Windows Firewall. If you use a different firewall, make sure that these three ports are open (added to exceptions) for both incoming and outgoing requests.

After the remote installation is complete, port **25001** is automatically closed through Windows Firewall. Ports **445** and **43234** need to remain open if you want to update the agent remotely in the future. Port **25001** is automatically opened and closed through Windows Firewall during each update. If you use a different firewall, keep all the three ports open.

Note

Remote installation is not supported on machines running Windows XP.

Note

Remote installation is not supported on domain controllers. To learn how to install a protection agent on a domain controller, refer to "Installation in Windows" (p. 117). Ensure that you customize the installation settings by selecting **Use the following account** under **Logon account for the agent service**. To learn more about this option, refer to "Required user rights for the service logon account" (p. 88).

Requirements on User Account Control (UAC)

On a machine that is running Windows 7 or later and which 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**.

Deployment agent

To install protection agents on remote machines from the Cyber Protect web console, at least one agent must be already installed in your environment. This agent will serve as a deployment agent for remote installation, and will connect to the management server and the target remote machine.

Usually, the first protection agent in the environment is the agent that you install together with the management server. However, you can select each Agent for Windows in the environment to be the deployment agent.

Note

When you use autodiscovery to install protection agents on multiple machines, the deployment agent is called discovery agent.

How the deployment agent works

1. The deployment agent connects to the management server and downloads the `web_installer.exe` file.
2. The deployment agent connects to the remote machine by using the host name or the IP address of that machine, and the administrator credentials that you specify, and then uploads the `web_installer.exe` file to it.
3. The `web_installer.exe` file runs on the remote machine in the unattended mode.
4. Depending on the scope of the required installation, the web installer retrieves additional installation packages from the `installation_files` folder on the management server, and then installs them on the target machine, by using the `msiexec` command.

The `installation_files` folder is located in:

- Windows: `\Program Files\Acronis\RemoteInstallationFiles\`
- Linux: `/usr/lib/Acronis/RemoteInstallationFiles/`

5. After the installation completes, the agent is registered on the management server.

Components for remote installation

The components for remote installation are installed by default when you install the management server.

Depending on the operating system of the machine on which the management server runs, you can find these components in the following locations:

- Windows: `%Program Files%\Acronis\RemoteInstallationFiles\installation_files`
- Linux: `/usr/lib/Acronis/RemoteInstallationFiles/installation_files`

These locations might not be available if you upgraded from an older version of Acronis Cyber Protect or if you explicitly excluded **Components for Remote installation** when you installed the management server. In this case, you need to add the components for remote installation manually, by updating and modifying your existing installation of Acronis Cyber Protect.

To add the components for remote installation to an existing installation

1. Download the latest installation file for Acronis Cyber Protect from the [Acronis website](#).
Select the installation file that corresponds to the bitness of your operating system. In most cases, you will need the **Windows 64-bit** installation file. If you need to install protection agents remotely on 32-bit machines, download the **Windows 32/64-bit** installation file.
2. On the machine on which the management server runs, start the installation file, and then select **Update**.

3. After the update completes, start the installation file again, and then select **Modify the current installation**.
4. Select **Components for Remote installation**, and then click **Done**.

After the installation completes, you will be able to install protection agents on remote machines from the Cyber Protect web console.

Adding a machine running Linux

You can add a Linux machine only by installing the protection agent locally. Remote installation is not supported.

To add a machine running Linux

1. In the Cyber Protect web console, click **All devices > Add**.
2. Click **Linux**.
The setup program is downloaded to your machine.
3. Run the setup program on the machine that you want to protect. For more information, refer to "Installation in Linux" (p. 119).

Adding a machine running macOS

You can add a macOS machine only by installing the protection agent locally. Remote installation is not supported.

To add a machine running macOS

1. In the Cyber Protect web console, click **All devices > Add**.
2. Click **Mac**.
The setup program is downloaded to your machine.
3. Run the setup program on the machine that you want to protect. For more information, refer to "Installation in macOS" (p. 120).

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 \(Virtual Appliance\)](#)

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 \(Windows\)](#)

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](#)".

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](#)

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](#)

This is a necessary step after you have installed Agent for VMware (Windows) manually or deployed [Acronis Cyber Protect appliance](#). Also, you can associate an already configured Agent for VMware with another vCenter Server or stand-alone ESXi host.

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](#) on the vCenter Server or ESXi.
5. Select the name or the IP address of the management server that the agent will use to access that server.

By default, the server name is selected. You may need to select the IP address instead if your management server has more than one network interface or if you are facing DNS issues that cause the agent registration to fail.
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**.

Installing Agent for VMware (Windows)

Preparation

Follow the preparatory steps described in the "[Adding a machine running Windows](#)" section.

Installation

1. Click **All devices > Add**.
2. Click **VMware ESXi**.
3. Select **Remotely install on a machine running Windows**.
4. Select the deployment agent.
5. Specify the host name or IP address of the target machine, and the credentials of an account with administrative privileges on that machine.
6. Select the name or the IP address of the management server that the agent will use to access that server.

By default, the server name is selected. You may need to select the IP address instead if your management server has more than one network interface or if you are facing DNS issues that cause the agent registration to fail.
7. Click **Connect**.
8. 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](#) on the vCenter Server or ESXi.
9. Click **Install** to install the agent.

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](#).

To register Agent for VMware

1. Click **All devices > Add**.
2. Click **VMware ESXi**.
3. Select **Register an already installed agent**.
4. Select the deployment agent.
5. 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.

6. Select the name or the IP address of the management server that the agent will use to access that server.
By default, the server name is selected. You may need to select the IP address instead if your management server has more than one network interface or if you are facing DNS issues that cause the agent registration to fail.
7. Click **Connect**.
8. 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](#) on the vCenter Server or ESXi.
9. Click **Register** to register the agent.

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](#) on the vCenter Server or ESXi.
6. Click **Configure** to save the changes.

Adding a Scale Computing HC3 cluster

To add a Scale Computing HC3 cluster to the Cyber Protect management server

1. [Deploy an Agent for Scale Computing HC3 \(Virtual Appliance\)](#) in the cluster.
2. [Configure](#) its connection both to this cluster and to the Cyber Protect management server.

Installing agents locally

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 Cyber Protect setup program.
2. [Optional] To change the language of the setup program, click **Setup language**.
3. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
4. Select **Install a protection agent**.
5. Do any of the following:
 - Click **Install**.

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
 - Cyber Protect 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" (p. 86).
 - 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" \(p. 192\)](#).
6. 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 "Step 1: Generating a registration token" (p. 193).
 - c. Click **Done**.
7. 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 "Units and administrative accounts" (p. 634).

8. Proceed with the installation.
9. After the installation completes, click **Close**.
10. 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 Cyber Protect web 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" (p. 452).

To install Agent for VMware (Windows), Agent for Office 365, Agent for Oracle, or Agent for Exchange on a machine without Microsoft Exchange Server

1. Log on as an administrator and start the Acronis Cyber Protect setup program.
2. [Optional] To change the language of the setup program, click **Setup language**.
3. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
4. Select **Install a protection agent**, and then click **Customize installation settings**.
5. Next to **What to install**, click **Change**.
6. 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.
7. Specify the management server where the machine with the agent will be registered:
 - a. Next to **Acronis Cyber Protect 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 "Step 1: Generating a registration token" (p. 193).
 - d. Click **Done**.
8. 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 "Units and administrative accounts" (p. 634).
9. [Optional] Change other installation settings as described in "Customizing installation settings" (p. 86).
10. Click **Install** to proceed with the installation.
11. After the installation completes, click **Close**.
12. [Only when installing Agent for VMware (Windows)] Perform the procedure described in "Configuring an already registered Agent for VMware" (p. 116).

13. [Only when installing Agent for Exchange] Open the Cyber Protect web 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" (p. 452).

Installation in Linux

Preparation

1. Ensure that the necessary [Linux packages](#) are installed on the machine.
2. When installing the agent in SUSE Linux, ensure that you use `su -` instead of `sudo`. Otherwise, the following error occurs when you try to register the agent via the Cyber Protect web console:
Failed to launch the web browser. No display available.
Some Linux distributions, such as SUSE, do not pass the `DISPLAY` variable when using `sudo`, and the installer cannot open the browser in the graphical user interface (GUI).

Installation

To install Agent for Linux, you need at least 2 GB of free disk space.

To install Agent for Linux

1. As the root user, navigate to the directory with the installation file (.i686 or .x86_64 file), make the file executable, and then run it.

```
chmod +x <installation file name>
```

```
./<installation file name>
```

2. Accept the terms of the license agreement.
3. Specify the components to install:
 - a. Clear the **Acronis Cyber Protect 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.
 - 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

The installation generates a new key that is used for signing the kernel modules. You must enroll this new key to the Machine Owner Key (MOK) list by restarting the machine. Without enrolling the new key, your agent will not be operational. If you enable the UEFI Secure Boot after the agent is installed, you need to reinstall the agent.

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

Installation in macOS

To install Agent for Mac

1. Double-click the installation file (.dmg).
2. Wait while the operating system mounts the installation disk image.
3. Double-click **Install**, and then click **Continue**.
4. [Optional] Click **Change install location** to change the disk where the software will be installed.
By default, the system startup disk is selected.
5. Click **Install**. If prompted, enter the administrator's user name and password.
6. 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.
 - c. Click **Register**.
7. If prompted, select whether the machine with the agent will be added to the organization or to one of the units, and then click **Done**.
This prompt appears if the account specified in the previous step administers more than one unit or an organization with at least one unit.
8. After the installation completes, click **Close**.

Unattended installation or uninstallation

Unattended installation or uninstallation in Windows

This section describes how to install or uninstall Acronis Cyber Protect 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" (p. 192).

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. [Not available in all setup programs] In **Component bitness**, select **32-bit** or **64-bit**.
4. In **What to install**, select the components that you want to install, and then click **Done**.
The installation packages for these components will be extracted from the setup program.
5. In **Acronis Cyber Protect Management Server**, select **Use credentials** or **Use registration token**. Depending on your choice, specify the credentials or the registration token, and then click **Done**.
For more information on how to generate a registration token, refer to "Step 1: Generating a registration token" (p. 193).
6. [Only when installing on a domain controller] In **Logon account for the agent service**, select **Use the following account**. Specify the user account under which the agent service will run, and then click **Done**. For security reasons, the setup program does not automatically create new accounts on a domain controller.

Note

The user account that you specify must be granted the Log on as a service right.

This account must have already been used on the domain controller, in order for its profile folder to be created on that machine.

For more information about installing the agent on a read-only domain controller, refer to [this knowledge base article](#).

7. Review or modify other installation settings that will be added to the `.mst` file, and then click **Proceed**.
8. Select the folder where the `.mst` transform will be generated and the `.msi` and `.cab` installation packages will be extracted, and then 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

On the command line, run the following command:

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

Where:

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

For example, `msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`

Installing or uninstalling the product by specifying parameters manually

On the command line, 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.

Available parameters and their values are described in "Common parameters" (p. 123).

Examples

- Installing Management Server and Components for Remote Installation.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn  
ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature  
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_  
AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
```

- Installing Agent for Windows, Command-Line Tool, and Cyber Protect Monitor. Registering the machine with the agent on a previously installed management server.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn  
ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor  
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_  
AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
```

- Updating Management Server, Storage Node, Catalog Service, and the protection agent.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn  
ADDLOCAL=AcronisCentralizedManagementServer,BackupAndRecoveryAgent,AgentsCoreComponen  
ts,StorageServer,CatalogBrowser CATALOG_DATA_MIGRATION_PATH="C:\MyFolder\tmp"
```

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](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
ComponentRegisterFeature	AcronisCentralizedManagementServer	32-bit/64-bit	Components for Remote Installation
AtpScanService	AcronisCentralizedManagementServer	32-bit/64-bit	Scan Service
AgentsCoreComponents		32-bit/64-bit	Core components for agents
BackupAndRecoveryAgent	AgentsCoreComponents	32-bit/64-bit	Agent for Windows
ArxAgentFeature	BackupAndRecoveryAgent	32-	Agent for

		bit/64-bit	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
ArxOnlineAgentFeature	AgentsCoreComponents	32-bit/64-bit	Agent for Office 365
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)
ScaleVirtualAppliance		32-bit/64-bit	Agent for Scale Computing HC3 (Virtual Appliance)
CommandLineTool		32-bit/64-bit	Command-Line Tool
TrayMonitor	BackupAndRecoveryAgent	32-bit/64-bit	Cyber Protect Monitor
BackupAndRecoveryBootableComponents		32-bit/64-bit	Bootable Media

		bit	Builder
PXEServer		32-bit/64-bit	PXE Server
StorageServer	BackupAndRecoveryAgent	64-bit	Storage Node
CatalogBrowser	JRE 8 Update 111 or later	64-bit	Catalog Service

TARGETDIR=<path>

The folder where the product will be installed.

REBOOT=ReallySuppress

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

CURRENT_LANGUAGE=<language ID>

The product language. Available values are as follows: en, en_GB, cs, da, de, es_ES, fr, ko, it, hu, nl, ja, pl, pt, pt_BR, ru, tr, zh, zh_TW.

ACEP_AGREEMENT={0,1}

If the value is 1, the machine will participate in the Acronis Customer Experience Program (ACEP).

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

The host name or IP address of the machine where the management server is installed. Agents, Storage Node, and Catalog Service 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).

With this parameter, 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 Cyber Protect web console as described in [Deploying agents through Group Policy](#).

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, Storage Node, and Catalog Service specified in the ADDLOCAL parameter will be added to this unit.

To learn a unit ID, in the Cyber Protect web console, click **Settings > Accounts**, 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

HTTP_PROXY_ADDRESS=<IP address> and HTTP_PROXY_PORT=<port>

The HTTP proxy server to be used by the agent. Without these parameters, no proxy server will be used.

HTTP_PROXY_LOGIN=<login> and HTTP_PROXY_PASSWORD=<password>

The credentials for the HTTP proxy server. Use these parameters if the server requires authentication.

HTTP_PROXY_ONLINE_BACKUP={0, 1}

If the value is 0, or the parameter is not specified, the agent will use the proxy server only for backup and recovery from the cloud. If the value is 1, the agent also will connect to the management server through the proxy server.

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"](#).

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.

Storage node installation parameters

Account under which the storage node service will run

Specify one of the following parameters:

- `ASN_USE_SYSTEM_ACCOUNT={0,1}`
If the value is 1, the system account will be used.
- `ASN_CREATE_NEW_ACCOUNT={0,1}`
If the value is 1, a new account will be created.
- `ASN_SERVICE_USERNAME=<user name>` and `ASN_SERVICE_PASSWORD=<password>`
The specified account will be used.

Catalog service installation parameters

`CATALOG_DATA_MIGRATION_PATH=<path>`

Use this parameter to migrate the catalog data to the new version of the catalog service in Acronis Cyber Protect 15 Update 4. Specify the path to the temporary folder where the catalog data will be exported.

`SKIP_CATALOG_DATA_MIGRATION=1`

Use this parameter to skip the migration of catalog data.

The parameters `SKIP_CATALOG_DATA_MIGRATION` and `CATALOG_DATA_MIGRATION_PATH` are mutually exclusive.

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.

Unattended installation or uninstallation in Linux

This section describes how to install or uninstall Acronis Cyber Protect 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

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

--language=<language ID>

The product language. Available values are as follows: en, en_GB, cs, da, de, es_ES, fr, ko, it, hu, nl, ja, pl, pt, pt_BR, ru, tr, zh, zh_TW.

{-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`
 - Does 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.

With this parameter, you must specify either the token parameter, or the login and password parameters.

`--token=<token>`

The registration token that was generated in the Cyber Protect web console as described in [Deploying agents through Group Policy](#).

`{-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 Cyber Protect web console, click **Settings** > **Accounts**, 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 `nothttps`, 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.

- `--http-proxy-host=<IP address>` and `--http-proxy-port=<port>`
 - The HTTP proxy server that the agent will use for backup and recovery from the cloud and for connection to the management server. Without these parameters, no proxy server will be used.
- `--http-proxy-login=<login>` and `--http-proxy-password=<password>`
 - The credentials for the HTTP proxy server. Use these parameters if the server requires authentication.
- `--no-proxy-to-ams`
 - The protection agent will connect to the management server without using the proxy server that is specified by the `--http-proxy-host` and `--http-proxy-port` parameters.

Uninstallation parameters

`{-u|--uninstall}`

Uninstalls the product.

`--purge`

Removes the product's logs, tasks, 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.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Installing Management Server, specifying custom ports.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --  
web-server-port 6543 --ams-tcp-port 8123
```

- Installing Agent for Linux and registering it on the specified Management Server.

```
./AcronisCyberProtect_15_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.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -  
-login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

Unattended installation or uninstallation in macOS

This section describes how to install, register, and uninstall the protection agent in the unattended mode on a machine running macOS, by using the command line. For information on how to download the installation file (.dmg), refer to ["Adding a machine running macOS"](#).

To install Agent for Mac

1. Create a temporary directory where you will mount the installation file (.dmg).

```
mkdir <dmg_root>
```

Here, the <dmg_root> is a name of your choice.

2. Mount the .dmg file.

```
hdiutil attach <dmg_file> -mountpoint <dmg_root>
```

Here, the <dmg_file> is the name of the installation file. For example, **AcronisCyberProtect_15_MAC.dmg**.

3. Run the installer.

```
sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
```

4. Detach the installation file (.dmg).

```
hdiutil detach <dmg_root>
```

Examples

-

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/AcronisCyberProtect_15_MAC.dmg -mountpoint mydirectory
```

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

To register Agent for Mac

Do one of the following:

- Register the agent under a specific administrator account.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> -u <user name> -p <password>
```

The <management server address:port> is the host name or the IP address of the machine where the Acronis Cyber Protect Management Server is installed. The port number is mandatory if it is different from the default one (9877).

The <user name> and <password> are the credentials for the administrator account under which the agent will be registered.

- Register the agent in a specific unit.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> -u <user name> -p <password> --tenant <unit ID>
```

To learn the unit ID, in the Cyber Protect web console, click **Settings > Accounts**, select the desired unit, and then click **Details**.

Important

Administrators can register agents by specifying the unit ID only at their level of the organization hierarchy. Unit administrators can register machines in their own units and their subunits.

Organization administrators can register machines in all units. For more information about the different administrator accounts, refer to ["Administering user accounts and organization units"](#).

- Register the agent by using a registration token.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> --token <token>
```

The registration token is a series of 12 characters, separated by hyphens in three segments. You can generate one in the Cyber Protect web console, as described in ["Deploying agents through Group Policy"](#).

Important

In macOS 10.14 or later, you need to grant the protection agent full disk access. To do so, go to **Applications > Utilities**, and then run **Cyber Protect Agent Assistant**. Then, follow the instructions in the application window.

Examples

Registration with a user name and password.

- ```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

Registration with a unit ID and administrator credentials.

- ```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 4dd941c1-c03f-11ea-
86d8-005056bdd3a0
```

Registration with a token.

- ```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 --token D91D-DC46-4F0B
```

### *To uninstall Agent for Mac*

Run the following command:

- ```
sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
Uninstall.app/Contents/MacOS/AgentUninstall /confirm
```

To uninstall the Agent for Mac and remove all logs, tasks and configuration settings, run the following command:

- ```
sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
```

## Registering and unregistering machines manually

Machines are automatically registered on the management server when you install the protection agent on them. When you uninstall the protection agent, the machines are automatically unregistered and disappear from the Cyber Protect web console.

You can also register a machine manually, by using the command line interface. You might need to use the manual registration, for example, if the automatic registration fails or if you want to register an existing machine under a new user account.

You can find the registration tool in the following locations:

- Windows: Program Files\Acronis\RegisterAgentTool\register\_agent.exe
- Linux: /usr/lib/Acronis/RegisterAgentTool/RegisterAgent
- macOS: /Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent

### ***To register a machine by using a user name and password***

#### ***In Windows***

At the command line, run the following command:

```
<path to the registration tool> -o register -a <management server address:port> -u <user name> -p <password>
```

For example:

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

#### ***In Linux***

At the command line, run the following command:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a <management server address:port> -u <user name> -p <password>
```

For example:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

#### ***In macOS***

At the command line, run the following command:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -a <management server address:port> -u <user name> -p <password>
```

For example:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

The <management server address:port> is the host name or the IP address of the machine on which the management server is installed. If you use the default port 9877, you can omit specifying it in this command.

The <user name> and <password> are the credentials of the account under which the agent will be registered. If your password contains special characters or blank spaces, see "Passwords with special characters or blank spaces" (p. 138).

### ***To register a machine in a specific unit by using a user name and password***

#### ***In Windows***

At the command line, run the following command:

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <password> --tenant <unit ID>
```

For example:

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

#### ***In Linux***

At the command line, run the following command:

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <password> --tenant <unit ID>
```

For example:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

#### ***In macOS***

At the command line, run the following command:

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <password> --tenant <unit ID>
```

For example:



```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant
590b1dd7-8adb-11ea-bf44-0050569deecf
```

The <management server address:port> is the host name or the IP address of the machine on which the management server is installed. If you use the default port 9877, you can omit specifying it in this command.

The <user name> and <password> are the credentials of account under which the agent will be registered. If your password contains special characters or blank spaces, see "Passwords with special characters or blank spaces" (p. 138).

To check the unit ID, in the Cyber Protect web console, go to **Settings > Accounts**. Select the unit that you need, and then click **Details**.

---

### Important

You can register agents only at your level of the organization hierarchy. Unit administrators can register agents in their own units and their subunits. Organization administrators can register agents in all units. For more information about the different administrator accounts, see "Administering user accounts and organization units" (p. 634).

---

### *To register a machine by using a registration token*

#### *In Windows*

At the command line, run the following command:

```
<path to the registration tool> -o register -a <management server address:port> --token
<token>
```

For example:

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

#### *In Linux*

At the command line, run the following command:

```
<path to the registration tool> -o register -a <management server address:port> --token
<token>
```

For example:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

#### *In macOS*

At the command line, run the following command:

```
<path to the registration tool> -o register -a <management server address:port> --token <token>
```

For example:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -a https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB
```

### ***To unregister a machine***

#### ***In Windows***

At the command line, run the following command:

```
<path to the registration tool> -o unregister
```

For example:

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

#### ***In Linux***

At the command line, run the following command:

```
<path to the registration tool> -o unregister
```

For example:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

#### ***In macOS***

At the command line, run the following command:

```
<path to the registration tool> -o unregister
```

For example:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

## Passwords with special characters or blank spaces

If your password contains special characters or blank spaces, enclose it in quotation marks when you type it on the command line.

### ***On-premises deployment***

- Command template

```
<path to the registration tool> -o register -a <management server address:port> -u
<user name> -p <"password">
```

- Windows

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johnspassword"
```

- Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johnspassword"
```

- macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johnspassword"
```

## **Cloud deployment**

- Command template

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user
name> -p <"password">
```

- Windows

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://cloud.company.com -u johndoe -p "johnspassword"
```

- Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p "johnspassword"
```

- macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p "johnspassword"
```

If this command fails, encode your password into base64 format at <https://www.base64encode.org/>. Then, at the command line, specify the encoded password by using the -b or --base64 parameter.

## **On-premises deployment**

- Command template

```
<path to the registration tool> -o register -a <management server address:port> -u
<user name> -b -p <encoded password>
```

- Windows

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

- Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

- macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

## Cloud deployment

- Command template

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user
name> -b -p <encoded password>
```

- Windows

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

- Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

- macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

## Checking for software updates

This functionality is available only to [organization administrators](#).

Each time you sign in to the Cyber Protect web console, Acronis Cyber Protect checks whether a new version is available on the Acronis website. If so, the Cyber Protect web console shows a download

link for the new version at the bottom of each page under the **Devices**, **Plans**, and **Backup storage** tabs. The link is also available on the **Settings > Agents** page.

To enable or disable the automatic checks for updates, change the **Updates** system setting.

To check for updates manually, click the question mark icon in the top-right corner > **About > Check for updates** or the question mark icon > **Check for updates**.

## Migrating the management server

You can migrate a management server running on a Windows machine to another Windows machine in the same environment.

The migration process consists of the following phases:

1. "Operations on the source machine" (p. 141)  
In this phase, you prepare the data on the original management server for migration.
2. "Operations on the target machine" (p. 143)  
In this phase, you install and configure a new management server, and then copy the data from the original management server to the new one.

## Prerequisites

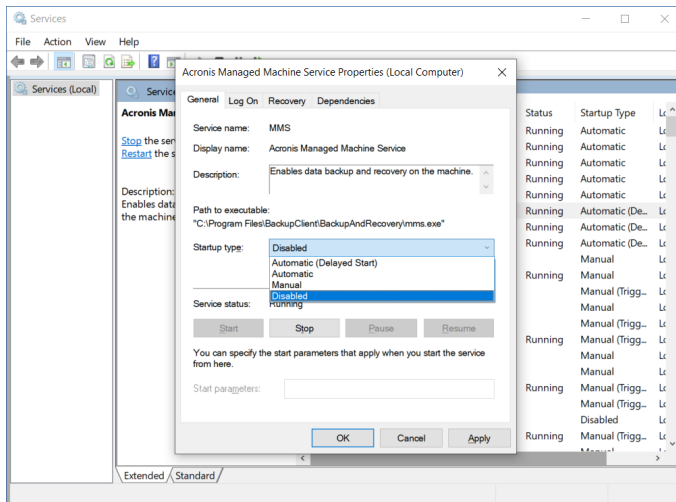
- The management server uses an external Microsoft SQL Server database. The Microsoft SQL Server instance is running on a dedicated machine.
- The protection agents are registered on the management server by using its host name, not its IP address.
- The version of management server is Acronis Cyber Protect Update 4 (build 29486) or later.
- The same version of the management server is installed on both the source and the target machine.

## Operations on the source machine

In this phase, you prepare the data from the original management server for migration.

### *To prepare the data for migration*

1. On the original management server machine, stop all Acronis services.
  - a. Open **Services**, and then disable the startup of the Acronis services, except for **Acronis Active Protection Service** and **Acronis Cyber Protection Service**.



- b. Open **Regedit**, and then disable **Acronis Active Protection Service** and **Acronis Cyber Protection Service**, by editing their keys:
  - In the key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService, open the **Start** value, and then set the value data to 4.
  - In the key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService, open the **Start** value, and then set the value data to 4.
2. Restart the management server machine, and then verify that the disabled Acronis services are not running.

### Note

Two services, **Acronis Scheduler Service Helper** and **Acronis TIB Mounter Monitor**, might still be running. You can safely ignore them.

3. [If the Cyber Protect Monitor component is installed on the management server machine] Quit Acronis Cyber Protect Monitor.
4. In Windows Command Prompt, change the owner of the %ProgramData%\Acronis and %ProgramFiles%\Acronis folders, by running the following commands:

```
takeown /f "%ProgramData%\Acronis" /r /d y
```

```
takeown /f "%ProgramFiles%\Acronis" /r /d y
```

5. Edit the access permissions to these folders and their subfolders, by running the following commands:

```
icacls "%ProgramData%\Acronis" /grant everyone:F /t
```

```
icacls "%ProgramFiles%\Acronis" /grant everyone:F /t
```

6. Copy the %ProgramData%\Acronis and %ProgramFiles%\Acronis folders to a network share that the new management server machine can access.
7. Shut down the original management server machine.

Next, follow the procedure in "Operations on the target machine" (p. 143).

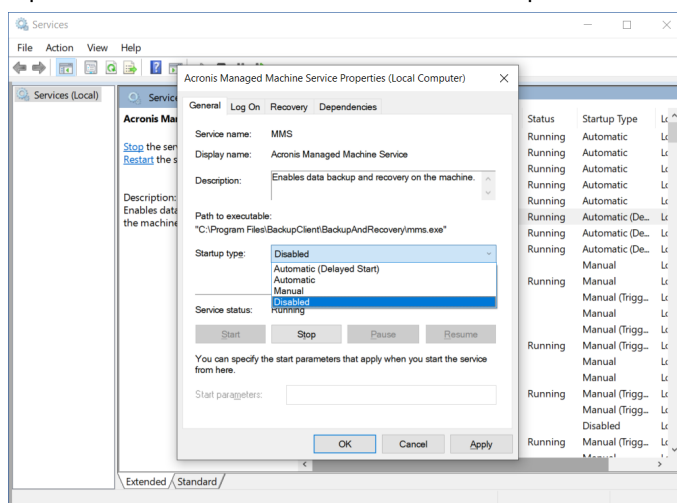
## Operations on the target machine

In this phase, you install and configure a new management server, and then you migrate the data to it.

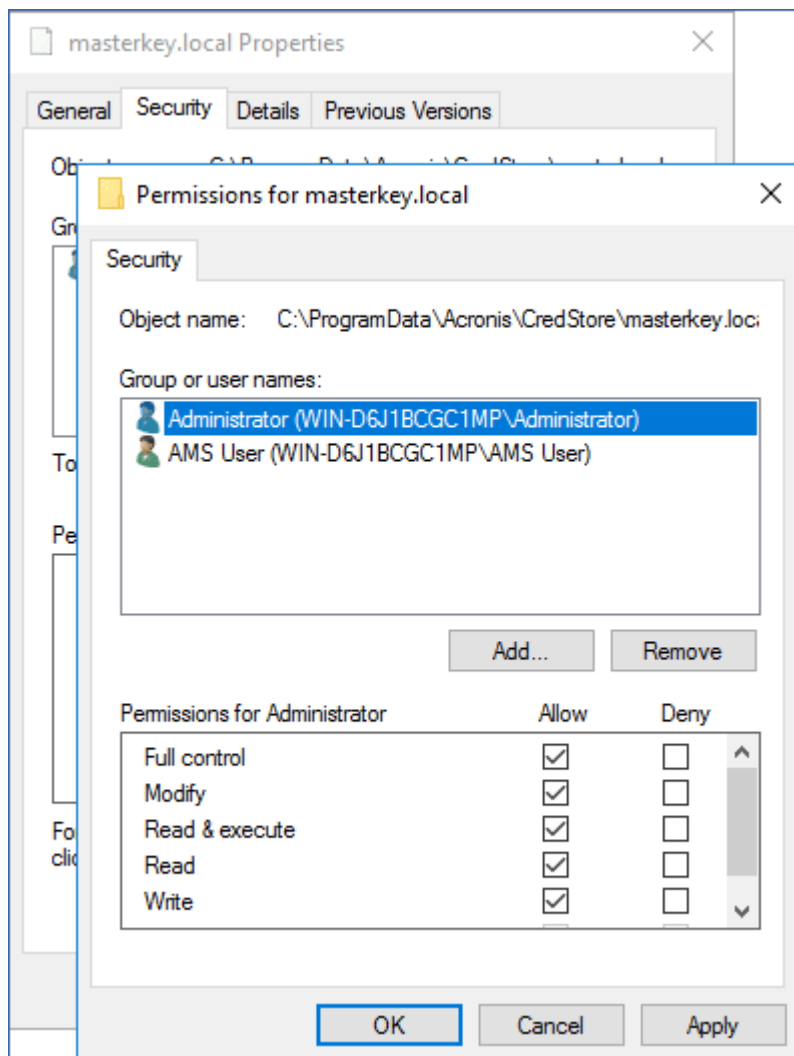
Before performing the operations on the target machine, ensure that you completed the procedure in "Operations on the source machine" (p. 141).

### *To migrate the data to the new management server*

1. Set the host name of the machine on which you will install the new management server. This name must be the same as the name of the machine with the original management server.
2. Create a firewall rule to block all traffic on TCP port 9877.
3. Run the Acronis Cyber Protect setup program.
  - a. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
  - b. Click **Customize installation settings**.
  - c. In **What to install**, select only the following components, and then click **Done**.
    - Management Server
    - Components for Remote Installation
    - Bootable Media Builder
    - Command-Line Tool
  - d. In **Database for the management server**, keep the default option **Use built-in SQLite**.
  - e. In **Logon account for the management server service**, use the same option as on the original management server.
4. Stop all Acronis services.
  - a. Open **Services**, and then disable the startup of all Acronis services.



- b. Restart the machine, and then verify that the disabled Acronis services are not running.
5. Navigate to %ProgramData%\Acronis\CredStore, and then adjust the permissions for the masterkey.local file, as follows:
  - a. Grant the file ownership to the **Administrator** user account.
  - b. Grant the **Administrator** user account **Full control** permissions.



6. Navigate to %ProgramData%\Acronis\AMS\AccessVault\config, and then grant the **Administrator** user account **Full control** permissions for the following files:
  - %ProgramData%\Acronis\AMS\AccessVault\config\preferred
  - %ProgramData%\Acronis\AMS\AccessVault\config\preferred.json
7. Replace the following folders with the folders that you copied from the original management server machine to a network share:
  - %ProgramData%\Acronis
  - %ProgramFiles%\Acronis

---

### Important

Overwrite the existing folders without deleting them first.

---



---

**Note**

If you see a message that the %ProgramFiles%\Acronis\ShellExtentions folder cannot be replaced, you can safely skip this folder.

---

8. Restore the permissions for the following files:

- %ProgramData%\Acronis\CredStore\masterkey.local – Remove the **Administrator** user account from the list of users with permissions.
- %ProgramData%\Acronis\AMS\AccessVault\config\preferred – Grant the **Administrator** user account only **Read** permission.
- %ProgramData%\Acronis\AMS\AccessVault\config\preferred.json – Grant the **Administrator** user account only **Read** permission.

9. Create a directory junction for the NGMP\latest folder.

- In Windows Command Prompt, navigate to %ProgramData%\Acronis\NGMP, and then delete the latest folder.

```
cd %ProgramData%\Acronis\NGMP
```

```
rmdir latest
```

- Create directory junction latest and point it to the folder named after the current NGMP version, for example:

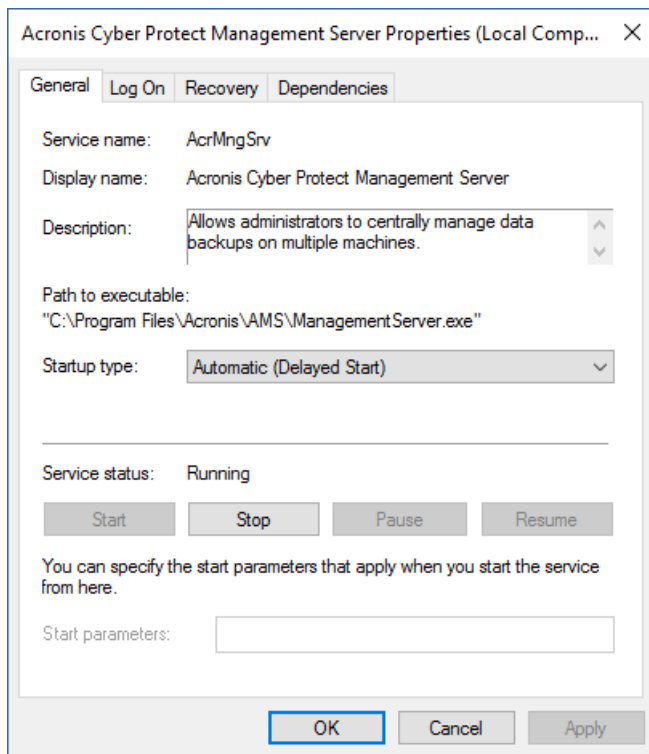
```
mklink /j latest C:\ProgramData\Acronis\NGMP\1.0.2653.0
```

10. Point the new management server to the Microsoft SQL Server database that the original management server used.

- a. Open **Regedit**.
- b. In the key HKEY\_LOCAL\_MACHINE\SOFTWARE\Acronis\AMS\Settings, modify the AmsDmldbProtocol value, by changing its data to config://C:\ProgramData\Acronis\AMS\mssql\dm1\_mssql.config.

11. Open **Services**, and then enable all disabled Acronis services.

Set the startup type of **Acronis Cyber Protect Management Server** to **Automatic (Delayed Start)** and the startup type of all other Acronis services to **Automatic**.



12. In the firewall, allow all traffic on TCP port 9877.
13. Restart the machine, and then verify the all Acronis services are running.
14. Run the Acronis Cyber Protect setup program and install the following items:
  - Agent for Windows
  - [Optional] Cyber Protect Monitor
15. Restart the machine.

## Cloud deployment

### Activating the account

When an administrator creates an account for you, an email message is sent to your email address. The message contains the following information:

- **An account activation link.** Click the link and set the password for the account. Remember your login that is shown on the account activation page.
- **A link to the Cyber Protect web console login page.** Use this link to access the console in the future. The login and password are the same as in the previous step.

## Preparation

### Step 1

Choose the agent, depending on what you are going to back up. For the information about the agents, refer to "Components" (p. 47).

## Step 2

Download the setup program. To find the download links, click **All devices > Add**.

The **Add devices** page provides web installers for each agent that is installed in Windows. A web installer is a small executable file that downloads the main setup program from the Internet and saves it as a temporary file. This file is deleted immediately after the installation.

If you want to store the setup programs locally, download a package containing all agents for installation in Windows by using the link at the bottom of the **Add devices** page. Both 32-bit and 64-bit packages are available. These packages enable you to customize the list of components to install. These packages also enable unattended installation, for example, via Group Policy. This advanced scenario is described in "Deploying agents through Group Policy" (p. 192).

To download the setup program for Agent for Office 365, click the account icon in the top-right corner, and then click **Downloads > Agent for Office 365**.

Installation in Linux and macOS is performed from ordinary setup programs.

All setup programs require an Internet connection to register the machine in the Cyber Protection service. If there is no Internet connection, the installation will fail.

## Step 3

Before the installation, ensure that your firewalls and other components of your network security system (such as a proxy sever) allow both inbound and outbound connections through the following TCP ports:

- Ports **443** and **8443**  
These ports are used for accessing the Cyber Protect web console, registering the agents, downloading the certificates, user authorization, and downloading files from the cloud storage.
- Ports in the range **7770 – 7800**  
The agents use these ports to communicate with the management server.
- Ports **44445** and **55556**  
The agents use these ports for data transfer during backup and recovery.

If a proxy server is enabled in your network, refer to "Configuring proxy server settings" (p. 149) to understand whether you need to configure these settings on each machine that runs a protection agent.

The minimum Internet connection speed required for managing an agent from the cloud is 1 Mbit/s (not to be confused with the data transfer rate acceptable for backing up to the cloud). Consider this if you use a low-bandwidth connection technology such as ADSL.

## TCP ports required for backup and replication of VMware virtual machines

- Port **443**

Agent for VMware (both Windows and Virtual Appliance) connects to this port on the ESXi host/vCenter server to perform VM management operations, such as create, update, and delete VMs on vSphere during backup, recovery, and VM replication operations.

- Port **902**

Agent for VMware (both Windows and Virtual Appliance) connects to this port on the ESXi host to establish NFC connections to read/write data on VM disks during backup, recovery, and VM replication operations.

- Port **3333**

If the Agent for VMware (Virtual Appliance) is running on the ESXi host/cluster that is the target for VM replication, VM replication traffic does not go directly to the ESXi host on port **902**. Instead, the traffic goes from the source Agent for VMware to TCP port **3333** on the Agent for VMware (Virtual Appliance) located on the target ESXi host/cluster.

The source Agent for VMware that reads data from the original VM disks can be anywhere else and can be of any type: Virtual Appliance or Windows.

The service that is responsible for accepting VM replication data on the target Agent for VMware (Virtual Appliance) is called "Replica disk server." This service is responsible for the WAN optimization techniques, such as traffic compression and deduplication during VM replication, including replica seeding (see [Seeding an initial replica](#)). When no Agent for VMware (Virtual Appliance) is running on the target ESXi host, this service is not available, and therefore the replica seeding scenario is not supported.

## Step 4

On the machine where you plan to install the protection agent, verify that the following local ports are not in use by other processes.

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**
- 127.0.0.1:**9850**

---

### Note

You do not have to open them in the firewall.

---

The Active Protection service is listening at TCP port **6109**. Verify that it is not in use by another process.

## Changing the ports used by the protection agent

Some of the ports required by the protection agent might be in use by other applications in your environment. To avoid conflicts, you can change the default ports used by the protection agent by modifying the following files.

- In Linux: /opt/Acronis/etc/aakore.yaml
- In Windows: \ProgramData\Acronis\Agent\etc\aakore.yaml

## Configuring proxy server settings

The protection agents can transfer data through an HTTP/HTTPS proxy server. The server must work through an HTTP tunnel without scanning or interfering with the HTTP traffic. Man-in-the-middle proxies are not supported.

Because the agent registers itself in the cloud during the installation, the proxy server settings must be provided during the installation or in advance.

### ***For Windows***

If a proxy server is configured in **Control panel > Internet Options > Connections**, the setup program reads the proxy server settings from the registry and uses them automatically.

Use this procedure if you want to perform the following tasks.

- Configure the proxy settings before the installation of the agent.
- Update the proxy settings after the installation of the agent.

To configure the proxy settings during the installation of the agent, see "Installing agents" (p. 153).

---

### **Note**

This procedure is valid only when the http-proxy.yaml file does not exist on the machine. If the http-proxy.yaml file exists on the machine, you must update the proxy settings in the file, as it overrides the settings in the aakore.yaml file.

The %programdata%\Acronis\Agent\var\aakore\http-proxy.yaml file is created when you configure the proxy server settings by using Cyber Protect Monitor. To open this file, you must be member of the Administrators group in Windows.

---

### ***To configure the proxy settings***

1. 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\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Replace proxy.company.com with your proxy server host name/IP address, and 000001bb with the hexadecimal value of the port number. For example, 000001bb is port 443.

4. If your proxy server requires authentication, replace proxy\_login and proxy\_password with the proxy server credentials. Otherwise, delete these lines from the file.
5. Save the document as proxy.reg.
6. Run the file as an administrator.
7. Confirm that you want to edit the Windows registry.
8. If the agent is not installed on this workload yet, install it now. If the agent is already installed on the workload, continue to the next step.
9. Open the %programdata%\Acronis\Agent\etc\aaakore.yaml file in a text editor.  
To open this file, you must be member of the Administrators group in Windows.
10. Locate the **env** section or create it, and then add the following lines.

```
env:
 http-proxy: proxy_login:proxy_password@proxy_address:port
 https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. Replace proxy\_login and proxy\_password with the proxy server credentials, and proxy\_address:port with the address and port number of the proxy server.
12. In the **Start** menu, click **Run**, type: **cmd**, and then click **OK**.
13. Restart the aakore service by running the following commands.

```
net stop aakore
net start aakore
```

14. Restart the agent by running the following commands.

```
net stop mms
net start mms
```

### **For Linux**

To configure the proxy setting during the installation of the agent, run the installation file with the --http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD parameters.

Use the following procedure to update the proxy settings after the installation of the protection agent.

### **To configure the proxy settings**

1. Open the /etc/Acronis/Global.config file in a text editor.
2. Do one of the following:
  - If the proxy settings were specified during the agent installation, locate the following section.

```
<key name="HttpProxy">
 <value name="Enabled" type="Tdword">"1"</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>
```

- If the proxy settings were not specified during the agent installation, copy the following lines and paste them into the file between the <registry name="Global">...</registry> tags.

```
<key name="HttpProxy">
 <value name="Enabled" type="Tdwor" >"1"</value>
 <value name="Host" type="TString">"ADDRESS"</value>
 <value name="Port" type="Tdwor" >"PORT"</value>
 <value name="Login" type="TString">"LOGIN"</value>
 <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

3. Replace ADDRESS with the new proxy server host name/IP address, and PORT with the decimal value of the port number.
4. If your proxy server requires authentication, replace LOGIN and PASSWORD with the proxy server credentials. Otherwise, delete these lines from the file.
5. Save the file.
6. Open file /opt/acronis/etc/aakore.yaml in a text editor.
7. Locate the **env** section or create it and add the following lines:

```
env:
 http-proxy: proxy_login:proxy_password@proxy_address:port
 https-proxy: proxy_login:proxy_password@proxy_address:port
```

8. Replace proxy\_login and proxy\_password with the proxy server credentials, and proxy\_address:port with the address and port number of the proxy server.
9. Restart the aakore service by running the following command.

```
sudo service aakore restart
```

10. Restart the agent by executing the running command in any directory.

```
sudo service acronis_mms restart
```

### **For macOS**

Use this procedure if you want to perform the following tasks.

- Configure the proxy settings before the installation of the agent.
- Update the proxy settings after the installation of the agent.

To configure the proxy settings during the installation of the agent, see "Installing agents" (p. 153).

### **To configure the proxy settings**

1. Create the /Library/Application Support/Acronis/Registry/Global.config file and open it in a text editor, such as Text Edit.

2. Copy and paste the following lines into the file.

```
<?xml version="1.0" ?>
<registry name="Global">
 <key name="HttpProxy">
 <value name="Enabled" type="Tdword">"1"</value>
 <value name="Host" type="TString">"proxy.company.com"</value>
 <value name="Port" type="Tdword">"443"</value>
 <value name="Login" type="TString">"proxy_login"</value>
 <value name="Password" type="TString">"proxy_password"</value>
 </key>
</registry>
```

3. Replace proxy.company.com with your proxy server host name/IP address, and 443 with the decimal value of the port number.
4. If your proxy server requires authentication, replace proxy\_login and proxy\_password with the proxy server credentials. Otherwise, delete these lines from the file.
5. Save the file.
6. If the agent is not installed on this workload yet, install it now. If the agent is already installed on the workload, continue to the next step.
7. Open the /Library/Application Support/Acronis/Agent/etc/aakore.yaml file in a text editor.
8. Locate the **env** section or create it and then add the following lines.

```
env:
 http-proxy: proxy_login:proxy_password@proxy_address:port
 https-proxy: proxy_login:proxy_password@proxy_address:port
```

9. Replace proxy\_login and proxy\_password with the proxy server credentials, and proxy\_address:port with the address and port number of the proxy server.
10. Go to **Applications > Utilities > Terminal**.
11. Restart the aakore service by running the following commands.

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. Restart the agent by running the following commands.

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

### ***For bootable media***

When working under bootable media, you might need to access the cloud storage via a proxy server. To configure the proxy server settings, click **Tools > Proxy server**, and then configure the proxy server host name/IP address, port, and credentials.



# Installing agents

## In Windows

1. Ensure that the machine is connected to the Internet.
2. Log on as an administrator and start the setup program.
3. [Optional] Click **Customize installation settings** and make the appropriate changes if you want:
  - To change the components to install (in particular, to disable installation of Cyber Protect Monitor and Command-Line Tool).
  - To change the method of registering the machine in the Cyber Protection service. You can switch from **Use Cyber Protect console** (default) to **Use credentials** or **Use registration token**.
  - To change the installation path.
  - To change the account for the agent service.
  - To verify or change the proxy server host name/IP address, port, and credentials. If a proxy server is enabled in Windows, it is detected and used automatically.
4. Click **Install**.
5. [Only when installing Agent for VMware] Specify the address and access credentials for the vCenter Server or stand-alone ESXi host whose virtual machines the agent will back up, and then click **Done**. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the [necessary privileges](#) on the vCenter Server or ESXi.
6. [Only when installing on a domain controller] Specify the user account under which the agent service will run, and then click **Done**. For security reasons, the setup program does not automatically create new accounts on a domain controller.

---

### Note

The user account that you specify must be granted the Log on as a service right.

This account must have already been used on the domain controller, in order for its profile folder to be created on that machine.

---

For more information about installing the agent on a read-only domain controller, refer to [this knowledge base article](#).

7. If you kept the default registration method **Use Cyber Protect console** in step 3, wait until the registration screen appears, and then proceed to the next step. Otherwise, no more actions are required.
8. Do one of the following:
  - Click **Register the machine**. In the opened browser window, sign in to the Cyber Protect web console, review the registration details, and then click **Confirm registration**.
  - Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. In this case, you will need to enter the registration code in the registration form. The

registration code is valid for one hour.

Alternatively, you can access the registration form by clicking **All devices > Add**, scrolling down to **Registration via code**, and then clicking **Register**.

---

9. **Note**

Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program, and then click **Register the machine**.

---

As a result, the machine will be assigned to the account that was used to log in to the Cyber Protect web console.

## In Linux

1. Ensure that the machine is connected to the Internet.

2. As the root user, run the installation file.

If a proxy server is enabled in your network, when running the file, specify the server host name/IP address and port in the following format: `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORD`.

If you want to change the default method of registering the machine in the Cyber Protection service, run the installation file with one of the following parameters:

- `--register-with-credentials` - to ask for a user name and password during the installation
- `--token=STRING` - to use a registration token
- `--skip-registration` - to skip the registration

3. Select the check boxes for the agents that you want to install. The following agents are available:

- **Agent for Linux**
- **Agent for Virtuozzo**

Agent for Virtuozzo cannot be installed without Agent for Linux.

4. If you kept the default registration method in step 2, proceed to the next step. Otherwise, enter the user name and password for the Cyber Protection service, or wait until the machine will be registered by using the token.

5. Do one of the following:

- Click **Register the machine**. In the opened browser window, sign in to the Cyber Protect web console, review the registration details, and then click **Confirm registration**.
- Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. In this case, you will need to enter the registration code in the registration form. The registration code is valid for one hour.

Alternatively, you can access the registration form by clicking **All devices > Add**, scrolling down to **Registration via code**, and then clicking **Register**.

---

6. **Note**

Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program and repeat the installation procedure.

---

As a result, the machine will be assigned to the account that was used to log in to the Cyber Protect web console.

7. 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, a new 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.

---

8. 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**

## In macOS

1. Ensure that the machine is connected to the Internet.
2. Double-click the installation file (.dmg).
3. Wait while the operating system mounts the installation disk image.
4. Double-click **Install**.
5. If a proxy server is enabled in your network, click **Protection agent** in the menu bar, click **Proxy server settings**, and then specify the proxy server host name/IP address, port, and credentials.
6. If prompted, provide administrator credentials.
7. Click **Continue**.
8. Wait until the registration screen appears.
9. Do one of the following:
  - Click **Register the machine**. In the opened browser window, sign in to the Cyber Protect web console, review the registration details, and then click **Confirm registration**.
  - Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. In this case, you will need to enter the registration code in the registration form. The

registration code is valid for one hour.

Alternatively, you can access the registration form by clicking **All devices > Add**, scrolling down to **Registration via code**, and then clicking **Register**.

10. **Tip** Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program and repeat the installation procedure.

As a result, the machine will be assigned to the account that was used to log in to the Cyber Protect web console.

## Changing the logon account on Windows machines

On the **Select components** screen, define the account under which the services will run by specifying **Logon account for the agent service**. You can select 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**

The account name will be Agent User for the agent.

- **Use the following account**

If you install the agent on a domain controller, the system prompts you to specify existing accounts (or the same account) for the agent. For security reasons, the system does not automatically create new accounts on a domain controller.

The user account that you specify when the setup program runs on a domain controller must be granted the Log on as a service right. This account must have already been used on the domain controller, in order for its profile folder to be created on that machine.

For more information about installing the agent on a read-only domain controller, refer to [this knowledge base article](#).

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.

## Privileges required for the logon account

A protection agent is run as a Managed Machine Service (MMS) on a Windows machine. The account under which the agent will run must have specific rights for the agent to work correctly. Thus, the MMS user should be assigned the following privileges:

1. Included in the **Backup Operators** and **Administrators** groups. On a Domain Controller, the user must be included in the group **Domain Admins**.
2. Granted the **Full Control** permission on the folder %PROGRAMDATA%\Acronis (in Windows XP and Server 2003, %ALLUSERSPROFILE%\Application Data\Acronis) and on its subfolders.

3. Granted the **Full Control** permission on certain registry keys in the following key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Acronis.
4. Assigned the following user rights:
  - Log on as a service
  - Adjust memory quotas for a process
  - Replace a process level token
  - Modify firmware environment values

### How to assign the user rights

Follow the instructions below to assign the user rights (this example uses the **Log on as service** user right, the steps are the same for other user rights):

1. Log on to the computer by using an account with administrative privileges.
2. Open **Administrative Tools** from **Control Panel** (or click Win+R, type **control admintools**, and press Enter) and open **Local Security Policy**.
3. Expand **Local Policies** and click on **User Rights Assignment**.
4. In the right pane, right-click **Log on as a service** and select **Properties**.
5. Click on the **Add User or Group...** button to add a new user.
6. In the **Select Users, Computers, Service Accounts, or Groups** window, find the user you wish to enter and click **OK**.
7. Click **OK** in the **Log on as a service Properties** to save the changes.

---

#### Important

Ensure that the user which you have added to the **Log on as service** user right is not listed in the **Deny log on as a service** policy in **Local Security Policy**.

---

Note that it is not recommended to change logon accounts manually after the installation is completed.

## Unattended installation or uninstallation

### Unattended installation or uninstallation in Windows

This section describes how to install or uninstall protection agents 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" (p. 192).

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 on 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, and then click **Done**.  
The installation packages for these components will be extracted from the setup program.
4. In **Registration settings**, select **Use credentials** or **Use registration token**. For more information on how to generate a registration token, refer to "Step 1: Generating a registration token" (p. 193).
5. [Only when installing on a domain controller] In **Logon account for the agent service**, select **Use the following account**. Specify the user account under which the agent service will run, and then click **Done**. For security reasons, the setup program does not automatically create new accounts on a domain controller.

---

### Note

The user account that you specify must be granted the Log on as a service right.

This account must have already been used on the domain controller, in order for its profile folder to be created on that machine.

---

For more information about installing the agent on a read-only domain controller, refer to [this knowledge base article](#).

6. Review or modify other installation settings that will be added to the .mst file, and then click **Proceed**.
7. Select the folder where the .mst transform will be generated and the .msi and .cab installation packages will be extracted, and then click **Generate**.

## Installing the product by using the .mst transform

On the command line, run the following command.

*Command template:*

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

Where:

- <package name> is the name of the .msi file.
- <transform name> is the name of the transform.

*Command example:*

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

## Installing or uninstalling the product by specifying parameters manually

On the command line, run the following command.

*Command template (installing):*

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

Here, <package name> is the name of the .msi file. All available parameters and their values are described in "Basic parameters" (p. 159).

*Command template (uninstalling):*

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

The .msi package must be of the same version as the product that you want to uninstall.

## 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](https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx).

### Installation parameters

## Basic parameters

ADDLOCAL=<list of components>

The components to be installed, separated by commas and 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
MmsMspComponents		32-bit/64-bit	Core components for agents
BackupAndRecoveryAgent	MmsMspComponents	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

ArxOnlineAgentFeature	MmsMspComponents	32-bit/64-bit	Agent for Office 365
OracleAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Oracle
AcronisESXSupport	MmsMspComponents	64-bit	Agent for VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32-bit/64-bit	Agent for Hyper-V
CommandLineTool		32-bit/64-bit	Command-Line Tool
TrayMonitor	BackupAndRecoveryAgent	32-bit/64-bit	Cyber Protect Monitor

TARGETDIR=<path>

The folder where the product will be installed. By default, this folder is: C:\Program Files\BackupClient.

REBOOT=ReallySuppress

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

/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.

CURRENT\_LANGUAGE=<language ID>

The product language. Available values are as follows: en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt\_BR, ru, fi, sr, sv, tr, zh, zh\_TW.

If this parameter is not specified, the product language will be defined by your system language on the condition that it is in the list above. Otherwise, the product language will set to English (en).

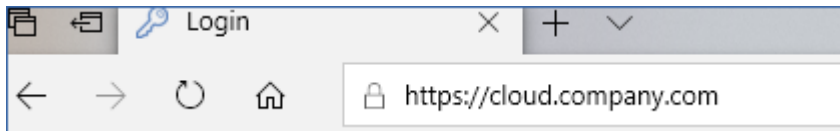
## Registration parameters

REGISTRATION\_ADDRESS

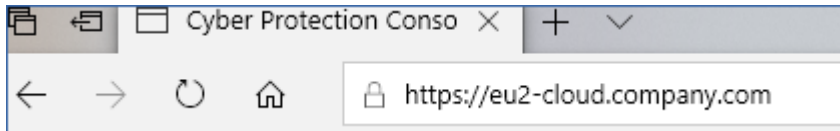
This is the URL for the Cyber Protect service. You can use this parameter either with the REGISTRATION\_LOGIN and REGISTRATION\_PASSWORD parameters, or with the REGISTRATION\_TOKEN one.

- When you use REGISTRATION\_ADDRESS with REGISTRATION\_LOGIN and REGISTRATION\_PASSWORD parameters, specify the address that you use **to log in** to the Cyber Protect service. For example, <https://cloud.company.com>:





- When you use REGISTRATION\_ADDRESS with the REGISTRATION\_TOKEN parameter, specify the exact datacenter address. This is the URL that you see **once you are logged in** to the Cyber Protect service. For example, https://eu2-cloud.company.com.



Do not use https://cloud.company.com here.

REGISTRATION\_LOGIN and REGISTRATION\_PASSWORD

Credentials for the account under which the agent will be registered in the Cyber Protect service. This cannot be a partner administrator account.

REGISTRATION\_PASSWORD\_ENCODED

Password for the account under which the agent will be registered in the Cyber Protect service, encoded in base64. For more information on how to encode your password, refer to ["Registering machines manually"](#).

REGISTRATION\_TOKEN

The registration token is a series of 12 characters, separated by hyphens in three segments. You can generate one in the web console, as described in ["Deploying agents through Group Policy"](#).

REGISTRATION\_REQUIRED={0,1}

Defines how the installation will finish if the registration fails. If the value is 1, the installation also fails. The default value is 0, so if you don't specify this parameter, the installation completes successfully even though the agent is not registered.

## Additional parameters

To define the logon account for the agent service in Windows, use one of the following parameters:

- MMS\_USE\_SYSTEM\_ACCOUNT={0,1}

If the value is 1, the agent will run under the **Local System** account.

- MMS\_CREATE\_NEW\_ACCOUNT={0,1}

If the value is 1, the agent will run under a newly created account named **Acronis Agent User**.

- MMS\_SERVICE\_USERNAME=<user name> and MMS\_SERVICE\_PASSWORD=<password>

Use these parameters to specify an existing account under which the agent will run.

For more information on logon accounts, refer to ["Changing the logon account on Windows machines"](#).

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

- ESX\_HOST=<host name>

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.

HTTP\_PROXY\_ADDRESS=<IP address> and HTTP\_PROXY\_PORT=<port>

The HTTP proxy server to be used by the agent. Without these parameters, no proxy server will be used.

HTTP\_PROXY\_LOGIN=<login> and HTTP\_PROXY\_PASSWORD=<password>

The credentials for the HTTP proxy server. Use these parameters if the server requires authentication.

HTTP\_PROXY\_ONLINE\_BACKUP={0, 1}

If the value is 0, or the parameter is not specified, the agent will use the proxy server only for backup and recovery from the cloud. If the value is 1, the agent also will connect to the management server through the proxy server.

## Uninstallation parameters

REMOVE={<list of components>|ALL}

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

## Examples

- Installing Agent for Windows, Command-Line Tool, and Cyber Protection Monitor. Registering the machine in the Cyber Protect service by using a user name and password.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_SYSTEM_
ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_LOGIN=johndoe
REGISTRATION_PASSWORD=johnspassword
```

- Installing Agent for Windows, Command-Line Tool, and Cyber Protection Monitor. Creating a new logon account for the agent service in Windows. Registering the machine in the Cyber Protect service by using a token.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- Installing Agent for Windows, Command-Line Tool, Agent for Oracle and Cyber Protection Monitor. Registering the machine in the Cyber Protect service by using a user name and encoded in base64 password.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Installing Agent for Windows, Command-Line Tool, and Cyber Protection Monitor. Registering the machine in the Cyber Protect service by using a token. Setting an HTTP proxy.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

- Uninstalling all the agents and deleting their logs, tasks, and configuration settings.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_
SETTINGS=1 REBOOT=ReallySuppress
```

## Unattended installation or uninstallation in Linux

This section describes how to install or uninstall protection agents in the unattended mode on a machine running Linux, by using the command line.

### ***To install or uninstall a protection agent***

1. Open Terminal.
  2. Do one of the following:
- To start the installation by specifying the parameters on the command line, 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). All available parameters and their values are described in "[Unattended installation or uninstallation parameters](#)".

- To start the installation with parameters that are specified in a separate text file, run the following command:

```
<package name> -a --options-file=<path to the file>
```

This approach might be useful if you don't want to enter sensitive information on the command line. In this case, you can specify the configuration settings in a separate text file and ensure that only you can access it. Put each parameter on a new line, followed by the desired value, for example:

```
--rain=https://cloud.company.com
--login=johndoe
--password=johnspassword
--auto
```

or

```
-C
https://cloud.company.com
-g
johndoe
-w
johnspassword
-a
--language
en
```

If the same parameter is specified both on the command line and in the text file, the command line value precedes.

3. 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 (that 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.

## Unattended installation or uninstallation parameters

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

The minimal configuration for unattended installation includes -a and registration parameters (for example, --login and --password parameters; --rain and --token parameters). You can use more parameters to customize your installation.

## Installation parameters

### Basic parameters

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

The components to be installed, separated by commas and without space characters. The following components are available in the .x86\_64 installation package:

Component	Component description
BackupAndRecoveryAgent	Agent for Linux
AgentForPCS	Agent for Virtuozzo
OracleAgentFeature	Agent for Oracle

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

Both Agent for Virtuozzo and Agent for Oracle require that Agent for Linux is also installed.

The .i686 installation package contains only BackupAndRecoveryAgent.

`{-a|--auto}`

The installation and registration process will complete without any further user interaction. When using this parameter, you must specify the account under which the agent will be registered in the Cyber Protect service, either by using the `--token` parameter, or by using the `--login` and `--password` parameters.

`{-t|--strict}`

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

`{-n|--nodeps}`

The absence of required Linux packages will be ignored during the installation.

`{-d|--debug}`

Writes the installation log in the verbose mode.

`--options-file=<location>`

The installation parameters will be read from a text file instead of the command line.

`--language=<language ID>`

The product language. Available values are as follows: en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt\_BR, ru, fi, sr, sv, tr, zh, zh\_TW.

If this parameter is not specified, the product language will be defined by your system language on the condition that it is in the list above. Otherwise, the product language will set to English (en).

## Registration parameters

Specify one of the following parameters:

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

Credentials for the account under which the agent will be registered in the Cyber Protect service. This cannot be a partner administrator account.

- `--token=<token>`

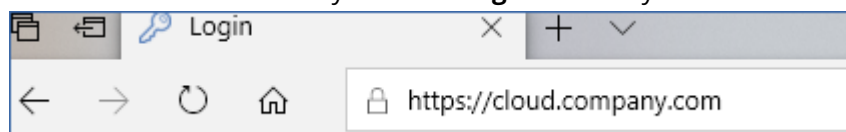
The registration token is a series of 12 characters, separated by hyphens in three segments. You can generate one in the web console, as described in ["Deploying agents through Group Policy"](#).

You cannot use the `--token` parameter along with `--login`, `--password`, and `--register-with-credentials` parameters.

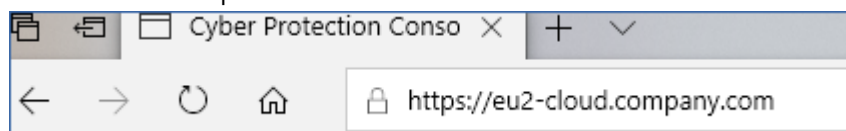
- `{-C|--rain=}<service address>`

The URL of the Cyber Protect service.

You don't need to include this parameter explicitly when you use `--login` and `--password` parameters for registration, because the installer uses the correct address by default – this would be the address that you use **to log in** to the Cyber Protect service. For example:



However, when you use `{-C|--rain=}` with the `--token` parameter, you must specify the exact datacenter address. This is the URL that you see **once you are logged in** to the Cyber Protect service. For example:



- `--register-with-credentials`

If this parameter is specified, the installer's graphical interface will start. To finish the registration, enter the user name and password for the account under which the agent will be registered in the Cyber Protect service. This cannot be a partner administrator account.

- `--skip-registration`

Use this parameter if you need to install the agent but you plan to register it in the Cyber Protect service later. For more information on how to do this, refer to ["Registering machines manually"](#).

## Additional parameters

`--http-proxy-host=<IP address>` and `--http-proxy-port=<port>`

The HTTP proxy server that the agent will use for backup and recovery from the cloud, and for connection to the management server. Without these parameters, no proxy server will be used.

`--http-proxy-login=<login>` and `--http-proxy-password=<password>`

The credentials for the HTTP proxy server. Use these parameters if the server requires authentication.

`--tmp-dir=<location>`

Specifies the folder where the temporary files are stored during the installation. The default folder is **/var/tmp**.

`{-s|--disable-native-shared}`

Redistributable libraries will be used during the installation, even though they might have already been present on your system.

`--skip-prereq-check`

There will be no check of whether the packages required for compiling the snapapi module are already installed.

`--force-weak-snapapi`

The installer will not compile a snapapi module. Instead, it will use a ready-made module that might not match the Linux kernel exactly. Using this option is not recommended.

`--skip-svc-start`

The services will not start automatically after the installation. Most often, this parameter is used with the `--skip-registration` one.

## 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.

`--snapapi-list`

Shows the available ready-made snapapi modules.

`--components-list`

Shows the installer components.

## Parameters for legacy features

These parameters relate to a legacy component, agent.exe.

`{-e|--ssl=}<path>`

Specifies the path to a custom certificate file for SSL communication.

`{-p|--port=}<port>`

Specifies the port on which agent.exe listens for connections. The default port is 9876.

## Uninstallation parameters

`{-u|--uninstall}`

Uninstalls the product.

`--purge`

Uninstalls the product and removes its logs, tasks, and configuration settings. You don't need to specify the `--uninstall` parameter explicitly when you use the `--purge` one.

## Examples

- Installing Agent for Linux without registering it.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- Installing Agent for Linux, Agent for Virtuozzo, and Agent for Oracle, and registering them by using credentials.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
```

- Installing Agent for Oracle and Agent for Linux, and registering them by using a registration token.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- Installing Agent for Linux, Agent for Virtuozzo, and Agent for Oracle with configuration settings in a separate text file.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
```

- Uninstalling Agent for Linux, Agent for Virtuozzo, and Agent for Oracle, and removing all its logs,



tasks, and configuration settings.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

## Unattended installation and uninstallation in macOS

This section describes how to install, register, and uninstall the protection agent in the unattended mode on a machine running macOS, by using the command line. For information on how to download the installation file (.dmg), refer to ["Adding a machine running macOS"](#).

### *To install Agent for Mac*

1. Create a temporary directory where you will mount the installation file (.dmg).

```
mkdir <dmg_root>
```

Here, the <dmg\_root> is a name of your choice.

2. Mount the .dmg file.

```
hdiutil attach <dmg_file> -mountpoint <dmg_root>
```

Here, the <dmg\_file> is the name of the installation file. For example, **AcronisAgentMspMacOSX64.dmg**.

3. Run the installer.

```
sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
```

4. Detach the installation file (.dmg).

```
hdiutil detach <dmg_root>
```

## Examples

- 

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory
```

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

### *To register Agent for Mac*

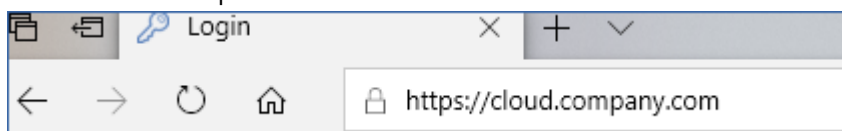
Do one of the following:

- Register the agent under a specific account, by using a user name and password.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
<service address> -u <user name> -p <password>
```

Here:

The <Cyber Protect service address> is the address that you use **to log in** to the Cyber Protect service. For example:



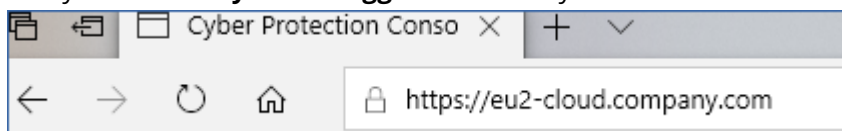
The <user name> and <password> are the credentials for the account under which the agent will be registered. This cannot be a partner administrator account.

- Register the agent by using a registration token.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
<service address> --token <token>
```

The registration token is a series of 12 characters, separated by hyphens in three segments. You can generate one in the Cyber Protect web console, as described in "[Deploying agents through Group Policy](#)".

When you use a registration token, you must specify the exact datacenter address. This is the URL that you see **once you are logged in** to the Cyber Protect service. For example:




---

## Important

If you use macOS 10.14 or later, grant the protection agent full disk access. To do so, go to **Applications > Utilities**, and then run **Cyber Protect Agent Assistant**. Then, follow the instructions in the application window.

---

## Examples

Registration with a user name and password.

- ```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

Registration with a token.

- ```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
https://eu2-cloud company.com --token D91D-DC46-4F0B
```

### ***To uninstall Agent for Mac***

Run the following command:

- ```
sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
Uninstall.app/Contents/MacOS/AgentUninstall /confirm
```

To remove all logs, tasks and configuration settings during the uninstallation, run the following command:

- ```
sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
```

## Registering and unregistering machines manually

Machines are automatically registered in the Cyber Protect service when you install the protection agent on them. When you uninstall the protection agent, the machines are automatically unregistered and disappear from the Cyber Protect web console.

You can also register a machine manually, by using the command line interface. You might need to use the manual registration, for example, if the automatic registration fails or if you want to register an existing machine under a new account.

You can find the registration tool in the following locations:

- Windows: Program Files\Acronis\RegisterAgentTool\register\_agent.exe
- Linux: /usr/lib/Acronis/RegisterAgentTool/RegisterAgent
- macOS: /Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent

### ***To register a machine by using a user name and password***

#### ***In Windows***

At the command line, run the following command:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <password>
```

For example:

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

#### ***In Linux***

At the command line, run the following command:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <password>
```

For example:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

### ***In macOS***

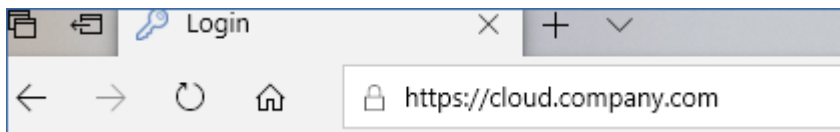
At the command line, run the following command:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <password>
```

For example:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

The <service address> is the URL that you use **to log in** to the Cyber Protect service. For example, <https://cloud.company.com>.



The <user name> and <password> are the credentials of the account under which the agent will be registered. This cannot be a partner administrator account. If your password contains special characters or blank spaces, see "Passwords with special characters or blank spaces" (p. 138).

### ***To register a machine by using a registration token***

#### ***In Windows***

At the command line, run the following command:

```
<path to the registration tool> -o register -t cloud -a <service address> --token
<registration token>
```

For example:

```
<path to the registration tool> -o register -t cloud -a https://au1-cloud.company.com --
token 3B4C-E967-4FBD
```

#### ***In Linux***

At the command line, run the following command:

```
<path to the registration tool> -o register -t cloud -a <service address> --token
<registration token>
```

For example:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

### ***In macOS***

At the command line, run the following command:

```
<path to the registration tool> -o register -t cloud -a <service address> --token
<registration token>
```

For example:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

### ***Virtual appliance***

1. In the console of the virtual appliance, press CTRL+SHIFT+F2 to open the command-line interface.
2. At the command prompt, run the following command:

```
register_agent -o register -t cloud -a <service address> --token <registration token>
```

For example:

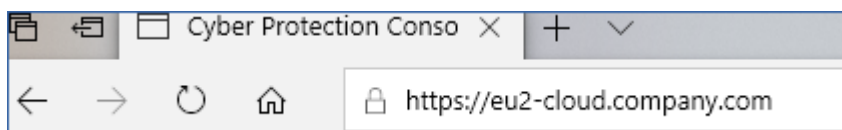
```
register_agent -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-
8C39-4A5C
```

3. To return to the graphical interface of the appliance, press ALT+F1.

---

### **Note**

When you use a registration token, you must specify the exact data center address. This is the URL that you see **after you log in** to the Cyber Protect service. For example, <https://eu2-cloud.company.com>.



Do not use <https://cloud.company.com> here.

The registration token is a series of 12 characters, separated into three segments by hyphens. For more information on how to generate one, see "To generate a registration token" (p. 193).

---

### ***To unregister a machine***

#### ***In Windows***

At the command line, run the following command:

```
<path to the registration tool> -o unregister
```

For example:

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

#### ***In Linux***

At the command line, run the following command:

```
<path to the registration tool> -o unregister
```

For example:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

#### ***In macOS***

At the command line, run the following command:

```
<path to the registration tool> -o unregister
```

For example:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

#### ***Virtual appliance***

1. In the console of the virtual appliance, press CTRL+SHIFT+F2 to open the command-line interface.
2. At the command prompt, run the following command:

```
register_agent -o unregister
```

3. To return to the graphical interface of the appliance, press ALT+F1.

## **Deploying Agent for oVirt (Virtual Appliance)**

For information about how to deploy and configure Agent for oVirt (Virtual Appliance), refer to the [Cyber Protection Cloud documentation](#).

## Deploying Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance)

For information about how to deploy and configure Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance), refer to the [Cyber Protection Cloud documentation](#).

## Autodiscovery of machines

Using autodiscovery, you can:

- Automate the installation of protection agents and the registration of machines to the management server by detecting the machines in your Active Directory domain or local network.
- Install and update protection agents on multiple machines.
- Use synchronization with Active Directory, in order to reduce the efforts for provisioning resources and managing machines in a large Active Directory domain.

## Prerequisites

To perform autodiscovery, you need at least one machine with an installed protection agent in your local network or Active directory domain. This agent is used as a discovery agent.

---

### Important

Only agents that are installed on Windows machines can be discovery agents. If there are no discovery agents in your environment, you will not be able to use the **Multiple devices** option in the **Add devices** panel.

Remote installation of agents is supported only for machines running Windows (Windows XP is not supported). For remote installation on a machine running Windows Server 2012 R2, you must have [Windows update KB2999226](#) installed on this machine.

---

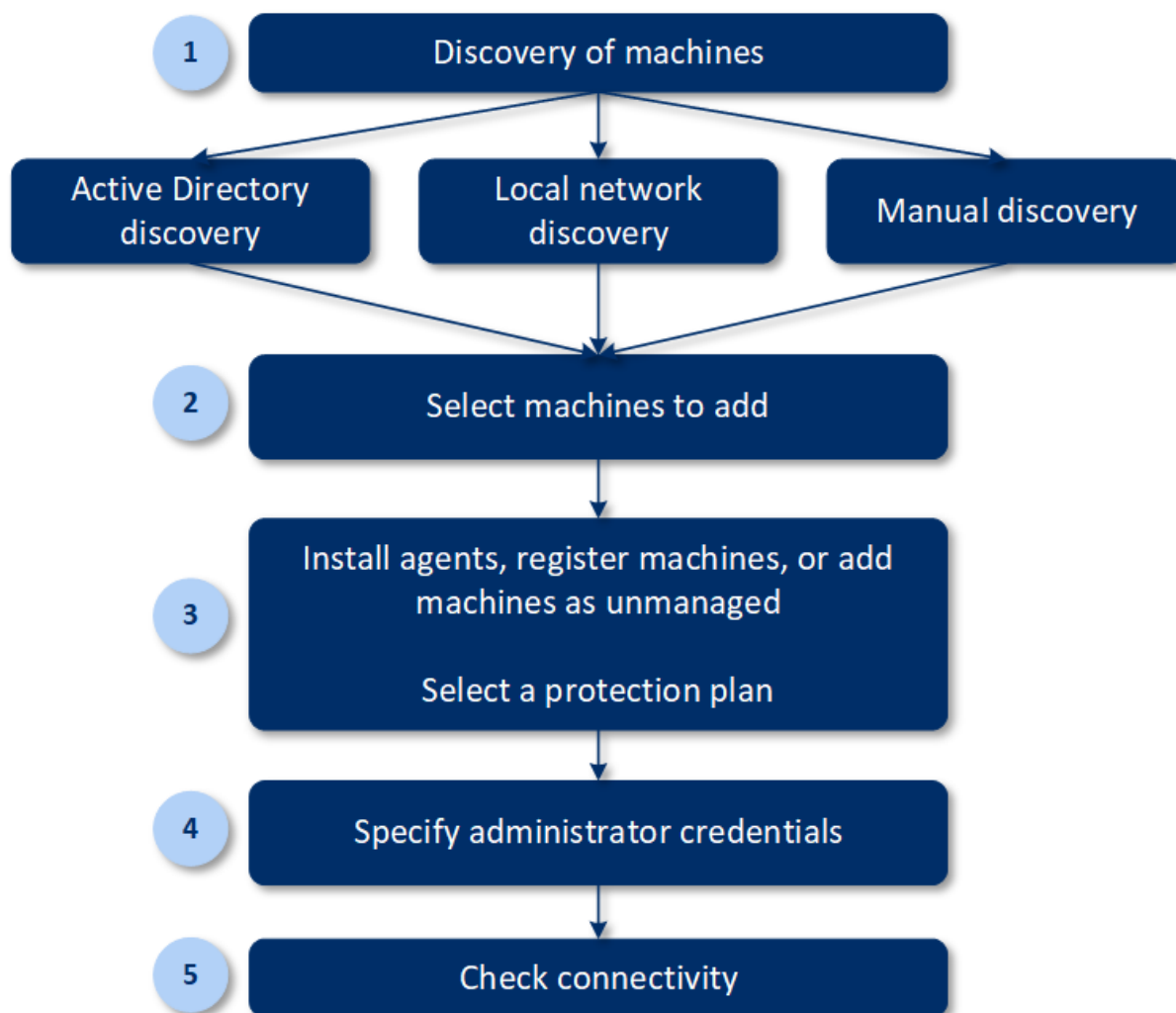
## How autodiscovery works

During a local network discovery, the discovery agent collects the following information for each machine in the network, by using NetBIOS discovery, Web Service Discovery (WSD), and the Address Resolution Protocol (ARP) table:

- Name (short/NetBIOS host name)
- Fully qualified domain name (FQDN)
- Domain/workgroup
- IPv4/IPv6 addresses
- MAC addresses
- Operating system (name/version/family)
- Machine category (workstation/server/domain controller)

During an Active Directory discovery, the discovery agent, in addition to the list above, collects information about the Organizational Unit (OU) of the machines and detailed information about their names and operating systems. However, the IP and MAC addresses are not collected.

The following diagram summarizes the autodiscovery process.



1. Select the discovery method:

- Active Directory discovery
- Local network discovery
- Manual discovery – By using a machine IP address or host name, or by importing a list of machines from a file

The results of an Active directory discovery or a local network discovery exclude machines with installed protection agents.

During a manual discovery, the existing protection agents are updated and re-registered. If you perform autodiscovery by using the same account under which an agent is registered, the agent will only be updated to the latest version. If you perform autodiscovery by using another account, the agent will be updated to the latest version and re-registered under the tenant to which the account belongs.



2. Select the machines that you want to add to your tenant.
3. Select how to add these machines:
  - Install a protection agent and additional components on the machines, and register them in the web console.
  - Register the machines in the web console (if a protection agent was already installed).
  - Add the machines to the web console as **Unmanaged machines**, without installing a protection agent.

You can also apply an existing protection plan to the machines on which you install a protection agent or which you register in the web console.

4. Provide administrator credentials for the selected machines.
5. Select the name or the IP address of the management server that the agent will use to access that server.

By default, the server name is selected. You may need to select the IP address instead if your management server has more than one network interface or if you are facing DNS issues that cause the agent registration to fail.

6. Verify that you can connect to the machines by using the provided credentials.

The machines that are shown in the Cyber Protect web console, fall into the following categories:

- **Discovered** – Machines that are discovered, but a protection agent is not installed on them.
- **Managed** – Machines on which a protection agent is installed.
- **Unprotected** – Machines to which a protection plan is not applied. Unprotected machines include both discovered machines and managed machines with no protection plan applied.
- **Protected** – Machines to which a protection plan is applied.

## Autodiscovery and manual discovery

Before starting the discovery, ensure that the [prerequisites](#) are met.

### *To discover machines*

1. In the web console, go to **Devices > All devices**.
2. Click **Add**.
3. In **Multiple devices**, click **Windows only**. The discovery wizard opens.
4. [If there are units in your organization] Select a unit. Then, in **Discovery agent** you will be able to select the agents associated with the selected unit and its child units.
5. Select the discovery agent that will perform the scan to detect machines.
6. Select the discovery method:
  - **Search Active Directory**. Ensure that the machine with the discovery agent is the Active Directory domain member.
  - **Scan local network**. If the selected discovery agent cannot not find any machines, select another discovery agent.

- **Specify manually or import from file.** Manually define the machines to be added or import them from a text file.
7. [If the Active Directory discovery method is selected] Select how to search for machines:
- **In organizational unit list.** Select the group of machines to be added.
  - **By LDAP dialect query.** Use the [LDAP dialect](#) query to select the machines. **Search base** defines where to search, while **Filter** allows you to specify the criteria for machine selection.
8. [If the Active Directory or local network discovery method is selected] Use a list to select the machines that you want to add.

[If the Manual discovery method is selected] Specify the machine IP addresses or host names, or import the machine list from a text file. The file must contain IP addresses/host names, one per line. Here is an example of a file:

```
156.85.34.10
156.85.53.32
156.85.53.12
EN-L00000100
EN-L00000101
```

After adding machine addresses manually or importing them from a file, the agent tries to ping the added machines and define their availability.

9. Select what to do after the discovery:
- **Install agents and register machines.** You can select which components to install on the machines by clicking **Select components**. For more details, refer to "[Selecting components for installation](#)". You can install up to 100 agents simultaneously.  
On the **Select components** screen, define the account under which the services will run by specifying **Logon account for the agent service**. You can select 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**  
The account name will be Agent User for the agent.
    - **Use the following account**  
If you install the agent on a domain controller, the system prompts you to specify existing accounts (or the same account) for the agent. For security reasons, the system does not automatically create new accounts on a domain controller.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.
  - **Register machines with installed agents.** This option is used if the agent is already installed on machines and you need only to register them in Cyber Protect. If no agent is found inside the machines, then they will be added as **Unmanaged** machines.

- **Add as unmanaged machines.** The agent will not be installed on the machines. You will be able to view them in the web console and install or register the agent later.

[If the **Install agents and register machines** post-discovery action is selected] **Restart the machine if required** – if the option is enabled, the machine will be restarted as many times as required to complete the installation.

Restart of the machine may be required in one of the following cases:

- Installation of prerequisites is completed and restart is required to continue the installation.
- Installation is completed but restart is required as some files are locked during installation.
- Installation is completed but restart is required for other previously installed software.

[If **Restart the machine if required** is selected] **Do not restart if the user logged in** – if the option is enabled, the machine will not be automatically restarted if the user is logged in to the system. For example, if a user is working while installation requires restart, the system will not be restarted.

If the prerequisites were installed and then the reboot was not done because a user was logged in, then to complete the agent installation you need to reboot the machine and start the installation again.

If the agent was installed but then the reboot was not done, then you need to reboot the machine.

[If there are units in your organization] **Unit where to register the machines** – select the unit where the machines will be registered.

If you have selected one of the first two post-discovery actions, then there is also an option to apply the protection plan to the machines. If you have several protection plans, you can select which one to use.

10. Specify the credentials of the user with administrator rights for all of the machines.

---

### Important

Note that remote installation of agent works without any preparations only if you specify the credentials of the built-in administrator account (the first account created when the operating system is installed). If you want to define any custom administrator credentials, then you must do additional manual preparations as described in [Adding a machine running Windows > Preparation](#).

---

11. Select the name or the IP address of the management server that the agent will use to access that server.  
By default, the server name is selected. You may need to select the IP address instead if your management server has more than one network interface or if you are facing DNS issues that cause the agent registration to fail.
12. The system checks connectivity to all of the machines. If the connection to some of the machines fails, you can change the credentials for these machines.

When the discovery of machines is initiated, you will find the corresponding task in **Dashboard > Activities > Discovering machines** activity.

## Selecting components for installation

You can find the description of mandatory and additional components in the following table:

Component	Description
<b>Mandatory component</b>	
Agent for Windows	This agent backs up disks, volumes, files and will be installed on Windows machines. It will be always installed, not selectable.
<b>Additional components</b>	
Agent for Hyper-V	This agent backs up Hyper-V virtual machines and will be installed on Hyper-V hosts. It will be installed if selected and detected Hyper-V role on a machine.
Agent for SQL	This agent backs up SQL Server databases and will be installed on machines running Microsoft SQL Server. It will be installed if selected and application detected on a machine.
Agent for Exchange	This agent backs up Exchange databases and mailboxes and will be installed on machines running the Mailbox role of Microsoft Exchange Server. It will be installed if selected and application detected on a machine.
Agent for Active Directory	This agent backs up the data of Active Directory Domain Services and will be installed on domain controllers. It will be installed if selected and application detected on a machine.
Agent for VMware (Windows)	This agent backs up VMware virtual machines and will be installed on Windows machines that have network access to vCenter Server. It will be installed if selected.
Agent for Office 365	This agent backs up Microsoft 365 mailboxes to a local destination and will be installed on Windows machines. It will be installed if selected.
Agent for Oracle	This agent backs up Oracle databases and will be installed on machines running Oracle Database. It will be installed if selected.
Cyber Protect Monitor	This component enables a user to monitor execution of running tasks in the notification area and will be installed on Windows machines. It will be installed if selected.
Command-line Tool	Cyber Protect supports the command-line interface with the <code>acrocnd</code> utility. <code>acrocnd</code> does not contain any tools that physically execute the commands. It only provides the command-line interface to Cyber Protect components - agents and the management server. It will be installed if selected.

Bootable Media Builder	This component enables users to create bootable media and will be installed on Windows machines, if selected.
------------------------	---------------------------------------------------------------------------------------------------------------

## Managing discovered machines

After the discovery process is performed, you can find all of the discovered machines in **Devices > Unmanaged machines**.

This section is divided into subsections by the discovery method used. The full list of machine parameters is shown below (it may vary depending on the discovery method):

Name	Description
<b>Name</b>	The name of the machine. The IP address will be shown if the name of the machine could not be discovered.
<b>IP address</b>	The IP address of the machine.
<b>Discovery type</b>	The discovery method that was used to detect the machine.
<b>Organizational unit</b>	The organizational unit in Active Directory that the machine belongs to. This column is shown if you view the list of machines in <b>Unmanaged machines &gt; Active Directory</b> .
<b>Operating system</b>	The operating system installed in the machine.

There is an **Exceptions** section, where you can add the machines that must be skipped during the discovery process. For example, if you do not need the exact machines to be discovered, you can add them to this list.

To add a machine to **Exceptions**, select it in the list and click **Add to exceptions**. To remove a machine from **Exceptions**, go to **Unmanaged machines > Exceptions**, select the machine, and click **Remove from exceptions**.

You can install the protection agent and register a batch of discovered machines in Cyber Protect by selecting them in the list and clicking **Install and register**. The opened wizard also allows you to assign the protection plan to a batch of machines.

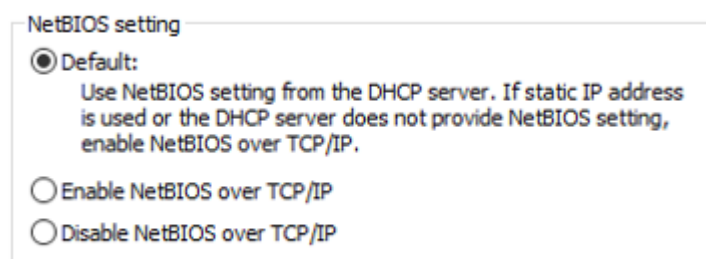
After the protection agent is installed on machines, those machines will be shown in the **Devices > Machines with agents** section.

To check your protection status, go to **Dashboard > Overview** and add the **Protection status** widget or the **Discovered machine** widget.

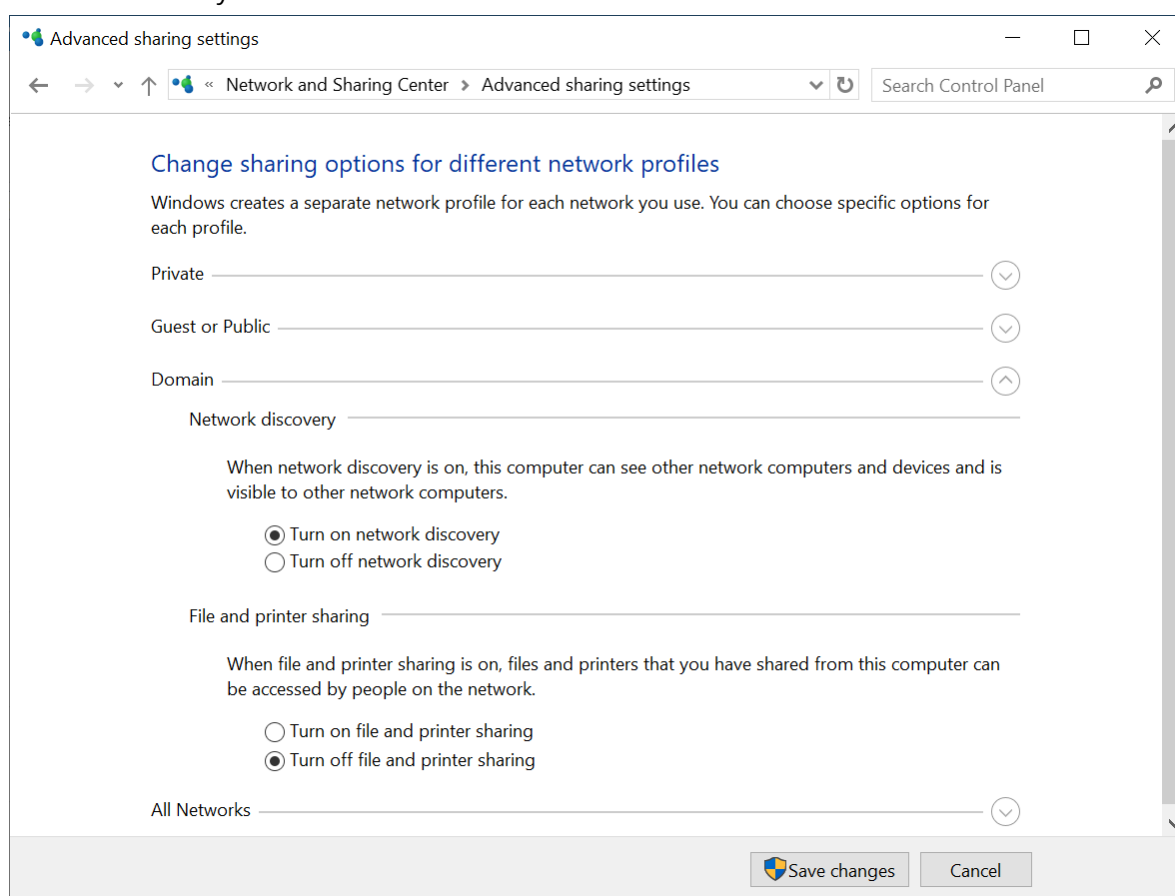
## Troubleshooting

If you have any issues with the autodiscovery functionality, try the following:

- Verify that NetBIOS over TCP/IP is enabled or set to default.



- In **Control Panel > Network and Sharing Center > Advanced sharing settings**, turn on network discovery.



- Verify that the **Function Discovery Provider Host** service is running on the machine that does discovery and on the machines to be discovered.
- Verify that the **Function Discovery Resource Publication** service is running on the machines to be discovered.

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

## 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.

To improve the backup performance and avoid failures related to insufficient RAM memory, we recommend increasing these resources to 16 GB of RAM and 4 vCPUs in more demanding cases. For example, increase the assigned resources when you expect the backup traffic to exceed 100 MB per second or if you back up simultaneously multiple virtual machines with large hard drives (500 GB or more).

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.

---

#### Note

vStorage APIs must be installed on the ESXi host to enable virtual machine backups. See <https://kb.acronis.com/content/14931>.

---

### 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](#)".

### 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**.

## Deploying the OVF template

### Location of the OVF template

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

### In on-premises deployments

After the management server is installed, the virtual appliance's OVF package is located in the folder **%ProgramFiles%\Acronis\ESXAppliance** (in Windows) or **/usr/lib/Acronis/ESXAppliance** (in Linux).

### In cloud deployments

1. Click **All devices > Add > VMware ESXi > Virtual Appliance (OVF)**.

The .zip archive is downloaded to your machine.

2. Unpack the .zip archive.

## Deploying the OVF template

1. Ensure that the OVF template files can be accessed from the machine running the vSphere Client.
2. Start the vSphere Client and log on to the vCenter Server.
3. Deploy the OVF template.
  - When configuring storage, select the shared datastore, if it exists. Thick or thin disk format does not matter, as it does not affect the appliance performance.
  - When configuring network connections in cloud deployments, be sure to select a network that allows an Internet connection, so that the agent can properly register itself in the cloud. When configuring network connections in on-premises deployments, select a network that includes the management server.

## Configuring the virtual appliance

1. **Starting the virtual appliance**

In the vSphere Client, display the **Inventory**, right-click the virtual appliance's name, and then select **Power > Power On**. Select the **Console** tab.

2. **Proxy server**

If a proxy server is enabled in your network:

- a. To start the command shell, press CTRL+SHIFT+F2 while in the virtual appliance UI.
- b. Open the file **/etc/Acronis/Global.config** in a text editor.



c. Do one of the following:

- If the proxy settings were specified during the agent installation, find the following section:

```
<key name="HttpProxy">
 <value name="Enabled" type="Tdwor" >"1"</value>
 <value name="Host" type="TString">"ADDRESS"</value>
 <value name="Port" type="Tdwor" >"PORT"</value>
 <value name="Login" type="TString">"LOGIN"</value>
 <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Otherwise, copy the above lines and paste them into the file between the `<registry name="Global">...</registry>` tags.

- d. Replace ADDRESS with the new proxy server host name/IP address, and PORT with the decimal value of the port number.
- e. If your proxy server requires authentication, replace LOGIN and PASSWORD with the proxy server credentials. Otherwise, delete these lines from the file.
- f. Save the file.
- g. Open the file `/opt/acronis/etc/aakore.yaml` in a text editor.
- h. Locate the **env** section or create it and add the following lines:

```
env:
 http-proxy: proxy_login:proxy_password@proxy_address:port
 https-proxy: proxy_login:proxy_password@proxy_address:port
```

- i. Replace proxy\_login and proxy\_password with the proxy server credentials, and proxy\_address:port with the address and port number of the proxy server.

j. Run the **reboot** command.

Otherwise, skip this step.

### 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/ESX(i)

Under **Agent options**, in **vCenter/ESX(i)**, click **Change** and specify the vCenter Server name or IP address. The agent will be able to back up and recover any virtual machine managed by the vCenter Server.

If you do not use a vCenter Server, specify the name or IP address of the ESXi host whose virtual machines you want to back up and recover. Normally, backups run faster when the agent backs up virtual machines hosted on its own host.

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](#) on the vCenter Server or ESXi.

You can 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**, do one of the following:
  - For an on-premises deployment, select **Local**. Specify the host name or IP address of the machine where the management server is installed.
  - For a cloud deployment, select **Cloud**. The software displays the Cyber Protection service address. Do not change this address unless instructed otherwise.
- c. In **User name** and **Password**, do one of the following:
  - For an on-premises deployment, specify the user name and password of a management server administrator.
  - For a cloud deployment, specify the user name and password for the Cyber Protection service. The agent and the virtual machines managed by the agent will be registered under this account.

## 6. Time zone

Under **Virtual machine**, in **Time zone**, click **Change**. 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](#).

Add the disk by editing the settings of the virtual machine and click **Refresh**. The **Create storage** link becomes available. Click this link, select the disk, and then specify a label for it.

# Deploying Agent for Scale Computing HC3 (Virtual Appliance)

## Before you start

This appliance is a pre-configured virtual machine that you deploy in a Scale Computing HC3 cluster. It contains a protection agent that enables you to administer cyber protection for all virtual machines in the cluster.

## System requirements for the agent

When deploying the virtual appliance, you can choose between different combinations of vCPUs and RAM. 2 vCPUs and 4 GiB of RAM are optimal and sufficient for most operations. We recommend increasing these resources to 4 vCPUs and 8 GiB of RAM 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.

## How many agents do I need?

One agent can protect the entire cluster. However, you can have more than one agent in the cluster if you need to distribute the backup traffic bandwidth load.

If you have more than one agent in a cluster, the virtual machines are automatically evenly distributed between the agents, so that each agent manages an equal number of machines.

Automatic redistribution takes place when a load imbalance among the agents reaches 20 percent. This may happen, for example, when a machine or an agent is added or removed. For example, you realize that you need more agents to help with throughput and you 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 manually from the Scale Computing HC3 cluster. Redistribution will start only after you remove such an agent from the Cyber Protect web interface.

You can view the result of the automatic distribution:

- In the **Agent** column for each virtual machine in the **All devices** section
- In the **Assigned virtual machines** section of the **Details** panel when an agent is selected in **Settings > Agents**

## Deploying the virtual appliance

1. Log in to your Cyber Protect account.
2. Click **Devices > All devices > Add > Scale Computing HC3**.
3. Select the number of virtual appliances that you want to deploy.
4. Specify the IP address or the host name of the Scale Computing HC3 cluster.
5. Specify credentials of an account that has the **VM Create/Edit role assigned** in this cluster.
6. Specify a network share that will be used for temporary storage of the image file for the virtual appliance. A minimum of 2GB of free space is required.
7. Specify credentials of an account that has read and write access to this network share.
8. Click **Deploy**.

After the deployment completes, [configure the virtual appliance](#).

## Configuring the virtual appliance

After deploying the virtual appliance, you need to configure it so that it can reach both the Scale Computing HC3 cluster that it will protect and the Cyber Protect management server.

### *To configure the virtual appliance*

1. Log in to your Scale Computing HC3 account.
2. Select the virtual machine with the agent that you need to configure, and then click **Console**.

3. Configure the network interfaces of the appliance. There may be one or more interfaces to configure – it depends on the number of networks that the appliance uses. Ensure that automatically assigned DHCP addresses (if any) are valid within the networks that your virtual machine uses, or assign them manually.

Agent for Scale Computing

Specify the required parameters below. After the agent is configured, the virtual machines will appear in the web console.

Agent status: To connect the agent to the Scale Computing server, [specify the server and its access credentials](#).

**AGENT OPTIONS**

Scale Computing	Specify the Scale Computing cluster address and the access credentials.	<a href="#">Change...</a>
Management Server	Specify Management Server and the access credentials.	<a href="#">Change...</a>
eth0	Address type: Assigned by DHCP IP address: 10.34.16.191	<a href="#">Change...</a>

**VIRTUAL MACHINE**

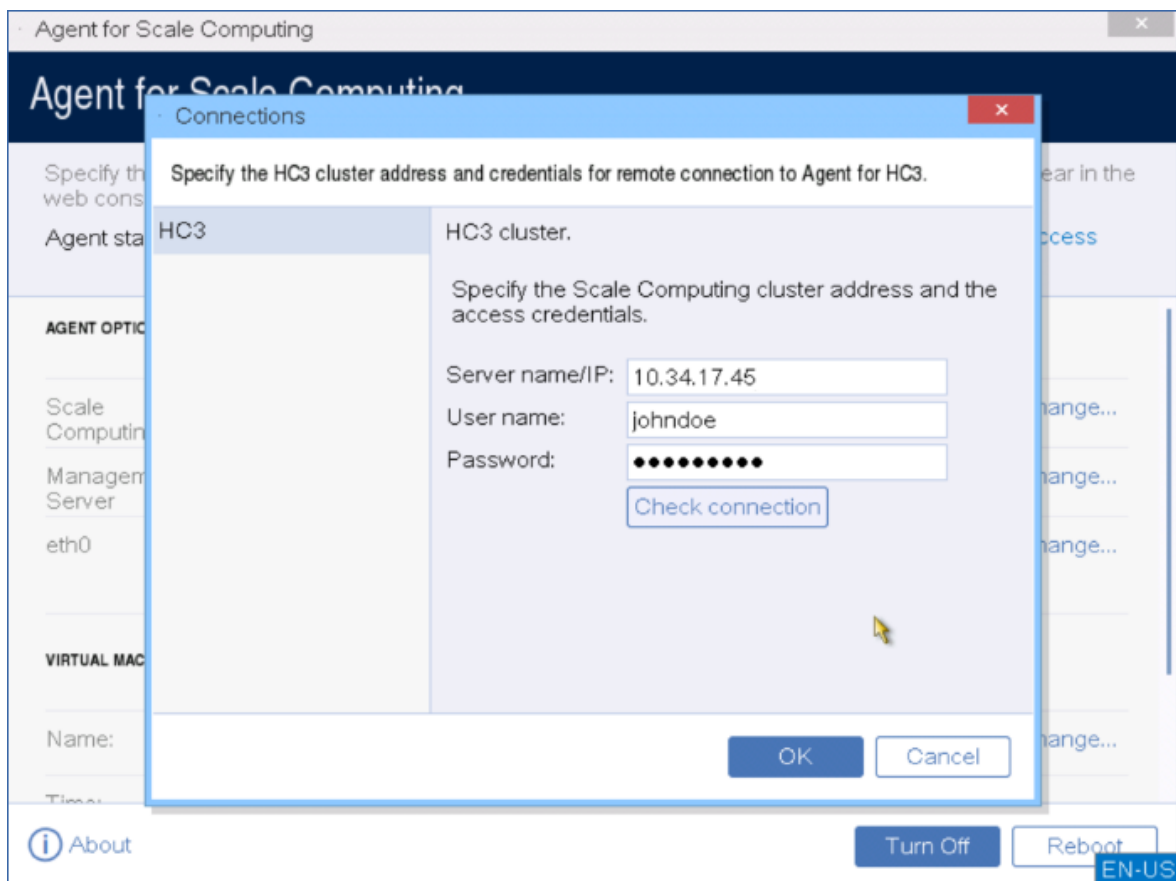
Name: localhost [Change...](#)

Time: Thu Jul 11 10:00:05 AM

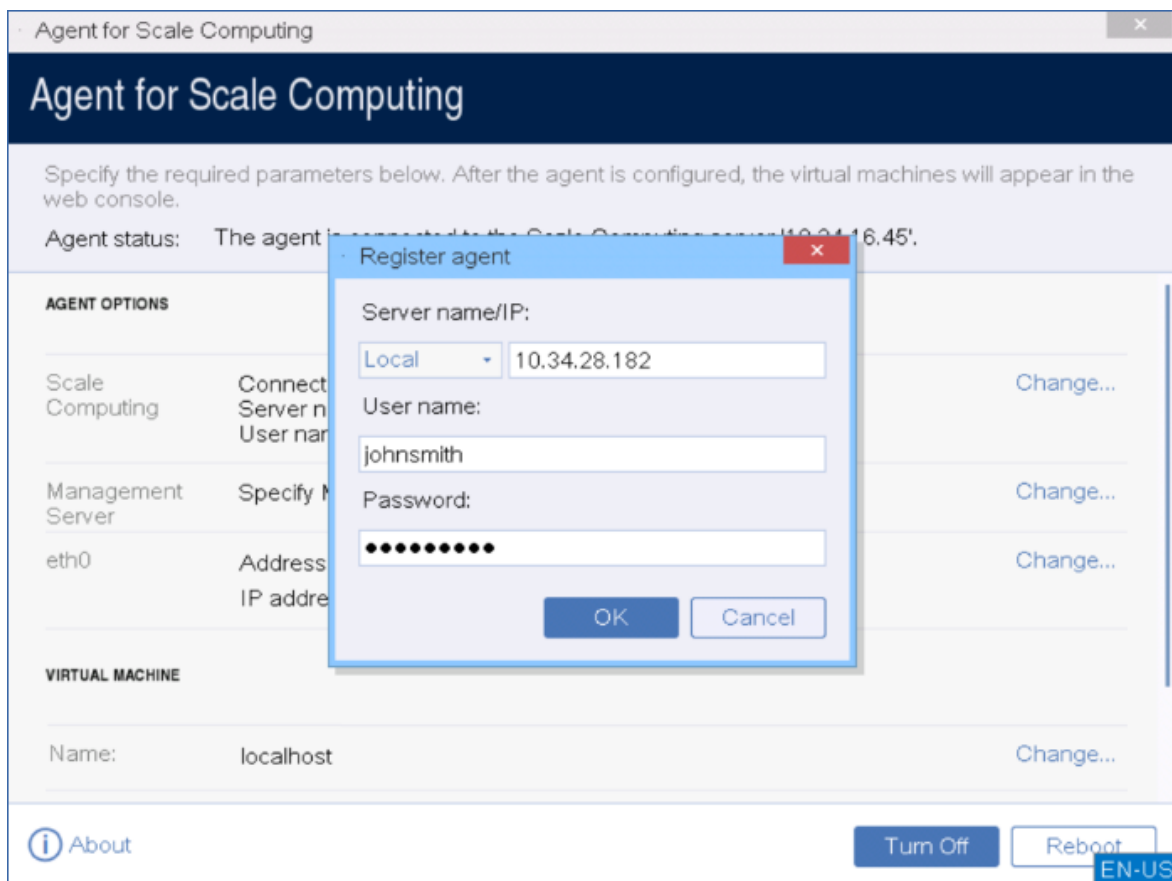
[About](#) [Turn Off](#) [Reboot](#) [EN-US](#)

4. Specify the Scale Computing HC3 cluster address and credentials:
- DNS name or IP address of the cluster.
  - In the **User name** and **Password** fields, enter the credentials for the Scale Computing HC3 account that has [the appropriate roles assigned](#).

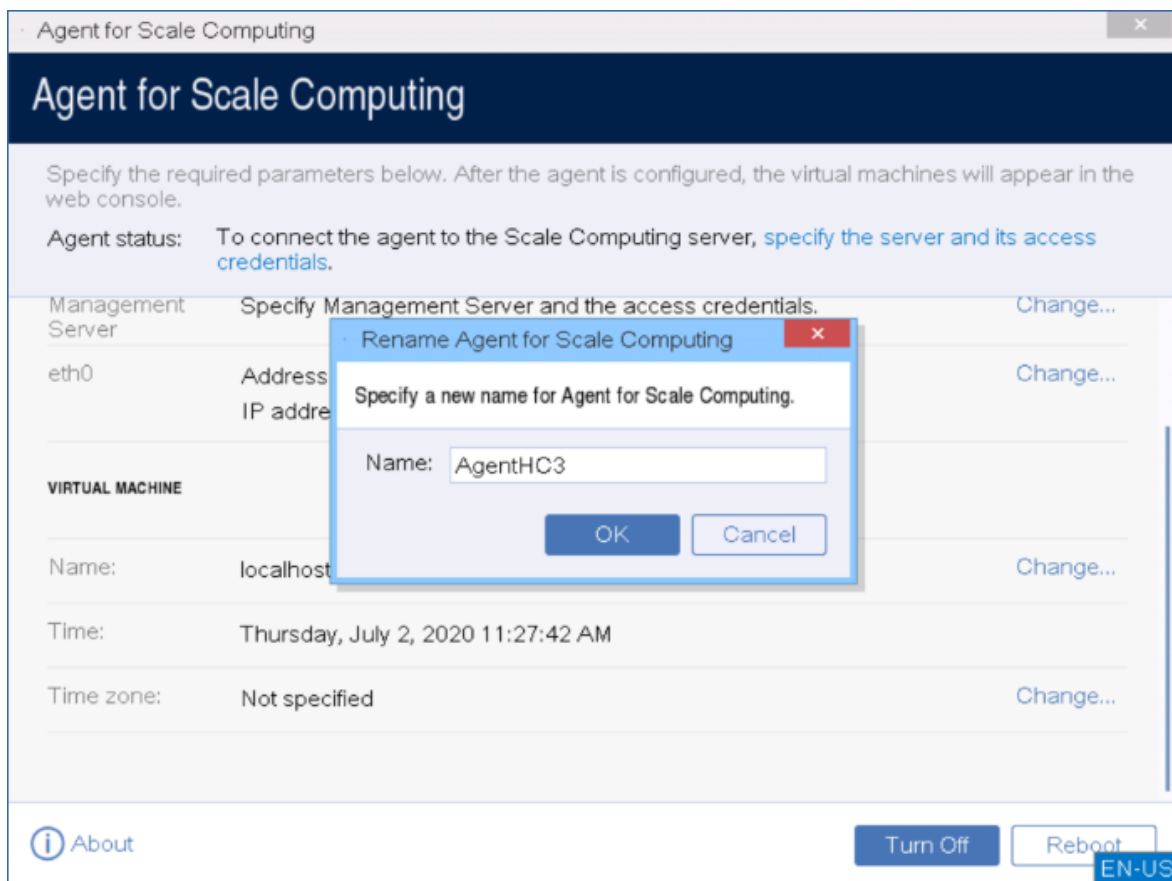
You can click **Check connection** to ensure the access credentials are correct.



5. Specify the Cyber Protect management server address and credentials for accessing it.



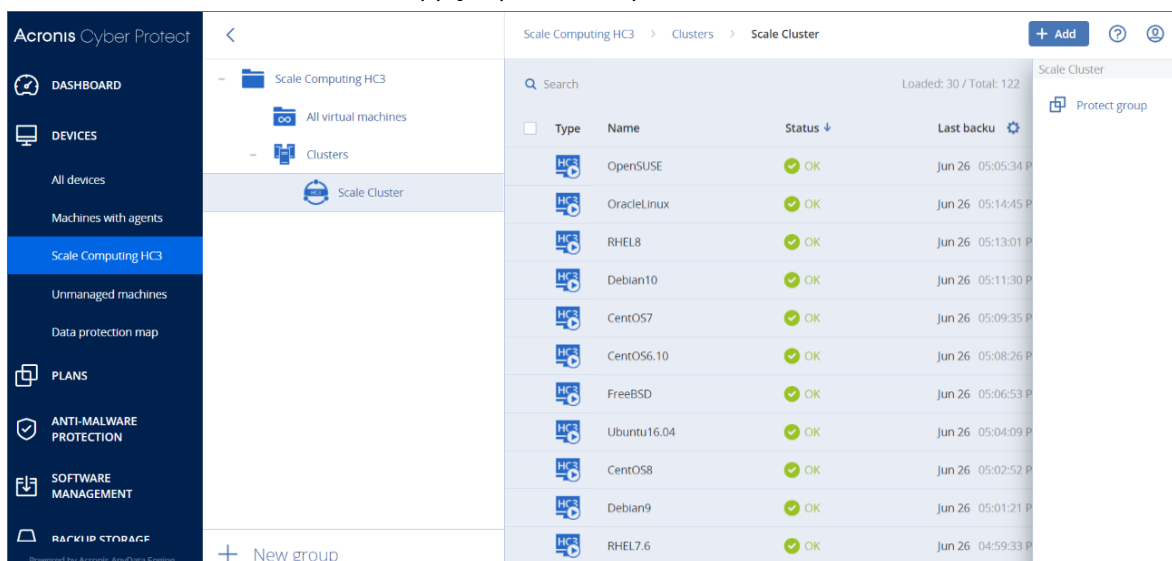
6. [Optional] Specify a name for the agent. This name will be shown in the Cyber Protect web console.



7. [Optional] Select the time zone of your location to ensure that the scheduled operations run at the appropriate time.

### ***To protect the virtual machines in the Scale Computing HC3 cluster***

1. Log in to your Cyber Protect account.
2. Navigate to **Devices > Scale Computing HC3 > <your cluster>** or find your machines in **Devices > All devices**.
3. Select the desired machines and apply a protection plan for them.



## Agent for Scale Computing HC3 – required roles

This section describes the roles required for operations with Scale Computing HC3 virtual machines and, additionally, for virtual appliance deployment.

Operation	Role
Back up a virtual machine	Backup VM Create/Edit VM Delete
Recover to an existing virtual machine	Backup VM Create/Edit VM Power Control VM Delete Cluster Settings
Recover to a new virtual machine	Backup VM Create/Edit VM Power Control VM Delete Cluster Settings
Virtual appliance deployment	VM Create/Edit

## 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 Cyber Protect web 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 Cyber Protect web 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 Cyber Protect web 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.

## 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**.
10. Select the agent's .msi installation package in the shared folder that you previously created, and then click **Open**.
11. In the **Deploy Software** dialog box, click **Advanced**, and then click **OK**.
12. On the **Modifications** tab, click **Add**, and then select the .mst transform that you previously created.
13. Click **OK** to close the **Deploy Software** dialog box.

## Updating virtual appliances

### On-premises deployments

To update a virtual appliance (Agent for VMware or Agent for Scale Computing HC3) whose version is below 15.24426 (released September, 2020), follow the procedure in "Updating agents" (p. 195).

#### ***To update virtual appliance version 15.24426 or later***

1. Download the update package as described in <http://kb.acronis.com/latest>.
2. Save the tar.bz files in the following directory of the management server machine:
  - Windows: C:\Program Files\Acronis\VirtualAppliances\va-updates
  - Linux: /usr/lib/Acronis/VirtualAppliances/va-updates
3. In the Cyber Protect web console, click **Settings > Agents**.

The software displays the list of machines. The machines with outdated virtual appliances are marked with an orange exclamation mark.

4. Select the machines that you want to update the virtual appliances on. These machines must be online.
5. Click **Update agent**.
6. Select the deployment agent.
7. Specify the credentials of an account with administrative privileges on the target machine.
8. 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 error during the virtual appliance registration.

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

---

**Note**

During the update, any backups that are in progress will fail.

---

## Cloud deployment

For information on how to update a virtual appliance in cloud deployment, refer to [Updating agents](#) in the cloud documentation.

## Updating agents

### Prerequisites

On Windows machines, Cyber Protect features require Microsoft Visual C++ 2017 Redistributable. Please ensure that it is already installed on your machine or install it before updating the agent. After the installation, a restart may be required. The Microsoft Visual C++ Redistributable package can be found here <https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows>.

To find the agent version, select the machine, and then click **Details**.

You can update agents by using the Cyber Protect web console or by repeating their installation in any available way. To update multiple agents simultaneously, use the following procedure.

#### ***To update agents by using the Cyber Protect web console***

1. [Only in on-premises deployments] Update the management server.
2. [Only in on-premises deployments] Ensure that the installation packages are present on the machine with the management server. For the exact steps, refer to ["Adding a machine running Windows"](#) > "Installation packages".
3. In the Cyber Protect web console, click **Settings** > **Agents**.

The software displays the list of machines. The machines with outdated agent versions are marked with an orange exclamation mark.

4. Select the machines that you want to update the agents on. The machines must be online.
5. Click **Update agent**.
6. Select the deployment agent.
7. Specify the credentials of an account with administrative privileges on the target machine.
8. Select the name or the IP address of the management server that the agent will use to access that server.

By default, the server name is selected. You may need to select the IP address instead if your management server has more than one network interface or if you are facing DNS issues that cause the agent registration to fail.

9. [Only in on-premises deployments] The update progress is shown on the **Activities** tab.

---

**Note**

During the update, any backups that are in progress will fail.

---

***To update the Cyber Protect definitions on a machine***

1. Click **Settings > Agents**.
2. Select the machine on which you want to update the Cyber Protect definitions and click **Update definitions**. The machine must be online.

***To assign the Updater role to an agent***

1. Click **Settings > Agents**.
2. Select the machine to which you want to assign the [Updater role](#), click **Details**, then in the **Cyber Protect definitions** section, enable **Use this agent to download and distribute patches and updates**.

***To clear cached data on an agent***

1. Click **Settings > Agents**.
2. Select the machine on which you want to clear the cached data (outdated update files and patch management data) and click **Clear cache**.

## Updating agents on BitLocker-protected workloads

Agent updates that introduce changes to Startup Recovery Manager interfere with BitLocker on workloads on which both BitLocker and Startup Recovery Manager are enabled. In this case, after a restart, the BitLocker recovery key is required. To mitigate this issue, suspend or disable BitLocker before you update the agent.

You can check whether an update introduces changes to Startup Recovery Manager in the release notes of each new version of Acronis Cyber Protect.

***To install the update***

1. On the workload on which you will update the agent, suspend or disable BitLocker.
2. Update the agent.
3. Restart the workload.
4. Enable BitLocker.

## Upgrading to Acronis Cyber Protect 15

You can upgrade an earlier product to Acronis Cyber Protect 15 in the following ways:

- Directly, without uninstalling the earlier product.  
This option is only available for Acronis Backup 12.5 Update 5 (build 16180) and later.
- By uninstalling the earlier product and installing a fresh copy of Acronis Cyber Protect 15.  
This option is available for all eligible products. For more information about these products, refer to [this knowledge base article](#).

---

### Note

We recommend that you back up your system before upgrading. This will allow you to roll back to the original configuration if your upgrade fails.

---

To start the upgrade, run the installer and follow the on-screen instructions.

The management server in Acronis Cyber Protect 15 is backward compatible and supports the version 12.5 agents. However, these agents do not support the [Cyber Protect features](#).

Upgrading the agents does not interfere with the existing backup sets and their settings.

## Uninstalling the product

If you want to remove individual product components from a machine, run the setup program, choose to modify the product, and clear the selection of the components that you want to remove. The links to the setup programs are present on the **Downloads** page (click the account icon in the top-right corner > **Downloads**).

If you want to remove all of the product components from a machine, follow the steps described below.

---

### Warning!

In on-premises deployments, be very careful when selecting the components to uninstall.

If you uninstall the management server by mistake, the Cyber Protect web console will become unavailable and you will no longer be able to back up and recover the machines that were registered on the uninstalled management server.

---

## In Windows

1. Log on as an administrator.
2. Go to **Control panel**, and then select **Programs and Features (Add or Remove Programs in Windows XP) > Acronis Cyber Protect > Uninstall**.
3. [Optional] Select the **Remove the logs 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 Cyber Protect web console and the backups of the old machine may not be associated with the new machine.
4. Confirm your decision.

## 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 Cyber Protect web console and the backups of the old machine may not be associated with the new machine.
3. Confirm your decision.

## In macOS

1. Double-click the installation file (.dmg).
2. Wait while the operating system mounts the installation disk image.
3. Inside the image, double-click **Uninstall**.
4. If prompted, provide administrator credentials.
5. Confirm your decision.

## Removing Agent for VMware (Virtual Appliance)

1. Start the vSphere Client and log on to the vCenter Server.
2. If the virtual appliance is powered on, right-click it, and then click **Power > Power Off**. Confirm your decision.
3. If the virtual appliance 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 virtual appliance, 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 virtual

appliance.

4. Right-click the virtual appliance, and then click **Delete from Disk**. Confirm your decision.

## Removing machines from the Cyber Protect web console

After uninstalling an agent, it will be unregistered from the management server, and the machine where the agent was installed will be automatically removed from the Cyber Protect web console.

However, if during this operation the connection to the management server is lost – due to a network problem, for example – the agent might be uninstalled but its machine might still be shown in the web console. In this case, you need to remove the machine from the web console manually.

### ***To remove a machine from the web console manually***

1. In the Cyber Protect web console, go to **Settings > Agents**.
2. Select the machine where the agent was installed.
3. Click **Delete**.

# Accessing the Cyber Protect web console

To access the Cyber Protect web console, enter the login page address into the web browser address bar, and then sign in as described below.

## On-premises deployment

The login page address is the IP address or name of the machine where the management server is installed.

Both the HTTP and the HTTPS protocols are supported on the same TCP port, which can be configured during the [management server installation](#). The default port is 9877.

You can [configure the management server](#) to prohibit accessing the Cyber Protect web console via HTTP and to use a third-party SSL certificate.

## In Windows

If the management server is installed in Windows, there are two ways to sign in to the Cyber Protect web console:

- Click **Sign in** to sign in as the current Windows user.

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](#).

Otherwise, the browser will ask for a user name and password. However, you can disable this option.

- 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"](#).

### ***To disable the Sign in as the current Windows user option***

1. On the machine where the management server is installed, go to C:\Program Files\Acronis\AccountServer.
2. Open the file **account\_server.json** for editing.
3. Navigate to the "connectors" section, and then delete the following lines:

```
{
 "type": "sspi",
```



```
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. Navigate to the "checksum" section, and then change the "sum" value as follows:

```
"sum": "FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbj pzU="
```

5. Restart Acronis Service Manager Service as described in ["Using a certificate issued by a trusted certificate authority."](#)

## 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"](#).

## Cloud deployment

The login page address is <https://backup.acronis.com/>. The user name and password are those of your Acronis account.

If your account was created by the backup administrator, you need to activate the account and set the password by clicking the link in your activation email.

## Changing the language

When logged in, you can change the language of the web interface by clicking the account icon in the top-right corner.

## Configuring a web browser for Integrated Windows Authentication

When you access the Cyber Protect web console from a Windows machine and a [supported web browser](#), you can use Integrated Windows Authentication. Without Integrated Windows Authentication, you must specify a user name and password to access the Cyber Protect web console.

### **Configuring Edge, Opera, or Chrome**

- If you access the Cyber Protect web console from a machine 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. See how to do this in "Adding the console to the list of local intranet sites" (p. 202).

- If the machines are not in the same Active Directory domain, add the console's login page to the list of **Trusted sites** and enable the **Automatic logon with current user name and password** setting. See how to do this in "Adding the console to the list of trusted sites" (p. 204).

---

**Note**

You can also configure the browsers by using a Group Policy in the Active Directory domain.

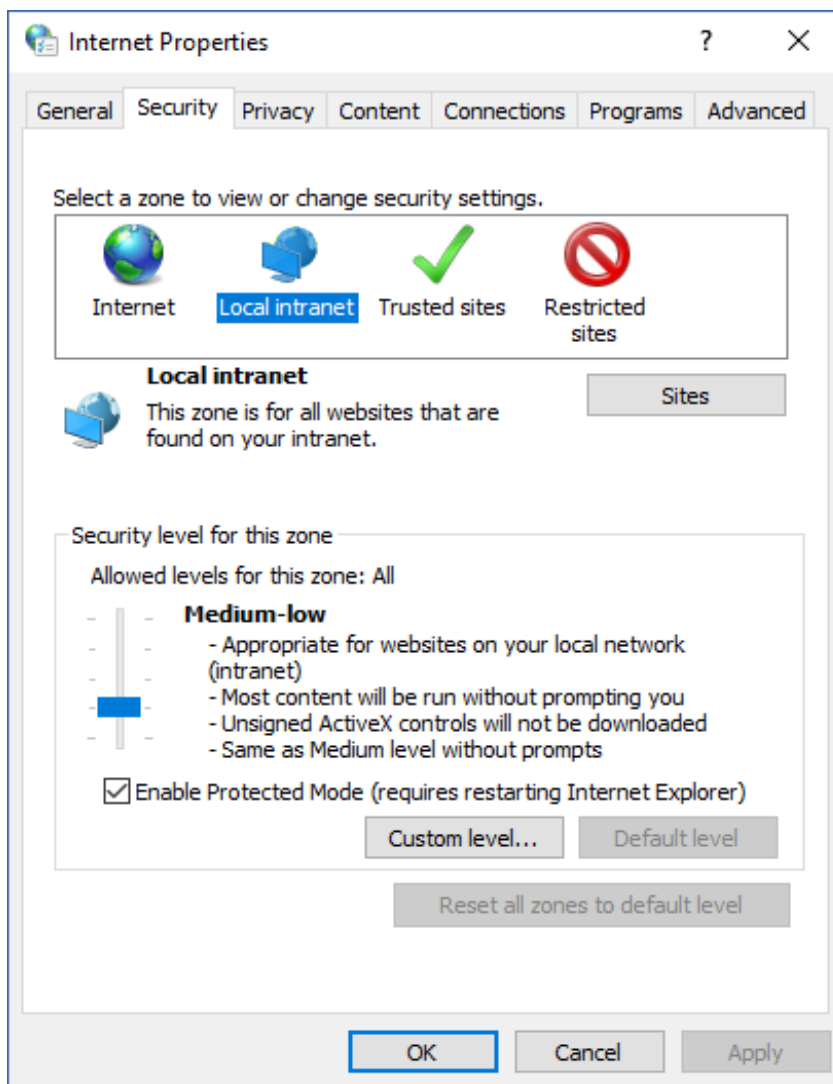
---

**Configuring Firefox**

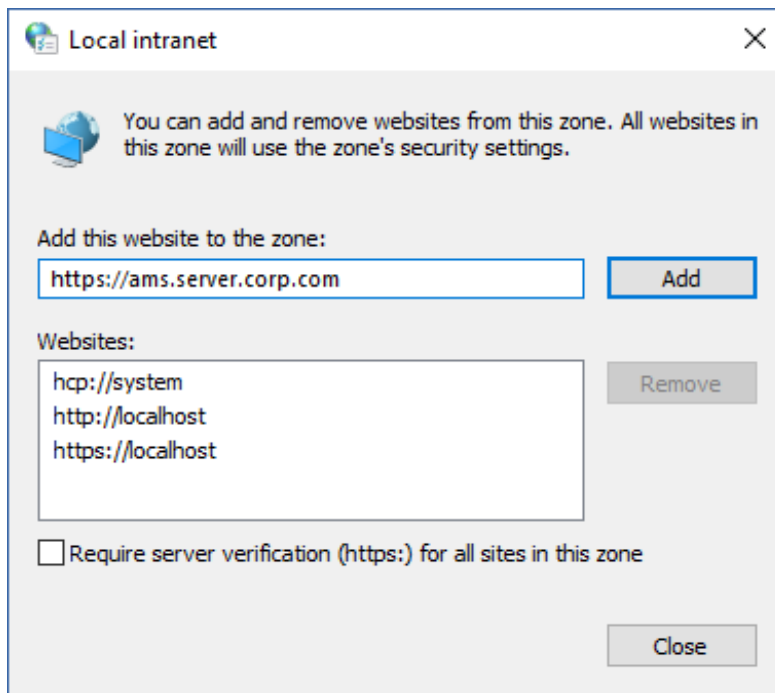
1. In the Firefox address bar, enter `about:config`, and then press Enter.
2. Click **Accept the Risk and Continue**.
3. In the search field, enter `network.negotiate-auth.trusted-uris`.
4. Double-click the `network.negotiate-auth.trusted-uris` preference, and then enter the address of the Cyber Protect web console login page.
5. In the search field, enter `network.automatic-ntlm-auth.trusted-uris`.
6. Double-click the `network.automatic-ntlm-auth.trusted-uris` preference, and then enter the address of the Cyber Protect web console login page.
7. Close the `about:config` window.

## 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**.



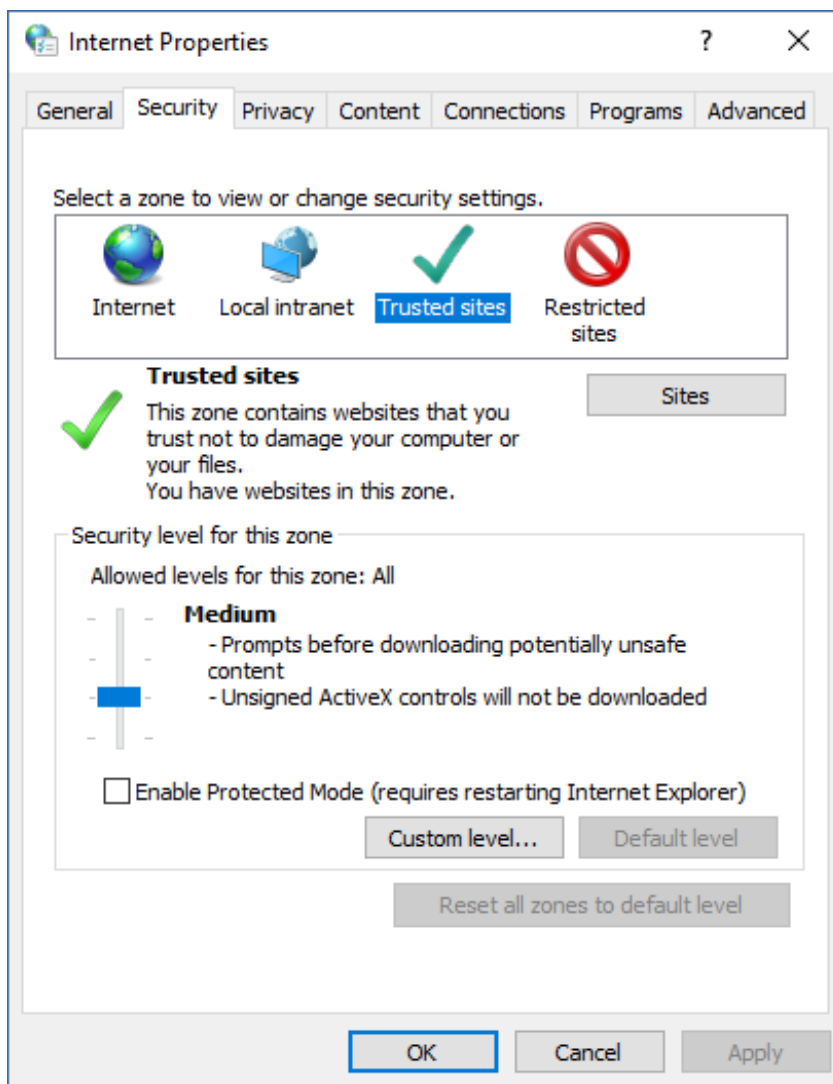
3. Click **Sites**.
4. In **Add this website to the zone**, enter the address of the Cyber Protect web console login page, and then click **Add**.



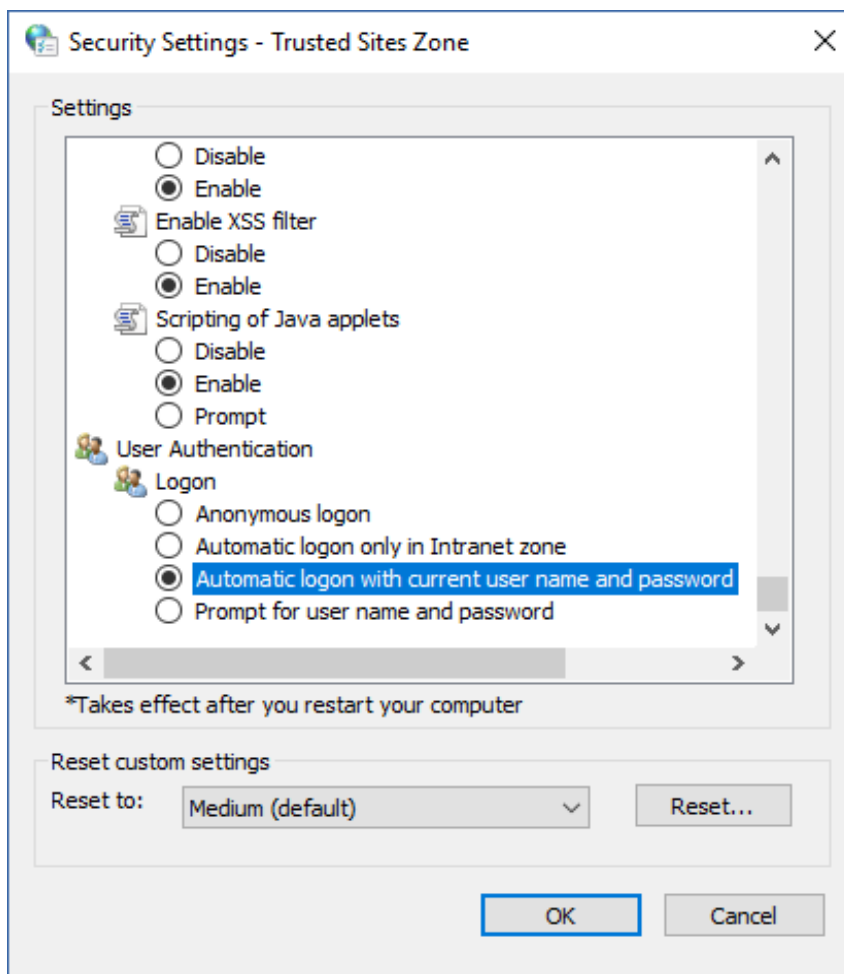
5. Click **Close**.
6. Click **OK**.

## Adding the console to the list of trusted sites

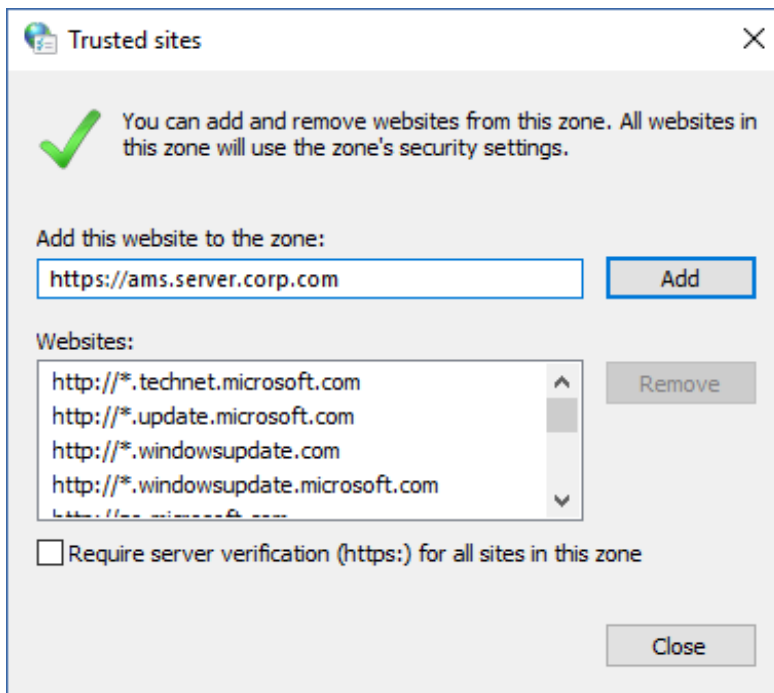
1. Go to **Control Panel > Internet Options**.
2. On the **Security** tab, select **Trusted sites**, and then click **Custom level**.



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 Cyber Protect web console login page, and then click **Add**.



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

## Allowing only HTTPS connections to the web console

### Note

Accessing the Cyber Protect web console via HTTPS is available only if you use certificates in the PEM format. If you use PFX certificates, convert them to PEM files.

For security reasons, you can prevent users from accessing the Cyber Protect web console via the HTTP protocol, and allow only HTTPS connections.

### ***To allow only HTTPS connections to the web console***

1. On the machine running the management server, 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
2. Locate the following section:

```
"tls": {
 "auto_redirect" : false,
 "cert_file": "cert.pem",
```

3. Change the "auto\_redirect" value from false to true.  
If the "auto\_redirect" line is missing, add it manually:

```
"auto_redirect": true,
```

4. 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.

---

5. Restart Acronis Service Manager Service as described below.

**To restart Acronis Service Manager Service in Windows****In Windows**

1. In the **Start** menu, click **Run**, and then type: **cmd**
2. Click **OK**.
3. Run the following commands:

```
net stop asm
net start asm
```

**In Linux**

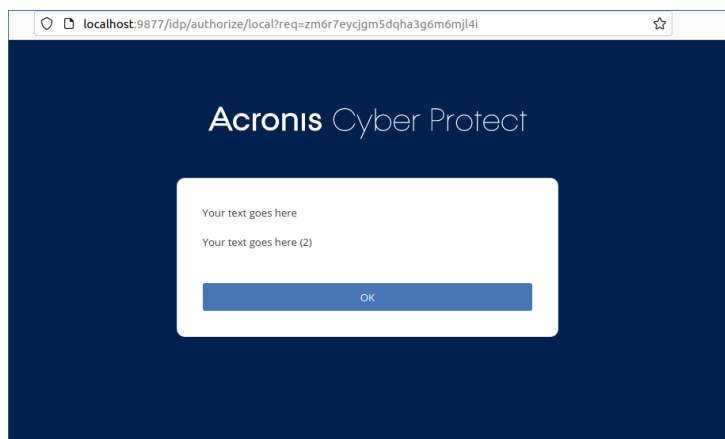
1. Open **Terminal**.
2. Run the following command in any directory:

```
sudo service acronis_asm restart
```

## Adding a custom message to the web console

You can add a custom message to the Cyber Protect web console.

This message will be shown before every login attempt.



## Prerequisites

If any protection plans are applied to the machine on which the management server runs, ensure that the self-protection feature is disabled. Otherwise, you will not be able to edit the configuration



file.

For more information on how to disable or enable the self-protection feature, refer to "Self-protection" (p. 511).

### ***To add a custom message to the web console***

#### ***In Windows***

1. Log in to the machine on which the management server is installed. Your account must have administrator rights.
2. Navigate to %Program Files%\Acronis\AccountServer.
3. [Optional] Make a backup copy of the AccountServer.zip file.
4. Navigate to %Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale.
5. Unpack the JSON file that corresponds to the language that you use in the Cyber Protect web console. For example, if you use English, unpack the en.json file.

---

#### **Note**

To be able to edit the file, you must unpack it, and not just open the file by double-clicking it.

---

6. Open the unpacked file for editing. You can use a text editor, such as Notepad or Notepad++.
7. Navigate to the following line, and then add a comma at the end:

```
"APP_LOGINFORM_LOGIN_BUTTON": "Log in",
```

8. Under the "APP\_LOGINFORM\_LOGIN\_BUTTON": "Log in" line, add the following lines:

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

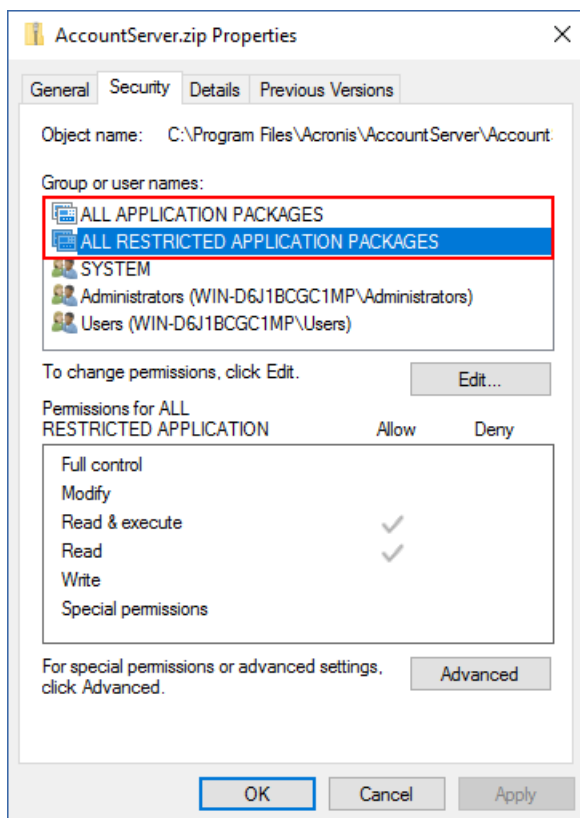
```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON": "OK"
```

For example:

```
16 "APP_LOGINFORM_SSPI_HINT": "Sign in as current Windows user",
17 "APP_LOGINFORM_LOCAL_HINT": "Enter user name and password",
18 "APP_ADVANCED_LICENSE_MISSING": "An Advanced license is missing",
19 "APP_LOGINFORM_LOGOUT": "You logged out",
20 "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
21 "APP_LOGINFORM_NOTICE": "Your text goes here /n Your text goes here (2) ",
22 "APP_LOGINFORM_IS_SCS": "true",
23 "APP_LOGINFORM_OK_BUTTON": "OK"
24 }
```

9. Save the changes, and then place the edited JSON file back in %Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale.
10. Right-click the AccountServer.zip file, and then navigate to **Properties > Security** to verify that ALL APPLICATION PACKAGES and ALL RESTRICTED APPLICATION PACKAGES are added under **Group or user names** with **Read** and **Read & Execute** rights.



### Note

If ALL RESTRICTED APPLICATION PACKAGES is missing, remove ALL APPLICATION PACKAGES from that list, and then add it again. ALL RESTRICTED APPLICATION PACKAGES will appear automatically when you add ALL APPLICATION PACKAGES.

11. Restart **Acronis Service Manager Service** as described in "To restart Acronis Service Manager Service" (p. 214).

### In Linux

1. Log in to the machine on which the management server is installed.
2. Navigate to /usr/lib/Acronis/AccountServer.
3. Ensure that you have write permissions for the AccountServer.zip file.
4. [Optional] Make a backup copy of the AccountServer.zip file.
5. Navigate to /usr/lib/Acronis/AccountServer/static/locale.
6. Unpack the JSON file that corresponds to the language that you use in the Cyber Protect web console. For example, if you use English, unpack the en.json file.
7. Open the unpacked file for editing.
8. Navigate to the following line, and then add a comma at the end:

```
"APP_LOGINFORM_LOGIN_BUTTON": "Log in",
```

9. Under the "APP\_LOGINFORM\_LOGIN\_BUTTON": "Log in" line, add the following lines:

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON": "OK"
```

For example:

```
16 "APP_LOGINFORM_SSPI_HINT": "Sign in as current Windows user",
17 "APP_LOGINFORM_LOCAL_HINT": "Enter user name and password",
18 "APP_ADVANCED_LICENSE_MISSING": "An Advanced license is missing",
19 "APP_LOGINFORM_LOGOUT": "You logged out",
20 "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
21 "APP_LOGINFORM_NOTICE": "Your text goes here /n Your text goes here (2) ",
22 "APP_LOGINFORM_IS_SCS": "true",
23 "APP_LOGINFORM_OK_BUTTON": "OK"
24 }
```

10. Save the changes, and then place the edited JSON file back in  
/usr/lib/Acronis/AccountServer/static/locale.
11. Restart **Acronis Service Manager Service** as described in "To restart Acronis Service Manager Service" (p. 214).

## SSL certificate settings

This section describes how:

- To configure a protection agent that uses a self-signed Secure Socket Layer (SSL) certificate generated by the management server.
- To change the self-signed 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 Cyber Protect web console by using the HTTPS protocol.

Optionally, you can configure the management server to prohibit accessing the Cyber Protect web console via HTTP, by redirecting all users to HTTPS. For more information, see "Allowing only HTTPS connections to the web console" (p. 207).

---

### Note

Accessing the Cyber Protect web console via HTTPS is available only if you use certificates in the PEM format. If you use PFX certificates, convert them to PEM files.

---

## Using a self-signed certificate

### *To configure a protection agent in Windows*

1. On the machine with the agent, open Registry Editor.
2. Locate the following registry key: **HKEY\_LOCAL\_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions**.
3. Set the **VerifyPeer** value to **0**.

4. Ensure that **VerifyHost** value is set to **0**.
5. Restart Managed Machine Service (MMS):
  - 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 configure a protection agent in Linux***

1. On the machine with the agent, open the file **/etc/Acronis/BackupAndRecovery.config** for editing.
2. Navigate to the **CurlOptions** key and set the value for **VerifyPeer** to **0**. Ensure that the value for **VerifyHost** is also set to **0**.
3. Save your edits.
4. Restart the Managed Machine Service (MMS) by executing the following command in any directory:

```
sudo service acronis_mms restart
```

### ***To configure a protection agent in macOS***

1. On the machine with the agent, stop the Managed Machine Service (MMS):
  - a. Go to **Applications > Utilities > Terminal**
  - b. Run the following command:

```
sudo launchctl stop acronis_mms
```

2. Open the file **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** for editing.
3. Navigate to the **CurlOptions** key and set the value for **VerifyPeer** to **0**. Ensure that the value for **VerifyHost** is also set to **0**.
4. Save your edits.
5. Start the Managed Machine Service (MMS), by running the following command in Terminal:

```
sudo launchctl start acronis_mms
```

## Using a certificate issued by a trusted certificate authority

### ***To configure the SSL certificate settings***

1. Ensure that you have all of the following:

If you use certificate and key files	If you use a PFX file
The certificate file (in the .pem format)	The PFX file
The file with the private key for the certificate (usually in the .key format)	
The private key password (if the key is password-protected)	The password for the PFX file, if the file is password-protected

---

**Important**

All aliases of the management server must be included in the certificate as Subject Alternative Names (SAN).

---

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": "",
```

5. Between the quotation marks in the "cert\_file" line, specify the full path to the certificate file or the PFX file.

For example:

Operating system	If you use certificate and key pair	If you use a .pfx file
Windows (note the forward slashes)	"cert_file": "C:/certificate/local-domain.ams.pem"	"cert_file": "C:/certificate/local-domain.ams.pfx"
Linux	"cert_file": "/home/user/local-domain.ams.pem"	"cert_file": "/home/user/local-domain.ams.pfx"

6. Between the quotation marks in the "key\_file" line, specify the full path to the private key file or the PFX file that contains the certificate key.

Usually, a PFX file includes both the certificate and its key. In this case, in the "key\_file" line, specify the same path as in the previous step.

For example:

Operating system	If you use certificate and key pair	If you use a .pfx file
Windows (note the forward slashes)	"key_file": "C:/certificate/private.key"	"cert_file": "C:/certificate/local-domain.ams.pfx"
Linux	"key_file": "/home/user/private.key"	"cert_file": "/home/user/local-domain.ams.pfx"

7. [Optional] If the private key or the PFX file is password-protected, between the quotation marks in the "passphrase" line, specify the password.

For example: "passphrase": "my password"

#### Note

If the "passphrase": "", line is missing in your api\_gateway.json configuration file, add it manually.

For example:

```
"tls": {
 "cert_file": "cert.pem",
 "key_file": "key.pem",
 "passphrase": "my password",
}
```

8. 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.

9. Restart Acronis Service Manager Service as described below.

#### To restart Acronis Service Manager Service

##### In Windows

1. In the **Start** menu, click **Run**, and then type: **cmd**
2. Click **OK**.
3. Run the following commands:

```
net stop asm
net start asm
```

##### In Linux

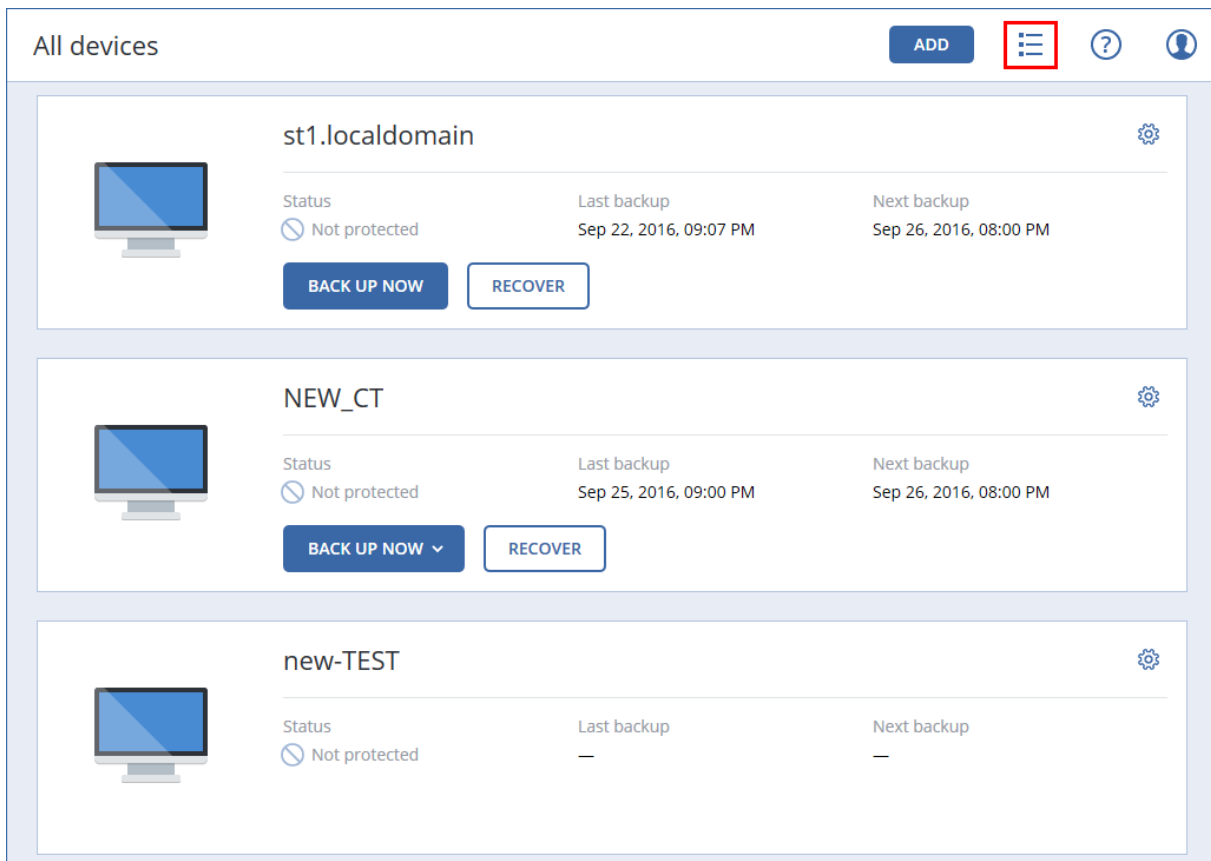
1. Open **Terminal**.
2. Run the following command in any directory:

```
sudo service acronis_asm restart
```

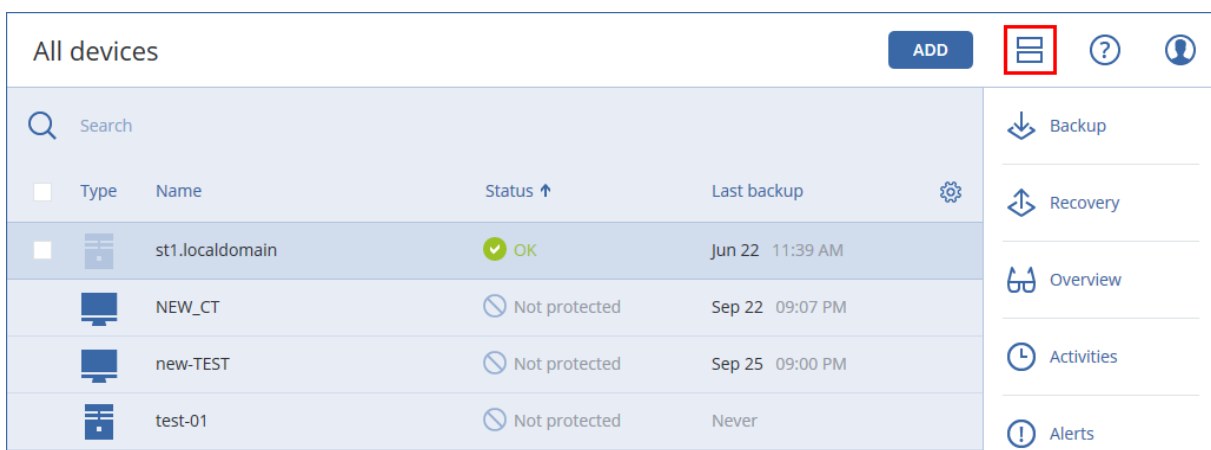
# Cyber Protect web console view

The Cyber Protect web console has two views: a simple view and a table view. To switch between the views, click the corresponding icon in the top right corner.

The simple view supports a small number of machines.



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



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



When a machine goes online or offline, it takes some time for its status to change in the Cyber Protect web console.

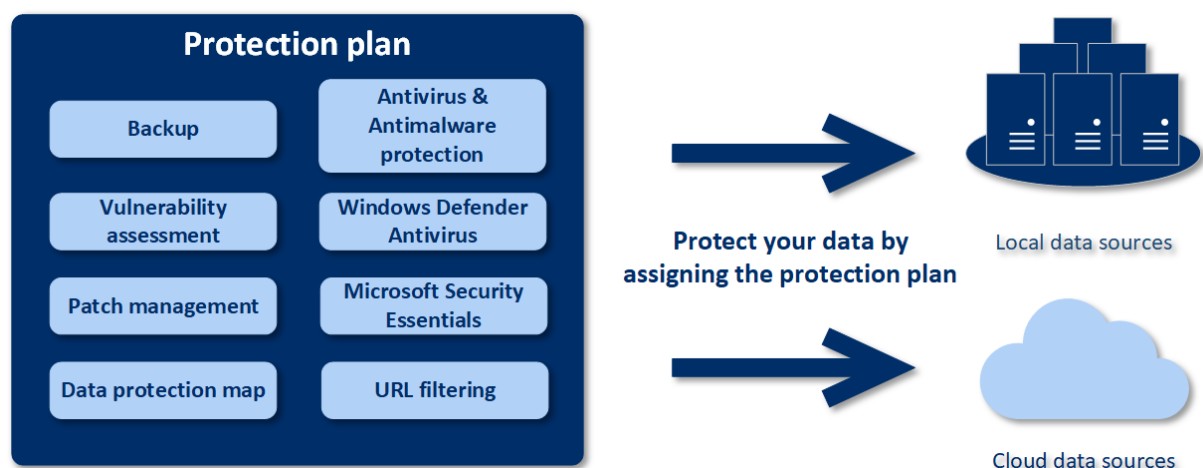
Machine status is checked every minute. If the agent installed on this machine is not transferring data, and there is no answer to five consecutive checks, the machine is shown as offline. The machine is shown as back online when it answers to a status check or starts transferring data.

# Protection plan and modules

The protection plan is a plan that combines several data protection modules including

- [Backup](#) – allows you to back up your data sources to local or cloud storage.
- [Antivirus & Antimalware protection](#) – allows you to check your machines with the built-in antimalware solution.
- [URL filtering](#) – allows you to protect your machines from threats coming from the Internet by blocking access to malicious URLs and content to be downloaded.
- [Windows Defender Antivirus](#) – allows you to manage the settings of Windows Defender Antivirus to protect your environment.
- [Microsoft Security Essentials](#) – allows you to manage the settings of Microsoft Security Essentials to protect your environment.
- [Vulnerability assessment](#) – automatically checks the Microsoft and third-party products installed on your machines for vulnerabilities and notifies you about them.
- [Patch management](#) – allows you to install patches and updates for the Microsoft and third-party products on your machines to close the discovered vulnerabilities.
- [Data protection map](#) – allows you to discover the data in order to monitor the protection status of important files.

The protection plan allows you to protect your data sources completely from external and internal threats. By enabling and disabling different modules and setting up the module settings, you can build flexible plans satisfying various business needs.



## Creating a protection plan

A protection plan can be applied to multiple machines at the time of its creation, or later. When you create a plan, the system checks the operating system and the device type (for example, workstation, virtual machine, etc.) and shows only those plan modules that are applicable to your devices.

A protection plan can be created in two ways:

- Let's consider the first way.

1. In the Cyber Protect web console, go to **Devices > All devices**.
2. Select the machines that you want to protect.
3. Click **Protect**, and then click **Create plan**. You will see the protection plan with the default settings.

219

4. [Optional] To modify the protection plan name, click on the pencil icon next to the name.
5. [Optional] To enable or disable a protection plan module, click the switch next to the module name.
6. [Optional] To configure the module parameters, click the corresponding section of the protection plan.
7. When ready, click **Create**.

The Backup, Antivirus & Antimalware protection, Vulnerability assessment, Patch management, and Data protection map modules can be performed on demand by clicking **Run now**.

## Resolving plan conflicts

A protection plan can be in the following statuses:

- **Active** – a plan that is assigned to devices and executed on them.
- **Inactive** – a plan that is assigned to devices but is disabled and not executed on them.

## Applying several plans to a device

You can apply several protection plans to a single device. As a result, you will get a combination of different protection plans assigned on a single device. For example, you may apply one plan that has only the Antivirus & Antimalware protection module enabled, and another plan that has only the Backup module enabled. The protection plans can be combined only if they do not have intersecting modules. If the same modules are enabled in more than one protection plan, you must resolve the conflicts between them.

## Resolving plan conflicts

### Plan conflicts with already applied plans

When you create a new plan on a device or devices with already applied plans that conflict with the new plan, you can resolve a conflict with one of the following ways:

- Create a new plan, apply it, and disable all already applied conflicting plans.
- Create a new plan and disable it.

When you edit a plan on a device or devices with already applied plans that conflict with the changes made, you can resolve a conflict with one of the following ways:

- Save changes to the plan and disable all already applied conflicting plans.
- Save changes to the plan and disable it.

### A device plan conflicts with a group plan

If a device is included in a group of devices with an assigned group plan, and you try to assign a new plan to a device, then the system will ask you to resolve the conflict by doing one of the following:

- Remove a device from the group and apply a new plan to the device.
- Apply a new plan to the whole group or edit the current group plan.

## License issue

The assigned quota on a device must be appropriate for the protection plan to be performed, updated, or applied. To resolve the license issue, do one of the following:

- Disable the modules that are unsupported by the assigned quota and continue using the protection plan.
- Change the assigned quota manually: go to **Devices** > **<Particular device>** > **Details** > **Service quota**. Then, revoke the existing quota and assign a new one.

## Operations with protection plans

For information about how to create a protection plan, refer to "[Creating a protection plan](#)".

### Available actions with a protection plan

You can perform the following actions with a protection plan:

- Rename a plan
- Enable/disable modules and edit each module settings
- Enable/disable a plan

A disabled plan will not be carried out on the device to which it is applied.

This action is convenient for administrators who intend to protect the same device with the same plan later. The plan is not revoked from the device and to restore the protection, the administrator must only re-enable the plan.

- Apply a plan to devices or group of devices
- Revoke a plan from a device

A revoked plan is not applied to a device anymore.

This action is convenient for administrators who do not need to protect quickly the same device with the same plan again. To restore the protection of a revoked plan, the administrator must know the name of this plan, select it from the list of available plans, and then re-apply it to the desired device.

- Import/export a plan

---

#### Note

You can only import protection plans created in Acronis Cyber Protect 15. Protection plans created in older versions are incompatible with Acronis Cyber Protect 15.

---

- Delete a plan

### ***To apply an existing protection plan***

1. Select the machines that you want to protect.
2. Click **Protect**. If a protection plan is already applied to the selected machines, click **Add plan**.
3. The software displays previously created protection plans.
4. Select the protection that you need, and then click **Apply**.

#### ***To edit a protection plan***

1. If you want to edit the protection 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 protection plan.
2. Click **Protect**.
3. Select the protection plan that you want to edit.
4. Click the ellipsis icon next to the protection plan name, and then click **Edit**.
5. To modify the plan parameters, click the corresponding section of the protection plan panel.
6. Click **Save changes**.
7. To change the protection plan for all machines to which it is applied, click **Apply the changes to this protection plan**. Otherwise, click **Create a new protection plan only for the selected devices**.

#### ***To revoke a protection plan from machines***

1. Select the machines that you want to revoke the protection plan from.
2. Click **Protect**.
3. If several protection plans are applied to the machines, select the protection plan that you want to revoke.
4. Click the ellipsis icon next to the protection plan name, and then click **Revoke**.

#### ***To delete a protection plan***

1. Select any machine to which the protection plan that you want to delete is applied.
2. Click **Protect**.
3. If several protection plans are applied to the machine, select the protection plan that you want to delete.
4. Click the ellipsis icon next to the protection plan name, and then click **Delete**.

As a result, the protection plan is revoked from all of the machines and completely removed from the web interface.

# Backup

A protection plan with the Backup module enabled is a set of rules that specify how the given data will be protected on a given machine.

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

---

## Note

In on-premises deployments, if only the Standard licenses are present on the management server, a protection plan cannot be applied to multiple physical machines. Each physical machine must have its own protection plan.

---

### ***To create the first protection plan with the Backup module enabled***

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

The software displays protection plans that are applied to the machine. If the machine does not have any plans already assigned to it, then you will see the default protection plan that can be

applied. You can adjust the settings as needed and apply this plan or create a new one.

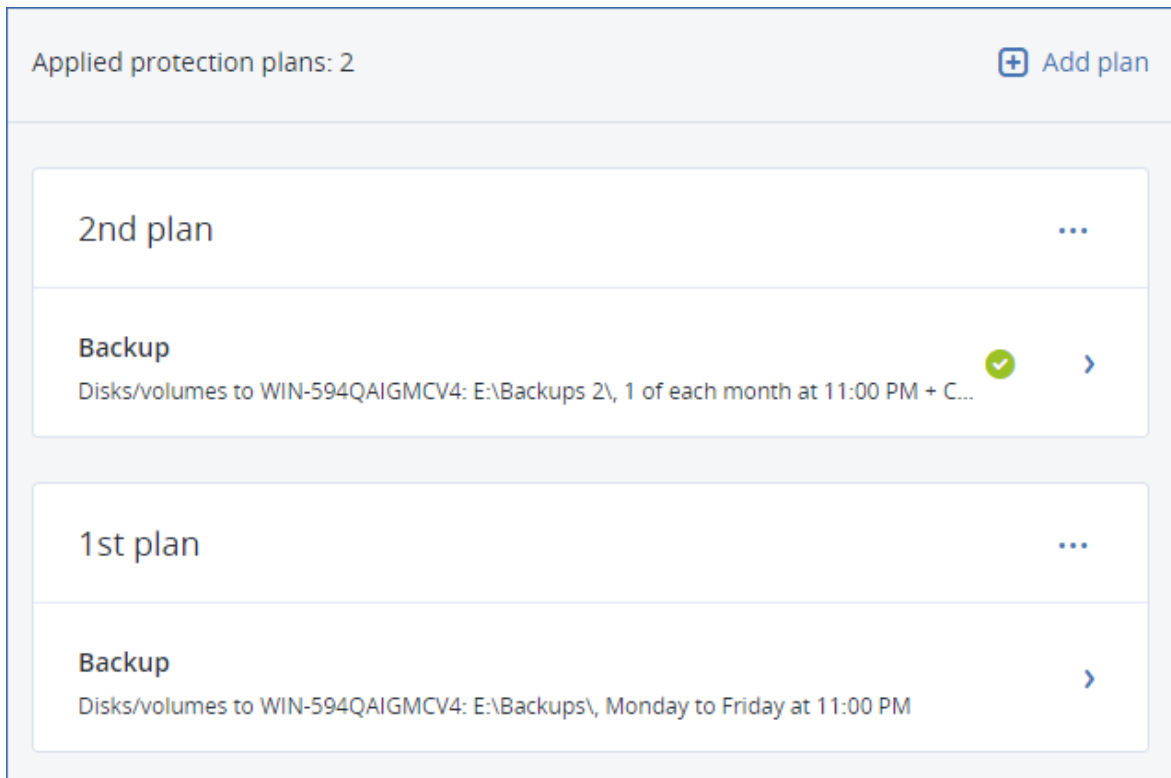
3. To create a new plan, click **Create plan**. Enable the **Backup** module and unroll the settings.
4. [Optional] To modify the protection plan name, click the default name.
5. [Optional] To modify the Backup module parameters, click the corresponding section of the protection plan panel.
6. [Optional] To modify the backup options, click **Change** next to **Backup options**.
7. Click **Create**.



### To apply an existing protection plan

1. Select the machines that you want to back up.
2. Click **Protect**. If a common protection plan is already applied to the selected machines, click **Add plan**.

The software displays previously created protection plans.



3. Select a protection plan to apply.
4. Click **Apply**.

## Backup module cheat sheet

### Important

Some of the features described in this section are only available for on-premises deployments.

The following table summarizes the available Backup module parameters. Use the table to create a protection plan that best fits your needs.

WHAT TO BACK UP	ITEMS TO BACK UP Selection methods	WHERE TO BACK UP	SCHEDULE Backup schemes (not for Cloud)	HOW LONG TO KEEP
Disks/volumes	Direct	Cloud	Always	By backup age (single

(physical machines)	selection Policy rules File filters	Local folder Network folder SFTP server* NFS* Secure Zone* Managed location* Tape device*	incremental (Single-file)* Always full Weekly full, Daily incremental Monthly full, Weekly differential, Daily incremental (GFS) Custom (F-D-I)	rule/per backup set)  By number of backups  By total size of backups*  Keep indefinitely
Disks/volumes (virtual machines)	Policy rules File filters	Cloud Local folder Network folder SFTP server* NFS* Managed location* Tape device*		
Files (physical machines only)	Direct selection Policy rules File filters	Cloud Local folder Network folder SFTP server* NFS* Secure Zone* Managed location* Tape device	Always full Weekly full, Daily incremental Monthly full, Weekly differential, Daily incremental (GFS) Always incremental (Single-file)* Custom (F-D-I)	
ESXi configuration	Direct selection	Local folder Network folder SFTP server NFS*		
SQL databases	Direct selection	Cloud Local folder Network folder Managed	Always full Weekly full, daily incremental Custom (F-I)	

		location* Tape device		
--	--	--------------------------	--	--

Exchange databases	Direct selection			By backup page (single file) or by peer backup
Exchange mailboxes	Direct selection			
Microsoft 365 mailboxes	Direct selection	Cloud Local folder Network folder Managed location*	Always incremental (Single-file)	

			u p s e t ) B y n u m b e r o f b a c k u p s K e e p i n d e x i n t e r y
--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

\* See the limitations below.

## Limitations

### SFTP server and tape device

- These locations cannot be a destination for backups of machines running macOS.
- 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.
- The **Always incremental (single-file)** backup scheme for Files (physical machines) is not available when backing up to NFS shares.

### Secure Zone

- Secure Zone cannot be created on a Mac.

### Managed location

- A managed location with enabled deduplication or encryption cannot be selected as the destination:
  - If the backup scheme is set to **Always incremental (single-file)**
  - If the backup format is set to **Version 12**
  - For disk-level backups of machines running macOS
  - For backups of Exchange mailboxes and Microsoft 365 mailboxes.
- The **By total size of backups** retention rule is not available for a managed location with enabled deduplication.

### 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.
- The **Always incremental (single-file)** backup scheme for Files (physical machines) is available only when the primary backup location is Acronis Cloud.

### 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.

# Selecting data to back up

## Selecting entire machine

A backup of an entire machine is a backup of all its non-removable disks.

To configure such a backup, in **What to back up**, select **Entire machine**.

---

### Important

External drives, such as USB flash drives or USB hard drives, are not included in the **Entire machine** backup. To back up these drives, configure a **Disks/volumes** backup. For more information about the disk backup, refer to "Selecting disks/volumes" (p. 231).

---

## 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 non-removable disks.

---

### Note

The OneDrive root folder is excluded from backup operations by default. If you select to back up specific OneDrive files and folders, they will be backed up. Files that are not available on the device will have invalid contents in the archive.

---

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](#).

## Direct selection

Direct selection is available only for physical machines. To enable direct selection of disks and volumes on a virtual machine, you must install the protection agent in its guest operating system.

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 protection 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 protection 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, Linux, and macOS

- [All Volumes] selects all volumes on machines running Windows and all mounted volumes on machines running Linux or macOS.

### 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 boot and system volumes. This combination is the minimal set of data that ensures recovery of the operating system from the backup.
- [BOOT+SYSTEM DISK (physical machines)] selects all volumes of the disk on which the boot and system volumes are located. If the boot and system volumes are not located on the same disk, nothing will be selected. This rule is applicable only to physical machines.
- [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_1-lv2
```



## Rules for macOS

- [Disk 1] Selects the first disk of the machine, including all volumes on that disk. To select another disk, type the corresponding number.

## What does a disk or volume backup store?

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** 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\FilesNotToBackup**. This means that in operating systems starting with Windows 7, Windows Restore Points are not backed up.
  - If the **Volume Shadow Copy Service (VSS) backup option** 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.

## Mac

A disk or volume backup stores all files and directories of the selected disk or volume, plus a description of the volume layout.

The following items are excluded:

- System metadata, such as the file system journal and Spotlight index
- The Trash
- Time machine backups

Physically, disks and volumes on a Mac are backed up at a file level. Bare metal recovery from disk and volume backups is possible, but the sector-by-sector backup mode is not available.

## 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.

---

### Note

The OneDrive root folder is excluded from backup operations by default. If you select to back up specific OneDrive files and folders, they will be backed up. Files that are not available on the device will have invalid contents in the archive.

---

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](#).

## 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 protection 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 protection 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.

## Selection rules for macOS

- Full path to a file or directory.
- Templates:

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

Examples:

- To back up **file.txt** on your desktop, specify **/Users/<username>/Desktop/file.txt**, where <username> is your user name.
- To back up all users' home directories, specify **/Users**.
- To back up the directory where the applications are installed, specify **/Applications**.

## 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.
- To back up the ESXi configuration, Agent for VMware uses an SSH connection to the ESXi host on TCP port 22. Ensure that your firewall does not block this connection.
- You must know the password for the 'root' account on the ESXi host.

## Limitations

- ESXi configuration backup is not supported for VMware vSphere 7.0 and later.
- An ESXi configuration cannot be backed up to the cloud storage.

### ***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.

# Continuous data protection (CDP)

Backups are usually performed with the regular but quite long time intervals due to performance reasons. If the system is suddenly damaged, the data changes between the last backup and the system failure will be lost.

The **Continuous data protection** functionality allows you to back up changes of the selected data between the scheduled backups on the continuous basis:

- By tracking changes in the specified files/folders
- By tracking changes of the files modified by the specified applications

You can select particular files for continuous data protection from the data selected for a backup. The system will back up every change of these files. You can recover these files to the last change time.

Currently, the **Continuous data protection** functionality is supported for the following operating systems:

- Windows 7 and later
- Windows Server 2008 R2 and later

The supported file system: NTFS only, local folders only (shared folders are not supported).

The **Continuous data protection** option is not compatible with the **Application backup** option.

---

## Note

The features vary between different editions. Some of the features described in this documentation may be unavailable with your license. For detailed information about the features included in each edition, refer to [Acronis Cyber Protect 15 Editions Comparison including Cloud deployment](#).

---

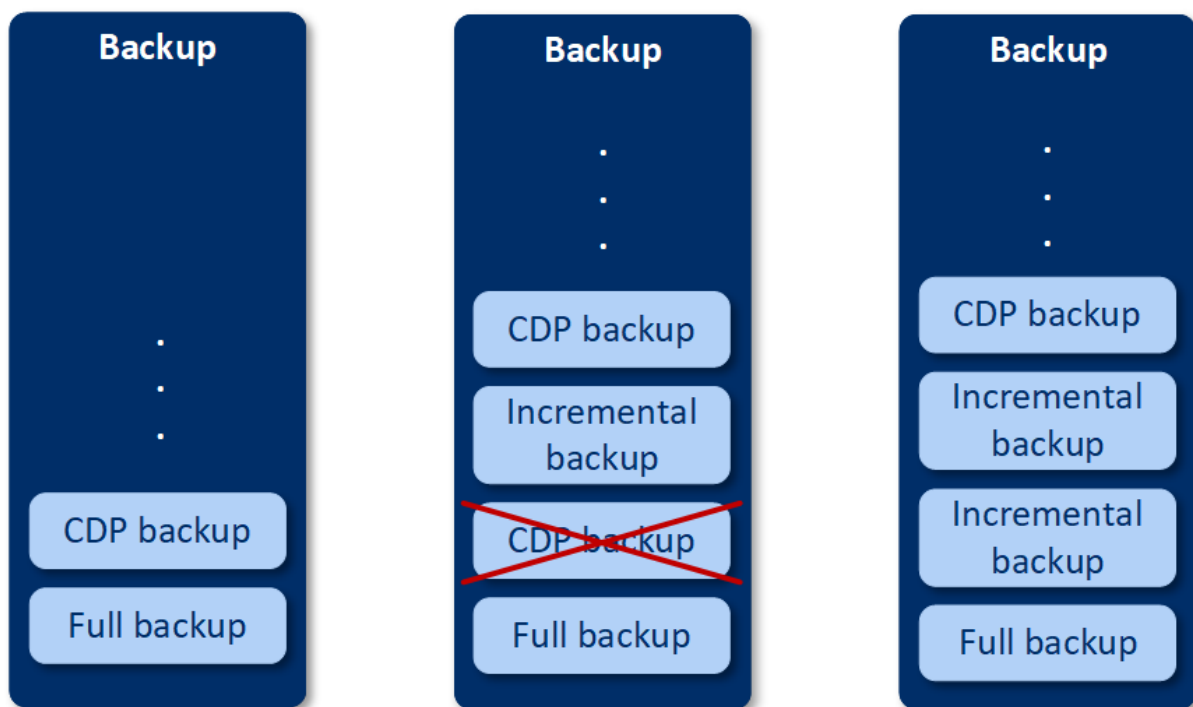
## How it works

Let's call the backup that is created on continuous basis the CDP backup. For the CDP backup to be created, a full backup or incremental backup has to be created preliminarily.

When you first run the protection plan with the Backup module and **Continuous data protection** enabled, a full backup is created first. Right after that the CDP backup for the selected or changed files/folders will be created. The CDP backup always contains data selected by you in the latest state. When you make changes to the selected files/folders, no new CDP backup is created, all changes are recorded to the same CDP backup.

When the time comes for a scheduled incremental backup, the CDP backup is dropped, and a new CDP backup is created after the incremental backup is done.

Thus, the CDP backup always stays as the latest backup in the backup chain having the latest actual state of the protected files/folders.



If you already have a protection plan with the Backup module enabled and you decided to enable **Continuous data protection**, then the CDP backup will be created right after enabling the option as the backup chain already has full backups.

## Supported data sources and destinations for continuous data protection

For continuous data protection proper work, you need to specify the following items for the following data sources:

What to back up	Items to back up
Entire machine	Either files/folders or applications must be specified
Disks/volumes	Disks/volumes and either files/folders or applications must be specified
Files/folders	Files/folders must be specified Applications can be specified (not mandatory)

The following backup destinations are supported for continuous data protection:

- Local folder
- Network folder
- Location defined by a script
- Cloud storage
- Acronis Cyber Infrastructure

### ***To protect the devices with continuous data protection***

1. In the Cyber Protect web console, create a protection plan with the **Backup** module enabled.
2. Enable the **Continuous data protection (CDP)** option.
3. Specify **Items to protect continuously**:
  - **Applications** (any file modified by the selected applications will be backed up). We recommend to use this option to protect your Office documents with the CDP backup.

Items to protect continuously

Choose files for continuous protection out of the data selected for backup. The software will back up every change of these files. You will be able to revert these files to the last change time.

Applications

Files/folders

Every file modified by the selected applications will be backed-up

Predefined application categories

☒ Office documents

☒ Engineering

☒ Imaging and video

Other applications

To add more applications, specify their paths in the format: C:\Program Files\Microsoft Office\Office16\WINWORD.EXE or \*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Add applications

OK

Cancel

- You can select the applications from the predefined categories or specify other applications by defining the path to the application executable file. Use one of the following formats:  
C:\Program Files\Microsoft Office\Office16\WINWORD.EXE

OR

\*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

- **Files/folders** (any file modified in the specified location(s) will be backed up). We recommend to use this option to protect those files and folders that are constantly changing.

Items to protect continuously

Choose files for continuous protection out of the data selected for backup. The software will back up every change of these files. You will be able to revert these files to the last change time.

Applications

Files/folders

Every change of the selected files, and of files in the selected folders, will be backed up.

Machine to browse from: WIN-JET0MF9HSFR

Select files and folders

Add files/folders

OK

Cancel

1. **Machine to browse from** – specify the machine whose files/folders you want to select for continuous data protection.

Click **Select files and folders** to select files/folders on the specified machine.

240

© Acronis International GmbH, 2003-2024



---

**Important**

If you manually specify a whole folder whose files will be continuously backed up, use the mask, for example:

Correct path: D:\Data\\*

Incorrect path: D:\Data\  

---

In the text field, you can also specify rules for selecting files/folders that will be backed up. For more details how to define rules, refer to "[Selecting files/folders](#)". When ready, click **Done**.

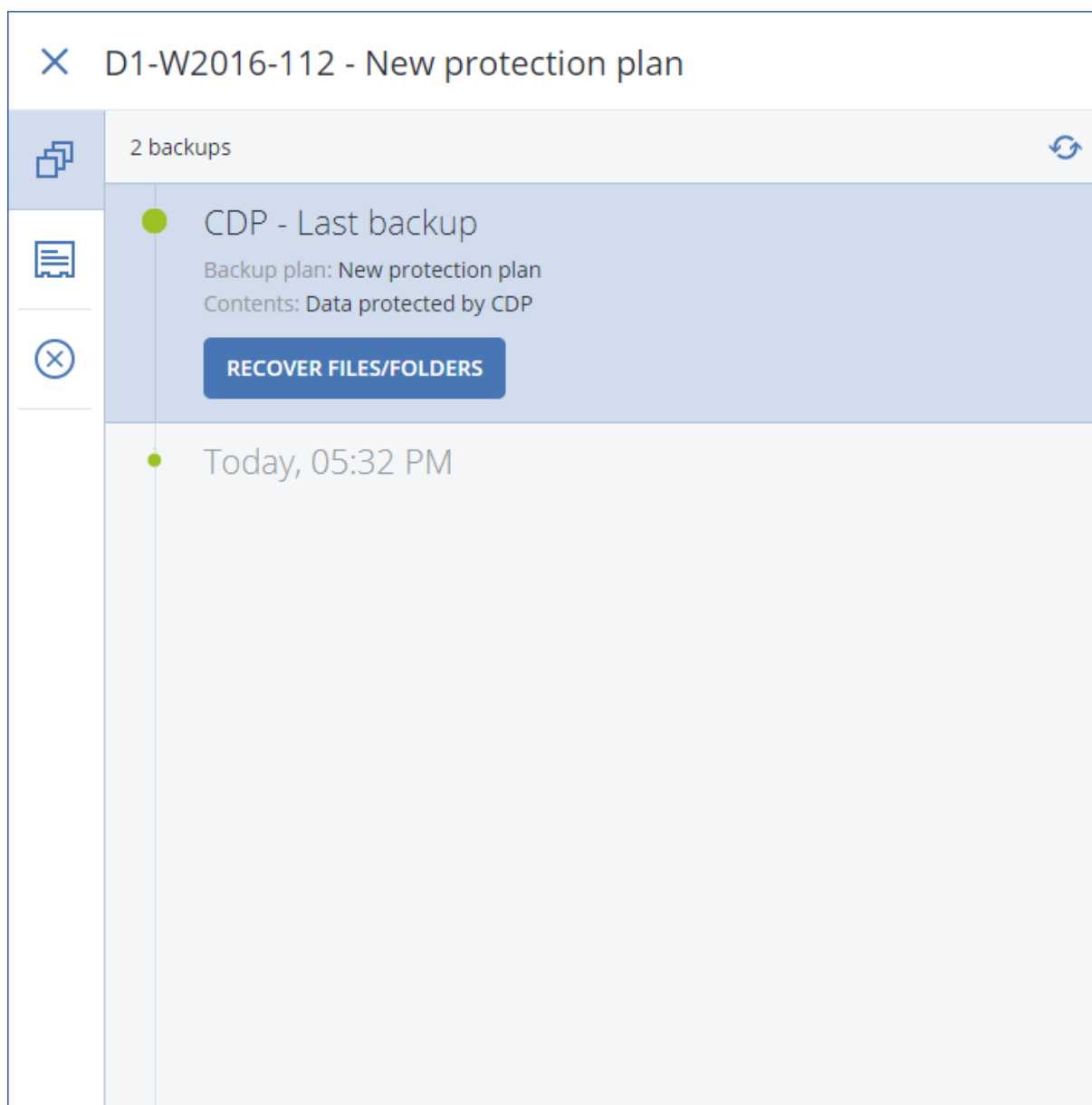
2. Click **Create**.

As a result, the protection plan with continuous data protection enabled will be assigned to the selected machine. After the first regular backup, the backups with the latest copy of the protected by CDP data will be created on the continuous basis. Both, the data defined via Applications and Files/folders, will be backed up.

Continuously backed-up data are retained according to the retention policy defined for the Backup module.

## How to distinguish backups that are protected on continuous basis

The backups that are backed up on continuous basis have the CDP prefix.



## How to recover your entire machine to the latest state

If you want to be able to recover an entire machine to the latest state, you can use the **Continuous data protection (CDP)** option in the Backup module of a protection plan.

You can recover either an entire machine or files/folders from a CDP backup. In first case, you will get an entire machine in the latest state, in the second case – files/folders in the latest state.

## Selecting a destination

---

### Important

Some of the features described in this section are only available for on-premises deployments.

---

### *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

- **Cloud storage**

Backups will be stored in the cloud data center.

- **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. You can change these credentials at any time by clicking the key icon next to the folder name.

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

- **Acronis Cyber Infrastructure**

Acronis Cyber Infrastructure can be used as highly reliable software-defined storage with data redundancy and automatic self-healing. The storage can be configured as a gateway for storing backups in Microsoft Azure or in one of a variety of storage solutions compatible with S3 or Swift. The storage can also employ the NFS back-end. For more information, refer to "[About Acronis Cyber Infrastructure](#)".

---

### Important

Backup to Acronis Cyber Infrastructure is not available for macOS machines.

---

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

Verify that the nfs-utils package is installed on the Linux machine where Agent for Linux is installed.

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"](#).

- **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

- **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 protection 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 **Backup storage** 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.

Examples:

- 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);
```

- The following **JScript** script outputs the backup location in a folder on the machine where the script runs:

```
WScript.Echo("C:\\Backup");
```

---

**Note**

The location path in these scripts is case-sensitive. Therefore, C:\Backup and C:\backup are displayed as different locations in the Cyber Protect web console. Also, use upper case for the drive letter.

---

- The following **VBScript** 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**.

- **Storage node**

A storage node is a server designed to optimize the usage of various resources (such as the corporate storage capacity, the network bandwidth, and the production servers' CPU load) that are required to protect enterprise data. This goal is achieved by organizing and managing the locations that serve as dedicated storages of the enterprise backups (managed locations).

You can select a previously created location or create a new one by clicking **Add location > Storage node**. For information about the settings, refer to ["Adding a managed location"](#).

You may be prompted to specify the user name and password for the storage node. Members of the following Windows groups on the machine where a storage node is installed have access to all managed locations on the storage node:

- **Administrators**
- **Acronis ASN Remote Users**

This group is created automatically when the storage node is installed. By default, this group is empty. You can add users to this group manually.

- **Tape**

If a tape device is attached to the backed-up machine or to a storage node, 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"](#).

## 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.

## 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**.

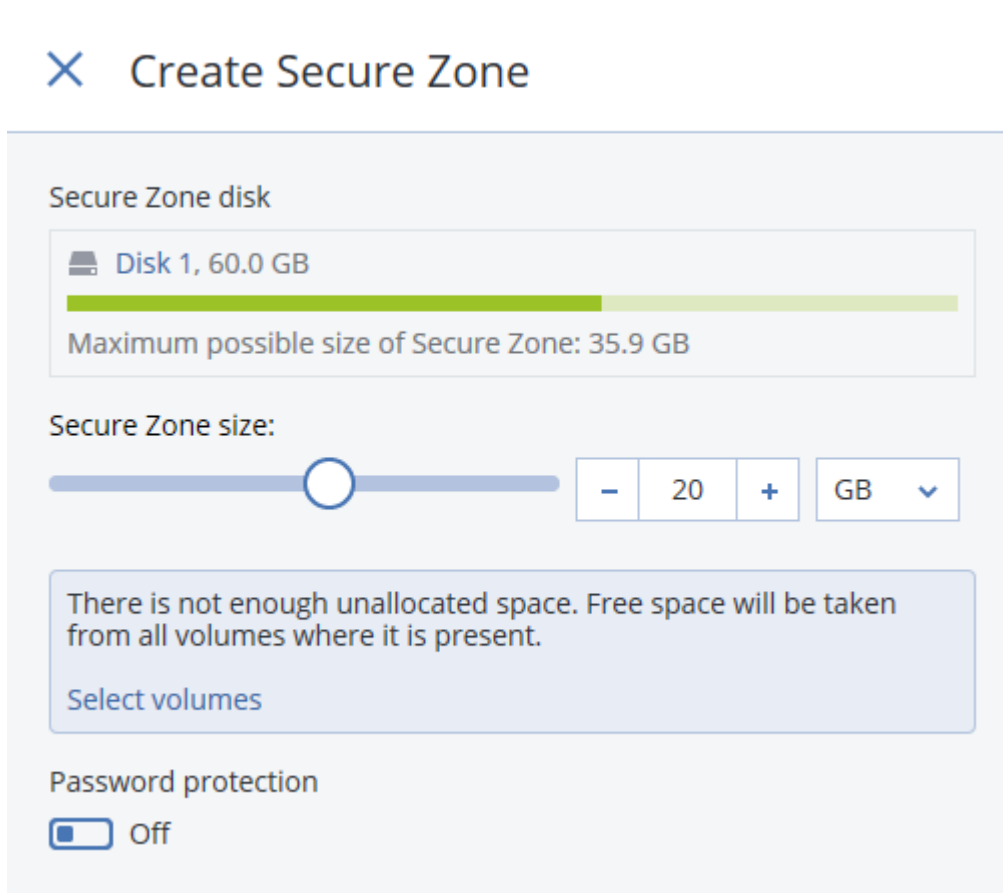
3. Under **Secure Zone disk**, click **Select**, and then select a hard disk (if several) on which to create the zone.

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 is 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 protection 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.

## About Acronis Cyber Infrastructure

Acronis Cyber Protect 15 supports integration with Acronis Cyber Infrastructure 3.5 Update 5 or later.

Backup to Acronis Cyber Infrastructure is not available for macOS machines.

## Deployment

In order to use Acronis Cyber Infrastructure, deploy it on bare metal on your premises. At least five physical servers are recommended to take full advantage of the product. If you only need the gateway functionality, you can use one physical or virtual server, or configure a gateway cluster with as many servers as you want.

Ensure that the time settings are synchronized between the management server and Acronis Cyber Infrastructure. The time settings for Acronis Cyber Infrastructure can be configured during deployment. Time synchronization via Network Time Protocol (NTP) is enabled by default.

You can deploy several instances of Acronis Cyber Infrastructure and register them on the same management server.

## Registration

The registration is performed in the Acronis Cyber Infrastructure web interface. Acronis Cyber Infrastructure can be registered only by organization administrators and only in the organization. Once registered, the storage becomes available to all of the organization units. It can be added as a backup location to any unit or to the organization.

The reverse operation (deregistration) is performed in the Acronis Cyber Protect interface. Click **Settings > Storage nodes**, click the required Acronis Cyber Infrastructure, and then click **Delete**.



## Adding a backup location

Only one backup location on each Acronis Cyber Infrastructure instance can be added to a unit or organization. A location added at a unit level is available to this unit and to the organization administrators. A location added at the organization level is available only to the organization administrators.

When adding a location, you create and enter its name. Should you need to add an existing location to a new or different management server, select the **Use an existing location...** check box, click **Browse**, and then select the location from the list.

If several instances of Acronis Cyber Infrastructure are registered on the management server, it is possible to select an Cyber Infrastructure instance when adding a location.

## Backup schemes, operations, and limitations

Direct access to Acronis Cyber Infrastructure from bootable media is not available. To work with Acronis Cyber Infrastructure, [register the media on the management server](#) and manage it via the Cyber Protect web console.

Access to Acronis Cyber Infrastructure via the command-line interface is not available.

In terms of available backup schemes and operations with backups, Acronis Cyber Infrastructure is similar to the cloud storage. The only difference is that backups can be replicated *from* Acronis Cyber Infrastructure during execution of a protection plan.

## Documentation

The full set of the Acronis Cyber Infrastructure documentation is available on the [Acronis web site](#).

## Schedule

---

### Important

Some of the features described in this section are only available for on-premises deployments.

---

The schedule employs the time settings (including the time zone) of the operating system where the agent installed. The time zone of Agent for VMware (Virtual Appliance) can be configured [in the agent's interface](#).

For example, if a protection plan is scheduled to run at 21:00 and applied to several machines located in different time zones, the backup will start on each machine at 21:00 local time.

The scheduling parameters depend on the backup destination.

## When backing up to cloud storage

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.

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, see "Schedule by events" (p. 252).

---

### Important

The first backup is full, which means that it is the most time-consuming. All subsequent backups are incremental and take significantly less time.

---

## When backing up to other locations

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

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

- **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<sup>1</sup>.

This scheme is not available when backing up to a tape device or an SFTP server.

- **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.

---

<sup>1</sup>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.

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 protection plan panel.

- **Custom**

Specify schedules for full, differential, and incremental backups.

Differential backup is not available when backing up SQL data, Exchange data, or system state.

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, see "Schedule by events" (p. 252).

## 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, see "Start conditions" (p. 255).
- 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. For more information, see "Scheduling" (p. 309).

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 protection plan is applied to the machine and remains the same until you edit the protection plan and change the maximum delay value.

---

### Note

In cloud deployments, this option is enabled by default, with the maximum delay set to 30 minutes. In on-premises deployments, by default all backups start exactly as scheduled.

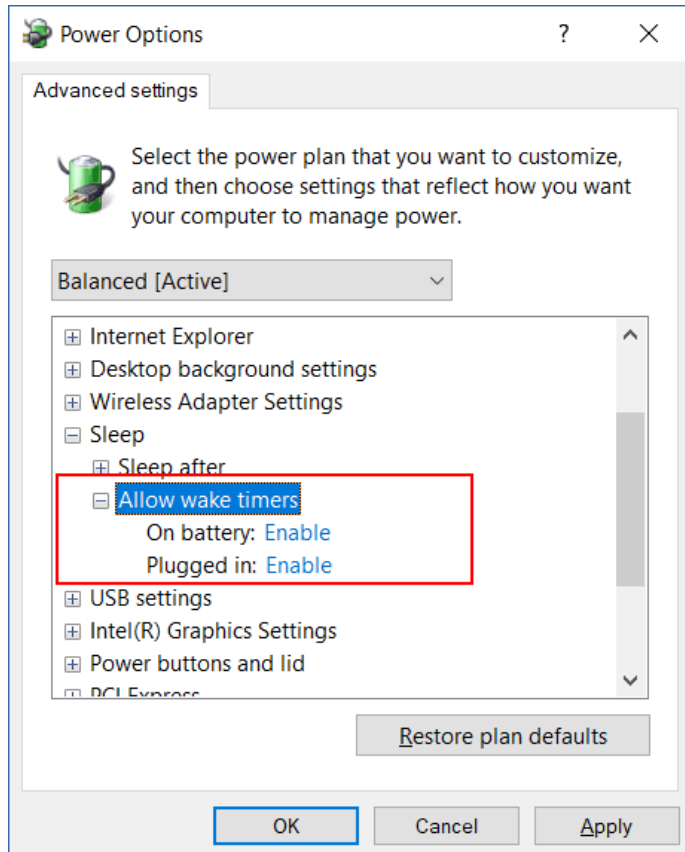
---

- [Only available with the Schedule by time option] 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 applicable only to machines running Windows that have the **Allow wake timers** setting enabled in their power plans.



This option does not use the Wake-on-LAN functionality and is not applicable to powered off machines.

## Schedule by events

When setting up a schedule for a protection 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 protection plan. You can specify the length of time.

---

### Note

Because the schedule is based on a successful backup event, if a backup fails, the scheduler will not run the job again until an operator runs the plan manually and the run completes successfully.

---

- **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](#).

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

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, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Disks/volumes (virtual machines)	Windows, Linux	-	-	-	-	-
ESXi configuration	Windows, Linux	-	-	-	-	-
Microsoft 365 mailboxes	Windows	-	-	-	-	Windows
Exchange databases and mailboxes	Windows	-	-	-	-	Windows
SQL databases	Windows	-	-	-	-	Windows

## 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 protection 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 protection 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.

## 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 protection plan.

The scheduler behavior, in case the condition (or any of multiple conditions) is not met, is defined by the [Backup start conditions](#) 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, Linux, and macOS.

WHAT TO BACK UP	Disks/volumes or files (physical machines)	Disks/volumes (virtual machines)	ESXi configuration	Microsoft 365 mailboxes	Exchange databases and mailboxes	SQL databases
User is idle	Windows	–	–	–	–	–
The backup location's host is available	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Users logged off	Windows	–	–	–	–	–
Fits the time	Windows, Linux,	Windows, Linux	–	–	–	–

interval	macOS					
Save battery power	Windows	-	-	-	-	-
Do not start when on metered connection	Windows	-	-	-	-	-
Do not start when connected to the following Wi-Fi networks	Windows	-	-	-	-	-
Check device IP address	Windows	-	-	-	-	-

## 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.



## 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 is effective for network folders, the cloud storage, and locations managed by a storage node.

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.

## 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.

## 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.

## 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](#) 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.

## 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.

## 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.

## 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.

## Retention rules

---

### Important

Some of the features described in this section are only available for on-premises deployments.

---

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 protection plan. By default, the retention rules are specified for each backup set<sup>1</sup> 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**

---

<sup>1</sup>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.

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 protection plan is kept in all cases, unless you configure a retention rule to clean up backups before starting a new backup operation and set the number of backups to keep to zero.

---

### Warning!

If you delete the only backup that you have by applying the retention rules in this way, then if the backup fails you will not have a backup with which to restore data because there will be no available backup to use.

---

- 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](#)" backup option.
- Retention rules are a part of a protection plan. They stop working for a machine's backups as soon as the protection 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](#)".

## Encryption

We recommend that you encrypt all backups that are stored in the cloud storage, especially if your company is subject to regulatory compliance.

---

### Important

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

---

## Encryption in a protection plan

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

### *To specify the encryption settings in a protection plan*

1. On the protection 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 protection 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 protection plans in the following way:

- **Protection plans that are already applied to the machine.** If the encryption settings in a protection plan are different, the backups will fail.
- **Protection plans that will be applied to the machine later.** The encryption settings saved on a machine will override the encryption settings in a protection plan. Any backup will be encrypted, even if encryption is disabled in the protection 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 protection 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 protection agent installation path. By default, it is **%ProgramFiles%\BackupClient** in cloud deployments and **%ProgramFiles%\Acronis** in on-premises deployments.

- 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 protection agent installation path. By default, it is **%ProgramFiles%\BackupClient** in cloud deployments and **%ProgramFiles%\Acronis** in on-premises deployments.

- In Linux: `/usr/sbin/acropsh -m manage_creds --reset`

### ***To change the encryption settings by using Cyber Protect Monitor***

1. Log on as an administrator in Windows or macOS.
2. Click the **Cyber Protect Monitor** icon in the notification area (in Windows) or the menu bar (in macOS).
3. Click the gear icon.
4. Click **Encryption**.
5. Do one of the following:
  - Select **Set a specific password for this machine**. Specify and confirm the encryption password.
  - Select **Use encryption settings specified in the protection plan**.
6. Click **OK**.

## 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.

## Notarization

Notarization enables you to prove that a file is authentic and unchanged since it was backed up. We recommend that you enable notarization when backing up your legal document files or other files



that require proved authenticity.

Notarization is available only for file-level backups. Files that have a digital signature are skipped, because they do not need to be notarized.

Notarization is *not* available:

- If the backup format is set to **Version 11**
- If the backup destination is Secure Zone
- If the backup destination is a managed location with enabled deduplication or encryption

## How to use notarization

To enable notarization of all files selected for backup (except for the files that have a digital signature), enable the **Notarization** switch when creating a protection plan.

When configuring recovery, the notarized files will be marked with a special icon, and you can [verify the file authenticity](#).

## How it works

During a backup, the agent calculates the hash codes of the backed-up files, builds a hash tree (based on the folder structure), saves the tree in the backup, and then sends the hash tree root to the notary service. The notary service saves the hash tree root in the Ethereum blockchain database to ensure that this value does not change.

When verifying the file authenticity, the agent calculates the hash of the file, and then compares it with the hash that is stored in the hash tree inside the backup. If these hashes do not match, the file is considered not authentic. Otherwise, the file authenticity is guaranteed by the hash tree.

To verify that the hash tree itself was not compromised, the agent sends the hash tree root to the notary service. The notary service compares it with the one stored in the blockchain database. If the hashes match, the selected file is guaranteed to be authentic. Otherwise, the software displays a message that the file is not authentic.

## Conversion to a virtual machine

---

### Important

Some of the features described in this section are only available for on-premises deployments.

---

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 protection plan**

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**

This method enables you to specify a separate conversion schedule.

- **Recovery to a new virtual machine**

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](#).

## What you need to know about conversion

### 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, Hyper-V, or Scale Computing HC3, you need an ESXi, Hyper-V, or Scale Computing HC3 host respectively and a protection agent (Agent for VMware, Agent for Hyper-V, or Agent for Scale Computing HC3) 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	Agent for Mac	Agent for Scale Computing HC3
VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–
VMware Workstation	+	+	+	+	–	–
VHDX files	+	+	+	+	–	–
Scale	–	–	–	–	–	+

Computing HC3						
------------------	--	--	--	--	--	--

## 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](#).
- Backups stored in Secure Zone can be converted only by the agent running on the same machine.
- Backups can be converted to Scale Computing HC3 virtual machine only in a [separate conversion plan](#).
- Backups that contain Linux logical volumes (LVM) can be converted only if they were created by Agent for VMware, Agent for Hyper-V, and Agent for Scale Computing HC3 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.

## Conversion to a virtual machine in a protection plan

You can configure the conversion to a virtual machine from any backup or replication location that is present in a protection 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"](#).

***To set up a conversion to a virtual machine in a protection plan***

1. Decide from which backup location you want to perform the conversion.
2. On the protection 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**.

## How regular conversion to VM works

The way the regular 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.

## Replication

---

### Important

Some of the features described in this section are only available for on-premises deployments.

---

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

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).

- **Using the cloud storage to protect data from a natural disaster**

Replicate the backups to the cloud storage by transferring only the data changes.

- **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
- Locations managed by a storage node

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

- A local folder
- A network folder
- The cloud storage
- An SFTP server
- Locations managed by a storage node
- A tape device

### ***To enable replication of backups***

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

The **Add location** control is available only if replication is supported *from* the last selected backup or replication 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](#)".
4. [Optional] In **Convert to VM**, specify the settings for conversion to a virtual machine, as described in "[Conversion to a virtual machine](#)".
5. [Optional] Click the gear icon > **Performance and backup window**, and then set the backup window for the chosen location, as described in "[Performance and backup window](#)". These settings will define the replication performance.

6. [Optional] Repeat steps 1-5 for all locations where you want to replicate the backups. Up to five consecutive locations are supported, including the primary one.

---

### Important

If you enable backup and replication in the same protection plan, ensure that the replication completes before the next scheduled backup. If the replication is still in progress, the scheduled backup will not start. For example, a scheduled backup that runs once every 24 hours will not start if the replication takes 26 hours to complete.

To avoid this dependency, use a separate plan for backup replication. For more information about this specific plan, refer to "Backup replication" (p. 356).

---

## Considerations for users with the Advanced license

### Tip

You can set up replication of backups *from* the cloud storage by creating a separate replication plan. For more information, refer to ["Off-host data processing"](#).

### Restrictions

- Replicating backups *from* a location managed by a storage node to a local folder is not supported. A local folder means a folder on the machine with the agent that created the backup.
- Replicating backups *to* a managed location with enabled deduplication is not supported for backups that have the **Version 12 backup format**.

### Which machine performs the operation?

Replicating a backup *from* any location is initiated by the agent that created the backup and is performed:

- By that agent, if the location *is not* managed by a storage node.
- By the corresponding storage node, if the location is managed. However, replication of a backup from the managed location to the cloud storage is performed by the agent that created the backup.

As follows from the above description, the operation will be performed only if the machine with the agent is powered on.

### Replicating backups between managed locations

Replicating a backup from one managed location to another managed location is performed by the storage node.

If deduplication is enabled for the target location (possibly on a different storage node), the source storage node sends only those blocks of data that are not present in the target location. In other

words, like an agent, the storage node performs deduplication at the source. This saves network traffic when you replicate data between geographically separated storage nodes.

## Starting a backup manually

1. Select a machine that has at least one applied protection plan.
2. Click **Backup**.
3. If more than one protection plans are applied, select the protection plan.
4. Do one of the following:
  - Click **Run now**. An incremental backup will be created.
  - If the backup scheme includes several backup methods, you can choose the method to use. Click the arrow on the **Run now** button, and then select **Full**, **Incremental**, or **Differential**.

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

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

## Backup options

### Important

Some of the features described in this section are only available for on-premises deployments.

To modify the backup options, click the gear icon next to the protection 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, macOS).
- The type of the data being backed up (disks, files, virtual machines, application data).
- The backup destination (the cloud storage, local or network folder).

The following table summarizes the availability of the backup options.

	Disk-level backup			File-level backup			Virtual machines			SQL and Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Scale Computing	Windows
Alerts	+	+	+	+	+	+	+	+	+	+



Backup consolidation	+	+	+	+	+	+	+	+	+	-
Backup file name	+	+	+	+	+	+	+	+	+	+
Backup format	+	+	+	+	+	+	+	+	+	+
Backup validation	+	+	+	+	+	+	+	+	+	+
Changed block tracking (CBT)	+	-	-	-	-	-	+	+	+	+
Cluster backup mode	-	-	-	-	-	-	-	-	-	+
Compression level	+	+	+	+	+	+	+	+	+	+
Email notifications	+	+	+	+	+	+	+	+	+	+
Error handling										
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										
File filters	+	+	+	+	+	+	+	+	+	-
File-level backup snapshot	-	-	-	+	+	+	-	-	-	-
Log truncation	-	-	-	-	-	-	+	+	-	SQL only
LVM snapshotting	-	+	-	-	-	-	-	-	-	-
Mount points	-	-	-	+	-	-	-	-	-	-
Multi-volume snapshot	+	+	-	+	+	-	-	-	-	-
Performance and backup window	+	+	+	+	+	+	+	+	+	+
Physical Data Shipping	+	+	+	+	+	+	+	+	+	-
Pre/Post commands	+	+	+	+	+	+	+	+	+	+
Pre/Post data capture commands	+	+	+	+	+	+	+	-	-	+
SAN hardware snapshots	-	-	-	-	-	-	+	-	-	-
Scheduling										
Distribute start times within a time window	+	+	+	+	+	+	+	+	+	+
Limit the number of simultaneously running	-	-	-	-	-	-	+	+	+	-

backups										
Sector-by-sector backup	+	+	-	-	-	-	+	+	+	-
Splitting	+	+	+	+	+	+	+	+	+	+
Tape management	+	+	+	+	+	+	+	+	+	+
Task failure handling	+	+	+	+	+	+	+	+	+	+
Task start conditions	+	+	-	+	+	-	+	+	+	+
Volume Shadow Copy Service (VSS)	+	-	-	+	-	-	-	+	-	+
Volume Shadow Copy Service (VSS) for virtual machines	-	-	-	-	-	-	+	+	+	-
Weekly backup	+	+	+	+	+	+	+	+	+	+
Windows event log	+	-	-	+	-	-	+	+	+	+

## 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 protection 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.

## 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 or the cloud storage.
- The backup scheme is set to **Always incremental (single-file)**.
- The [backup format](#) is set to **Version 12**.

Backups stored on tapes cannot be consolidated. Backups stored in the cloud storage, as well as 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.

## Backup file name

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

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

## What is a backup file?

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

	Always incremental (single-file)	Other backup schemes
<b>Version 11</b> backup format	One TIB file and one XML metadata file	Multiple TIB files and one XML metadata file (traditional format)
<b>Version 12</b> 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 protection plan.

---

### Note

Timestamp is added to the backup file name only in the version 11 backup format.

---

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 protection plan schedule.

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

## Where can I see backup file names?

Select the **Backup storage** 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 **Backup storage** 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

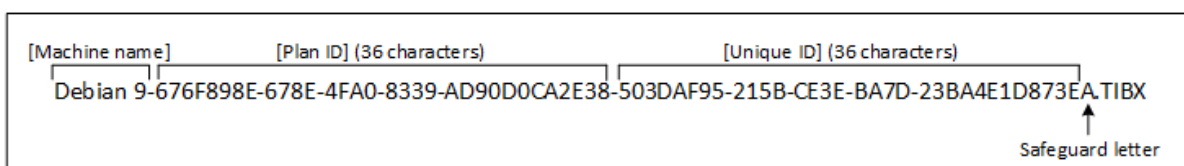
The default backup file name is [Machine Name]-[Plan ID]-[Unique ID]A.

The default backup file name for mailbox backup is [Mailbox ID]\_mailbox\_[Plan ID]A.

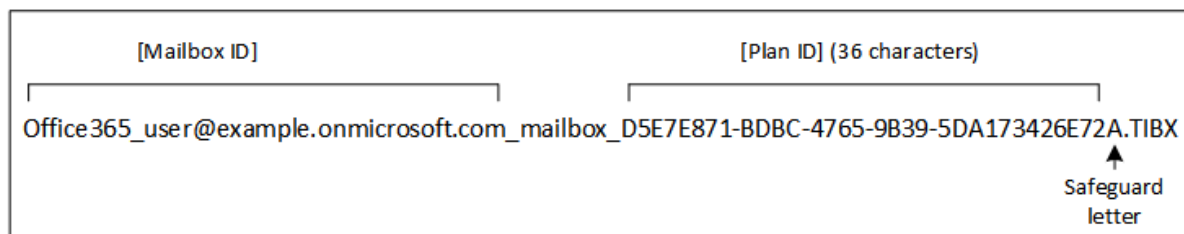
The name consists of the following variables:

- [Machine Name] This variable is replaced with the name of the machine (the same name that is shown in the Cyber Protect web console) for all types of backed up data, except for Microsoft 365 mailboxes. For Microsoft 365 mailboxes, it is replaced with the mailbox user's principal name (UPN).
- [Plan ID] This variable is replaced with a unique identifier of a protection 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 protection 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 Cyber Protect 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 protection plan is applied to a single machine, and you have to remove this machine from the Cyber Protect web 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 protection plan to continue backing up to the same backup or backup sequence. To do this, in the backup options of the protection plan, click **Backup file name**, and then click **Select** to select the desired backup.

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

File name template

[Machine Name]-[Plan ID]-[Unique ID]A SELECT

If the file name template is changed, the next backup will be a full backup.

The following variables can be used:

- [Machine Name]
- [Plan ID]
- [Plan name]
- [Unique ID]

- **Upgrade from previous product versions**

If during the upgrade a protection plan did not migrate automatically, recreate the plan and point it to the old backup file. If only one machine is selected for backup, click **Browse**, and then select the required backup. If multiple machines are selected for backup, re-create the old backup file name by using variables.

---

**Note**

The **Select** button is only available for protection plans that are created for and applied to a single device.

---

## Backup format

This option defines the format of the backups created by the protection plan. It is only available for protection plans that use the legacy backup format version 11. In this case, you can change it to the new format version 12. After this change, the option becomes inaccessible.

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 protection 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 preserved for backward compatibility. It allows you to append 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.

This format is automatically selected if the backup destination (or replication destination) is a managed location with enabled deduplication, or a managed location with enabled encryption. If you change the format to **Version 12**, the backups will fail.

---

**Note**

You cannot back up Database Availability Groups (DAG) by using the backup format version 11. Backing up of DAG is supported only in the version 12 format.

---

## 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](#) option. The following table lists the files that can be created per machine or mailbox.

	Always incremental (single-file)	Other backup schemes
<b>Version 11</b> backup format	One TIB file and one XML metadata file	Multiple TIB files and one XML metadata file (traditional format)
<b>Version 12</b> backup format	One TIBX file per backup chain (a full or differential backup, and all incremental backups that depend on it)	

## Changing the backup format to version 12 (TIBX)

If you change the backup format from version 11 (TIB format) to version 12 (TIBX format):

- The next backup will be full.
- In backup locations that can be browsed with a file manager (such as local or network folders), a new TIBX file will be created. The new file will have the name of the original file, appended with the **\_v12A** suffix.
- Retention rules and replication will be applied only to the new backups.
- The old backups will not be deleted and will remain available on the **Backup storage** tab. You can delete them manually.
- The old cloud backups will not consume the **Cloud storage** quota.
- The old local backups will consume the **Local backup** quota until you delete them manually.
- If your backup destination (or replication destination) is a managed location with enabled deduplication, the backups will fail.

## In-archive deduplication

The version 12 format supports in-archive deduplication.

In-archive deduplication uses client-side deduplication and brings the following advantages:

- Significantly reduced backup size, with built-in block-level deduplication for any type of data
- Efficient handling of hard links ensures that there are no storage duplicates
- Hash-based chunking

---

**Note**

In-archive deduplication is enabled by default for all backups in the TIBX format. You do not have to enable it in the backup options, and you cannot disable it.

---

## 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 protection plan is validated immediately after creation. This operation is performed by the protection agent.

The preset is: **Disabled**.

Validation calculates a checksum for every data block that can be recovered from the backup. The only exception is validation of file-level backups that are located in the cloud storage. These backups are validated by checking consistency of the metadata 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.

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](#) in the ESXi or Hyper-V environment.

## 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.

## Cluster backup mode

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 \(AAG\)"](#).

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 \(DAG\)"](#).

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.

## 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.

## Email notifications

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

This option is available only in on-premises deployments. In cloud deployments, the settings are configured per account when an account is created.

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"](#).

---

### Important

When the system settings are changed, all protection plans that use the system settings are affected.

---

Before enabling this option, ensure that the **Email server** settings are configured.

### ***To customize email notifications for a protection plan***

1. Select **Customize the settings for this protection 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.

## 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.

### Cloud storage

If the cloud storage is selected as a backup destination, the option value is automatically set to **Enabled. Number of attempts: 300. Interval between attempts: 30 seconds.**

In this case, the actual number of attempts is unlimited, but the timeout before the backup failure is calculated as follows: (300 seconds + **Interval between attempts**) \* (**Number of attempts** + 1).

Examples:

- With the default values, the backup will fail after  $(300 \text{ seconds} + 30 \text{ seconds}) * (300 + 1) = 99330$  seconds, or ~27.6 hours.
- If you set **Number of attempts** to 1 and **Interval between attempts** to 1 second, the backup will fail after  $(300 \text{ seconds} + 1 \text{ second}) * (1 + 1) = 602$  seconds, or ~10 minutes.

If the calculated timeout exceeds 30 minutes, and the data transfer has not started yet, the actual timeout is set to 30 minutes.

## 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.

## 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.

## File filters

By using file filters, you can include only specific files and folders in a backup, or exclude specific files and folders from a backup.

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

File filters are not effective when applied to dynamic disks (LVM or LDM volumes) of a virtual machine that is backed up by Agent for VMware, Agent for Hyper-V, or Agent for Scale Computing in the agentless mode.

### ***To enable file filters***

1. In a protection plan, expand the **Backup** module.
2. In **Backup options**, click **Change**.
3. Select **File filters**.
4. Use any of the options described below.

## Include or 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** and the backup destination is NOT cloud storage.

---

- **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 or macOS).

Both in Windows and Linux/macOS, 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**).

---

### Important

If the operating system of the backed-up machine is not detected correctly during a disk-level backup, full path file filters will not work. For an exclusion filter, a warning will be shown. If there is an inclusion filter, the backup will fail.

A full path filter includes the drive letter (in Windows) or the root directory (in Linux or macOS). For example, a file full path could be **C:\Temp\File.tmp**. A filter that includes the drive letter or the root directory—for example **C:\Temp\File.tmp** or **C:\Temp\\***—will result in warning or failure.

A filter that does not use the drive letter or the root directory (for example, **Temp\\*** or **Temp\File.tmp**) or a filter that starts with an asterisk (for example, **\*C:\**) will not result in warning or failure. However, if the operating system of the backed-up machine is not detected correctly, these filters will not work, either.

---

- **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**

[Only for backups in the **Version 12** format] 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.



---

**Note**

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.

---

## 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.

## Forensic data

Malicious activities on a machine can be carried out by viruses, malware, and ransomware. The other case that may require investigations is stealing or changing data on a machine by means of different programs. Such activities may need to be investigated but it is possible only if you keep digital evidence on a machine to investigate. Unfortunately, evidence (files, traces, and so on) may be deleted or a machine may become unavailable.

The backup option called **Forensic data** allows you to collect digital evidence that can be used in forensic investigations. The following items can be used as digital evidence: a snapshot of the unused disk space, memory dumps, and a snapshot of running processes. The **Forensic data** functionality is available only for an entire machine backup.

Currently, the **Forensic data** option is available only for Windows machines with the following OS versions:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

---

**Note**

- After a protection plan with the Backup module is applied to a machine, the forensic data settings cannot be modified. To use different forensic data settings, create a new protection plan.
  - Backups with forensic data collection are not supported for machines that are connected to your network through VPN and do not have direct access to the Internet.
- 

The supported locations for backups with forensic data are:

- Cloud storage
- Local folder

---

**Note**

1. The local folder is supported only on an external hard disk connected via USB.
  2. Local dynamic disks are not supported as a location for forensic backups.
- 

- Network folder

Backups with forensic data are automatically notarized. Forensic backups allow investigators to analyze disk areas that are usually not included in a regular disk backup.

## Forensic backup process

The system performs the following during a forensic backup process:

1. Collects raw memory dump and the list of running processes.
2. Automatically reboots a machine into the bootable media.
3. Creates the backup that includes both the occupied and unallocated space.
4. Notarizes the backed-up disks.
5. Reboots into the live operating system and continues plan execution (for example, replication, retention, validation and other).

### ***To configure forensic data collection***

1. In the Cyber Protect web console, go to **Devices > All devices**. Alternatively, the protection plan can be created from the **Plans** tab.
2. Select the device and click **Protect**.
3. In the protection plan, enable the **Backup** module.
4. In **What to back up**, select **Entire machine**.
5. In **Backup options**, click **Change**.
6. Find the **Forensic data** option.
7. Enable **Collect forensic data**. The system will automatically collect a memory dump and create a snapshot of running processes.

---

**Note**

Full memory dump may contain sensitive data such as passwords.

---

8. Specify the location.
9. Click **Run Now** to perform a backup with forensic data right away or wait until the backup is created according to the schedule.
10. Go to **Dashboard > Activities**, verify that the backup with forensic data was successfully created.

As a result, backups will include forensic data and you will be able to get them and analyze. Backups with forensic data are marked and can be filtered among other backups in **Backup storage > Locations** by using the **Only with forensic data** option.

## How to get forensic data from a backup?

1. In the Cyber Protect web console, go to **Backup storage**, select the location with backups that include forensic data.
2. Select the backup with forensic data and click **Show backups**.
3. Click **Recover** for the backup with forensic data.
  - To get only the forensic data, click **Forensic data**.  
The system will show a folder with forensic data. Select a memory dump file or any other forensic file and click **Download**.
  - To recover a full forensic backup, click **Entire machine**. The system will recover the backup without the boot mode. Thus, it will be possible to check that the disk was not changed.

You can use the provided memory dump with several of third-party forensic software, for example, use Volatility Framework at <https://www.volatilityfoundation.org/> for further memory analysis.

## Notarization of backups with forensic data

To ensure that a backup with forensic data is exactly the image that was taken and it was not compromised, the Backup module provides the notarization of backups with forensic data.

### How it works

Notarization enables you to prove that a disk with forensic data is authentic and unchanged since it was backed up.

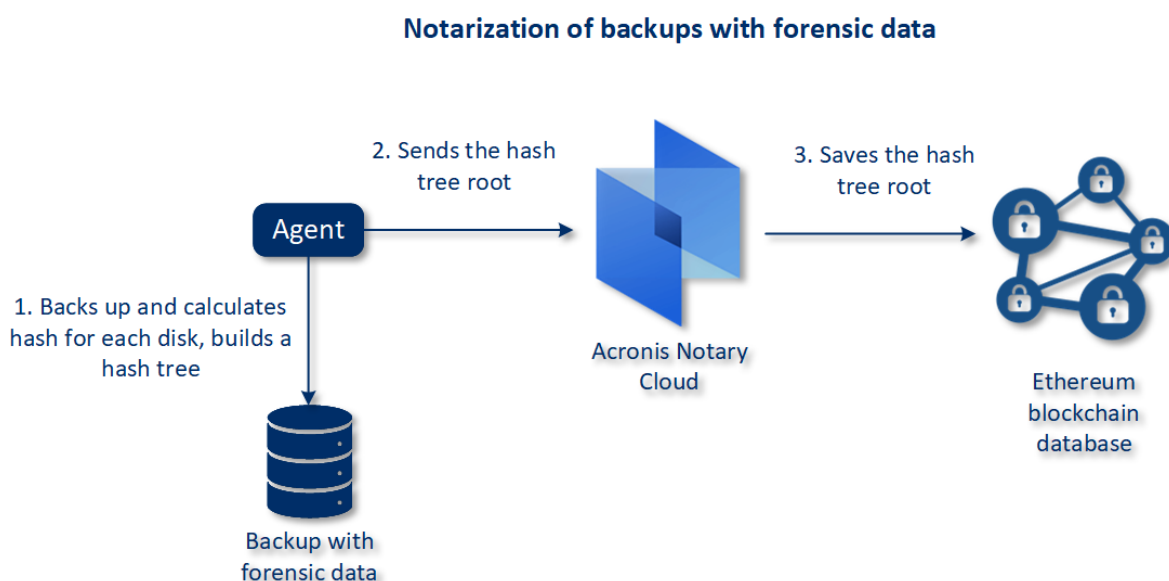
During a backup, the agent calculates the hash codes of the backed-up disks, builds a hash tree, saves the tree in the backup, and then sends the hash tree root to the notary service. The notary service saves the hash tree root in the Ethereum blockchain database to ensure that this value does not change.

When verifying the authenticity of the disk with forensic data, the agent calculates the hash of the disk, and then compares it with the hash that is stored in the hash tree inside the backup. If these

hashes do not match, the disk is considered not authentic. Otherwise, the disk authenticity is guaranteed by the hash tree.

To verify that the hash tree itself was not compromised, the agent sends the hash tree root to the notary service. The notary service compares it with the one stored in the blockchain database. If the hashes match, the selected disk is guaranteed to be authentic. Otherwise, the software displays a message that the disk is not authentic.

The scheme below shows shortly the notarization process for backups with forensic data.



To verify the notarized disk backup manually, you can get the certificate for it and follow the verification procedure shown with the certificate by using the [tibxread](#) tool.

## Getting the certificate for backups with forensic data

To get the certificate for a backup with forensic data from the console, do the following:

1. Go to **Backup storage** and select the backup with forensic data.
2. Recover the entire machine.
3. The system opens the **Disk Mapping** view.
4. Click the **Get certificate** icon for the disk.
5. The system will generate the certificate and open a new window in the browser with the certificate. Below the certificate you will see the instruction for manual verification of notarized disk backup.

## The tool "tibxread" for getting the backed-up data

Cyber Protect provides the tool, called `tibxread`, for manual check of the backed-up disk integrity. The tool allows you to get data from a backup and calculate hash of the specified disk. The tool is installed automatically with the following components: Agent for Windows, Agent for Linux, and Agent for Mac. It is located in: `C:\Program Files\Acronis\BackupAndRecovery`.

The supported locations are:

- The local disk
- The network folder (CIFS/SMB) that can be accessed without the credentials.

In case of a password-protected network folder, you can mount the network folder to the local folder by using the OS tools and then the local folder as the source for this tool.

- The cloud storage

You should provide the URL, port, and certificate. The URL and port can be obtained from the Windows registry key or configuration files on Linux/Mac machines.

For Windows:

```
HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
```

For Linux:

```
/etc/Acronis/BackupAndRecovery.config
```

For macOS:

```
/Library/Application Support/Acronis/Registry/BackupAndRecovery.config
```

The certificate can be found in the following locations:

For Windows:

```
%allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
```

For Linux:

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

For macOS:

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

The tool has the following commands:

- list backups
- list content
- get content
- calculate hash

## list backups

Lists recovery points in a backup.

### SYNOPSIS:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

## Options

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

### Output template:

```
GUID Date Date timestamp
---- -
<guid> <date> <timestamp>
```

<guid> – the backup GUID.

<date> – the creation date of the backup. Its format is: DD.MM.YYYY HH24:MM:SS. In local timezone by default (it can be changed by using the --utc option).

### Output example:

```
GUID Date Date timestamp
---- -
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

## list content

Lists content in a recovery point.

### SYNOPSIS:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

## Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

### Output template:

Disk	Size	Notarization status
-----	-----	-----
<number>	<size>	<notarization_status>

<number> – identifier of the disk.

<size> – size in bytes.

<notarization\_status> – the following statuses are possible: Without notarization, Notarized, Next backup.

#### Output example:

Disk	Size	Notary status
-----	-----	-----
1	123123465798	Notarized
2	123123465798	Notarized

## get content

Writes content of the specified disk in the recovery point to the standard output (stdout).

#### SYNOPSIS:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

#### Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

## calculate hash

Calculates the hash of the specified disk in the recovery point by using the SHA-256 algorithm and writes it to the stdout.

#### SYNOPSIS:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

#### Options

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

## Options description

Option	Description
--arc=BACKUP_NAME	The backup file name that you can get from the backup properties in the web console. The backup file must be specified with the extension .tibx.
--backup=RECOVERY_POINT_ID	The recovery point identifier
--disk=DISK_NUMBER	Disk number (the same as was written to the output of the "get content" command)
--loc=URI	<p>A backup location URI. The possible formats of the "--loc" option are:</p> <ul style="list-style-type: none"> <li>Local path name (Windows) c:/upload/backups</li> <li>Local path name (Linux) /var/tmp</li> <li>SMB/CIFS \\server\folder</li> <li>Cloud storage --loc=&lt;IP_address&gt;:443 --cert=&lt;path_to_certificate&gt; [--storage_path=/1] &lt;IP_address&gt; – you can find it in the registry key in Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\&lt;tenant_login&gt;\FesUri &lt;path_to_certificate&gt; – a path to the certificate file to access Cyber Cloud. For example, in Windows this certificate is located in C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\&lt;username&gt;.crt where &lt;username&gt; – is your account name to access Cyber Cloud.</li> </ul>
--log=PATH	Enables writing the logs by the specified PATH (local path only, format is the same as for --loc=URI parameter). Logging level is DEBUG.
--password=PASSWORD	An encryption password for your backup. If the backup is not encrypted, leave this value empty.
--raw	Hides the headers (2 first rows) in the command output. It is used when the command output should be parsed.



	<p>Output example without "--raw":</p> <pre> GUID      Date      Date timestamp ----- 516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865 516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925 </pre> <p>Output with "--raw":</p> <pre> 516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865 516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925 </pre>
--utc	Shows dates in UTC
--progress	<p>Shows progress of the operation.</p> <p>For example:</p> <pre> 1% 2% 3% 4% ... 100% </pre>

## 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.

## 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.

The snapshot is used only during the backup operation, and is automatically deleted when the backup operation completes. No temporary files are kept.

## 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](#) 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](#).

The preset is: **Disabled**.

---

### Note

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](#).

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.

## 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](#)" 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 protection 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.

## One-click recovery

One-click recovery allows users to recover the latest disk backup of their machines automatically. This can be a backup of the entire machine, or a backup of specific disks or volumes on this machine.

This feature is accessible on a user's machine after an administrator activates it, in conjunction with Startup Recovery Manager. The administrator can perform this operation only via the command-line interface. To learn more about how to activate Startup Recovery Manager and One-click recovery, refer to the [Command-line reference](#).

One-click recovery supports the following backup storages:

1. Secure Zone
2. Network storage
3. Cloud storage

If a specific type of storage is not available or there are no disk backups in it, the user is prompted to use the next type of storage.

If more than one backup set (also called *archive*) that contains disk backups is available in the storage, One-click recovery selects the backup set that was updated last. The user cannot select a different backup set.

One-click recovery supports the following operations:

- Automatic recovery from the latest backup
- Recovery from a specific backup (also called *recovery point*) within the automatically selected backup set

## Recovering a machine with One-click recovery

### Prerequisites

- An administrator has activated One-click recovery on the selected machine.
- There is at least one disk backup of the selected machine.

#### **To recover a machine**

1. Reboot the machine that you want to recover.
2. During the reboot, press F11 to enter Startup Recovery Manager.
3. Select the desired One-click recovery option:
  - To recover the latest backup automatically, press 1 on the keyboard.
  - To recover a different backup within the last updated backup set, press 2 on the keyboard.
    - To select the desired backup (also called *recovery point*), press the respective number on the keyboard.

The graphic user interface starts, and then disappears. The recovery procedure continues without it. When the recovery completes, your machine reboots.

## 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.

This option is not available for backups executed by the cloud agents, such as website backups or backups of servers located on the cloud recovery site.

You can configure this option separately for each location specified in the protection 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 protection 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.

Performance and backup window settings

No

Yes

	AM	00	03	06	09	12	PM	03	06	09	AM	00
Sun												
Mon												
Tue												
Wed												
Thu												
Fri												
Sat												

CPU priority

Low

Output speed

-

100

+

%

CPU priority

Low

Output speed

-

25

+

%

No backing up

## CPU priority

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

The available settings are:

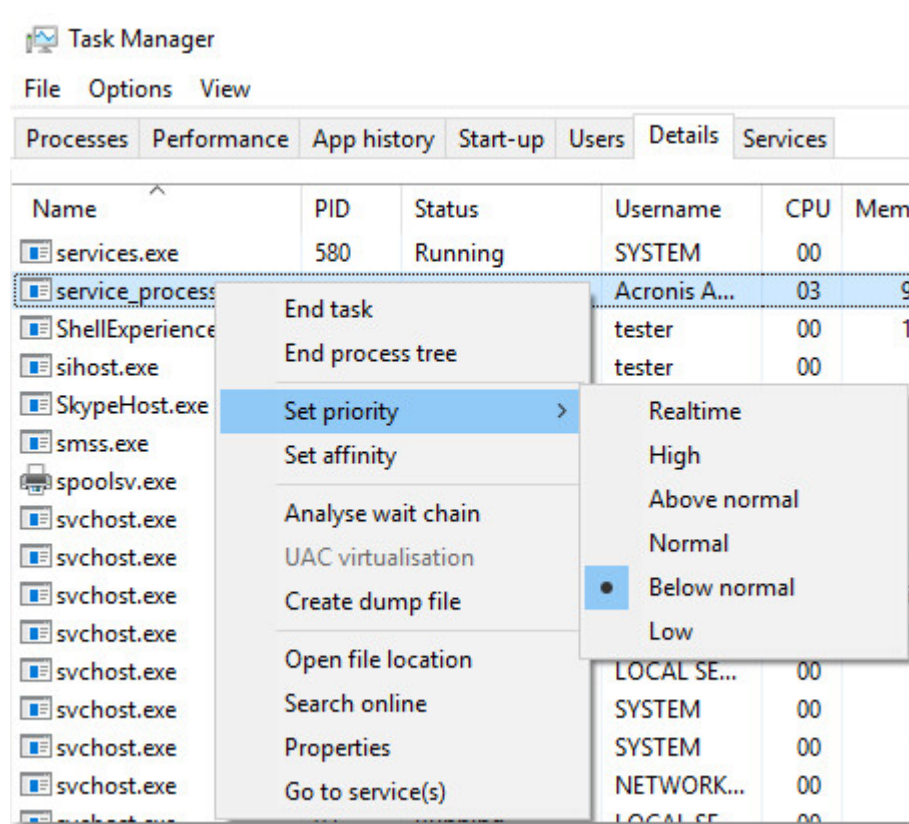
**Low** - in Windows, corresponds to **Below normal**.

**Normal** - in Windows, corresponds to **Normal**.

**High** - in Windows, corresponds to **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 or to cloud storage).

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 or cloud storage).

This setting works only if the agent is running in Windows.

- In KB/second (for all destinations).

## Physical Data Shipping

This option is effective if the backup destination is the cloud storage and the [backup format](#) is set to **Version 12**.

This option is effective for disk-level backups and file backups created by Agent for Windows, Agent for Linux, Agent for Mac, Agent for VMware, and Agent for Hyper-V. Backups created under bootable media are not supported.

This option determines whether the first full backup created by the protection plan will be sent to the cloud storage on a hard disk drive by using the Physical Data Shipping service. The subsequent incremental backups can be performed over the network.

The preset is: **Disabled**.

## About the Physical Data Shipping service

The Physical Data Shipping service web interface is available only to [organization administrators](#) in on-premises deployments and administrators in cloud deployments.

For detailed instructions about using the Physical Data Shipping service and the order creation tool, refer to the Physical Data Shipping Administrator's Guide. To access this document in the Physical Data Shipping service web interface, click the question mark icon.

## Overview of the physical data shipping process

1. Create a new protection plan. In this plan, enable the **Physical Data Shipping** backup option. You can back up directly to the drive or back up to a local or a network folder, and then copy/move the backup(s) to the drive.

---

### Important

Once the initial full backup is done, the subsequent backups must be performed by the same protection plan. Another protection plan, even with the same parameters and for the same machine, will require another Physical Data Shipping cycle.

---

2. After the first backup is complete, use the Physical Data Shipping service web interface to download the order creation tool and create the order.

To access this web interface, do one of the following:

- In on-premises deployments: log in to your Acronis account, and then click **Go to Tracking Console** under **Physical Data Shipping**.
- In cloud deployments: log in to the management portal, click **Overview > Usage**, and then click **Manage service** under **Physical Data Shipping**.

3. Package the drives and ship them to the data center.



---

### Important

Ensure that you follow the packaging instructions provided in the Physical Data Shipping Administrator's Guide.

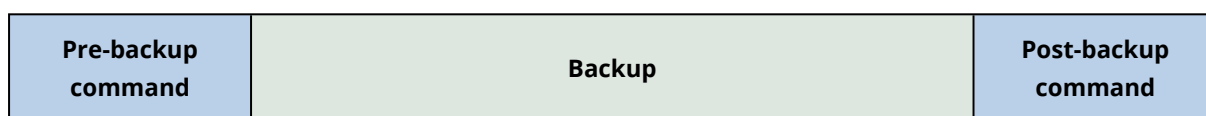
---

4. Track the order status by using the Physical Data Shipping service web interface. Note that the subsequent backups will fail until the initial backup is uploaded to the cloud storage.

## 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 protection plan copies *every* backup to subsequent locations.

The program 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").

## 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	Selected	Cleared	Selected	Cleared

<b>backup if the command execution fails*</b>				
<b>Do not back up until the command execution is complete</b>	Selected	Selected	Cleared	Cleared
<b>Result</b>				
	<b>Preset</b> 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.

## Post-backup command

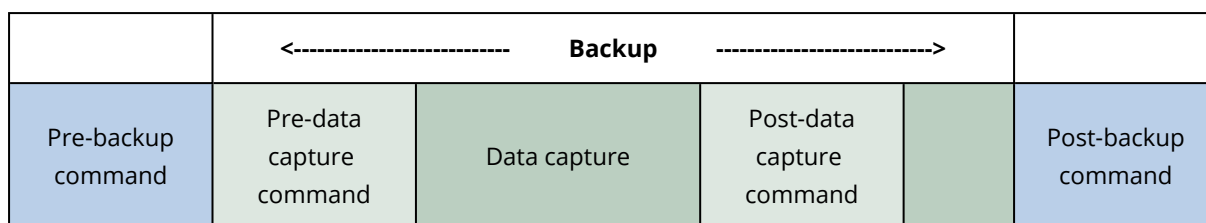
### *To specify a command/executable file to be executed after the backup is completed*

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**.

## 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](#) 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.

## 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			
<b>Fail the backup if the command execution fails*</b>	Selected	Cleared	Selected	Cleared
<b>Do not perform the data capture until the command execution is complete</b>	Selected	Selected	Cleared	Cleared
<b>Result</b>				

	<b>Preset</b> 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.

## 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			
<b>Fail the backup if the command execution fails*</b>	Selected	Cleared	Selected	Cleared
<b>Do not back up until the command execution is complete</b>	Selected	Selected	Cleared	Cleared
Result				
	<b>Preset</b> Continue the backup only after the command is	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.

	successfully executed.			
--	------------------------	--	--	--

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

## 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"](#).

## Scheduling

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

For more information about how to configure the backup schedule, see "Schedule" (p. 249).

The preset is:

- On-premises deployment: **Start all backups exactly as scheduled**
- Cloud deployment: **Distribute backup start times within a time window. Maximum delay: 30 minutes**

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 protection plan is applied to the machine and remains the same until you edit the protection plan and change the maximum delay value.

Virtual machines will be backed up one by one.

- **Limit the number of simultaneously running backups by**

Use this option to manage the parallel backup of virtual machines that are backed up on the hypervisor level (agentless backup).

Protection plans in which this option is selected can run together with other protection plans that are operated by the same agent at the same time. When you select this option, you must specify the number of parallel backups per plan. The total number of machines that are backed up simultaneously by all plans is limited to 10 per agent. To learn how to change the default limit, see "Limiting the total number of simultaneously backed-up virtual machines" (p. 502).

Protection plans in which this option is not selected run the backup operations sequentially, one virtual machine after another.

## 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**.

If this option is enabled, all disk or volume's sectors will be backed up, including unallocated space and those sectors that are free of data. The resulting backup will be equal in size to the disk being backed up (if the "[Compression level](#)" option is set to **None**). The software automatically switches to the sector-by-sector mode when backing up drives with unrecognized or unsupported file systems.

---

### Note

It will be impossible to perform a recovery of application data from the backups which were created in the sector-by-sector mode.

---

## Splitting

This option is effective for the **Always full; Weekly full, Daily incremental; Monthly full, Weekly differential, Daily incremental (GFS)**, and **Custom** backup schemes.

This option enables you to select the method of splitting of large backups into smaller files.

The preset is: **Automatic**.

The following settings are available:

- **Automatic**

A backup will be split if it exceeds the maximum file size supported by the file system.

- **Fixed size**

Enter the desired file size or select it from the drop-down list.

## Tape management

These options are effective when the backup destination is a tape device.

## Enable file recovery from disk backups stored on tapes

The preset is: **Disabled**.

If this check box is selected, at each backup, the software creates 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. The files are deleted automatically when the tape storing the respective backups is [erased](#), [removed](#) or overwritten.

The supplementary files' locations are as follows:

- In Windows XP and Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- In Windows 7 and later versions of Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- In Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

The space occupied by these supplementary files depends on the number of files in the respective backup. For a full backup of a disk containing approximately 20,000 files (the typical workstation disk backup), the supplementary files occupy around 150 MB. A full backup of a server containing 250,000 files may produce around 700 MB of supplementary files. So if you are certain that you will not need to recover individual files, you can leave the check box cleared to save the disk space.

If the supplementary files were not created during backup, or have been deleted, you still can create them by [rescanning](#) the tapes where the backup is stored.

## 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 protection 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 protection 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 protection plan.

A tape pool contains tapes from all tape devices attached to a machine, be it a storage node or a machine where a protection agent is installed, or both. 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 protection 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 protection 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.

## Multistreaming

The preset is: **Disabled**.

Multistreaming allows you to split the data from one agent into multiple streams, and then write those streams to different tapes simultaneously. This results in quicker backups and is particularly useful when the agent has higher throughput than the tape drive.

The **Multistreaming** check box is only available when you select more than one tape drive under the **Only selected devices and drives** option. The number of selected drives is equal to the number of simultaneous streams from an agent. If any selected drive is not available when a backup starts, this backup will fail.

To recover a multistreamed or both multistreamed and multiplexed backup, you need at least the same number of drives that were used to create this backup.

You cannot change the multistreaming settings of an existing protection plan. To use different settings or to change the selected tape drives, create a new protection plan.



Multistreaming is available both for locally attached tape drives and tape drives that are attached to a storage node.

## Multiplexing

The preset is: **Disabled**.

Multiplexing allows you to write data streams from multiple agents to a single tape. This results in better utilization of fast tape drives. By default, the multiplexing factor—that is, the number of agents that send data to a single tape—is set to two. You can increase it up to ten.

Multiplexing is useful for large environments with many backup operations. It does not improve the performance of a single backup.

To achieve the fastest backup in a large environment, you need to analyze the throughput of your agents, network, and tape drives. Then, set the multiplexing factor accordingly, without over multiplexing. For example, if your agents provide data at 70 Mbit/s, your tape drive writes at 250 Mbit/s, and there are no bottlenecks in your network, set the multiplexing factor to three. A multiplexing factor of four will lead to over multiplexing and decreased backup performance. Usually, the multiplexing factor is between two and five.

Because of their structure, multiplexed backups are slower to recover. The bigger the multiplexing factor, the slower the recovery. Simultaneous recovery of multiple backups written to a single multiplexed tape is not supported.

You can select one or more specific tape drives for multiplexing, or use the multiplexing option with any available tape drive. Multiplexing is not available for locally attached tape drives.

You cannot change the multiplexing settings of an existing protection plan. To use different settings, create a new protection plan.

In a protection plan, the following combinations of multistreaming and multiplexing are possible:

- **Both the multistreaming and multiplexing options are cleared.**  
Every agent sends data to a single tape drive.
- **Only the multistreaming option is selected.**  
Every agent sends data to at least two tape drives simultaneously.
- **Only the multiplexing option is selected.**  
Every agent sends data to a tape drive that accepts streams from multiple agents simultaneously. The maximum number of streams that a tape drive can accept is set in the protection plan and cannot be changed on the fly.
- **Both the multistreaming and multiplexing options are selected.**  
Every agent sends data to at least two tape drives that accept streams from multiple agents simultaneously.

A tape drive can write only one type of backup at a time—either multiplexed or not multiplexed, depending on which protection plan started first.

## 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 protection plan is applied.

You can also [specify tape sets](#) 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 protection 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.

## Task failure handling

This option determines the program behavior when a scheduled execution of a protection plan fails. This option is not effective when a protection plan is started manually.

If this option is enabled, the program will try to execute the protection 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**.

## 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](#)".

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.

## 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 snapshot is used only during the backup operation, and is automatically deleted when the backup operation completes. No temporary files are kept.

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, Microsoft SharePoint, 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](#) 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](#) backup option.

## 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](#)" 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. We recommend that you keep this option enabled at all times, even for virtual machines that do not run VSS-aware applications. Otherwise, even file-system consistency cannot be guaranteed inside the captured backup.

---

### Note

This option does not affect Scale Computing HC3 virtual machines. For them, quiescing depends on whether the Scale tools are installed on the virtual machine or not.

---

## 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**.

## 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**.

# Recovery

## 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)	<a href="#">Using the web interface</a> <a href="#">Using bootable media</a>
Physical machine (Mac)	<a href="#">Using bootable media</a>
Virtual machine (VMware, Hyper-V or Scale Computing HC3)	<a href="#">Using the web interface</a> <a href="#">Using bootable media</a>
ESXi configuration	<a href="#">Using bootable media</a>
Files/Folders	<a href="#">Using the web interface</a> <a href="#">Downloading files from the cloud storage</a> <a href="#">Using bootable media</a> <a href="#">Extracting files from local backups</a>
System state	<a href="#">Using the web interface</a>
SQL databases	<a href="#">Using the web interface</a>
Exchange databases	<a href="#">Using the web interface</a>
Exchange mailboxes	<a href="#">Using the web interface</a>
Microsoft 365 mailboxes	<a href="#">Using the web interface</a>
Oracle databases	<a href="#">Using Oracle Explorer tool</a>

### Note for Mac users

- Starting with 10.11 El Capitan, certain system files, folders, and processes are flagged for protection with an extended file attribute com.apple.rootless. This feature is called System Integrity Protection (SIP). The protected files include preinstalled applications and most of the folders in /system, /bin, /sbin, /usr.

The protected files and folders cannot be overwritten during a recovery under the operating system. If you need to overwrite the protected files, perform the recovery under bootable media.

- Starting with macOS Sierra 10.12, rarely used files can be moved to iCloud by the Store in Cloud feature. Small footprints of these files are kept on the file system. These footprints are backed up instead of the original files.

When you recover a footprint to the original location, it is synchronized with iCloud and the original file becomes available. When you recover a footprint to a different location, it cannot be synchronized and the original file will be unavailable.

## Safe recovery

A backed-up image of an operating system might be infected with a malware and can reinfect the machine on which it is being recovered.

Safe recovery allows you to prevent the recurrence of such infections by using the integrated [antimalware scanning](#) and malware deletion during the recovery process.

### Limitations:

- Safe recovery is only supported for physical and virtual Windows machines with Agent for Windows installed inside them.
- Only backups of type **Entire machine** or **Disks/volumes** are supported.
- Only volumes with NTFS file system are supported. Non-NTFS partitions will be recovered without being scanned for malware.
- Safe recovery is not supported for [Continuous data protection \(CDP\) backups](#). A machine will be recovered based on the last regular backup, without the data in the CDP backup. To recover the CDP data, run a **Files/folders** recovery.

## How it works

If you enable the Safe recovery option during the recovery process, then the system will perform the following:

1. Scan the image backup for malware and mark the infected files. One of the following statuses is assigned to the backup:
  - **No malware** – No malware was found in the backup during scanning.
  - **Malware detected** – Malware was found in the backup during scanning.
  - **Not scanned** – The backup was not scanned for malware.
2. Recover the backup to the selected machine.
3. Delete the detected malware.

You can filter backups by using the **Status** parameter.



Machine to browse from: D1-W2016-111 [Change](#)

Name:

Status:

☒ Malware detected

☒ No malware

☐ Not scanned

## 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 protection agent.

You can recover either Windows or Linux by using the same media. To recover macOS, create a separate media on a machine running macOS.

### ***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](#).

### ***To create bootable media in macOS***

1. On a machine where Agent for Mac is installed, click **Applications > Rescue Media Builder**.
2. The software displays the connected removable media. Select the one that you want to make bootable.

---

#### **Warning!**

All data on the disk will be erased.

---

3. Click **Create**.
4. Wait while the software creates the bootable media.

## Recovering a machine

---

### Recovering a physical machine

This section describes how to recover a physical machine by using the Cyber Protect web console.

Use the bootable media instead of the Cyber Protect web console if you need to recover any of the following:

- A macOS operating system
- 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 and recovery of volumes that are encrypted with BitLocker or CheckPoint requires a restart. For more information, refer to "Recovery with restart" (p. 328).

### ***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 cloud or 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 Backup storage tab](#).
  - Recover the machine as described in "[Recovering disks by using bootable media](#)".
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.

×

Recover machine

?

RECOVER TO  
Physical machine ▾

TARGET MACHINE  
ssd-win2016

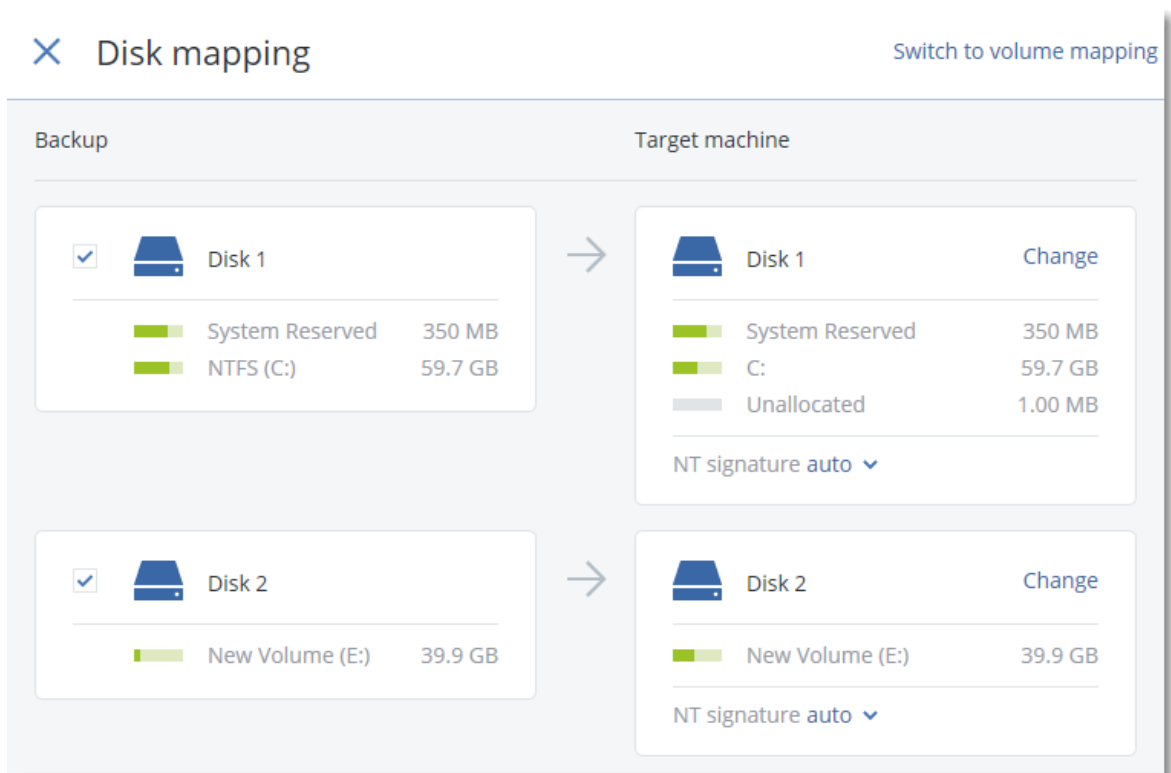
DISK MAPPING  
Disk 1 → Disk 1  
Disk 2 → Disk 2  
Disk 3 → Disk 3

SAFE RECOVERY  
☐ Off ⓘ

START RECOVERY

⚙ RECOVERY OPTIONS

5. If you are unsatisfied with the mapping result or if the disk mapping fails, click **Disk mapping** to re-map the disks manually.
- Additionally, in the mapping section, you can 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. [Optional] Enable the **Safe recovery** switch to scan the backup for malware. If malware is detected, it will be marked in the backup and deleted right after the recovery process completes.
7. Click **Start recovery**.
8. 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.

## Recovering a physical machine to a virtual machine

You can recover a backup of a physical machine to a virtual machine.

Recovering to a virtual machine is possible if at least one agent for the relevant target hypervisor is installed in your environment and registered on the management server. For example, recovery to VMware ESXi requires that Agent for VMware is installed in the environment and registered on the management server.

Some options are only available with the cloud deployment.

For more information about the supported paths for physical-to-virtual machine migration (P2V), refer to "Machine migration" (p. 504).

### Note

You cannot recover backups of macOS physical machines as virtual machines.

### ***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 cloud or shared storage (that is, 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 Backup storage tab](#).
  - Recover the machine as described in "Recovering disks and volumes by using bootable media" (p. 329).
4. Click **Recover > Entire machine**.
5. In **Recover to**, select **Virtual machine**.
6. Click **Target machine**.
  - a. Select the hypervisor.

---

**Note**

At least one agent for that hypervisor must be installed in your environment and registered on the management server.

---

- b. Select whether to recover to a new or existing machine. The new machine option is preferable because it does not require the disk configuration of the target machine to match exactly 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. [For Virtuozzo Hybrid Infrastructure] Click **VM settings**, and then select **Flavor**. Optionally, you can change the memory size, the number of processors, and the network connections of the virtual machine.
8. [Optional] [When recovering to a new machine] Configure the additional recovery options that you need:
  - [Not available for Virtuozzo Hybrid Infrastructure and Scale Computing HC3] To select the datastore for the virtual machine, click **Datastore** for ESXi, **Path** for Hyper-V and Virtuozzo, or **Storage domain** for Red Hat Virtualization (oVirt), and then select the datastore (storage) for the virtual machine.
  - To select the datastore (storage), interface, and the provisioning mode for each virtual disk, click **Disk mapping**. In the mapping section, you can choose individual disks for recovery.

---

**Note**

You can not change these settings if you are recovering a Virtuozzo container or Virtuozzo Hybrid Infrastructure virtual machine. For Virtuozzo Hybrid Infrastructure, you can only select the storage policy for the target disks. To do so, select the desired target disk, and then click **Change**. In the blade that opens, click the gear icon, select the storage policy, and then click **Done**.

---

- [Available for VMware ESXi, Hyper-V, Virtuozzo, and Red Hat Virtualization/oVirt] To change the memory size, the number of processors, and the network connections of the virtual machine, click **VM settings**.

RECOVER TO  
Virtual machine

TARGET MACHINE  
New machine on 10.250.22.17 New

DATASTORE  
datastore1 (1)

DISK MAPPING  
Disk 1 → datastore1 (1), 50.0 GB  
Disk 2 → datastore1 (1), 50.0 GB

VM SETTINGS  
Memory: 2.00 GB  
Virtual processors: 2  
Network adapters: 2

START RECOVERY ⚙️ RECOVERY OPTIONS

9. Click **Start recovery**.
10. [When recovering to an existing virtual machine] Confirm that you want to overwrite the disks.  
The recovery progress is shown on the **Activities** tab.

## Recovering a virtual machine

You can recover a backup of a virtual machine to a physical machine or to another virtual machine.

Recovering to a virtual machine is possible if at least one agent for the relevant target hypervisor is installed in your environment and registered on the management server. For example, recovery to VMware ESXi requires that Agent for VMware is installed in the environment and registered on the management server.

Some options are only available with the cloud deployment.

For more information about the supported paths for virtual-to-physical (V2P) or virtual-to-virtual (V2V) machine migration, refer to "Machine migration" (p. 504).

---

**Note**

You cannot recover macOS virtual machines to Hyper-V hosts because Hyper-V does not support macOS. You can recover macOS virtual machines to a VMware host that is installed on Mac hardware.

---

---

**Important**

A virtual machine must be stopped when you recover another machine to it. By default, the software stops the machine without a prompt. When the recovery is completed, you have to start the machine manually. You can change the default behavior 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 Backup storage tab](#).
2. Click **Recover > Entire machine**.
3. [When recovering to a physical machine] In **Recover to**, select **Physical machine**.

Recovery to a physical machine is possible only if the disk configuration of the target machine matches exactly the disk configuration in the backup. If this is the case, continue to step 4 in ["Recovering a physical machine" \(p. 322\)](#). Otherwise, we recommend that you perform the virtual-to-physical (V2P) migration by [using the bootable media](#).
4. [Optional] By default, the original machine is selected as a target machine. To recover to another virtual machine, click **Target machine**, and then do the following:
  - a. Select the hypervisor.

---

**Note**

At least one agent for that hypervisor must be installed in your environment and registered on the management server.

---

- b. Select whether to recover to a new or existing machine.
  - c. Select the host, and then specify the new machine name, or select an existing target machine.
  - d. Click **OK**.
5. [For Virtuozzo Hybrid Infrastructure] Click **VM settings**, and then select **Flavor**. Optionally, you can change the memory size, the number of processors, and the network connections of the virtual machine.
6. [Optional] [When recovering to a new machine] Configure the additional recovery options that you need:
  - [Not available for Virtuozzo Hybrid Infrastructure and Scale Computing HC3] To select the datastore for the virtual machine, click **Datastore** for ESXi, **Path** for Hyper-V and Virtuozzo, or **Storage domain** for Red Hat Virtualization (oVirt), and then select the datastore (storage) for the virtual machine.

- To select the datastore (storage), interface, and the provisioning mode for each virtual disk, click **Disk mapping**. In the mapping section, you can choose individual disks for recovery.

#### Note

You can not change these settings if you are recovering a Virtuozzo container or Virtuozzo Hybrid Infrastructure virtual machine. For Virtuozzo Hybrid Infrastructure, you can only select the storage policy for the target disks. To do so, select the desired target disk, and then click **Change**. In the blade that opens, click the gear icon, select the storage policy, and then click **Done**.

- [Available for VMware ESXi, Hyper-V, Virtuozzo, and Red Hat Virtualization/oVirt] To change the memory size, the number of processors, and the network connections of the virtual machine, click **VM settings**.

RECOVER TO  
Virtual machine

TARGET MACHINE

New machine on 10.250.22.17 New

DATASTORE

datastore1 (1)

DISK MAPPING

Disk 1 → datastore1 (1), 50.0 GB

Disk 2 → datastore1 (1), 50.0 GB


VM SETTINGS

Memory: 2.00 GB

Virtual processors: 2

Network adapters: 2

START RECOVERY

 RECOVERY OPTIONS

7. Click **Start recovery**.
8. [When recovering to an existing virtual machine] Confirm that you want to overwrite the disks.

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

## Recovery with restart

A restart is required when you recover the following:



- An operating system
- BitLocker or CheckPoint-encrypted volumes

---

**Important**

Backed-up encrypted volumes are recovered as non-encrypted.

---

## Requirements

- Recovery of encrypted volumes requires that there is a non-encrypted volume on the same machine, and that this volume has at least 1 GB of free space. Otherwise, the recovery will fail.
- Recovery of an encrypted system volume does not require any additional actions. To recover an encrypted non-system volume, you must lock it first, for example, by opening a file that resides on this volume. Otherwise, the recovery will continue without restart and the recovered volume might not be recognized by Windows.

## Troubleshooting

If the recovery fails and your machine restarts with the Cannot get file from partition error, disable Secure Boot. For more information on how to do it, refer to [Disabling Secure Boot](#) in the Microsoft documentation.

## Recovering disks and volumes by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (p. 321).

### ***To recover disks or volumes by using bootable media***

1. Boot the target machine by using bootable media.
2. [For macOS only] If you are recovering APFS-formatted volumes to a non-original machine or to bare metal, re-create the original disk configuration manually:
  - a. Click **Disk Utility**.
  - b. Re-create the original disk configuration. For instructions, refer to <https://support.apple.com/guide/disk-utility/welcome>.
  - c. Click **Disk Utility > Quit Disk Utility**.

---

**Note**

Starting with macOS 11 Big Sur, the System volume cannot be backed up and recovered. To recover a bootable macOS system, you need to recover the Data volume, and then to install macOS on it.

---

3. Click **Manage this machine locally** or click **Rescue Bootable Media** twice, depending on the media type you are using.
4. 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.

5. On the welcome screen, click **Recover**.
6. Click **Select data**, and then click **Browse**.
7. Specify the backup location:
  - To recover from cloud storage, select **Cloud storage**. Enter the credentials of the account to which the backed up machine is assigned.
  - To recover from a local or a network folder, browse to the folder under **Local folders** or **Network folders**.

Click **OK** to confirm your selection.

8. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
9. In **Backup contents**, select **Disks** or **Volumes**, and then select the items that you want to recover. Click **OK** to confirm your selection.

---

**Important**

If the backed-up machine has dynamic disks or logical volumes (LVM), select **Volumes**.

---

10. 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.

---

**Note**

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 macOS only] To recover an APFS-formatted Data volume as a bootable macOS system, in the **macOS Installation section**, keep the check box **Install macOS on the recovered macOS Data volume** selected.

After the recovery, the system reboots and the macOS installation starts automatically. You need an Internet connection for the installer to download the necessary files.

If you do not need to recover the APFS-formatted Data volume as a bootable system, clear the **Install macOS on the recovered macOS Data volume** check box. You can still make this volume bootable later, by installing macOS on it manually.

12. [For Linux only] If the backed-up machine has 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.
  - c. Confirm your choice.
13. [Optional] Click **Recovery options** to specify additional settings.
14. Click **OK** to start the recovery.

## 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](#).
5. Click **OK**.

## 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.

## 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.

## Recovering files

### 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 cloud or 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 Backup storage tab](#).
- [Download the files from the cloud storage](#).
- [Use bootable media](#).

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"](#)

---

**Note**

Search is not available for disk-level backups that are stored in the cloud storage.

---

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.

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, Agent for Hyper-V or Agent for Scale Computing HC3 is installed (if the files originate from an ESXi, Hyper-V or Scale Computing HC3 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

---

**Note**

Symbolic links are not supported.

---

- 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.

## Downloading files from the cloud storage

In the Web Restore console, you can browse the cloud storage, view the contents of the backups, and download backed-up files and folders.

You cannot browse backups of system state, SQL databases, and Exchange databases.

You cannot download backed-up disks, volumes, or whole recovery points.

### **To download files and folders from the cloud storage**

1. Log in to your Acronis account at <https://account.acronis.com>.
2. In the Cyber Protect console, select the required workload, and then click **Recovery**.
3. [If multiple backup locations are available] Select the backup location, and then click **More ways to recover**.
4. Click **Download files**.
5. [If prompted] Log in to the Cyber Protect Cloud console by using your Acronis account credentials.
6. Under **Machines**, click the workload name, and then click the backup archive.  
A backup archive contains one or more backups (recovery points).
7. Click the backup number (recovery point) from which you want to download files or folders, and then navigate to the required items.
8. Select the check boxes next to the items that you want to download.

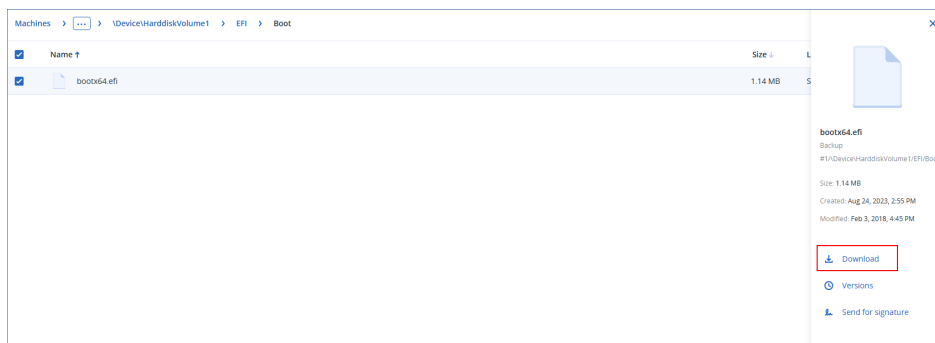
---

#### **Note**

If you select multiple items, they will be downloaded as a ZIP file.

---

9. Click **Download**.




## Verifying file authenticity with Notary Service

If notarization [was enabled during backup](#), you can verify the authenticity of a backed-up file.

### **To verify the file authenticity**

1. Select the file as described in steps 1-6 of the "[Recovering files by using the web interface](#)" section, or steps 1-5 of the "[Downloading files from the cloud storage](#)" section.

2. Ensure that the selected file is marked with the following icon: . This means that the file is notarized.
3. Do one of the following:
- Click **Verify**.  
The software checks the file authenticity and displays the result.
  - Click **Get certificate**.  
A certificate that confirms the file notarization is opened in a web browser window. The window also contains instructions that allow you to verify the file authenticity manually.

## Signing a file with ASign

ASign is a service that allows multiple people to sign a backed-up file electronically. This feature is available only for file-level backups stored in the cloud storage.

Only one file version can be signed at a time. If the file was backed up multiple times, you must choose the version to sign, and only this version will be signed.

For example, ASign can be used for electronic signing of the following files:

- Rental or lease agreements
- Sales contracts
- Asset purchase agreements
- Loan agreements
- Permission slips
- Financial documents
- Insurance documents
- Liability waivers
- Healthcare documents
- Research papers
- Certificates of product authenticity
- Nondisclosure agreements
- Offer letters
- Confidentiality agreements
- Independent contractor agreements

### ***To sign a file version***

1. Select the file as described in steps 1-6 of the ["Recovering files by using the web interface"](#) section.
2. Ensure that the correct date and time is selected on the left panel.
3. Click **Sign this file version**.
4. Specify the password for the cloud storage account under which the backup is stored. The login of the account is displayed in the prompt window.



The ASign service interface is opened in a web browser window.

5. Add other signees by specifying their email addresses. It is not possible to add or remove signees after sending invitations, so ensure that the list includes everyone whose signature is required.
6. Click **Invite to sign** to send invitations to the signees.

Each signee receives an email message with the signature request. When all the requested signees sign the file, it is notarized and signed through the notary service.

You will receive notifications when each signee signs the file and when the entire process is complete. You can access the ASign web page by clicking **View details** in any of the email messages that you receive.

7. Once the process is complete, go to the ASign web page and click **Get document** to download a .pdf document that contains:
  - The Signature Certificate page with the collected signatures.
  - The Audit Trail page with history of activities: when the invitation was sent to the signees, when each signee signed the file, and so on.

## Recovering files by using bootable media

For information about how to create bootable media, refer to "[Creating bootable media](#)".

### ***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:
    - To recover from cloud storage, select **Cloud storage**. Enter the credentials of the account to which the backed up machine is assigned.
    - To recover from a local or a network folder, browse 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 Cyber Backup Advanced: Changing the TapeLocation Folder \(KB 27445\)](#). For Windows PE, there is no workaround at the moment.

---

## 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 protection 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> - <protection 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.

## Recovering system state

1. Select the machine for which you want to recover the system state.
  2. Click **Recovery**.
  3. Select a system state recovery point. Note that recovery points are filtered by location.
  4. Click **Recover system state**.
  5. Confirm that you want to overwrite the system state with its backed-up version.
- The recovery progress is shown on the **Activities** tab.

## 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](#)".

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.

## 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, macOS, 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	macOS	Bootable media	ESXi, Hyper-V, Scale Computing HC3	Windows
Backup validation	+	+	+	+	+	+	+	+	+
Boot mode	+	-	-	-	-	-	-	+	-
Date and time for files	-	-	-	+	+	+	+	-	-
Error handling	+	+	+	+	+	+	+	+	+
File exclusions	-	-	-	+	+	+	+	-	-
Flashback	+	+	+	-	-	-	-	+	-
Full path recovery	-	-	-	+	+	+	+	-	-
Mount points	-	-	-	+	-	-	-	-	-
Performance	+	+	-	+	+	+	-	+	+
Pre/post command	+	+	-	+	+	+	-	+	+

ds									
SID changing	+	-	-	-	-	-	-	-	-
VM power management	-	-	-	-	-	-	-	+	-
"Tape management" (p. 347) > Use a disk cache to accelerate the recovery	-	-	-	+	+	+	-	-	-
Windows event log	+	-	-	+	-	-	-	Hyper-V only	+
Power on after recovery	-	-	-	-	-	-	+	-	-

## Backup validation

This option defines whether to validate a backup to ensure that the backup is not corrupted, before data is recovered from it. This operation is performed by the protection agent.

The preset is: **Disabled**.

Validation calculates a checksum for every data block saved in the backup. The only exception is validation of file-level backups that are located in the cloud storage. These backups are validated by checking consistency of the meta information 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.

---

### Note

Validation is available for cloud storage located in an Acronis data center and provided by Acronis partners.

---

## 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 7
  - 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.

## 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**.

## 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.

## 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.

---

## 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 their NTFS permissions from the folder to which they are recovered.

## Flashback

This option is effective when recovering disks and volumes on physical and virtual machines, except for Mac.

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 in the cloud storage or on a remote network folder).

When recovering a physical machine, the preset depends on the backup location:

- If the backup location is the cloud storage, the preset is: **Enabled**.
- For other backup locations, the preset is: **Disabled**.

When recovering a virtual machine, the preset is: **Enabled**.



## 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**.

## 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](#) 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.

---

## 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.

## 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.

## 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			
<b>Fail the recovery if the command execution fails*</b>	Selected	Cleared	Selected	Cleared
<b>Do not recover until the command execution is complete</b>	Selected	Selected	Cleared	Cleared
Result				
	<b>Preset</b> 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.

## 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.

---

## Tape management

You can use the following tape management recovery options.

### Use a disk cache to accelerate the recovery

The preset is: **Disabled**.

We strongly recommend that you use the **Use a disk cache to accelerate the recovery** option when you recover files from an image archive. Otherwise, restore operation can take a lot of time. With this option, tape reading is performed sequentially, without interruptions and rewinding.

### 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, Agent for Hyper-V or Agent for Scale Computing HC3.

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.

## VM power management

These options are effective when recovery to a virtual machine is performed by Agent for VMware, Agent for Hyper-V or Agent for Scale Computing HC3.

### 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.

## 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**.

### Power on after recovery

This option is effective when operating under bootable media.

The preset is: **Disabled**.

This option enables booting the machine into the recovered operating system without user interaction.

## Disaster recovery

This feature is available only in cloud deployments of Acronis Cyber Protect. For a detailed description of this functionality, please refer to <https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html>.

# Operations with backups

## The Backup storage tab

The **Backup storage** 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.

In Windows, backup files inherit the access permissions from their parent folder. Therefore, we recommend that you restrict the read permissions for this folder.

In the cloud storage, users have access only to their own backups. In a cloud deployment, an administrator can view backups on behalf of any account that belongs to the same group and its child groups. This account is indirectly chosen in **Machine to browse from**. The **Backup storage** tab shows backups of all machines ever registered under the same account as this machine is registered.

Backup locations that are used in protection plans are automatically added to the **Backup storage** 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.

---

### Warning!

Do not try editing the backup files manually because this may result in file corruption and make the backups unusable. Also, we recommend that you export backups or use the backup replication instead of moving backup files manually.

---

### *To select a recovery point by using the Backup storage tab*

1. On the **Backup storage** 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> - <protection 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.

## 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. This approach can also be used for granular recovery of Microsoft SharePoint data [by using SharePoint Explorer](#).

- **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> - <protection 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.

---

**Note**

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**

---

**Note**

Only the last backup in the archive (backup chain) can be mounted in read-write mode.

---

- **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.

## Validating backups

Validation is an operation that checks the possibility of data recovery from a backup. For more information about this operation, refer to "Validation" (p. 357).

***To validate a backup***

1. Select the backed-up workload.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.  
If the workload is offline, the recovery points are not displayed. Do any of the following:
  - If the backup location is cloud or shared storage (that is, other agents can access it), click **Select machine**, select a target workload that is online, and then select a recovery point.
  - Select a recovery point on the Backup storage tab. For more information about the backups there, refer to "The Backup storage tab" (p. 350).
4. Click the gear icon, and then click **Validate**.
5. Select the agent that will perform the validation.



6. Select the validation method.
7. If the backup is encrypted, provide the encryption password.
8. Click **Start**.

## 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](#).

The [backup file name](#) of the exported backup depends on the value of the [backup format](#) 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 cloud or 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 Backup storage tab](#).
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**.

# Deleting backups

---

## Warning!

When a backup is deleted, all of its data is permanently erased. Deleted data cannot be recovered.

---

### *To delete backups of a machine that is online and present in the Cyber Protect web 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 **Backup storage** 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> - <protection 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.

### *To delete backups directly from the cloud storage*

1. Log in to the cloud storage, as described in "[Downloading files from the cloud storage](#)".
2. Click the name of the machine whose backups you want to delete.  
The software displays one or more backup groups.
3. Click the gear icon corresponding to the backup group that you want to delete.
4. Click **Remove**.
5. Confirm the operation.

# The Plans tab

With an Advanced license, you can manage protection plans and other plans by using the **Plans** tab.

Each section of the **Plans** tab contains all the plans of a specific type. The following sections are available:

- **Protection**
- **Backup scanning**
- **Backup replication**
- **Validation**
- **Cleanup**
- **Conversion to VM**
- **VM replication**
- **Bootable media**. This section displays protection plans that were created for machines booted from bootable media, and can only be applied to such machines.

In each section, you can create, edit, disable, enable, delete, start, and monitor the running of a plan.

Cloning and stopping are available only for protection plans. Unlike stopping a backup from the **Devices** tab, stopping a protection plan will stop the backups on all devices where this plan is applied. If the backup start times for multiple devices are distributed within a time window, stopping a protection plan will stop the running backups or prevent backups from starting.

You can also export a plan to a file and import a previously exported plan.

## Off-host data processing

Most actions that are a part of a protection plan, such as replication, validation, and applying retention rules, are performed by the agent that performs the backup. This puts additional workload on the machine where the agent is running, even after the backup process is complete.

Separating the antimalware scanning, replication, validation, cleanup, and conversion plans from protection plans gives you the flexibility:

- To choose another agent(s) for performing these operations
- To schedule these operations for off-peak hours to minimize network bandwidth consumption
- To shift these operations outside of business hours, if setting up a dedicated agent is not in your plans

If you are using a storage node, installing a dedicated agent on the same machine makes sense.

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.

## Backup scanning plans

Antimalware scan of backups is available if the Scan Service component is installed with the Cyber Protect Management Server. For more information, see "Scan Service" (p. 92).

Backup scanning plans are supported for **Entire machine** and **Disk/volume** backups of Windows machines. Only volumes with the NTFS file system and GPT or MBR partitioning are scanned.

### *To create a backup scanning plan*

1. In the Cyber Protect web console, go to **Plans > Backup scanning**.
2. Click **Create plan**.
3. [Optional] To modify the plan name, click the pencil icon next to the default name.
4. Select the scanning agent.
5. Select backups or backup locations to scan.  
To include multiple backups in the plan, add them one by one.
6. [For backups in the cloud storage or in a network folder] If prompted, specify the access credentials for the storage.
7. [For encrypted backups] Specify the encryption password.  
You can specify one password for all selected backups or backup locations. If the password does not match a specific backup, an alert will be shown. Only backups with matching passwords are scanned.
8. Configure the scan schedule.
9. Click **Create**.

## 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
Cloud storage	+	+
Local folder	+	+
Network folder	+	+
NFS folder	–	–
Secure Zone	–	–
SFTP server	–	–
Managed location*	+	+
Tape device	–	+

\* Check the restrictions described in topic "Considerations for users with the Advanced license" (p. 271).

### ***To create 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](#)".
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**.

## 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](#)".

- **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 protection 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
Cloud storage	+	+
Local folder	+	+
Network folder	+	+
NFS folder	-	-
Secure Zone	-	-
SFTP server	-	-
Managed location	+	+
Tape device	+	-

### *To create 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. [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.

---

**Note**

The **VM heartbeat** switch is always enabled to validate the heartbeat status of the virtual machine reported by the hypervisor tools in the guest operating system (VMware Tools or Hyper-V Integration Services), by running a virtual machine from the backup. This switch is designed for future releases, so you cannot interact with it.

---

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**.

## 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](#)".
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**.

## 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.

---

### **Note**

VMs replicated via native Scale Computing VM replication functionality cannot be backed up.

---

For information about prerequisites and limitations, please refer to "[What you need to know about conversion](#)".

### ***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**
  - **Scale Computing HC3**
  - **VMware Workstation**



- **VHDX files**

---

**Note**

To save storage space, each conversion to VHDX files overwrites the VHDX files in the target location that were created during the previous conversion.

---

5. Do one of the following:

- [For VMware ESXi, Hyper-V, and Scale Computing HC3] 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. [Only for VMware ESXi and Hyper-V] Select the disk provisioning mode. The default setting is **Thin** for VMware ESXi and **Dynamically expanding** for Hyper-V.

10. [Optional] [For VMware ESXi, Hyper-V, and Scale Computing HC3] Click **VM settings** to modify the memory size, the number of processors, or the network connections of the virtual machine.

11. [Optional] Click **Schedule**, and then change the schedule.

12. 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.

13. [Optional] To modify the plan options, click the gear icon.

14. Click **Create**.

# Bootable media

---

## Important

Some of the features described in this section are only available for on-premises deployments.

---

## Bootable media

Bootable media is a physical media (CD, DVD, USB flash drive, or other removable media supported by the machine's BIOS as a boot device) that allows you to run the protection agent either in a Linux-based environment or a Windows Preinstallation Environment (WinPE), without the help of an operating system.

Bootable media is most often used to:

- Recover an operating system that cannot start
- Access and back up the data that has survived in a corrupted system
- Deploy an operating system on bare metal
- Create basic or dynamic volumes on bare metal
- Back up sector-by-sector a disk with an unsupported file system
- Back up offline any data that cannot be backed up online – for example, because the data is locked by a running application or because the access to it is restricted.

A machine can also be booted by using the network boot from Acronis PXE Server, Windows Deployment Services (WDS) or Remote Installation Services (RIS). These servers with uploaded bootable components can be thought of as a kind of bootable media too. You can create bootable media or configure the PXE server or WDS/RIS by using the same wizard.

## Create a bootable media or download a ready-made one?

By using the [Bootable Media Builder](#), you can create your own bootable media ([Linux-based](#) or [WinPE-based](#)) for Windows, Linux or macOS computers. For a fully-featured bootable media, you need to specify your Acronis Cyber Protect license key. Without this key, your bootable media will be capable of performing only recovery operations.

---

## Note

The bootable media does not support hybrid drives.

---

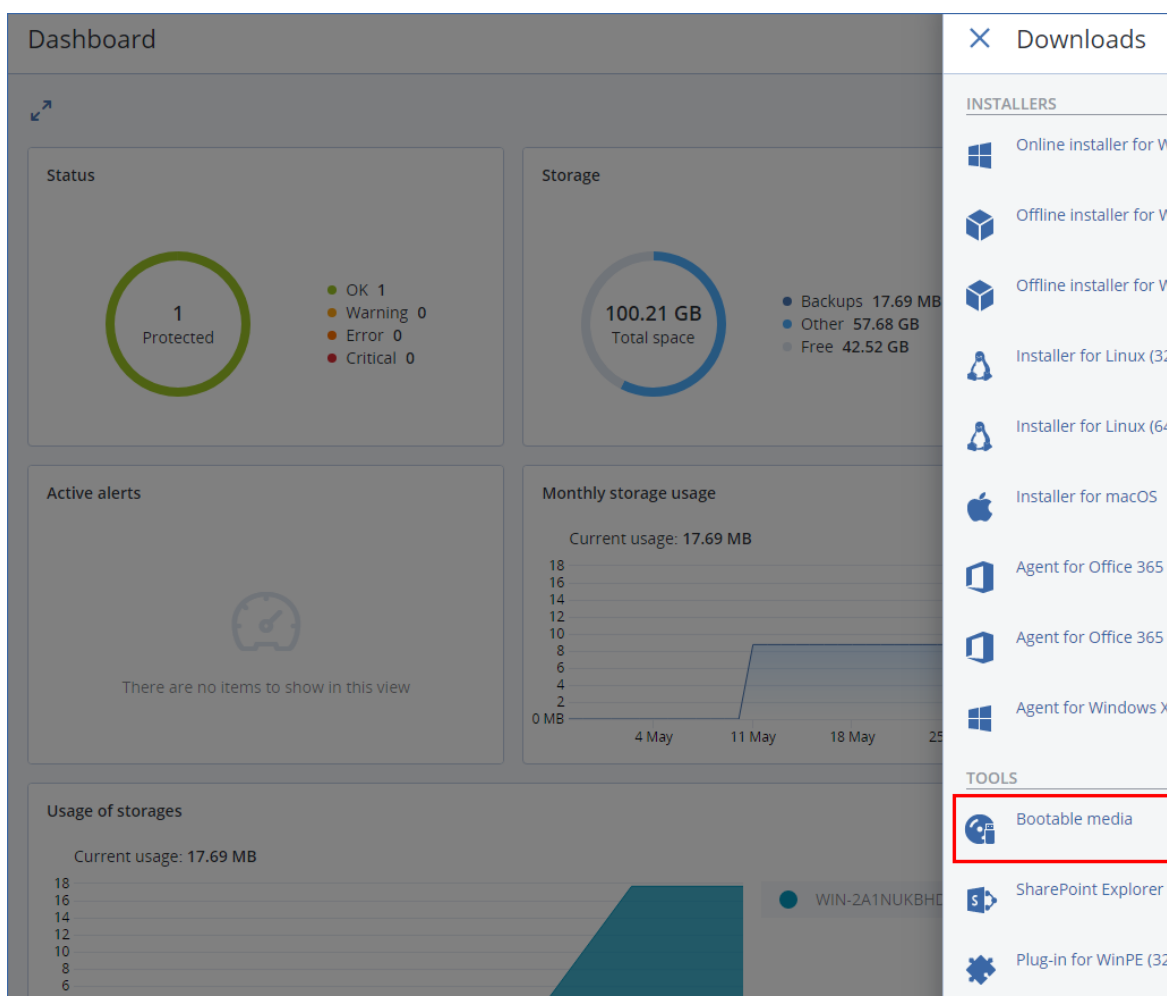
Also, you can download a ready-made bootable media (Linux-based only). You can use the downloaded bootable media only for recovery operations and access to Acronis Universal Restore. You cannot back up data, validate or export backups, manage disks, or use scripts with it. Downloaded bootable media is not suitable for macOS computers.

## Note

The ready-made bootable media does not support storage node, tape locations, and SFTP locations. If you want to use these storage locations in your n-premises deployment, you must create your own bootable media by using the Bootable Media Builder. See <https://kb.acronis.com/content/61566>.

### To download a ready-made bootable media

1. In the Cyber Protect web console, click the account icon in the top-right corner, and then click **Downloads**.
2. Select **Bootable media**.



You can burn the downloaded ISO file to a CD/DVD or create a bootable USB flash drive by using one of the free tools that are available online. Use ISO to USB or RUFUS if you need to boot an UEFI machine, or Win32DiskImager for a BIOS machine. In Linux, using the dd utility makes sense.

If the Cyber Protect web console is not accessible, you can download the ready-made bootable media from your account in Acronis Customer Portal:

1. Go to <https://account.acronis.com>.
2. Locate Acronis Cyber Protect, and then click **Downloads**.
3. On the page that opens, locate **Additional downloads**, and then click **Bootable Media ISO (for Windows and Linux)**.

## Linux-based or WinPE-based bootable media?

### Linux-based

**Linux-based bootable media** contains a bootable protection agent based on Linux kernel. The agent can boot and perform operations on any PC-compatible hardware, including bare metal and machines with corrupted or non-supported file systems. The operations can be configured and controlled either locally or remotely, in the Cyber Protect web console.

A list of the supported by Linux-based media hardware is available at:  
<http://kb.acronis.com/content/55310>.

### WinPE-based

**WinPE-based bootable media** contains a minimal Windows system called Windows Preinstallation Environment (WinPE) and Acronis Plugin for WinPE, that is, a modification of the protection agent that can run in the preinstallation environment.

WinPE proved to be the most convenient bootable solution in large environments with heterogeneous hardware.

#### **Advantages:**

- Using Acronis Cyber Protect in Windows Preinstallation Environment provides more functionality than using Linux-based bootable media. Having booted PC-compatible hardware into WinPE, you can use not only a protection agent, but also PE commands and scripts, and other plugins that you have added to the PE.
- PE-based bootable media helps overcome some Linux-related bootable media issues such as support for certain RAID controllers or certain levels of RAID arrays only. Media based on WinPE 2.x and later allow dynamic loading of the necessary device drivers.

#### **Limitations:**

- Bootable media based on WinPE versions earlier than 4.0 cannot boot on machines that use Unified Extensible Firmware Interface (UEFI).
- When a machine is booted with a PE-based bootable media, you cannot select optical media such as CD, DVD, or Blu-ray Discs (BD) as a backup destination.

## Bootable Media Builder

Bootable Media Builder is a dedicated tool for creating bootable media. It is available for on-premises deployments only.

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.

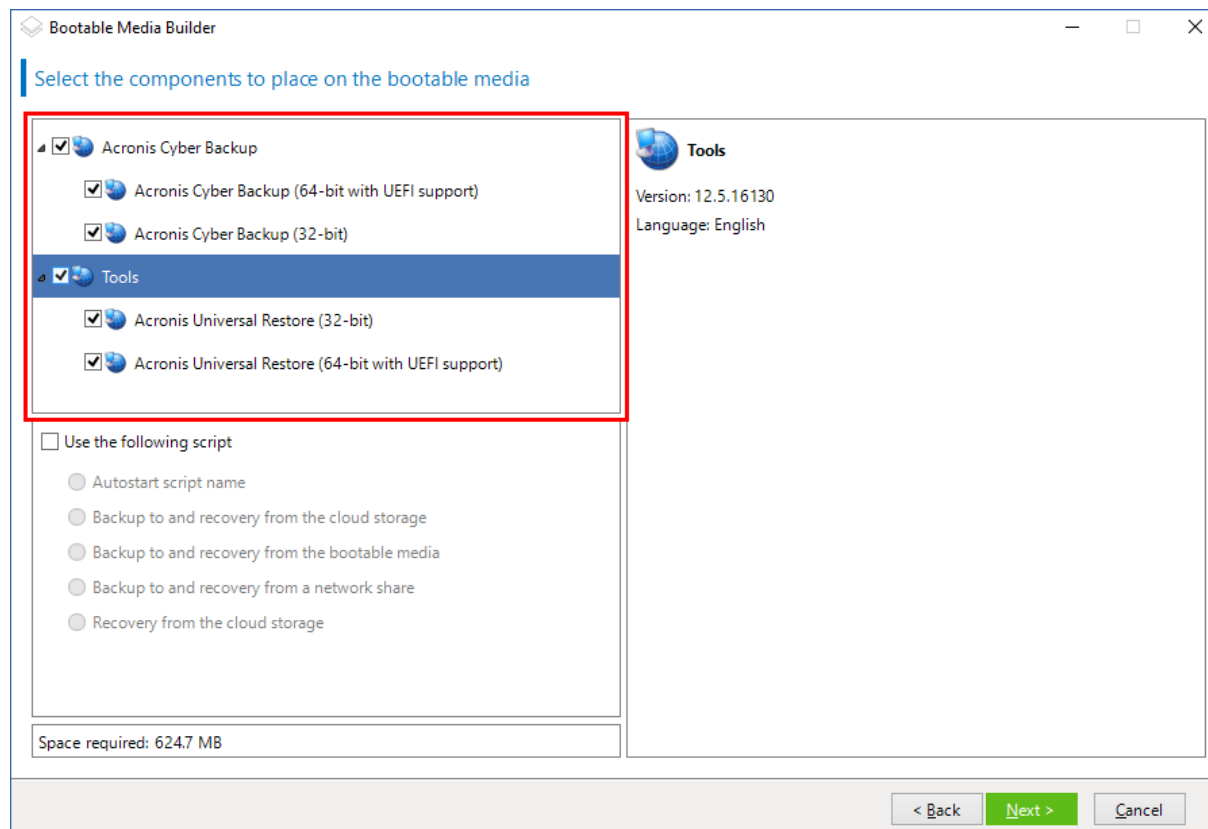
## Why use the media builder?

The ready-made bootable media that is available for download in the Cyber Protect web 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, full-featured [Linux-based](#) and [WinPE-based](#) bootable media with the backup functionality.
- Apart from creating physical bootable media, you can upload its components to Windows Deployment Services (WDS) and use a network boot.
- The ready-made bootable media does not support storage node, tape locations, and SFTP locations. If you want to use these storage locations in your local on-premises deployment, you must create your own bootable media by using the Bootable Media Builder. See <https://kb.acronis.com/content/61566>.

## 32- or 64-bit?

Bootable Media Builder creates media with both 32-bit and 64-bit components. In most cases, you will need a 64-bit media to boot a machine that uses Unified Extensible Firmware Interface (UEFI).

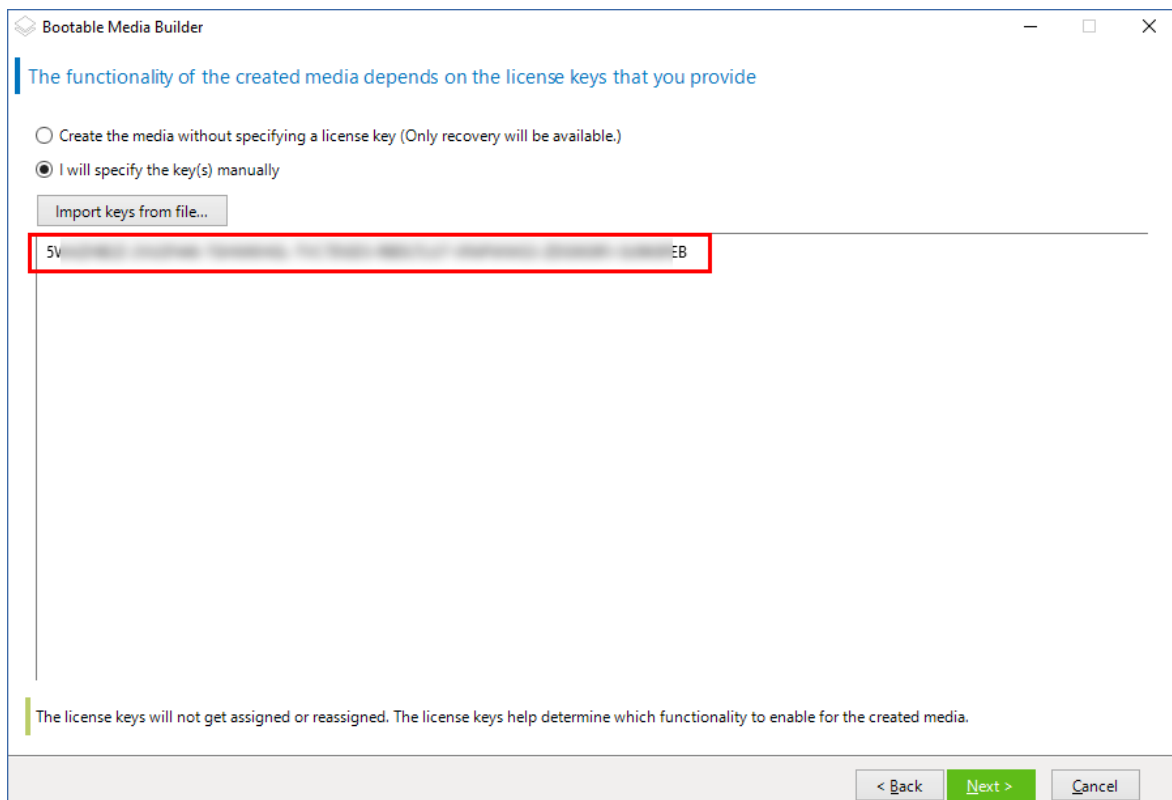


## Linux-based bootable media

### **To create a Linux-based bootable media**

1. Start the **Bootable Media Builder**.
2. To create a full-featured bootable media, specify an Acronis Cyber Protect license key. This key is used to determine which features will be included in the bootable media. No licenses will be revoked from any machines.

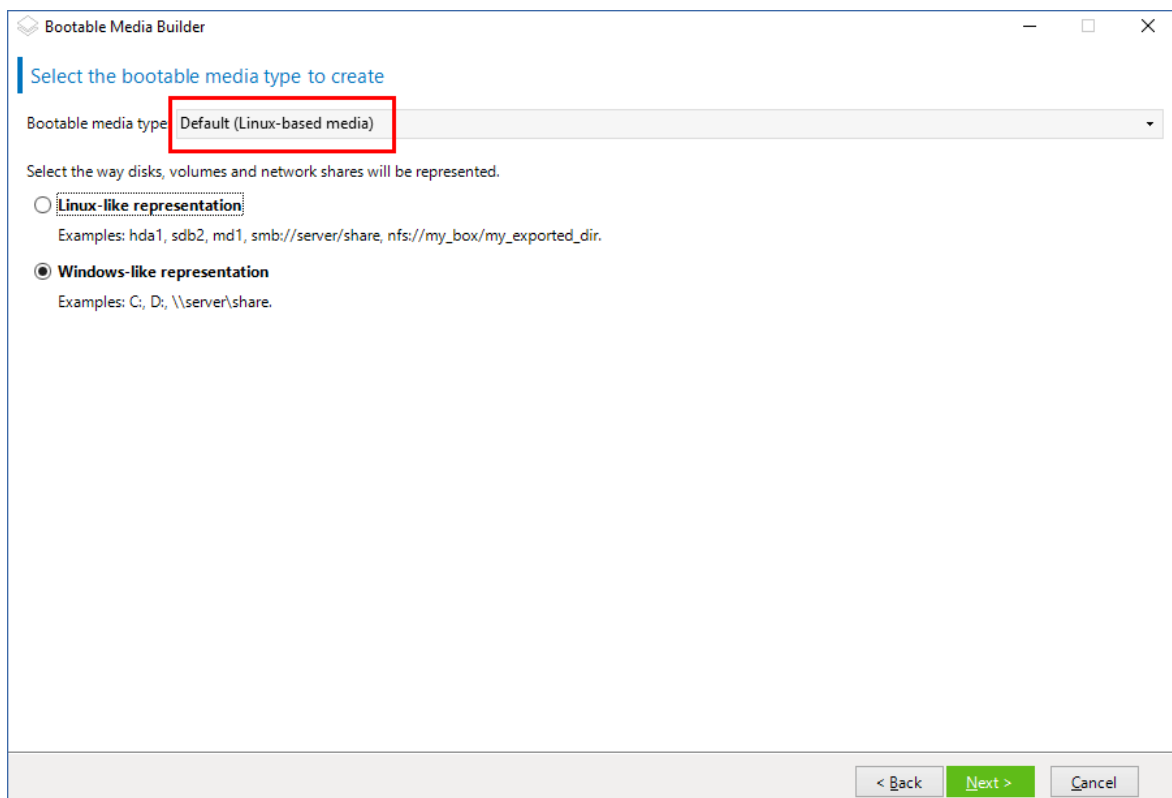
If you don't specify a license key, the resulting bootable media can only be used for recovery operations.



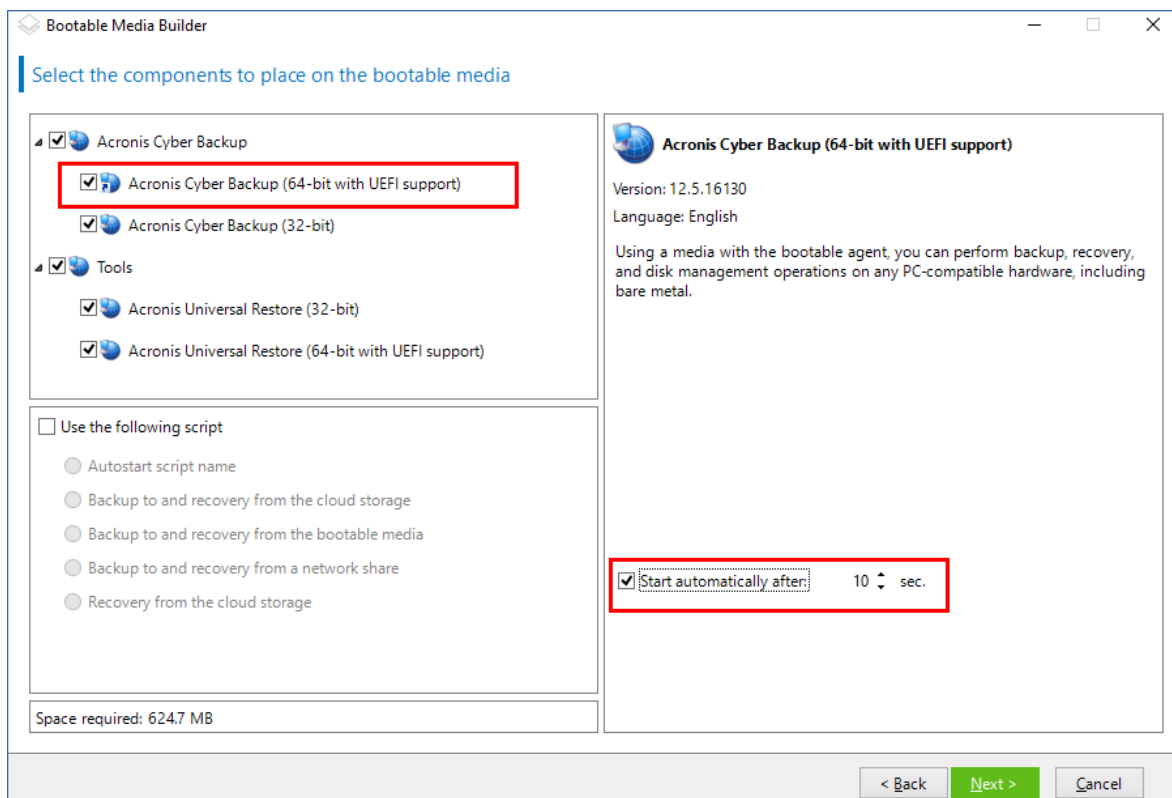
3. Select **Bootable media type: Default (Linux-based media)**.

Select how volumes and network resources will be represented:

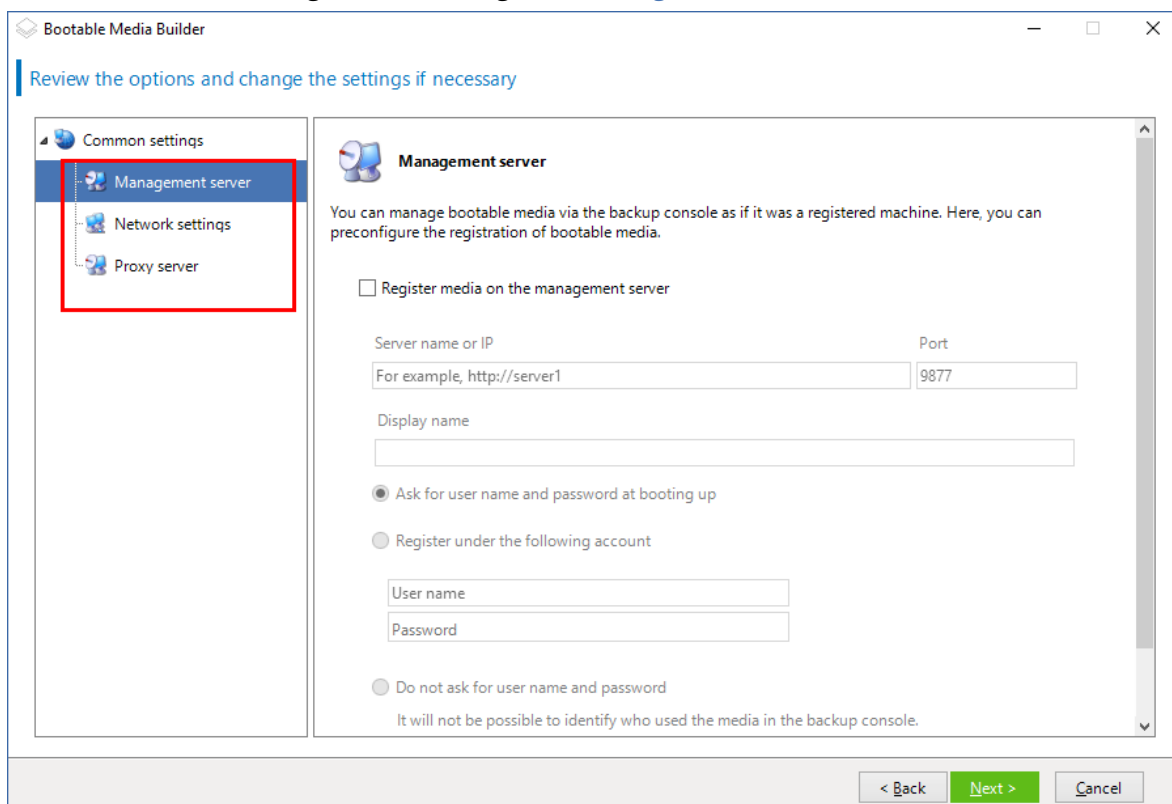
- A media with Linux-like volume representation displays the volumes as, for example, hda1 and sdb2. It tries to reconstruct MD devices and logical (LVM) volumes before starting a recovery.
- A media with Windows-like volume representation displays the volumes as, for example, C: and D:. It provides 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 more information about the available parameters, refer to [Kernel parameters](#).
5. [Optional] Select a language that will be used in the bootable media.
6. Select the components to be placed on the media: the Acronis Cyber Protect bootable agent, and/or Universal Restore if you plan to restore the system on dissimilar hardware.  
The bootable agent allows you to perform backup, recovery, and disk management operations on any PC-compatible hardware, including bare metal.  
[Universal Restore](#) allows you to boot an operating system recovered to dissimilar hardware or to a virtual machine. The tool finds and installs drivers for devices that are critical for starting the operating system, such as storage controllers, motherboard, or chipset.
7. [Optional] Specify the timeout interval for the boot menu, along with the component that will automatically start on timeout. To do so, click the desired component on the upper left pane, and then set the interval for it. This enables unattended onsite operation when booting from WDS/RIS.  
If this setting is not configured, the loader will wait for you to select whether to boot the operating system (if present) or the component.



8. [Optional] If you want to automate the bootable agent operations, select the **Use the following script** check box. Then, select **one of the scripts** and specify the script parameters.
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](#).





10. [Optional] Specify network settings: TCP/IP settings to be assigned to the machine network adapters. For more information, refer to "Network settings" (p. 379).
11. [Optional] Specify a [network port](#): The TCP port on which the bootable agent listens for an 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. You can:
  - Create an ISO image. Then you can burn it to a CD/DVD; use it to create a bootable USB flash drive; or connect it to a virtual machine.
  - Create a ZIP file.
  - 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](#). 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 then click **Proceed**.

## 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.

#### **LAYOUTS=en-US, de-DE, fr-FR, ...**

Specifies the keyboard layouts that can be used in the bootable media's graphical user interface.

Without this parameter, only two layouts can be used: English (USA) and the layout that corresponds to the language selected in the media's boot menu.

You can specify any of the following layouts:

Belgian: **be-BE**

Czech: **cz-CZ**

English: **en-GB**

English (USA): **en-US**

French: **fr-FR**

French (Swiss): **fr-CH**

German: **de-DE**

German (Swiss): **de-CH**

Italian: **it-IT**

Polish: **pl-PL**

Portuguese: **pt-PT**

Portuguese (Brazilian): **pt-BR**

Russian: **ru-RU**

Serbian (Cyrillic): **sr-CR**

Serbian (Latin): **sr-LT**

Spanish: **es-ES**

When working under bootable media, use CTRL + SHIFT to cycle through the available layouts.

## Scripts in bootable media

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 cloud storage (**entire\_pc\_cloud**)
- Backup to and recovery from the bootable media (**entire\_pc\_local**)
- Backup to and recovery from a network share (**entire\_pc\_share**)
- Recovery from the cloud storage (**golden\_image**)

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 cloud storage

This script will back up a machine to the cloud storage or recover the machine from its most recent backup created in the cloud storage by this script. 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 user name and password for the cloud storage.
2. [Optional] A password that the script will use to encrypt or access the backups.

### 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**

- a. In the Cyber Protect web console, go to **Backup storage > Locations**.
  - b. Select the network share (click **Add location** if the share is not listed).
  - c. Select the backup.
  - d. 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.

## Recovery from the cloud storage

This script will recover the machine from the most recent backup located in the cloud storage. On its start, the script will prompt the user to specify:

1. The user name and password for the cloud storage.
2. The password if the backup is encrypted.

We recommend that you store backups of only one machine under this cloud storage account. Otherwise, if a backup of another machine is newer than the backup of the current machine, the script will choose that machine backup.

## 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		
<code>displayName</code>	string	Yes	The script name to be displayed in Bootable Media Builder.
<code>description</code>	string	No	The script description to be displayed in Bootable Media Builder.
<code>timeout</code>	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.
<code>variables</code>	object	No	Any variables for <b>&lt;script_file&gt;.sh</b> 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 <b>&lt;script_file&gt;.sh</b> .
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).
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 <b>autostart.json</b> . 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.



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 Cyber Protect web 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 > Accounts**). In the Cyber Protect web 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 > Accounts**). In the Cyber Protect web 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.

## 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.

## 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 `acrocmbd` 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.

## 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 target machine 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**.

## WinPE-based bootable media

Bootable Media Builder provides two methods of integrating Acronis Cyber Protect 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 \(AIK\)](#) or [Windows Assessment and Deployment Kit \(ADK\)](#).

## 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 (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.

---

### Note

Disk management functionality is not available for bootable media based on Windows PE 4.0 and later. Thus, disk management is supported for Windows 7 and earlier operating systems. To perform disk management operations on Windows 8 and later, you need to install Acronis Disk Director. For more information, refer to this KB article: <https://kb.acronis.com/content/47031>.

---

## 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.

## 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.

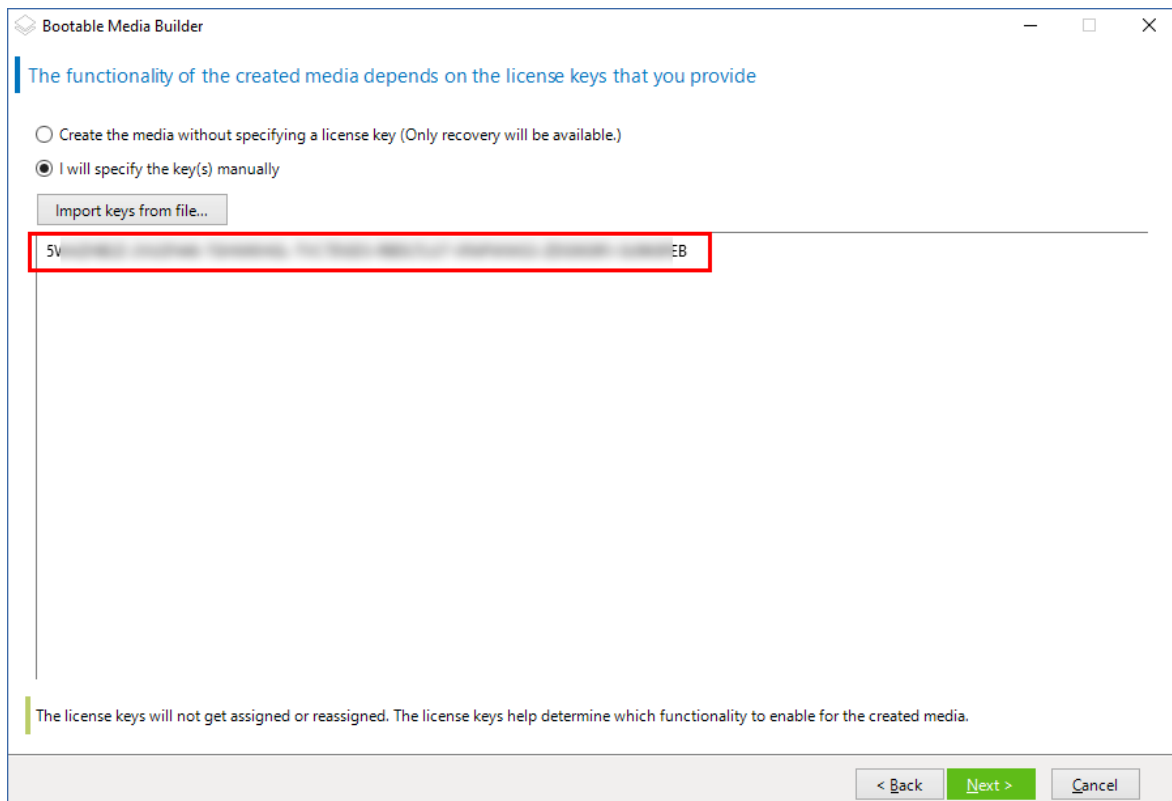
## Adding Acronis Plug-in to WinPE

### ***To add Acronis Plug-in to WinPE:***

1. Start the Bootable Media Builder.
2. To create a full-featured bootable media, specify an Acronis Cyber Protect license key. This key is used to determine which features will be included in the bootable media. No licenses will be

revoked from any machines.

If you don't specify a license key, the resulting bootable media can only be used for recovery operations.



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:

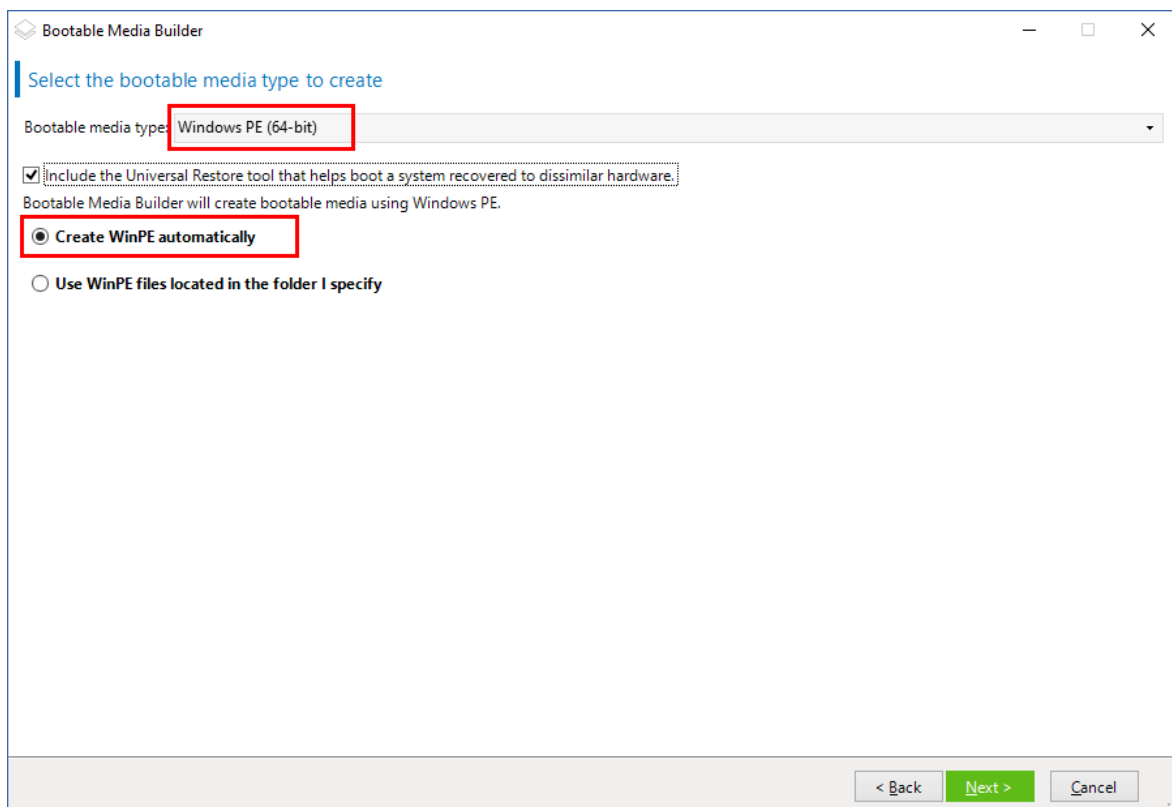
- Click **Download the Plug-in for WinPE (32-bit)**.
- Save the plug-in to **%PROGRAM\_FILES%\Acronis\BootableComponents\WinPE32**.

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 a language that will be used in the bootable media.
6. 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 the command line if the `acrocmd` utility is running on a different machine. You can also leave these fields empty, then a remote connection via the command line interface will be possible without credentials. These credentials are also required when you [register the media on the management server from the Cyber Protect web console](#).

7. Specify [network settings](#) for the machine network adapters or choose DHCP auto configuration.

#### Note

Network settings are available only with the Acronis Cyber Protect 15 Advanced and Acronis Cyber Protect 15 Backup Advanced licenses. For a detailed feature comparison, see [this knowledge base article](#).

8. [Optional] Select how to register the media on the management server on booting up. For more information about the registration settings, see [Management server](#).
9. [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 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 that you want to include in the resulting WinPE media.
10. Choose whether you want to create ISO or WIM image or upload the media on a server (WDS or RIS).

11. 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.
12. Check your settings in the summary screen, and then click **Proceed**.
13. Burn the .ISO to CD or DVD by using a third-party tool or prepare a bootable 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
```

---

**Warning!**

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.

## 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"](#).

## Registering media on the management server

Registering bootable media enables you to manage the media via the Cyber Protect web 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). However, it is not possible to register bootable media created in macOS.

Registering the media is possible only if at least one Acronis Cyber Protect Advanced 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](#) option of Bootable Media Builder. If all the registration parameters are pre-configured, the media will appear in the Cyber Protect web 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](#).

### ***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 > Accounts**). In the Cyber Protect web 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 Cyber Protect web 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**.

## Local operations with bootable media

Operations with the bootable media are similar to the backup and recovery operations that are performed under a running operating system. The differences are as follows:

1. Under a bootable media with Windows-like volume representation, a volume has the same drive letter as in Windows. Volumes that don't have drive letters in Windows (such as the System Reserved volume) are assigned free letters in order of their sequence on the disk.  
If the bootable media cannot detect Windows on the machine or detects more than one, all volumes, including those without drive letters, are assigned letters in order of their sequence on the disk. Thus, the volume letters may differ from those seen in Windows. For example, the D: drive under the bootable media might correspond to the E: drive in Windows.

---

### Note

We recommend that you assign unique names to the volumes.

---

2. The bootable media with Linux-like volume representation shows local disks and volumes as unmounted (`sda1`, `sda2`...).
3. Backups created using bootable media have simplified file names. Standard names are assigned to the backups only if these are added to an existing archive with standard file naming or if the destination does not support simplified file names.
4. The bootable media with a Linux-like volume representation cannot write backups to an NTFS-formatted volume. Switch to a media with Windows-like volume representation if you need to do so. To toggle the bootable media volume representations, click **Tools > Change volume representation**.
5. Tasks cannot be scheduled. If you need to repeat an operation, configure it from scratch.
6. The log lifetime is limited to the current session. You can save the entire log or the filtered log entries to a file.

7. Centralized vaults are not displayed in the folder tree of the **Archive** window.

To access a managed vault, type the following string in the **Path** field:

**bsp://node\_address/vault\_name/**

To access an unmanaged centralized vault, type the full path to the vault's folder.

After entering access credentials, you will see a list of archives located in the vault.

## Setting up a display mode

When you boot a machine via Linux-based bootable media, a display video mode is detected automatically based on the hardware configuration (monitor and graphics card specifications). If the video mode is detected incorrectly, do the following:

1. In the boot menu, press F11.
2. On the command line, enter the following: **vga=ask**, and then proceed with booting.
3. From the list of supported video modes, choose the appropriate one by typing its number (for example, **318**), and then press **Enter**.

If you don't want to follow this procedure every time you boot a given hardware configuration, re-create the bootable media with the appropriate mode number (in the example above, **vga=0x318**) typed in the **Kernel parameters** window.

## Backup with bootable media on-premises

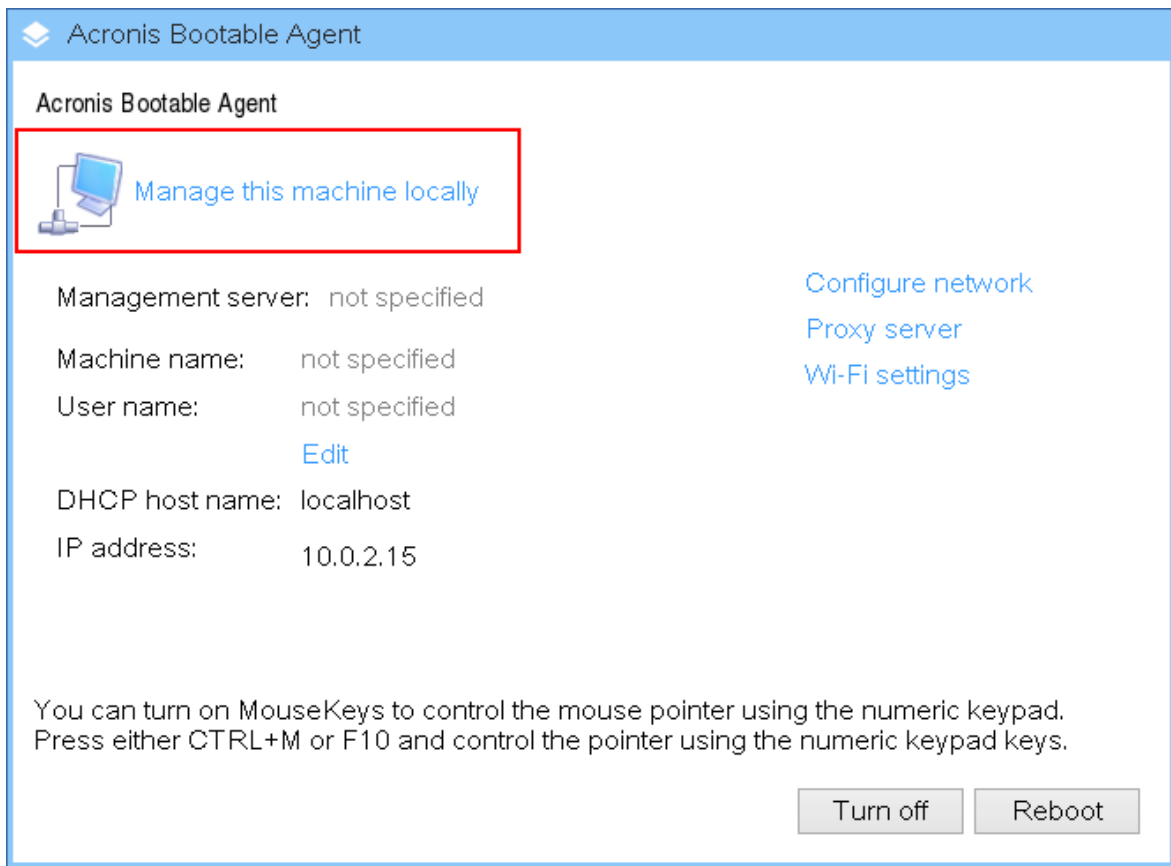
You can back up data only with a bootable media that you have created with Bootable Media Builder, and by using your Acronis Cyber Protect license key. For more information about how to create a bootable media, refer to [Linux-based bootable media](#) or [Windows-PE based bootable media](#), respectively.

***To backup up data under bootable media***

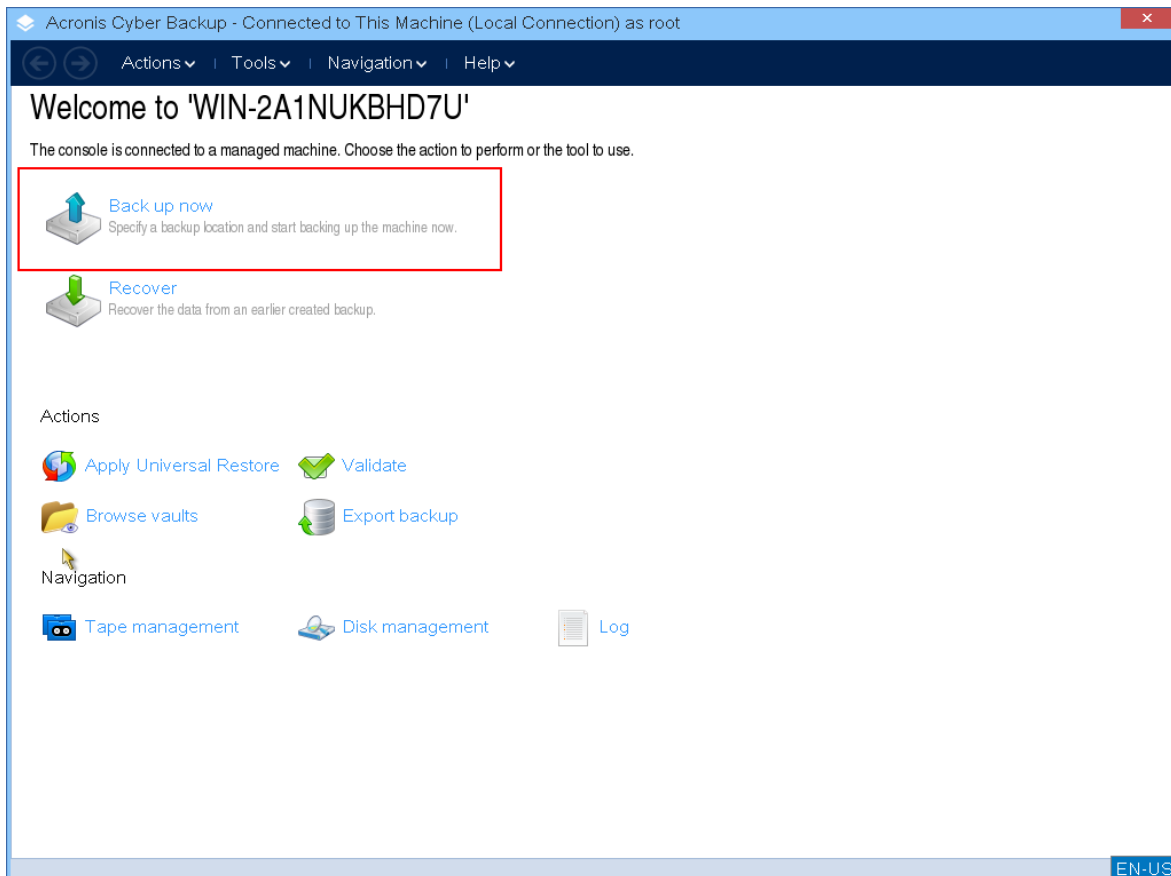
1. Boot from Acronis bootable rescue media.



2. To back up the local machine, click **Manage this machine locally**. For remote connections, refer to [Registering media on the management server](#).



3. Click **Back up now**.

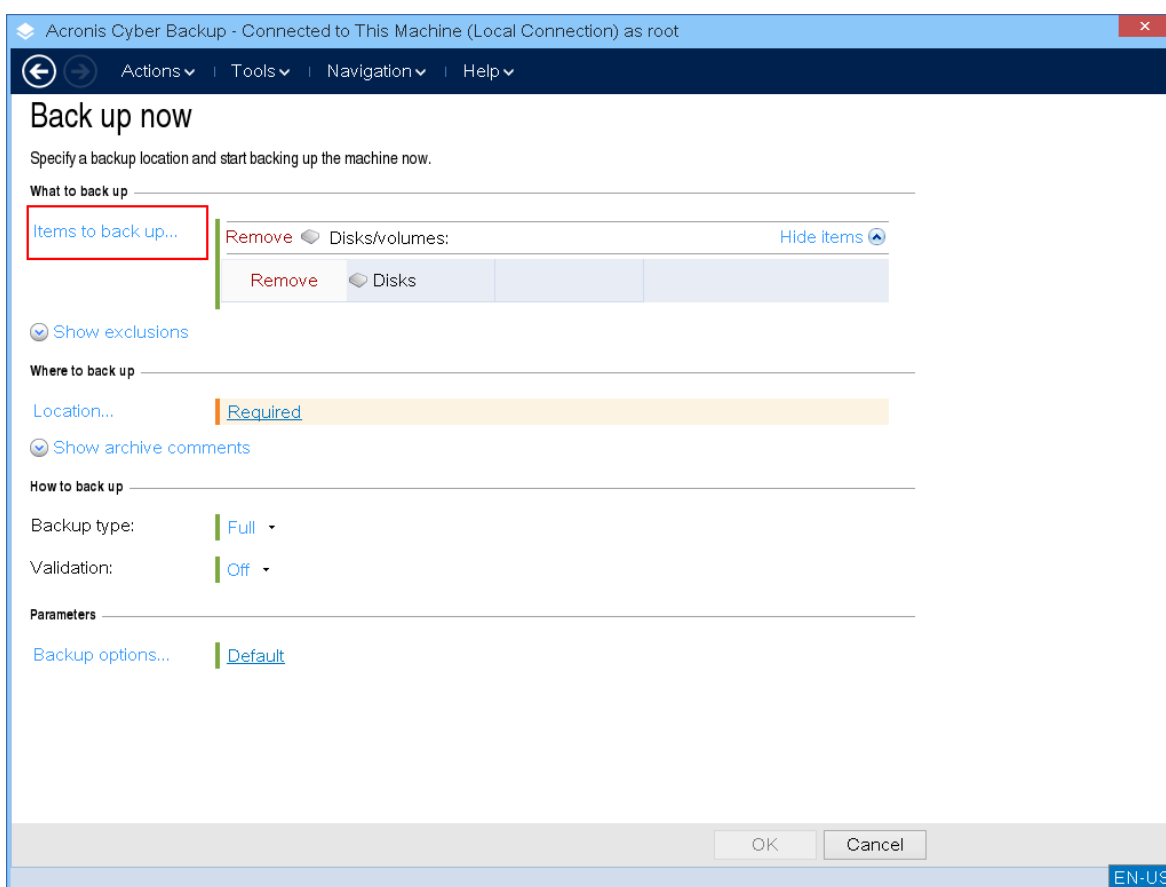




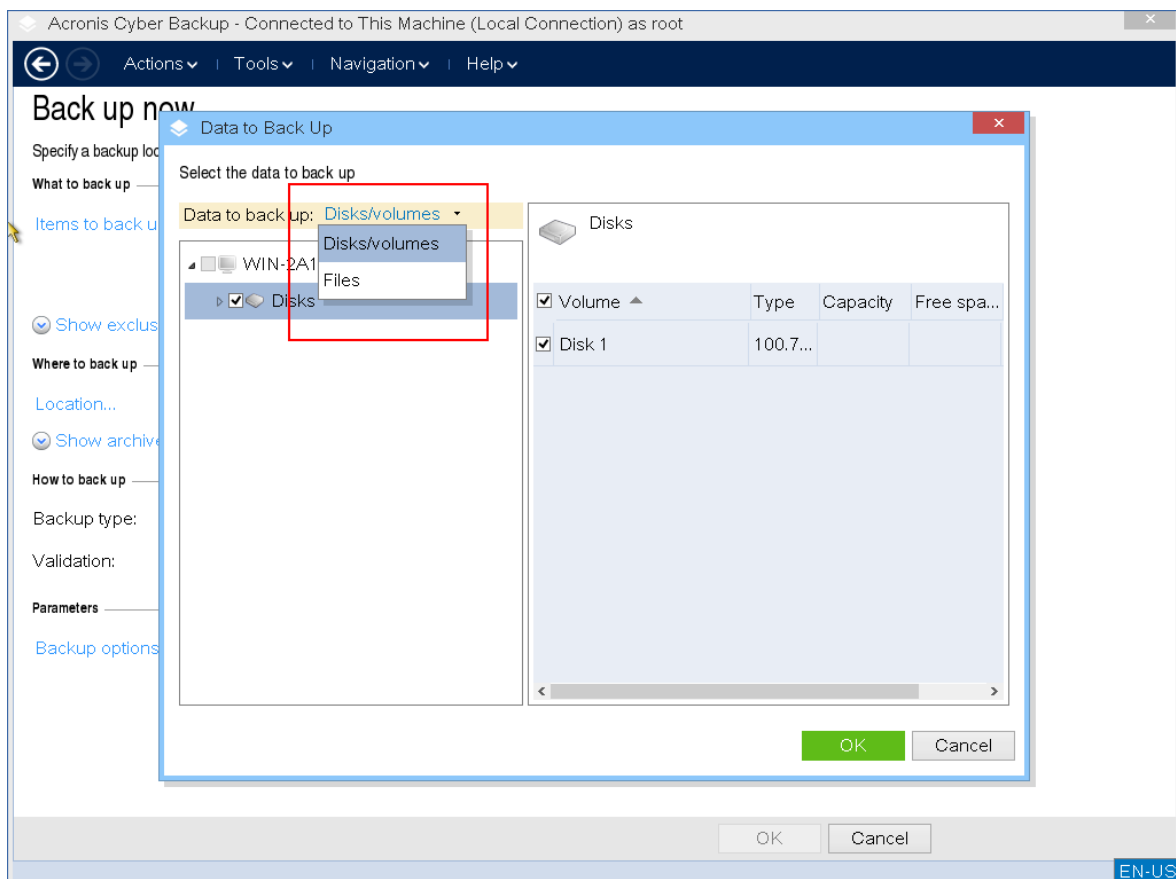
4. All non-removable disks of the machine are automatically selected for backup. To change the data that will be backed up, click **Items to backup**, and then select the desired disks or volumes. When selecting data to back up, you may see the following message: *"This machine cannot be selected directly. A previous agent version is installed on the machine. Use policy rules to select this machine for backup."* This is a GUI issue that can be safely ignored. Proceed with selecting the individual disks or volumes that you want to back up.

### Note

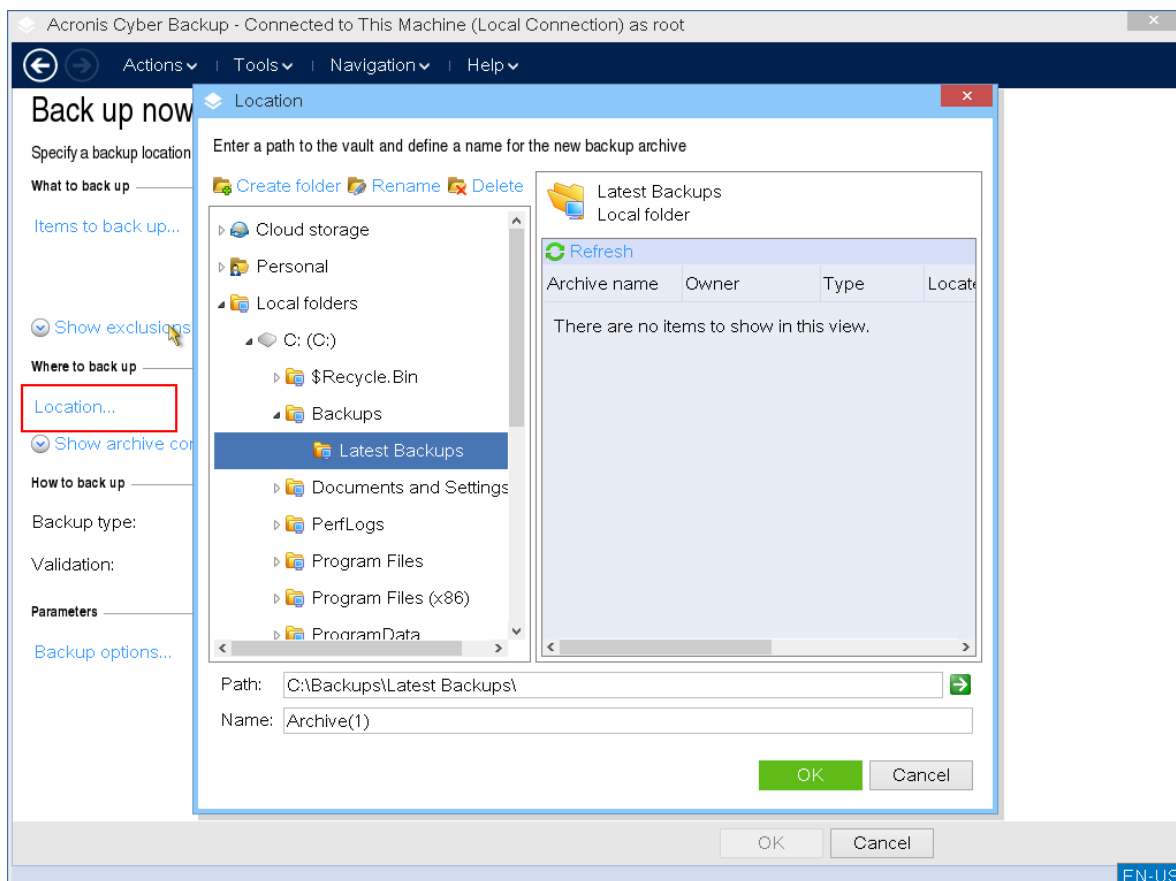
With the Linux-based bootable media you might see drive letters that are different from the ones in Windows. Try identifying the drive or partition that you need by its size or label.



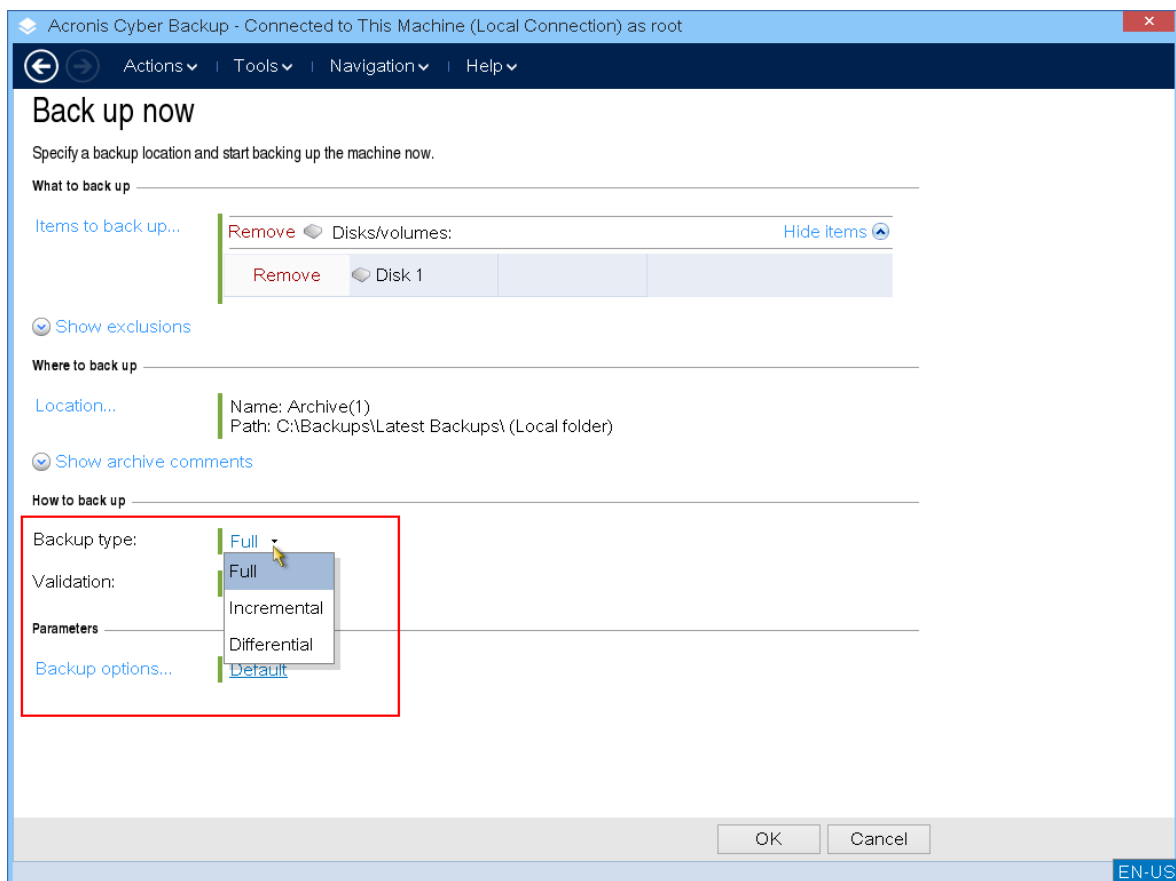
5. If you need to back up files or folders instead of disks, switch to **Files** in **Data to back up**. Only disk/partition and file/folder backup are available under bootable media. Other types of backups, such as database backup, are only available under the running operating system.



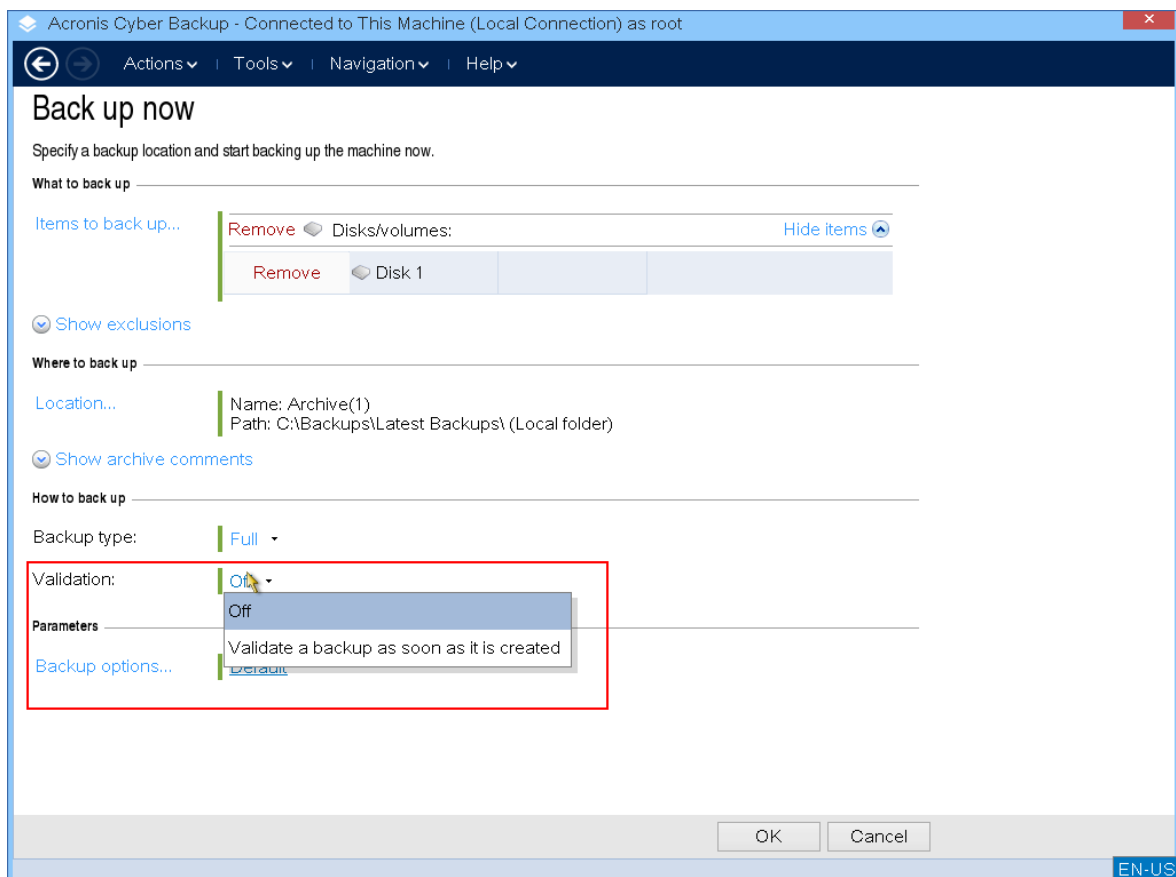
6. Click **Location** to select where the backup will be saved.



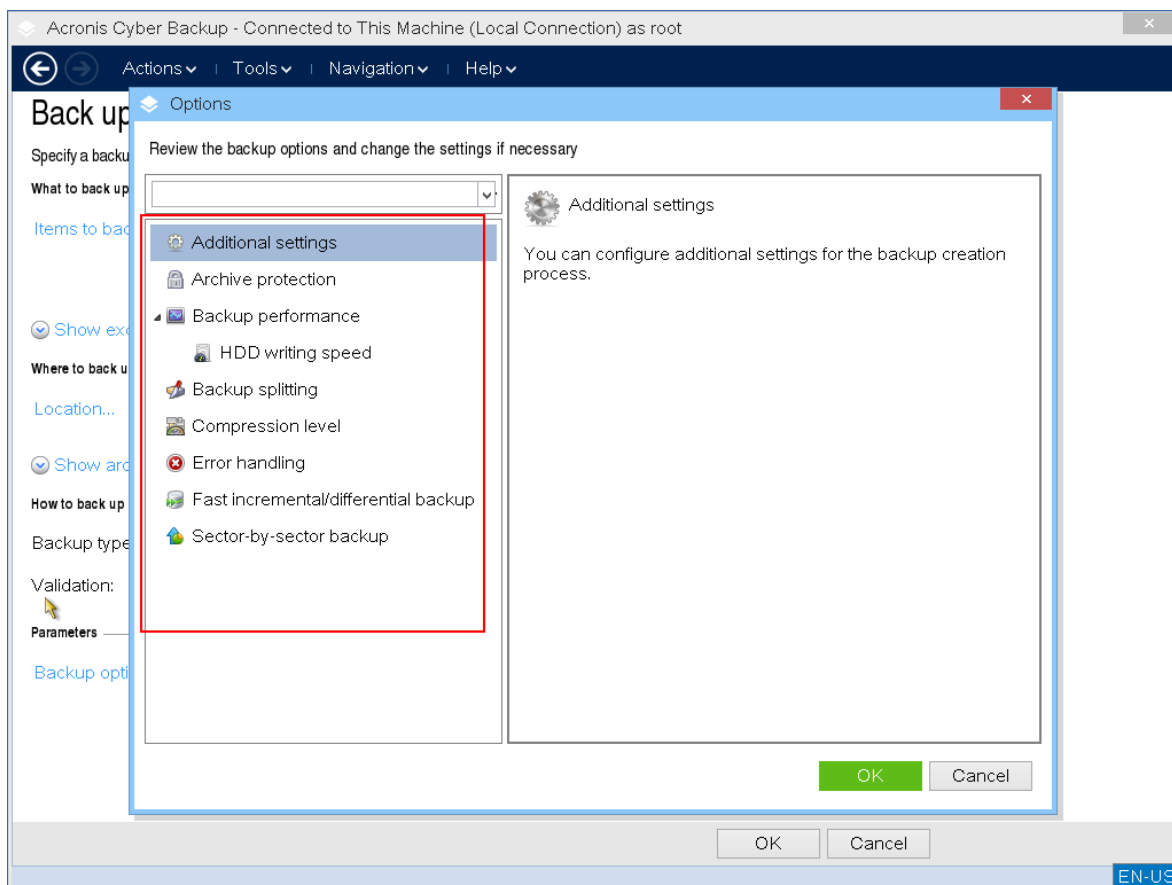
7. Specify the location and name for your backup.
8. Specify the backup type. If this is the first backup in this location, a full backup will be created. If you continue a chain of backups, you can select **Incremental** or **Differential**, to save space. For more information about the backup types, refer to <https://kb.acronis.com/content/1536>.



9. [Optional] If you want to validate the backup file, select **Validate a backup as soon as it is created**.



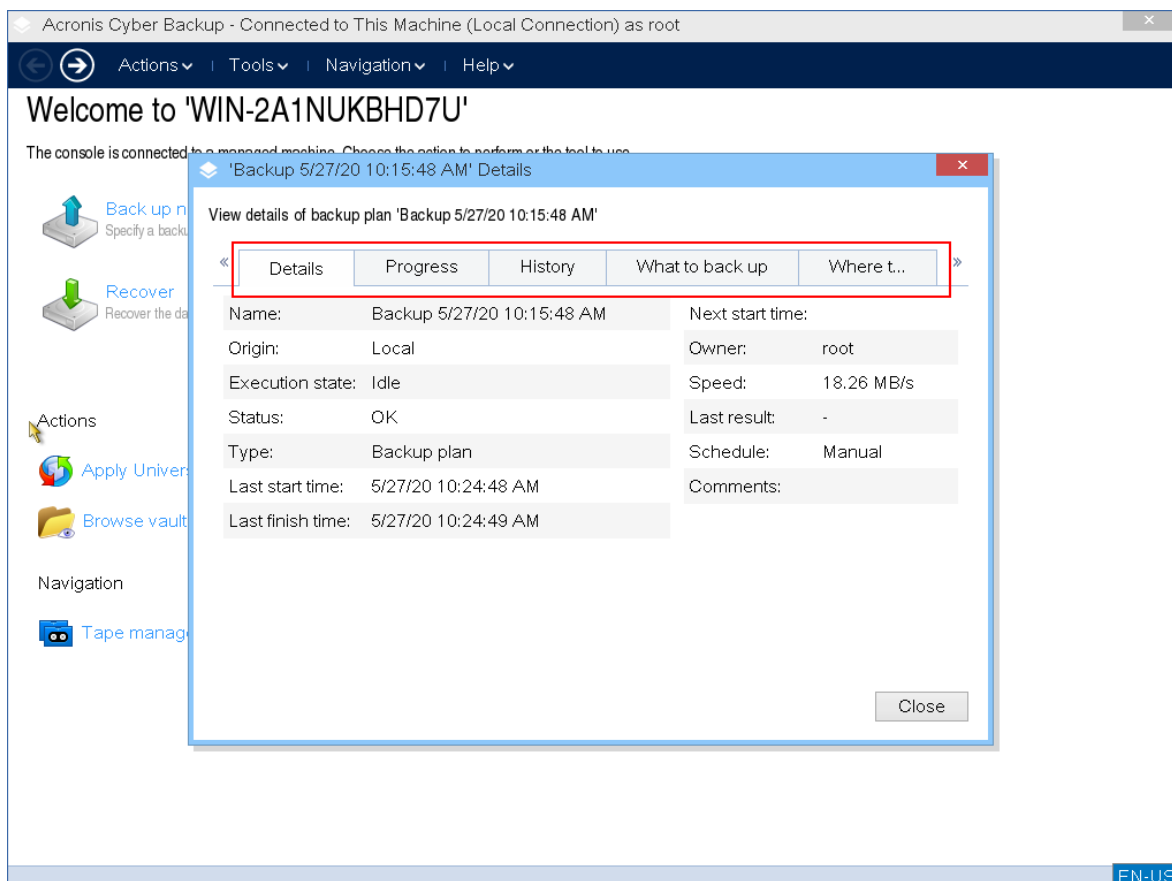
10. [Optional] Specify the backup options that you might need – such as password for the backup file, backup splitting, or error handling.



11. Click **OK** to start the backup.

The bootable media reads data from disk, compresses it into a .tib file, and then writes this file to the selected location. It does not create a disk snapshot as there are no running applications.

12. You can check the backup task status and additional information about the backup in the window that appears.

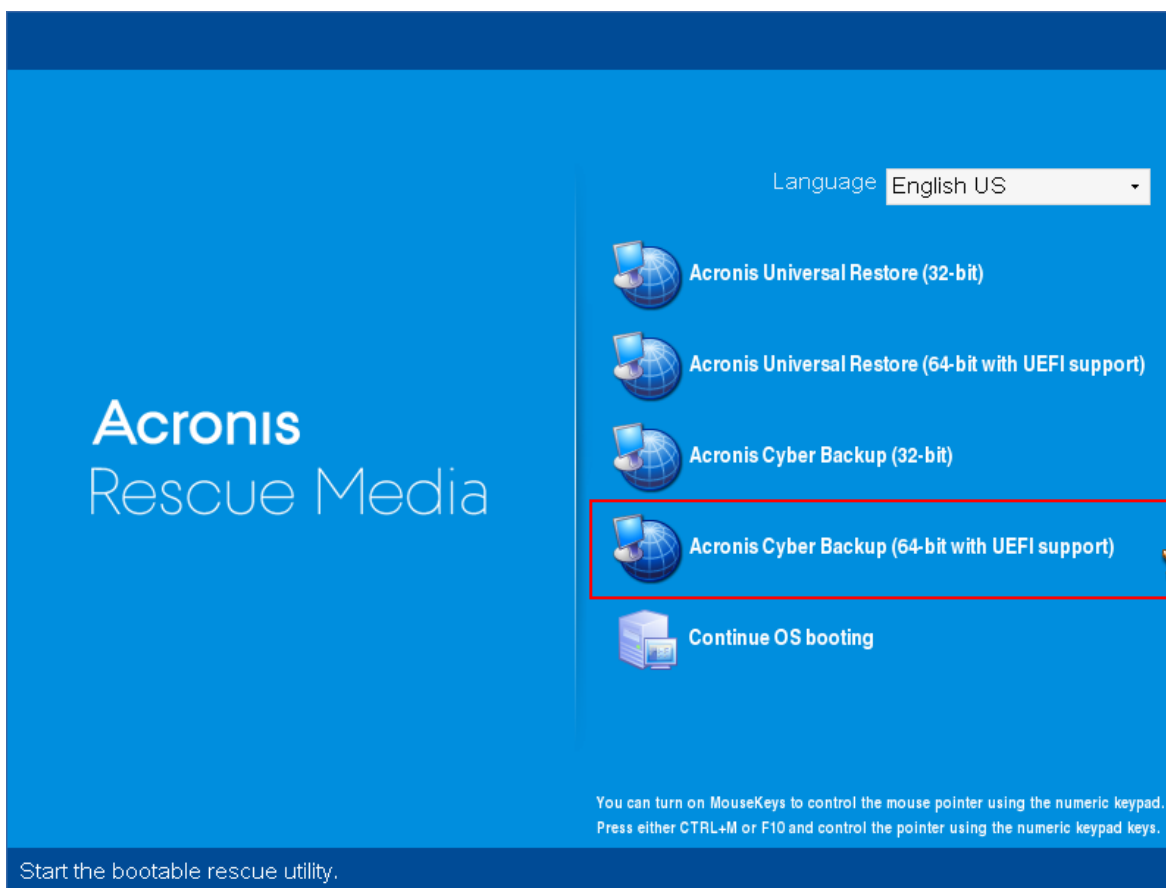


## Recovery with bootable media on-premises

The Recovery operation is available in both bootable media created with the Bootable Media Builder and downloaded ready-made bootable media.

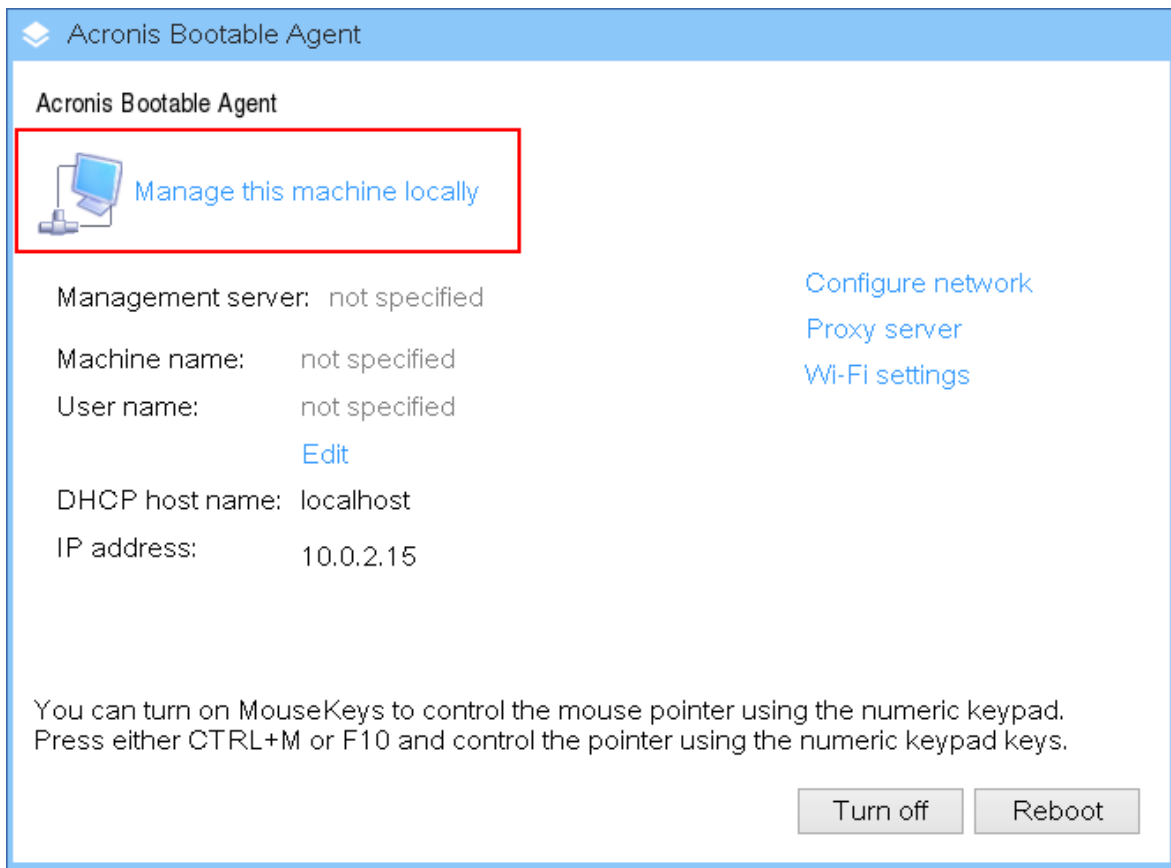
### ***To recover data under bootable media***

1. Boot from Acronis bootable rescue media.

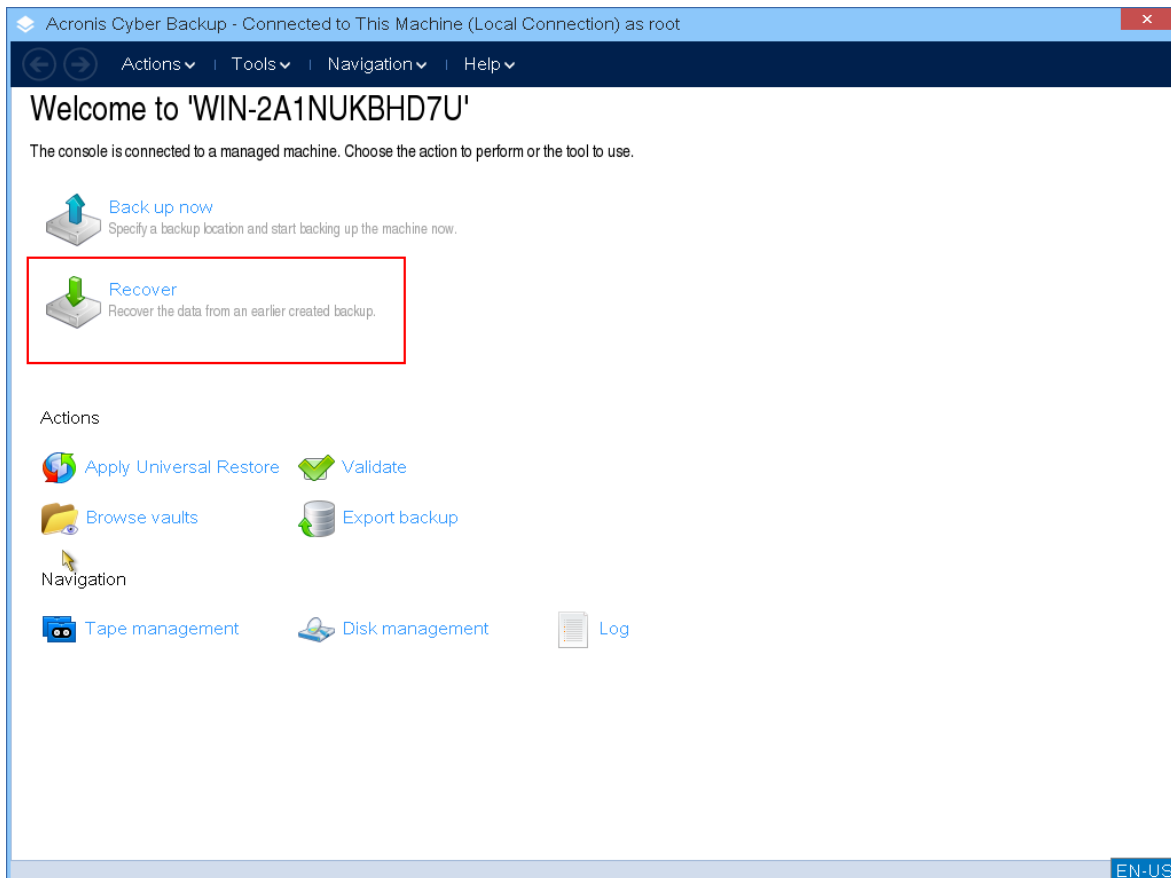


2. To recover data to the local machine, click **Manage this machine locally**. For remote connections, refer to [Registering media on the management server](#).

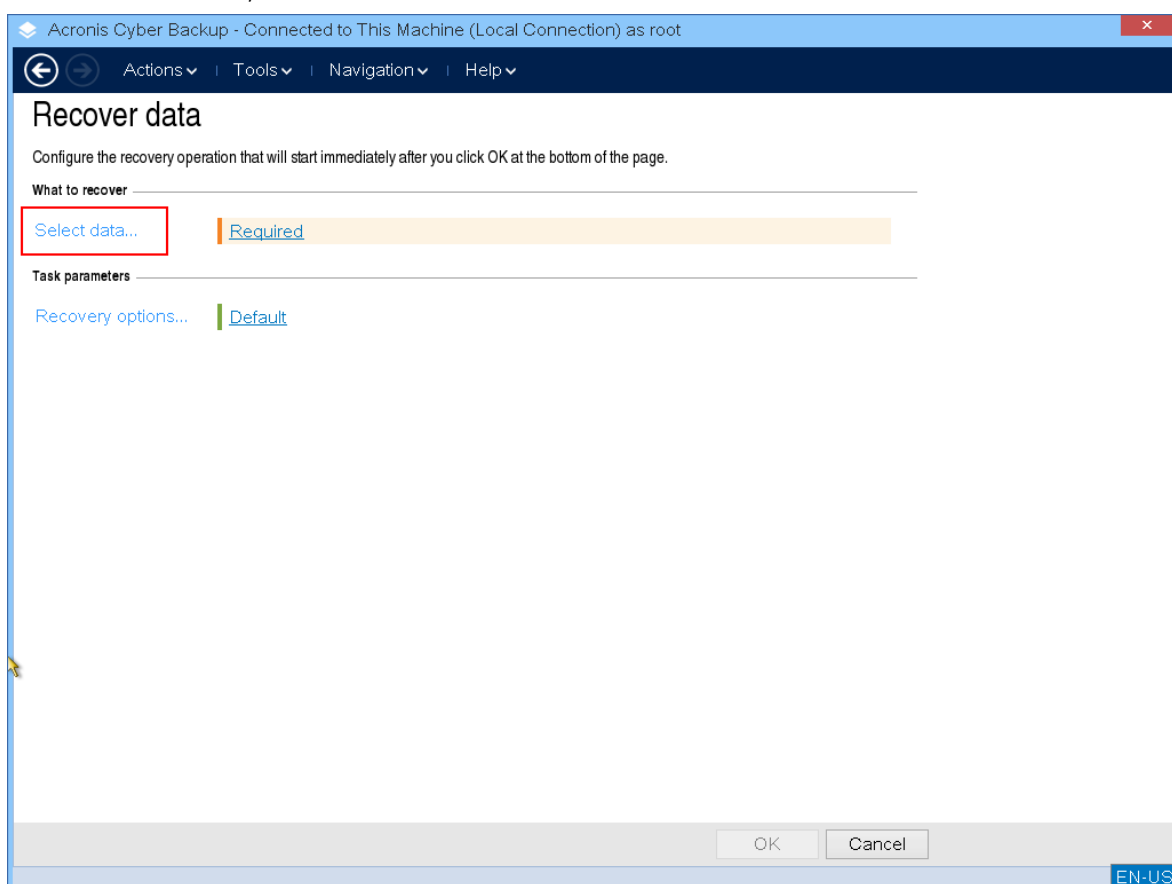




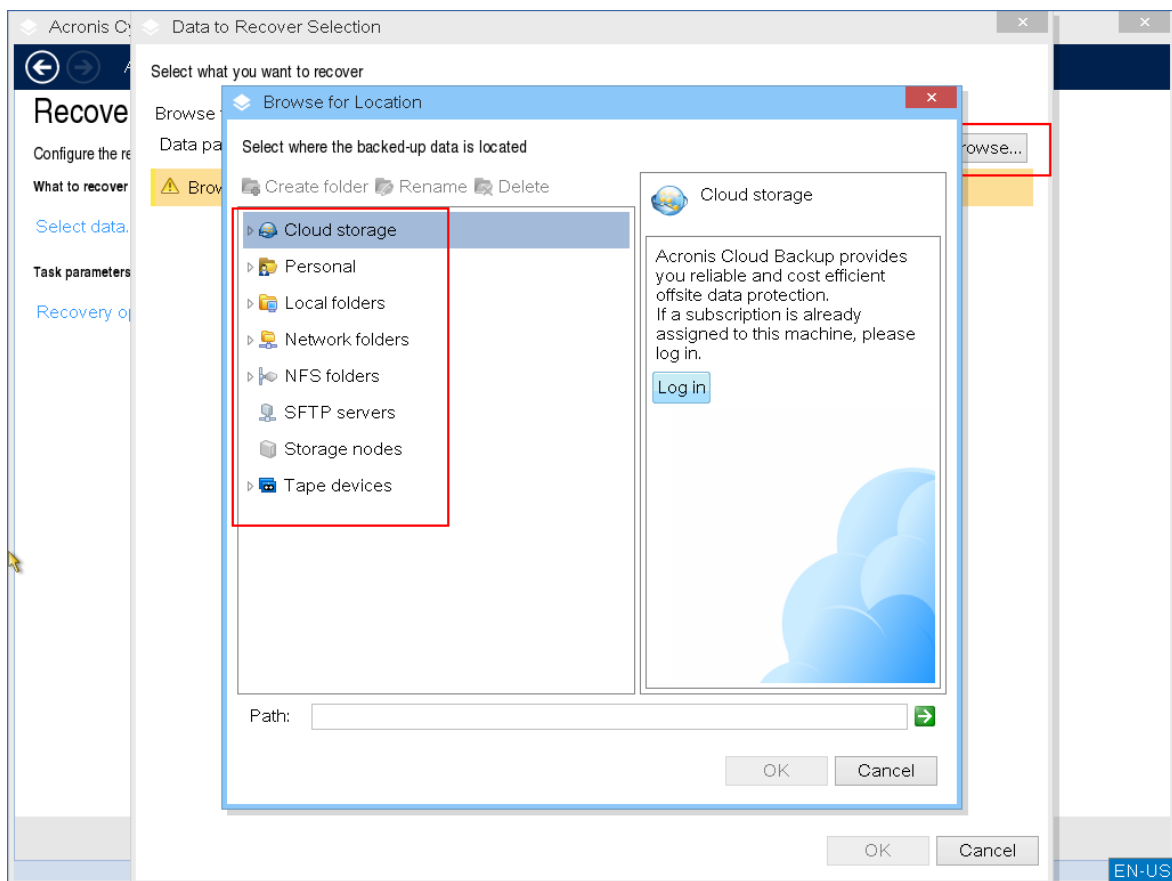
3. Click **Recover**.



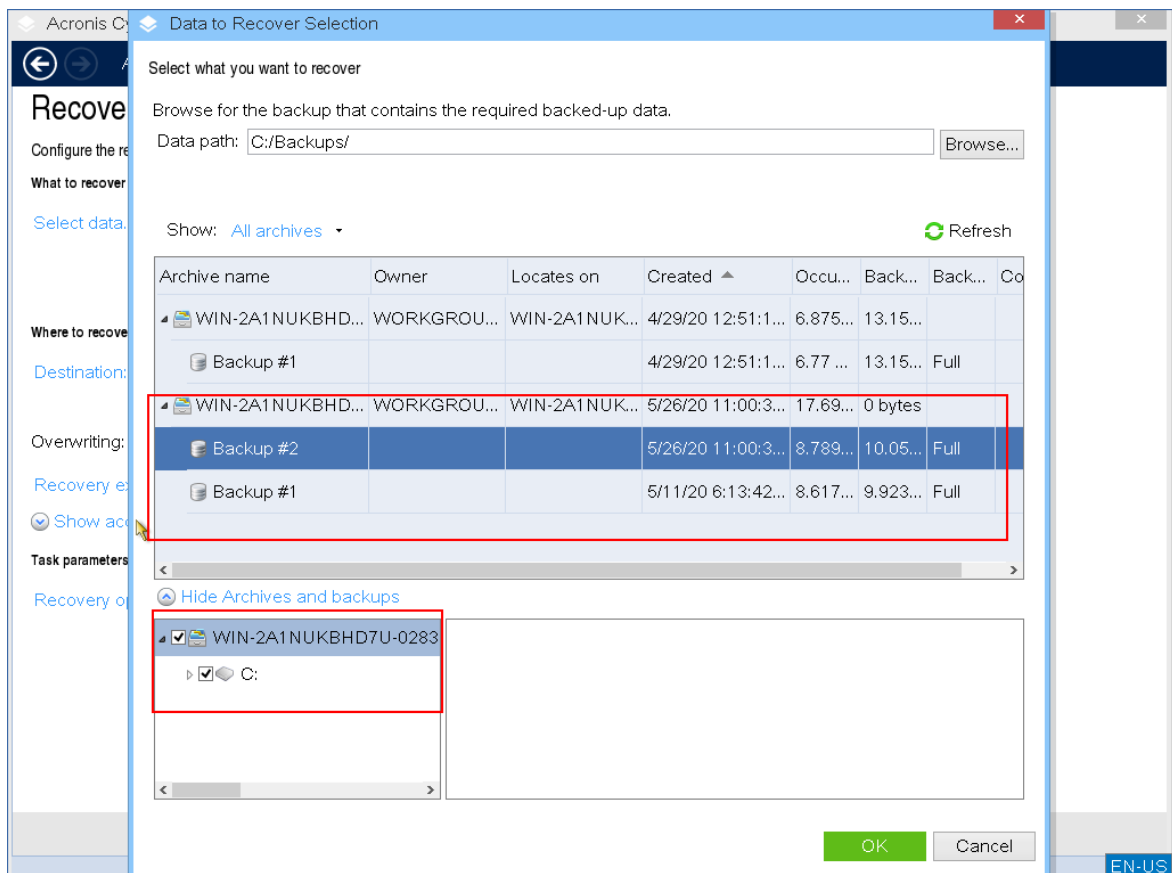
4. In **What to recover**, click **Select data**.



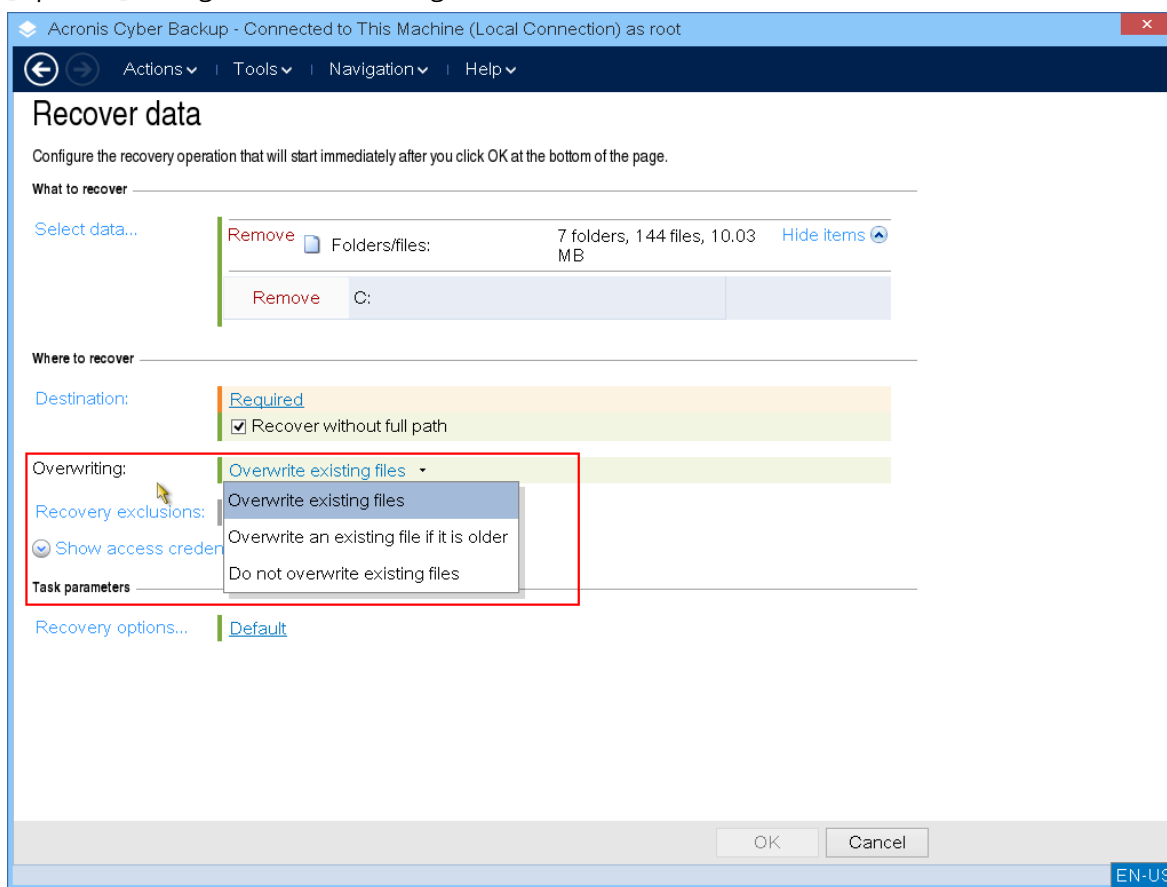
5. Click **Browse** and select the backup location.



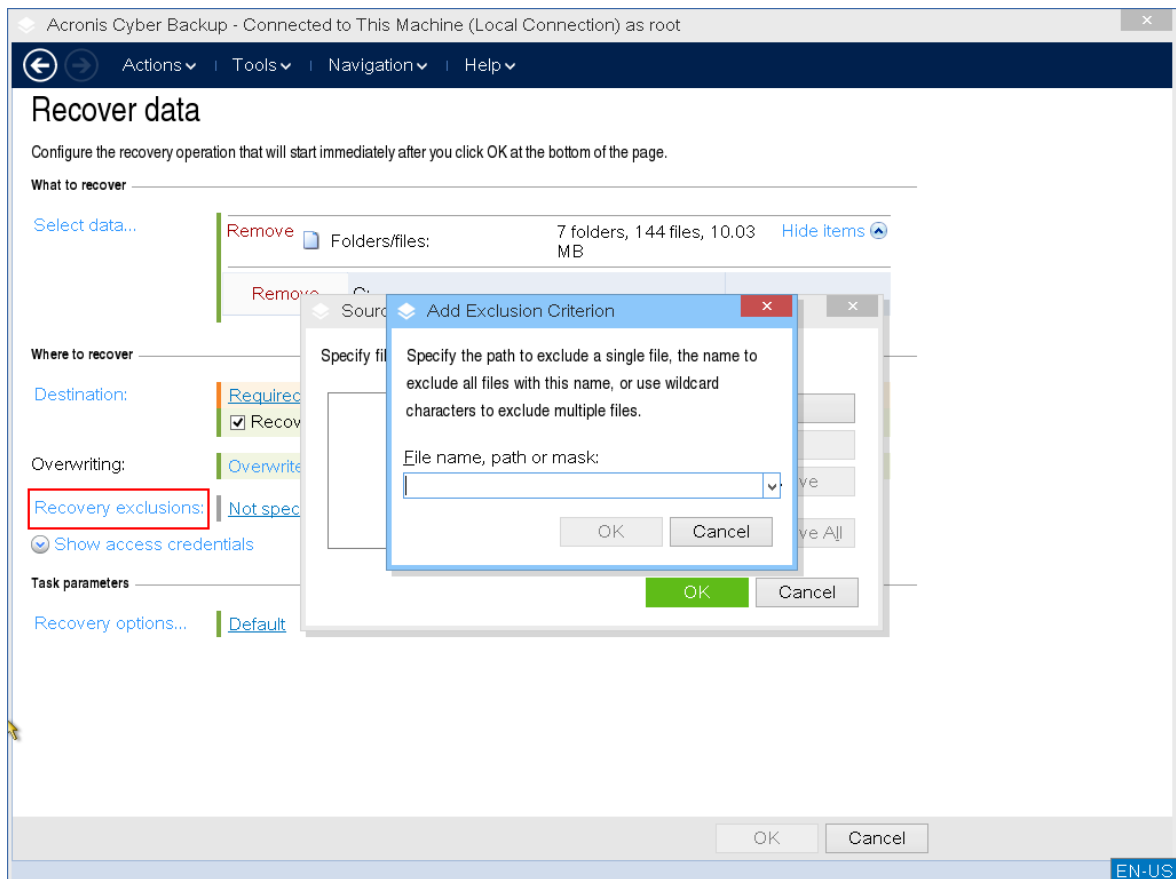
6. Select the backup file that you want to recover from.



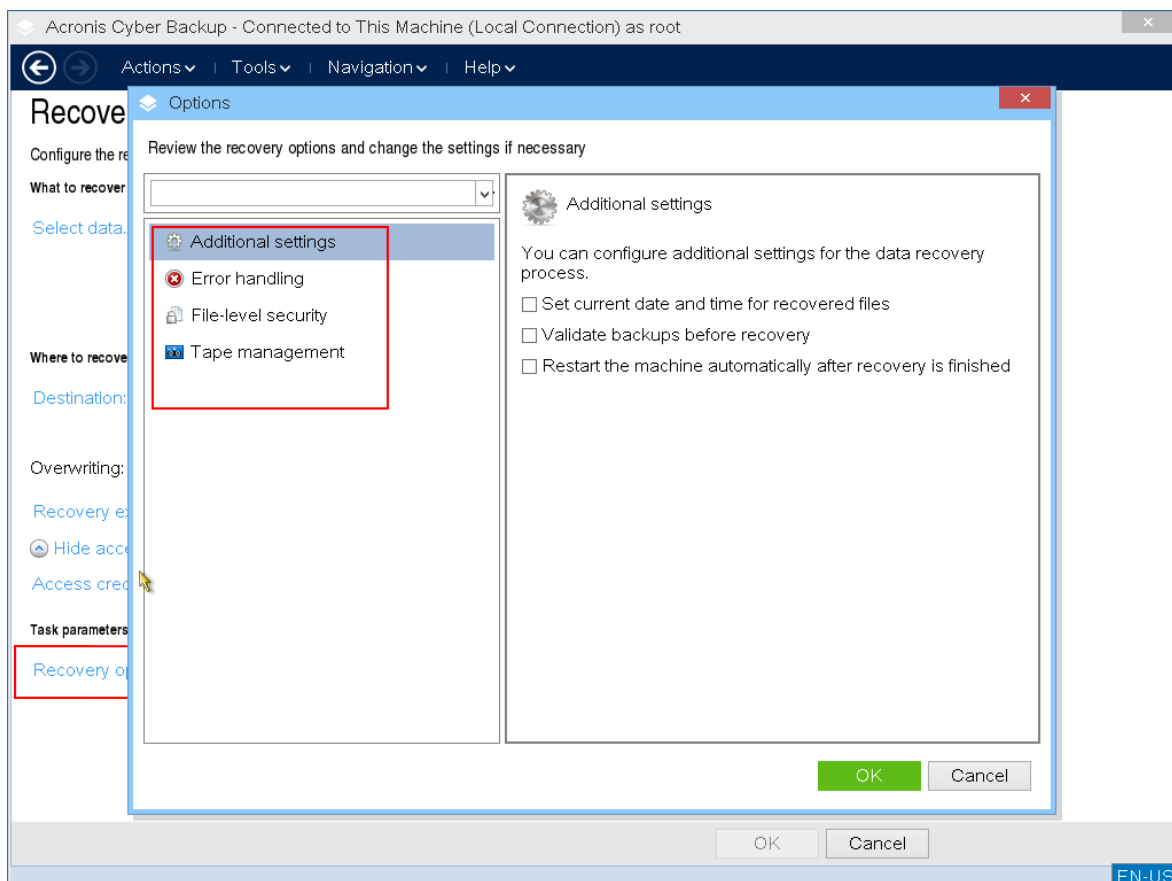
7. In the lower left pane, select the drives/volumes (or files/folders) that you want to recover, and then click **OK**.
8. [Optional] Configure the overwriting rules.



9. [Optional] Configure the recovery exclusions.



10. [Optional] Configure the recovery options.



11. Check that your settings are correct, and then click **OK**.

### Note

To recover data to dissimilar hardware, you have to use [Acronis Universal Restore](#).  
Acronis Universal Restore is not available when the backup is located in Acronis Secure Zone.

## Disk management with bootable media

With Acronis bootable media you can prepare a disk/volume configuration for recovering the volume images backed up with Acronis Cyber Protect.

Sometimes after the volume has been backed up and its image placed into a safe storage, the machine disk configuration might change due to a HDD replacement or hardware loss. In such a case, you can recreate the necessary disk configuration so that the volume image can be recovered exactly “as it was” or with some alteration of the disk or volume structure you might consider necessary.

To avoid possible data loss, take all necessary [precautions](#).

---

**Important**

All operations on disks and volumes involve a certain risk of data damage. Operations on system, bootable or data volumes must be carried out very carefully to avoid potential problems with the booting process or hard disk data storage.

Operations with hard disks and volumes take some time, and any power loss, unintentional turning off of the machine or accidental pressing of the Reset button during the procedure could result in volume damage and data loss.

---

You can perform disk management operations on a bare metal, on a machine that cannot boot or on a non-Windows machine. You will need a bootable media that you have created with Bootable Media Builder, and by using your Acronis Cyber Protect license key. For more information about how to create a bootable media, refer to [Linux-based bootable media](#) or [Windows-PE based bootable media](#), respectively.

---

**Note**

Disk management functionality is not available for bootable media based on Windows PE 4.0 and later. Thus, disk management is supported for Windows 7 and earlier operating systems. To perform disk management operations on Windows 8 and later, you need to install Acronis Disk Director. For more information, refer to this KB article: <https://kb.acronis.com/content/47031>.

---

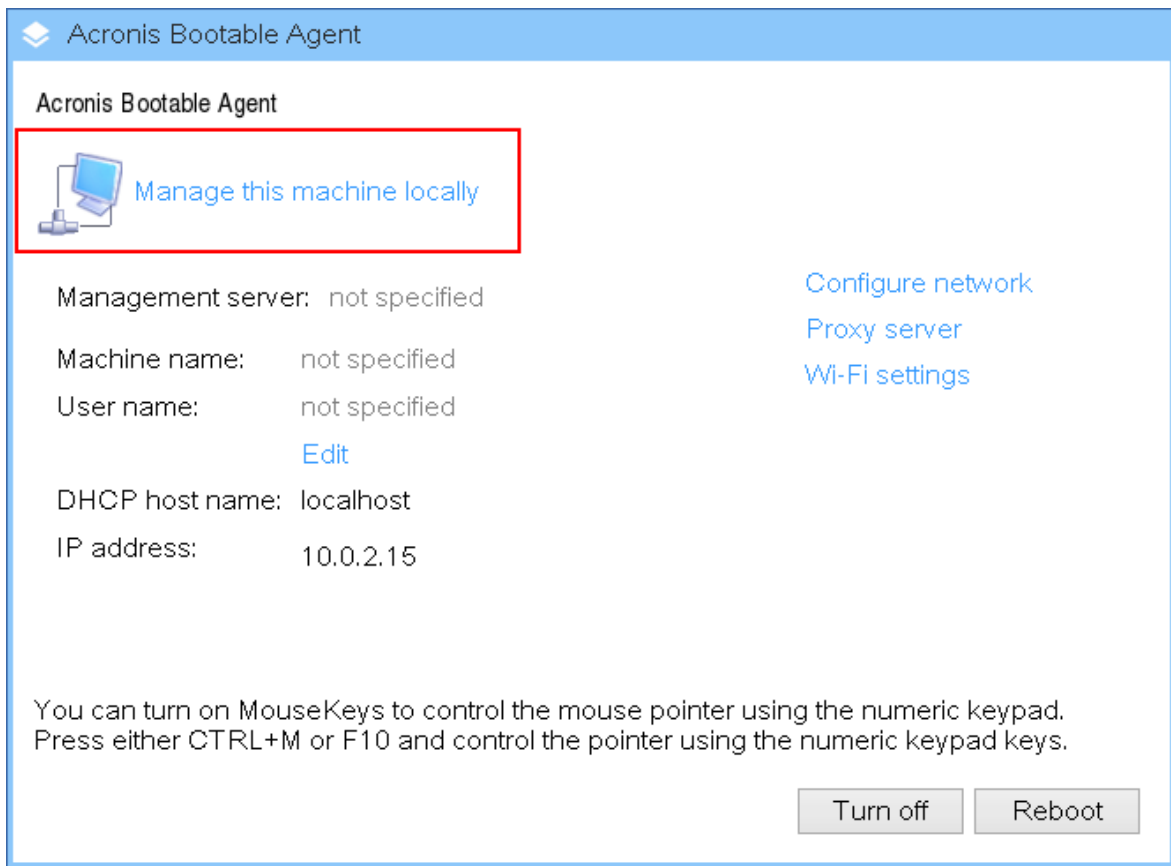
***To perform disk management operations***

1. Boot from Acronis bootable rescue media.

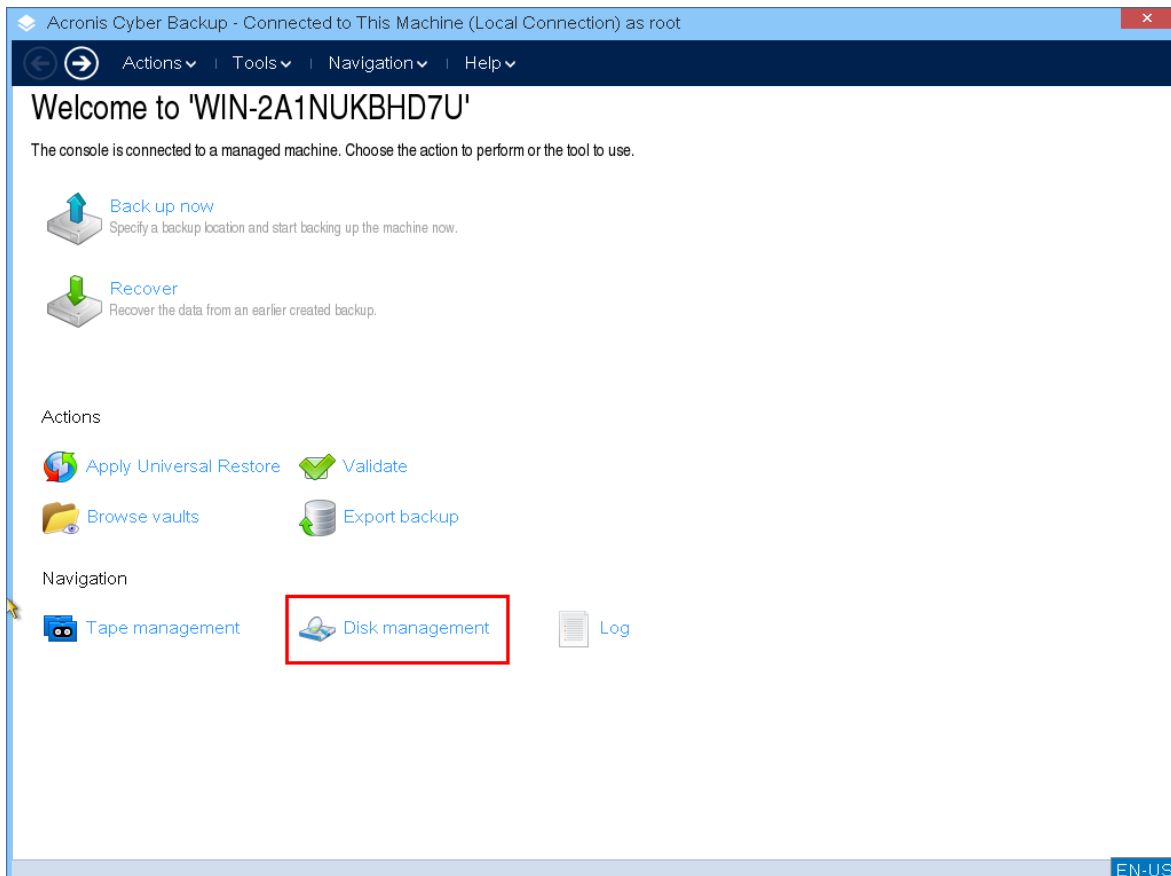


2. To work on the local machine, click **Manage this machine locally**. For remote connections, refer to [Registering media on the management server](#).





3. Click **Disk management**.



---

**Note**

Disk management operations under bootable media may work incorrectly if storage spaces are configured on the machine.

---

## Supported file systems

The bootable media supports disk management with the following file systems:

- FAT 16/32
- NTFS

If you need to perform operations on a volume with a different file system, use Acronis Disk Director. It provides more tools and utilities to manage disks and volumes with the following file systems:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

## Basic precautions

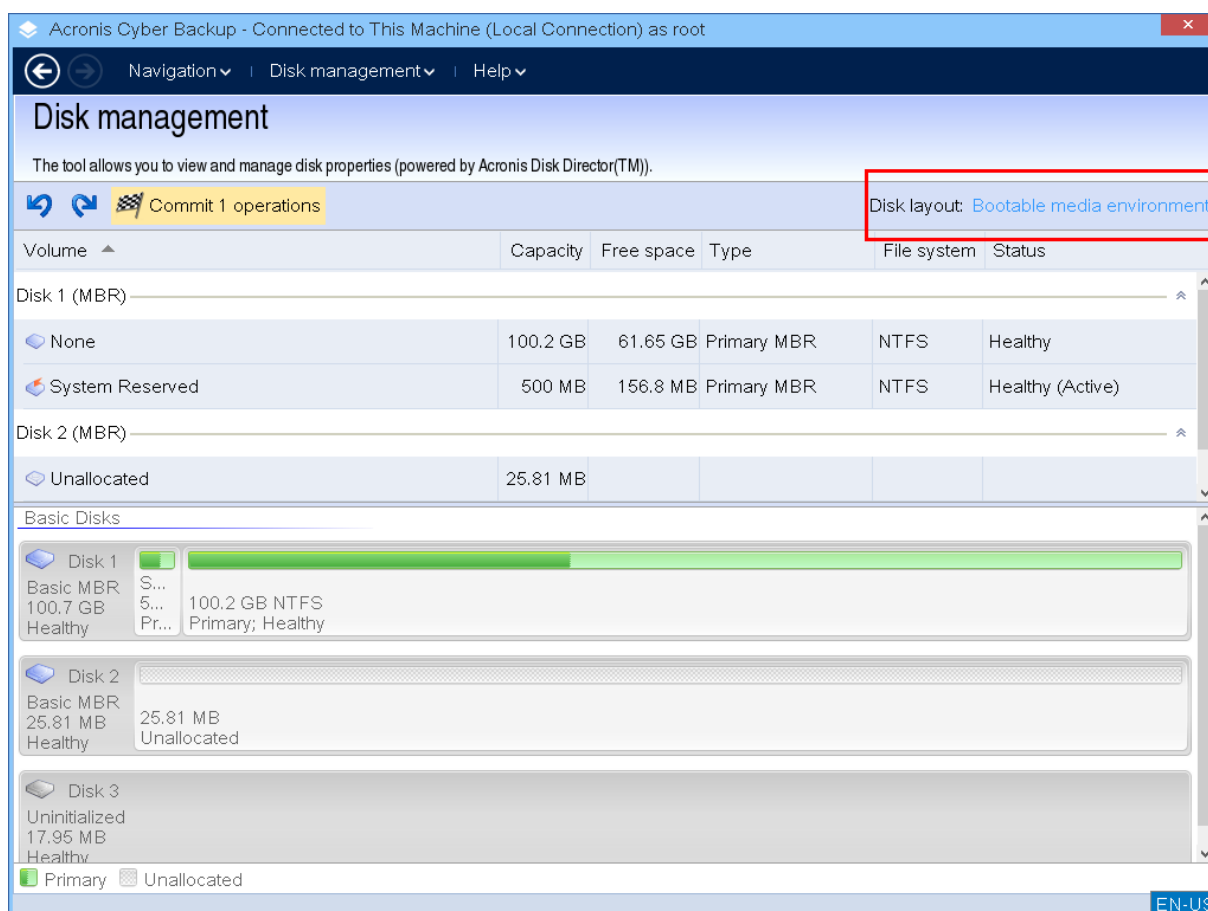
To avoid possible disk and volume structure damage or data loss, take all necessary precautions and follow these guidelines:

1. Back up the disk on which volumes will be created or managed. Having your most important data backed up to another hard disk, network share or removable media will allow you to work on disk volumes knowing that your data is safe.
2. Test your disk to make sure it is fully functional and does not contain bad sectors or file system errors.
3. Do not perform any disk/volume operations while running other software that has low-level disk access.

## Choosing the operating system for disk management

On a machine with two or more operating systems, representation of disks and volumes depends on which operating system is currently running. The same volume might have different letters under different operating systems.

When you perform a disk management operation, you have to specify disk layout for which operating system will be displayed. To do so, click the operating system name next to the **Disk layout** label and choose your desired operation system in the window that opens.



## Disk operations

With the bootable media, you can perform the following disk management operations:

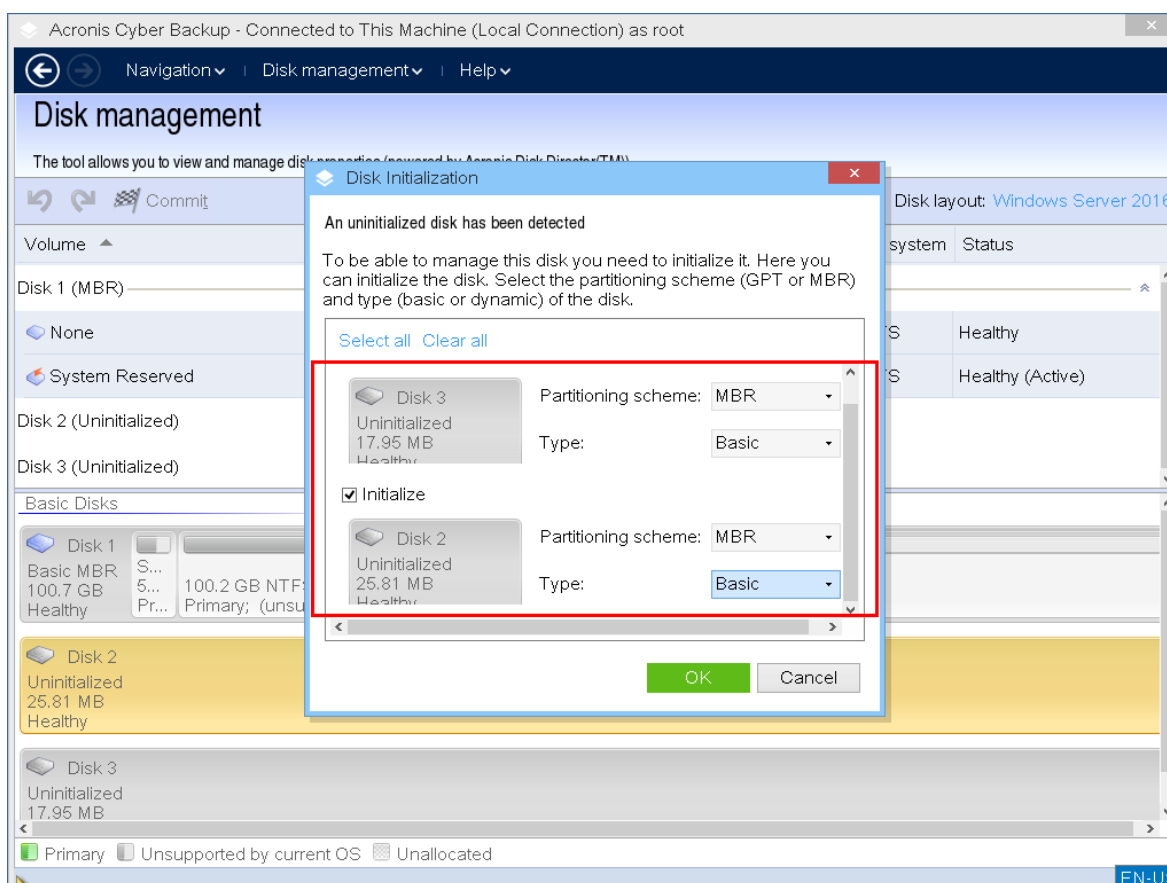
- [Disk Initialization](#) - Initializes a new hardware that was added to the system
- [Basic disk cloning](#) - Transfers complete data from a source basic MBR disk to a target disk
- [Disk conversion: MBR to GPT](#) - Converts an MBR partition table to GPT
- [Disk conversion: GPT to MBR](#) - Converts a GPT partition table to MBR
- [Disk conversion: Basic to Dynamic](#) - Converts a basic disk to dynamic
- [Disk conversion: Dynamic to Basic](#) - Converts a dynamic disk to basic

## Disk initialization

The bootable media shows a non-initialized disk as a gray block with a grayed icon, thus indicating that the disk is unusable by the system.

### **To initialize a disk**

1. Right-click the desired disk, and then click **Initialize**.
2. In the **Disk Initialization** window, set the disk partitioning scheme (MBR or GPT) and the disk type (basic or dynamic).
3. By clicking **OK**, you will add a pending operation of disk initialization.
4. To complete the added operation, [commit](#) it. Exiting the program without committing the operation will effectively cancel it.
5. After the initialization, the disk space remains unallocated. To be able to use it, you need to [create a volume](#) on it.



## Basic disk cloning

With a full-featured Linux-based bootable media, you can clone basic MBR disks. Disk cloning is not available in the ready-made bootable media that you can download or in a bootable media that is created without a license key.

### Note

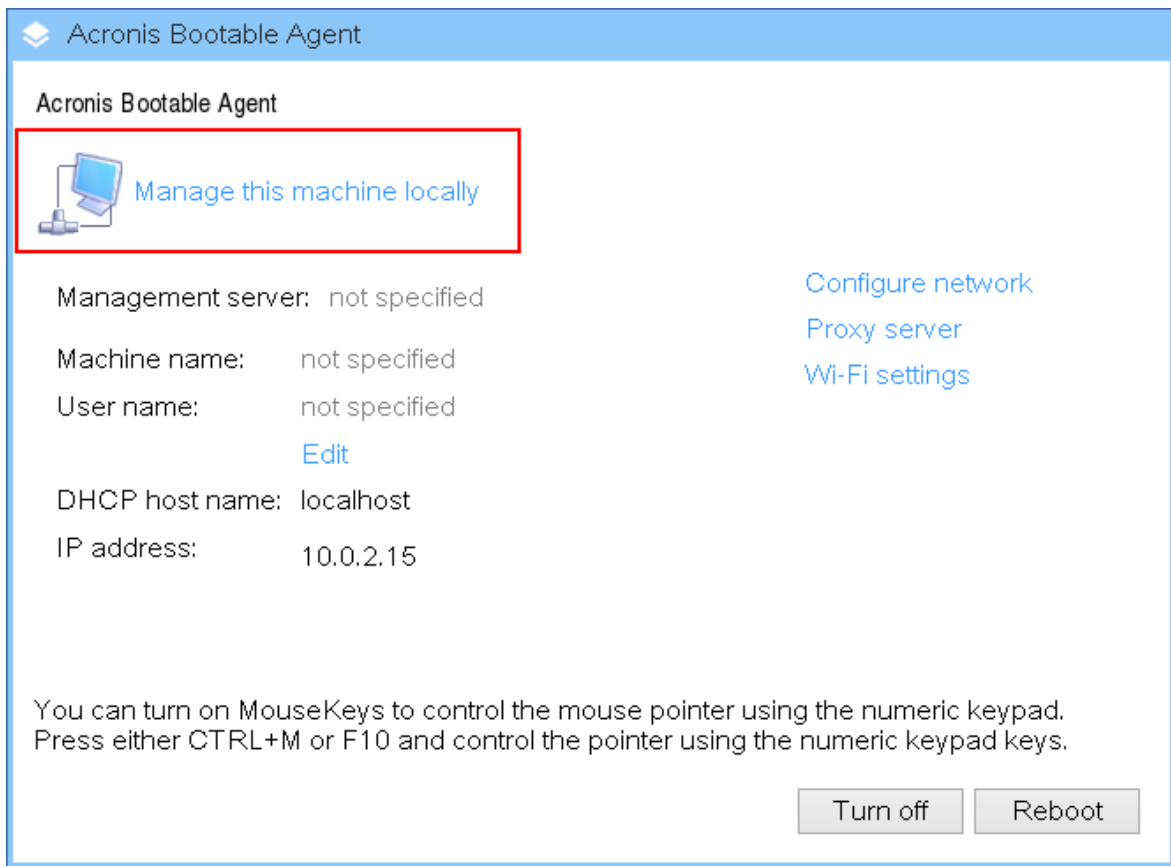
You can also clone disks by using the [Acronis Cyber Protect Command-Line utility](#).

### *To clone basic disks under bootable media*

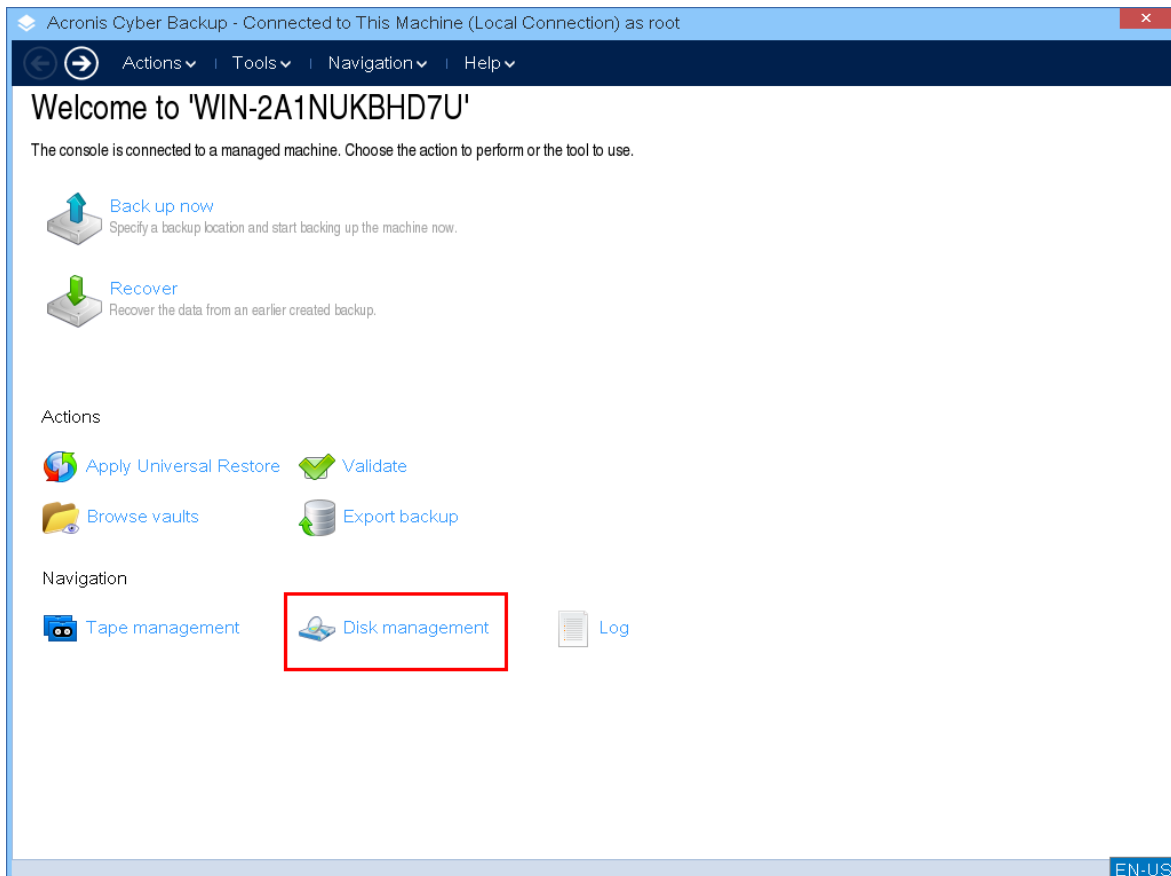
1. Boot from Acronis bootable rescue media.



2. To clone a disk of the local machine, click **Manage this machine locally**. For remote connection, refer to [Registering media on the management server](#).



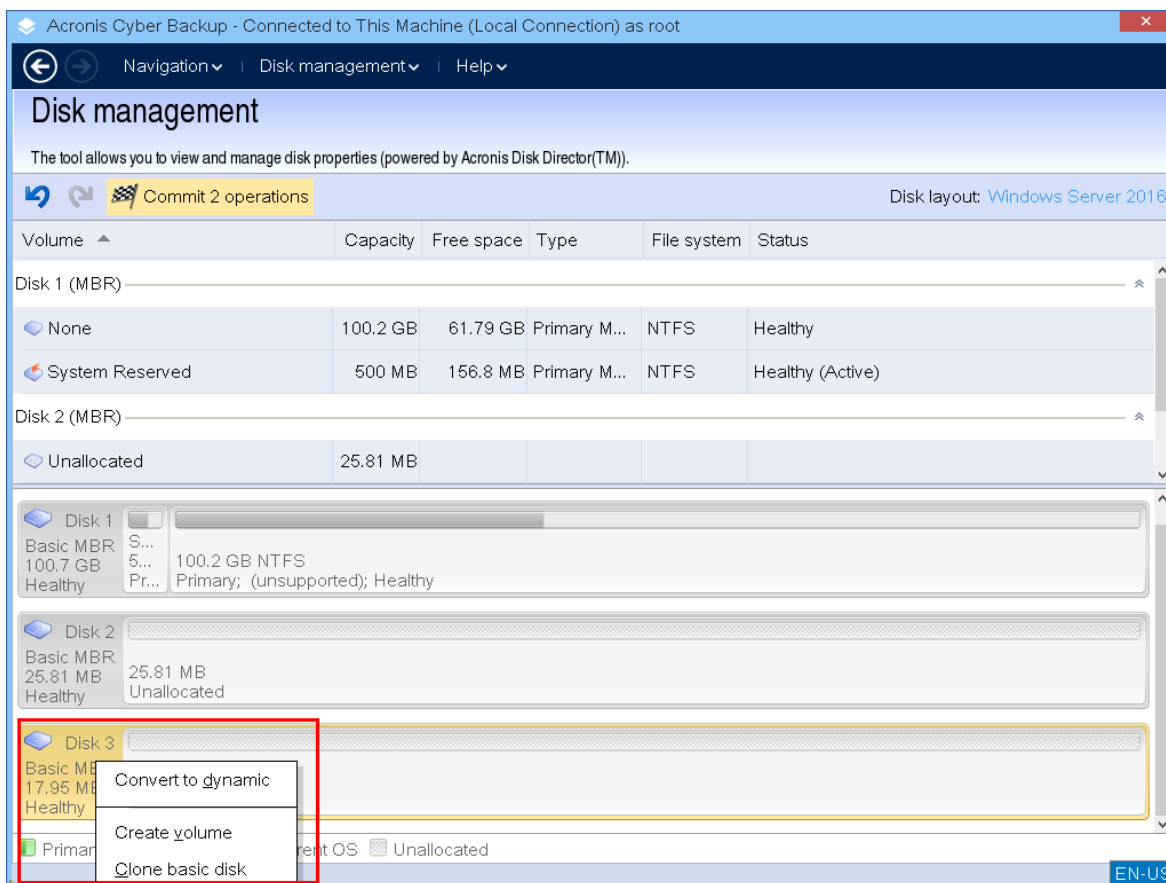
3. Click **Disk management**.



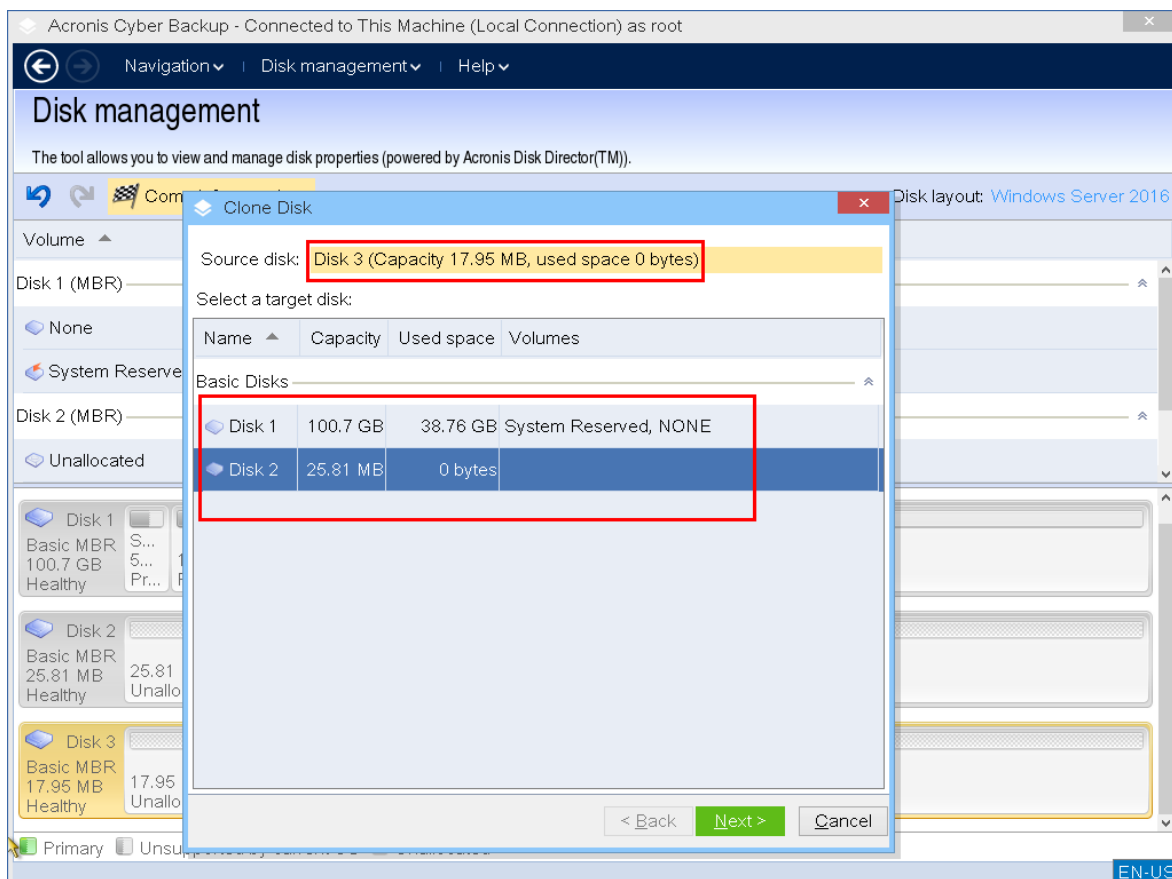
- The available disks are displayed. Right-click the disk that you want to clone, and then click **Clone basic disk**.

### Note

You can clone only entire disks. Partition cloning is not available.



- A list of possible target disks is displayed. The program allows you to select a target disk if it is large enough to hold all the data from the source disk without any loss. Select a target disk, and then click **Next**.

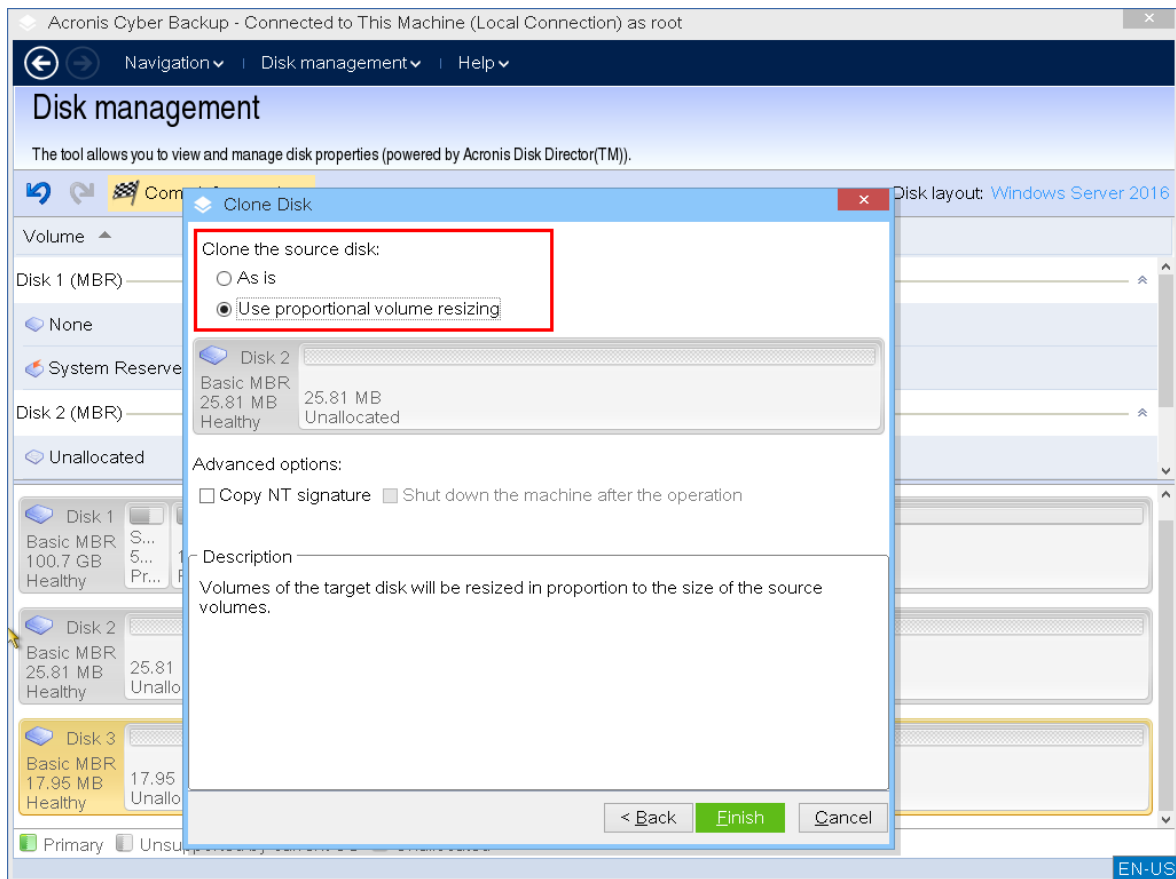


If the target disk is larger, you can clone the disk as is or resize the source disk volumes proportionally (default option), in order to avoid leaving unallocated space on the target disk. If the target disk is smaller, only proportional resizing is available. If safe cloning is impossible even with the proportional resizing, the you will not be able to continue the operation.

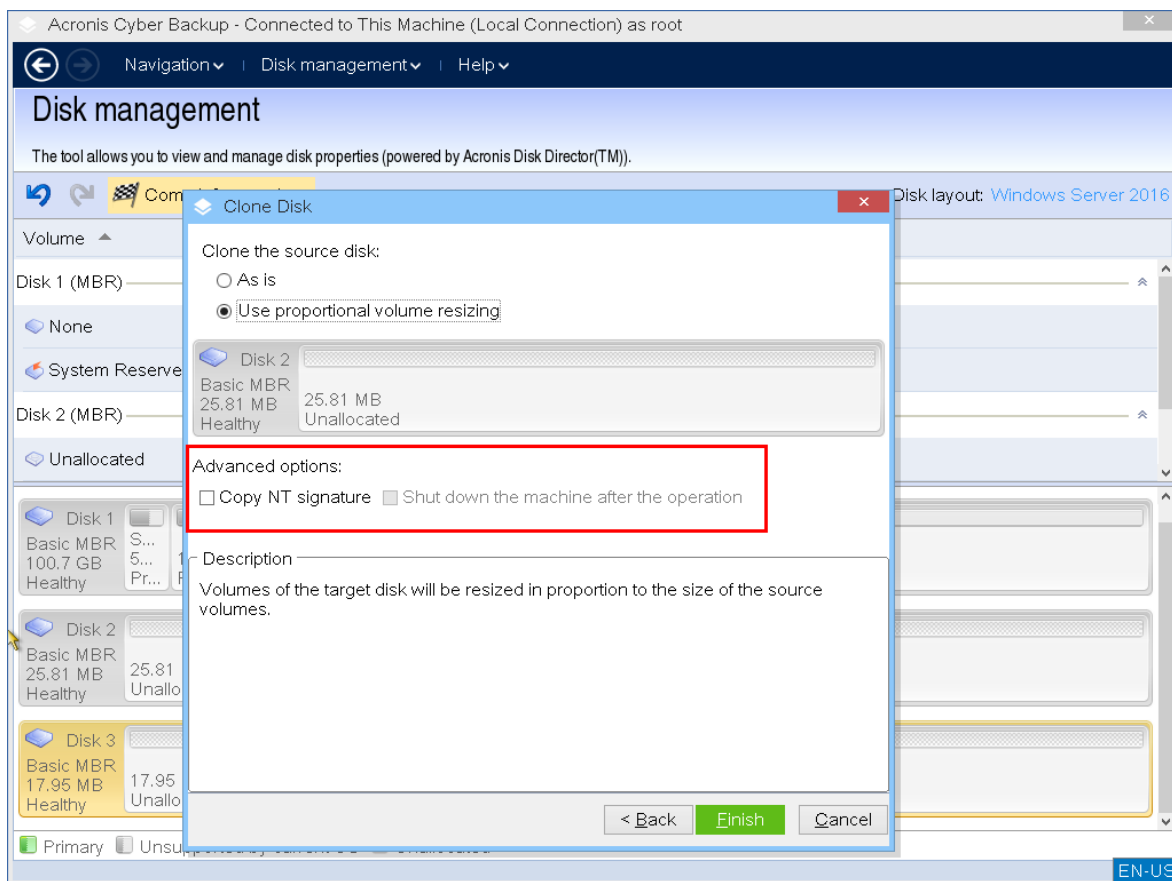
### Important

If there is data on the target disk, you will see the warning: *"The selected target disk is not empty. The data on its volumes will be overwritten."* If you proceed, all the data that is currently on the target disk will be lost irrevocably.





6. Select whether to copy the NT signature or not.



If you are cloning a disk comprising a system volume, you need to retain the operating system bootability on the target disk volume. It means that the operating system must have the system volume information (for example, volume letter) matched with the disk NT signature, which is kept in the MBR disk record. However, two disks with the same NT signature cannot work properly under one operating system.

If there are two disks with the same NT signature that comprise a system volume on a machine, at the startup the operating system runs from the first disk, discovers the same signature on the second one, and then automatically generates a new unique NT signature and assigns it to the second disk. As a result, all the volumes on the second disk will lose their letters, all paths will not be valid anymore, and programs won't find their files. The operating system on that disk will be unbootable.

To retain system bootability on the target disk volume you can:

- a. **Copy the NT signature** – provide the target disk with the source disk NT signature matched with the registry keys that will also be copied on the target disk.

To do so, select the **Copy NT signature** check box.

You will receive the warning: *"If there is an operating system on the hard disk, uninstall either the source or the target hard disk drive from your machine prior to starting the machine again. Otherwise, the OS will start from the first of the two, and the OS on the second disk will become unbootable."*

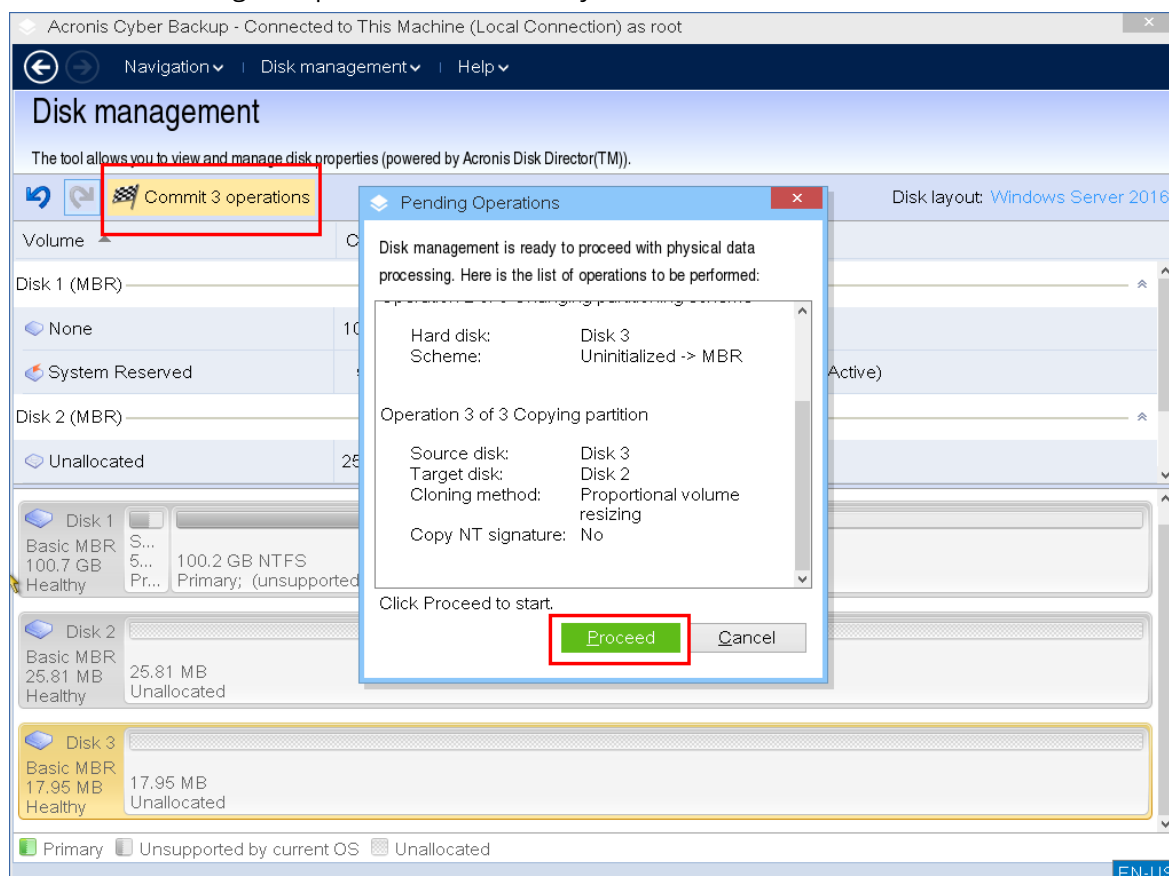
The **Shut down the machine after the operation** check box is selected and disabled automatically.

- b. **Leave the NT signature** – keep the old target disk signature and update the operating system according to the signature.

To do so, click to clear the **Copy NT signature** check box, if necessary.

The **Shut down the machine after the operation** check box will be cleared automatically.

7. Click **Finish** to add a pending operation of disk cloning.
8. Click **Commit**, and then click **Proceed** in the **Pending Operations** window. Exiting the program without committing the operation will effectively cancel it.



9. If you chose to copy the NT signature, wait until the operation is completed and the computer is turned off, and then disconnect either the source or the target hard disk drive from the machine.

## Disk conversion: MBR to GPT

You might want to convert an MBR basic disk to a GPT basic disk if you need:

- More than 4 primary volumes on one disk.
- Additional disk reliability against any possible data damage.

---

### Important

The basic MBR disk that contains the boot volume with the currently running operating system cannot be converted to GPT.

---

### *To convert a basic MBR disk to basic GPT disk*

1. Right-click the disk that you want to clone, and then click **Convert to GPT**.
2. By clicking **OK**, you will add a pending operation of MBR to GPT disk conversion.
3. To complete the added operation, [commit](#) it. Exiting the program without committing the operation will effectively cancel it.

---

**Note**

A GPT-partitioned disk reserves the space in the end of the partitioned area necessary for the backup area, which stores copies of the GPT header and the partition table. If the disk is full and the volume size cannot be automatically decreased, the conversion operation of the MBR disk to GPT will fail.

The operation is irreversible. If you have a primary volume belonging to an MBR disk and convert the disk first to GPT and then back to MBR, the volume will become logical and cannot be used as a system volume.

---

### Dynamic disk conversion: MBR to GPT

The bootable media does not support direct MBR to GPT conversion for dynamic disks. However, you can perform the following conversions to reach this goal:

1. MBR [disk conversion: dynamic to basic](#) using the **Convert to basic** operation.
2. Basic disk conversion: MBR to GPT using the **Convert to GPT** operation.
3. GPT [disk conversion: basic to dynamic](#) using the **Convert to dynamic** operation.

### Disk conversion: GPT to MBR

If you plan to install an OS that does not support GPT disks, conversion of the GPT disk to MBR is possible.

---

**Important**

The basic GPT disk that contains the boot volume with the currently running operating system cannot be converted to MBR.

---

#### ***To convert a GPT disk to MBR***

1. Right-click the disk that you want to clone, and then click **Convert to MBR**.
2. By clicking **OK**, you will add a pending operation of GPT to MBR disk conversion.
3. To complete the added operation, [commit](#) it. Exiting the program without committing the operation will effectively cancel it.

---

**Note**

After the operation, the volumes on this disk will become logical. This change is irreversible.

---

### Disk conversion: basic to dynamic

You might want to convert a basic disk to dynamic if you:

- Plan to use the disk as part of a dynamic disk group
- Want to achieve additional disk reliability for data storage

### ***To convert a basic disk to dynamic***

1. Right-click the disk that you want to convert, and then click **Convert to dynamic**.
2. Click **OK**.

The conversion will be performed immediately and your machine will be rebooted, if necessary.

---

#### **Note**

A dynamic disk occupies the last megabyte of the physical disk to store the database, including the four-level description (Volume-Component-Partition-Disk) for each dynamic volume. If during the conversion to dynamic it turns out that the basic disk is full and the size of its volumes cannot be decreased automatically, the operation will fail.

Conversion of disks comprising system volumes takes some time and any power loss, unintentional turning off of the machine or accidental pressing of the Reset button during the procedure could result in bootability loss.

---

In contrast to Windows Disk Manager, the program ensures bootability of an **offline operating system** on the disk after the operation.

### Disk conversion: dynamic to basic

You might want to convert dynamic disks back to basic ones, for example, if you want to use an operation system that does not support dynamic disks.

### ***To convert a dynamic disk to basic:***

1. Right-click the disk that you want to convert, and then click **Convert to basic**.
2. Click **OK**.

The conversion will be performed immediately and your machine will be rebooted, if necessary.

---

#### **Note**

This operation is not available for dynamic disks that contain Spanned, Striped, or RAID-5 volumes.

---

After the conversion, the last 8Mb of disk space is reserved for a future conversion of the disk from basic to dynamic. In some cases the possible unallocated space and the proposed maximum volume size might differ (for example, when the size of one mirror establishes the size of the other mirror, or the last 8Mb of disk space are reserved for the future conversion of the disk from basic to dynamic).

---

#### **Note**

Conversion of disks comprising system volumes takes some and any power loss, unintentional turning off of the machine or accidental pressing of the Reset button during the procedure could result in bootability loss.

---

In contrast to Windows Disk Manager, the program ensures:

- Safe conversion of a dynamic disk to basic when it contains volumes **with data** for simple and mirrored volumes
- In multiboot systems, bootability of a system that was **offline** during the operation

## Volume operations

With the bootable media, you can perform the following operations on volumes:

- [Create Volume](#) - Creates a new volume
- [Delete Volume](#) - Deletes the selected volume
- [Set Active](#) - Sets the selected volume active so that the machine will be able to boot with the OS installed there
- [Change Letter](#) - Changes the selected volume letter
- [Change Label](#) - Changes the selected volume label
- [Format Volume](#) - Formats a volume with the a file system

## Types of dynamic volumes

### Simple Volume

A volume created from free space on a single physical disk. It can consist of one region on the disk or several regions, virtually united by the Logical Disk Manager (LDM). It provides neither additional reliability or speed improvement, nor extra size.

### Spanned Volume

A volume created from free disk space virtually linked together by the LDM from several physical disks. Up to 32 disks can be included into one volume, thus overcoming the hardware size limitations. However, even if just one disk fails, all data will be lost. Also, no part of a spanned volume can be removed without destroying the entire volume. So, a spanned volume does not provide additional reliability or a better I/O rate.

### Striped Volume

A volume, also called RAID 0, consisting of equal sized stripes of data, written across each disk in the volume. That is, to create a striped volume, you need two or more dynamic disks. The disks in a striped volume don't have to be identical, but there must be unused space available on each disk that you want to include in the volume. The size of the volume will depend on the size of the smallest space. Access to the data on a striped volume is usually faster than access to the same data on a single physical disk, because the I/O is spread across more than one disk.

Striped volumes are created for improved performance, not for their better reliability – they don't contain redundant information.

## Mirrored Volume

A fault-tolerant volume, also called RAID 1, whose data is duplicated on two identical physical disks. All of the data on one disk is copied to another disk to provide data redundancy. Almost any volume can be mirrored, including the system and boot volumes, and if one of the disks fails, the data can still be accessed from the remaining disks. Unfortunately, the hardware limitations on size and performance are even more severe with the use of mirrored volumes.

## Mirrored-Striped Volume

A fault-tolerant volume, also sometimes called RAID 1+0, combining the advantage of the high I/O speed of the striped layout and redundancy of the mirror type. The disadvantage remains inherent with the mirror architecture – a low disk-to-volume size ratio.

## RAID-5

A fault-tolerant volume whose data is striped across an array of three or more disks. The disks don't need to be identical, but there must be equally sized blocks of unallocated space available on each disk in the volume. Parity (a calculated value that can be used to reconstruct data in case of failure) is also striped across the disk array and it is always stored on a different disk than the data itself. If a physical disk fails, the portion of the RAID-5 volume that was on that failed disk can be re-created from the remaining data and the parity. A RAID-5 volume provides reliability and is able to overcome the physical disk size limitations with a higher than mirrored disk-to-volume size ratio.

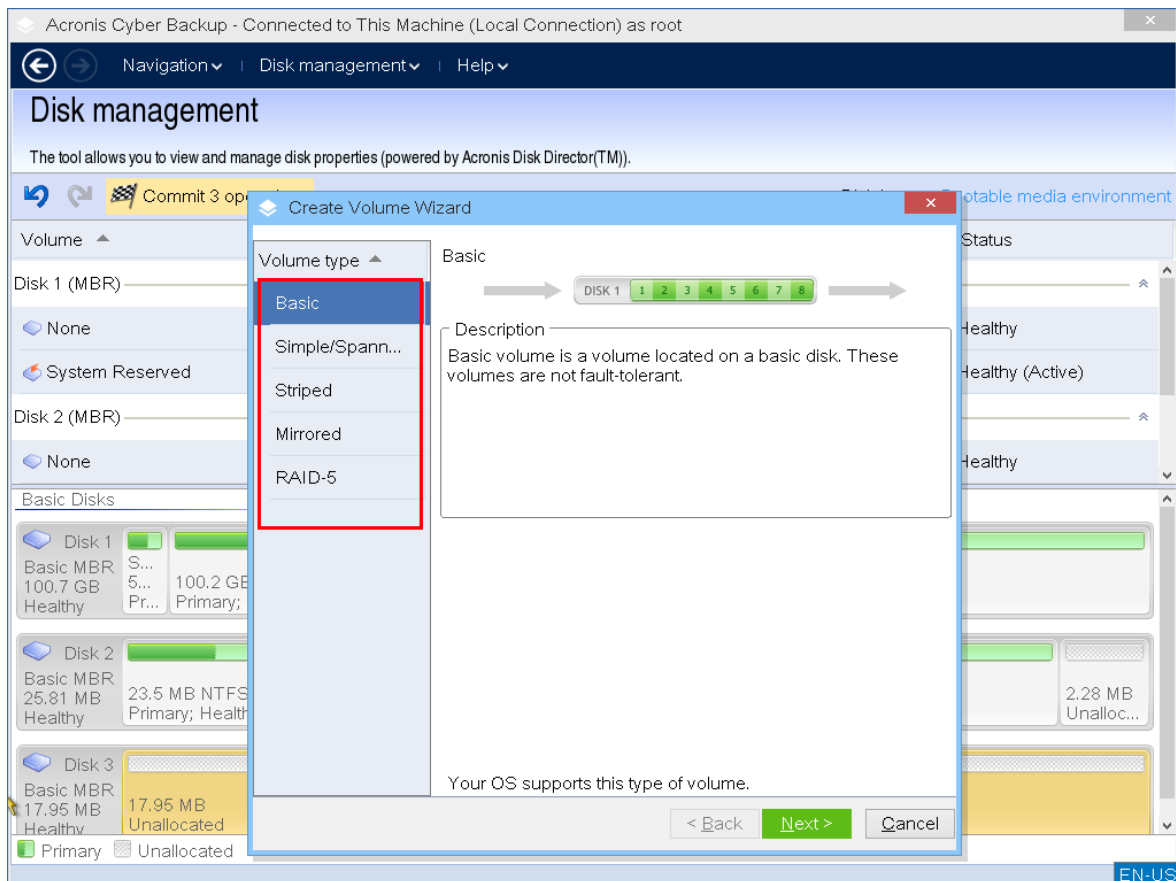
## Create a volume

You might need a new volume to:

- Recover a previously saved backup copy in the “exactly as was” configuration
- Store collections of similar files separately — for example, an MP3 collection or video files on a separate volume
- Store backups (images) of other volumes/disks on a special volume
- Install a new operating system (or swap file) on a new volume
- Add new hardware to a machine

### ***To create a volume***

1. Right-click any unallocated space in a disk, and then click **Create volume**. The **Create volume** wizard opens.



2. Select the type of volume. The following options are available:

- Basic
- Simple/Spanned
- Striped
- Mirrored
- RAID-5

If the current operating system does not support the selected type of volume , you will receive a warning and the **Next** button will be disabled. You have to select another type of volume to proceed.

3. Specify the unallocated space or select destination disks.

- For a basic volume, specify the unallocated space on the selected disk.
- For a simple/spanned volume, select one or more destination disks.
- For a mirrored volume, select two destination disks.
- For a striped volume, select two or more destination disks.
- For a RAID-5 volume, select three destination disks

If you are creating a **dynamic** volume and select one or several **basic** disks as its destination, you will receive a warning that the selected disk will be converted to dynamic automatically.

4. Set the volume size.

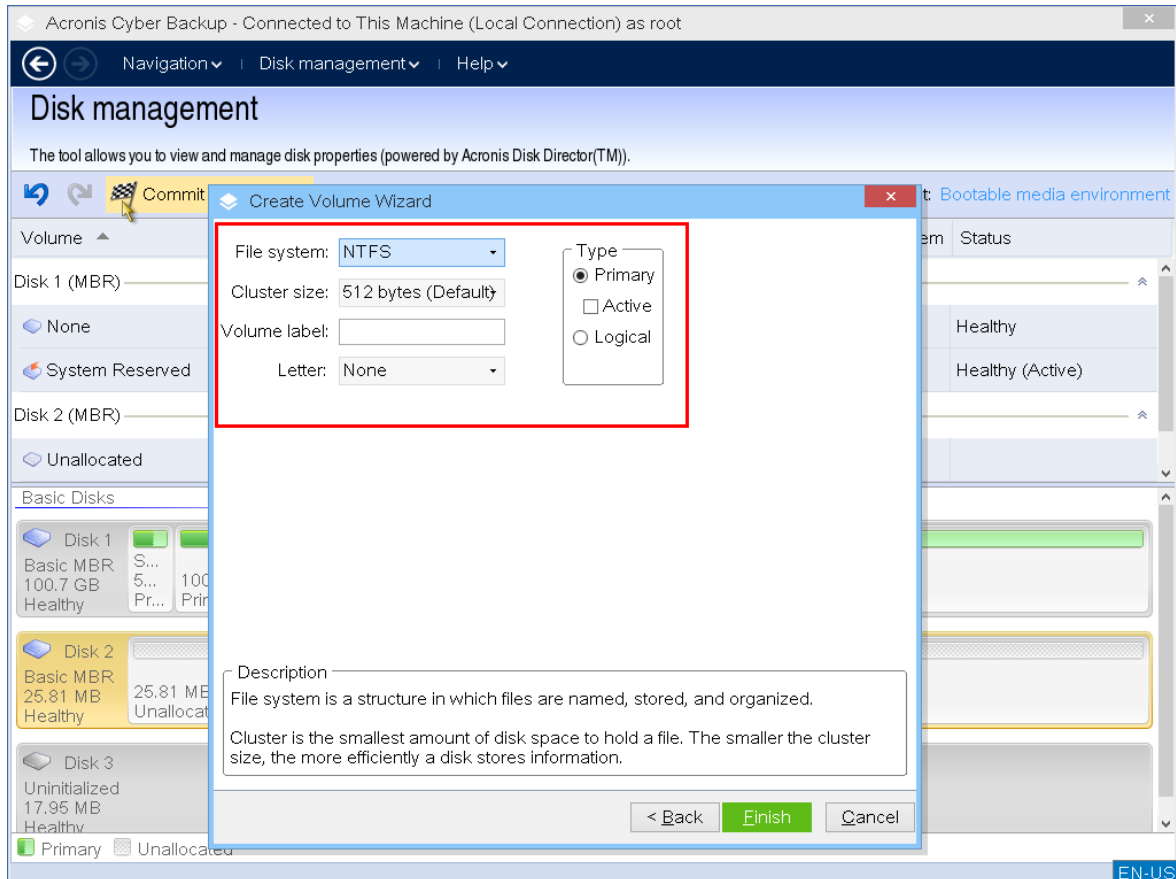
The maximum value normally reflects the maximum unallocated space possible. In some cases, the proposed maximum value might differ – for example, when the size of one mirror



establishes the size of the other mirror, or the last 8Mb of the disk space are reserved for the future conversion of the disk from basic to dynamic.

You can choose the position of a new basic volume on a disk, if the unallocated space on that disk is bigger than the volume.

5. Set the volume options.



You can assign the volume **Letter** (by default – the first free letter of the alphabet) and optionally – a **Label** (by default – none). You must also specify the **File system** and the **Cluster size**.

The possible file systems options are:

- FAT16 (disabled if the volume size has been set at more than 2 GB)
- FAT32 (disabled if the volume size has been set at more than 2 TB)
- NTFS
- Leave the volume unformatted.

When setting the cluster size, you can choose any number in the preset amount for each file system. The cluster size that is suggested by default is best suited to the volume with the chosen file system. If you set a 64K cluster size for FAT16/FAT32 or on 8KB-64KB cluster size for NTFS, Windows can mount the volume, but some programs (for example, Setup programs) might calculate its disk space incorrectly.

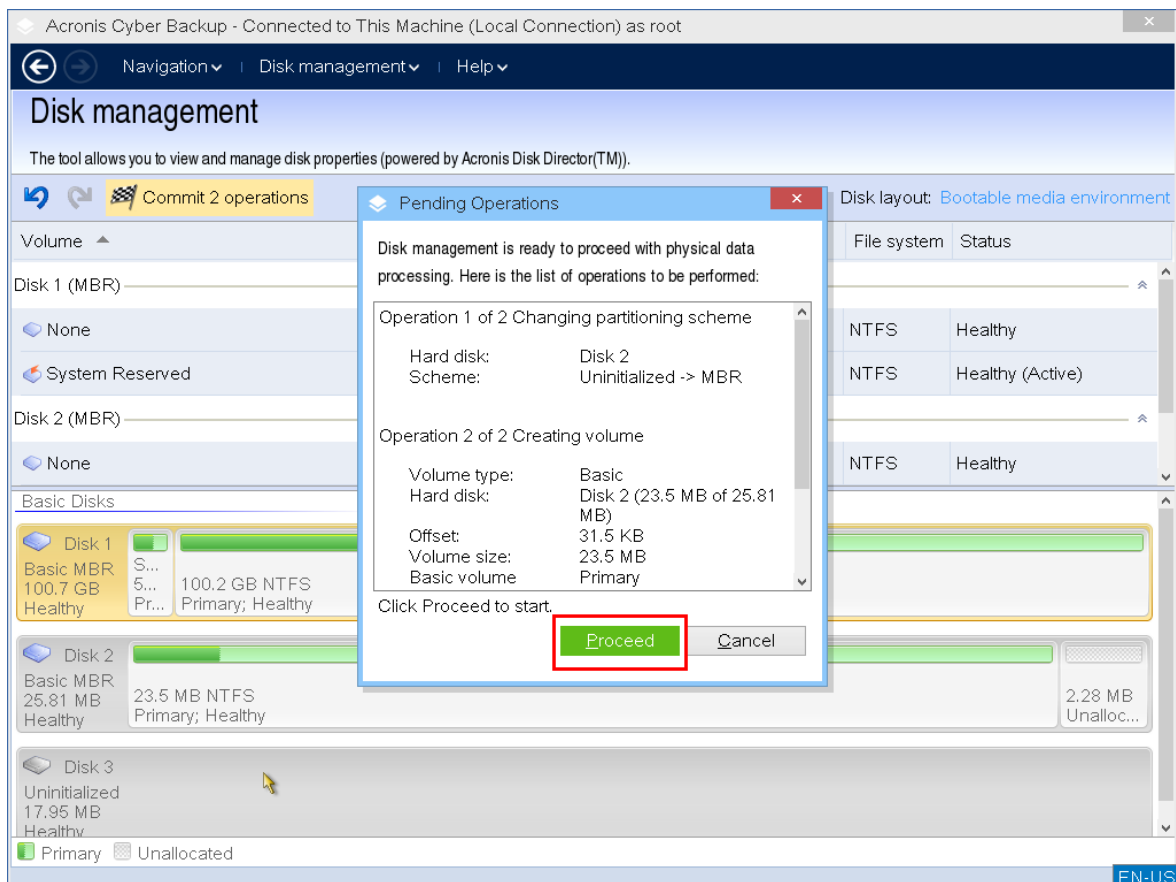
If you are creating a basic volume, which can be made a system volume, you can also select the volume type — **Primary (Active Primary)** or **Logical**. Typically, **Primary** is selected when you want to install an operating system to a volume. Select the **Active** (default) value if you want to

install an operating system on this volume to boot at machine startup. If the **Primary** button is not selected, the **Active** option will be inactive. If the volume is intended for data storage, select **Logical**.

#### Note

A basic disk can contain up to four primary volumes. If they already exist, the disk will have to be converted into dynamic, otherwise **Active** and **Primary** options will be disabled and you will only be able to select the **Logical** volume type.

- Click **Commit**, and then click **Proceed** in the **Pending Operations** window. Exiting the program without committing the operation will effectively cancel it.



## Delete a volume

### To delete a volume

- Right-click the volume that you want to delete.
- Click **Delete volume**.

#### Note

All the information on this volume will be lost irrevocably.

- By clicking **OK**, you will add a pending operation of volume deletion.

4. To complete the added operation, [commit](#) it. Exiting the program without committing the operation will effectively cancel it.

After a volume is deleted, its space is added to unallocated disk space. You can use it to create a new volume or to change another volume's type.

## Set active volume

If you have several primary volumes, you must specify one to be the boot volume. For this, you can set a volume to become active. A disk can have only one active volume.

### ***To set a volume active:***

1. Right-click the desired primary volume on a basic MBR, and then click **Mark as active**.  
If there is no other active volume in the system, the pending operation of setting active volume will be added. If another active volume is present in the system, you will receive a warning that the previous active volume must be set passive first.

---

#### **Note**

Due to setting the new active volume, the former active volume letter might be changed and some of the installed programs might stop running.

---

2. By clicking **OK**, you will add a pending operation of setting active volume.

---

#### **Note**

Even if you have the operating system on the new active volume, in some cases the machine will not be able to boot from it. You will have to confirm your decision to set the new volume as active.

---

3. To complete the added operation, [commit](#) it. Exiting the program without committing the operation will effectively cancel it.

## Change volume letter

Windows operating systems assign letters (C:, D:, etc) to hard disk volumes at startup. These letters are used by applications and operating systems to locate files and folders in the volumes.

Connecting an additional disk, as well as creating or deleting a volume on existing disks, might change your system configuration. As a result, some applications might stop working normally or user files might not be automatically found and opened. To prevent this, you can manually change the letters that are automatically assigned to the volumes by the operating system.

### ***To change a letter assigned to a volume by the operating system***

1. Right-click the desired volume, and then click **Change letter**.
2. In the **Change Letter** window, select a new letter .
3. By clicking **OK**, you will add a pending operation of volume letter assignment.
4. To complete the added operation, [commit](#) it. Exiting the program without committing the operation will effectively cancel it.

## Change volume label

The volume label is an optional attribute. It is a name assigned to a volume for easier recognition.

### *To change a volume label*

1. Right-click the desired volume, and then click **Change label**.
2. Enter a new label in the **Change label** window text field.
3. By clicking **OK**, you will add a pending operation of changing the volume label.
4. To complete the added operation, **commit** it. Exiting the program without committing the operation will effectively cancel it.

## Format volume

You might want to format a volume if you want to change its file system:

- To save additional space which is being lost due to the cluster size on the FAT16 or FAT32 file systems
- As a quick and more or less reliable way of destroying data, residing in this volume

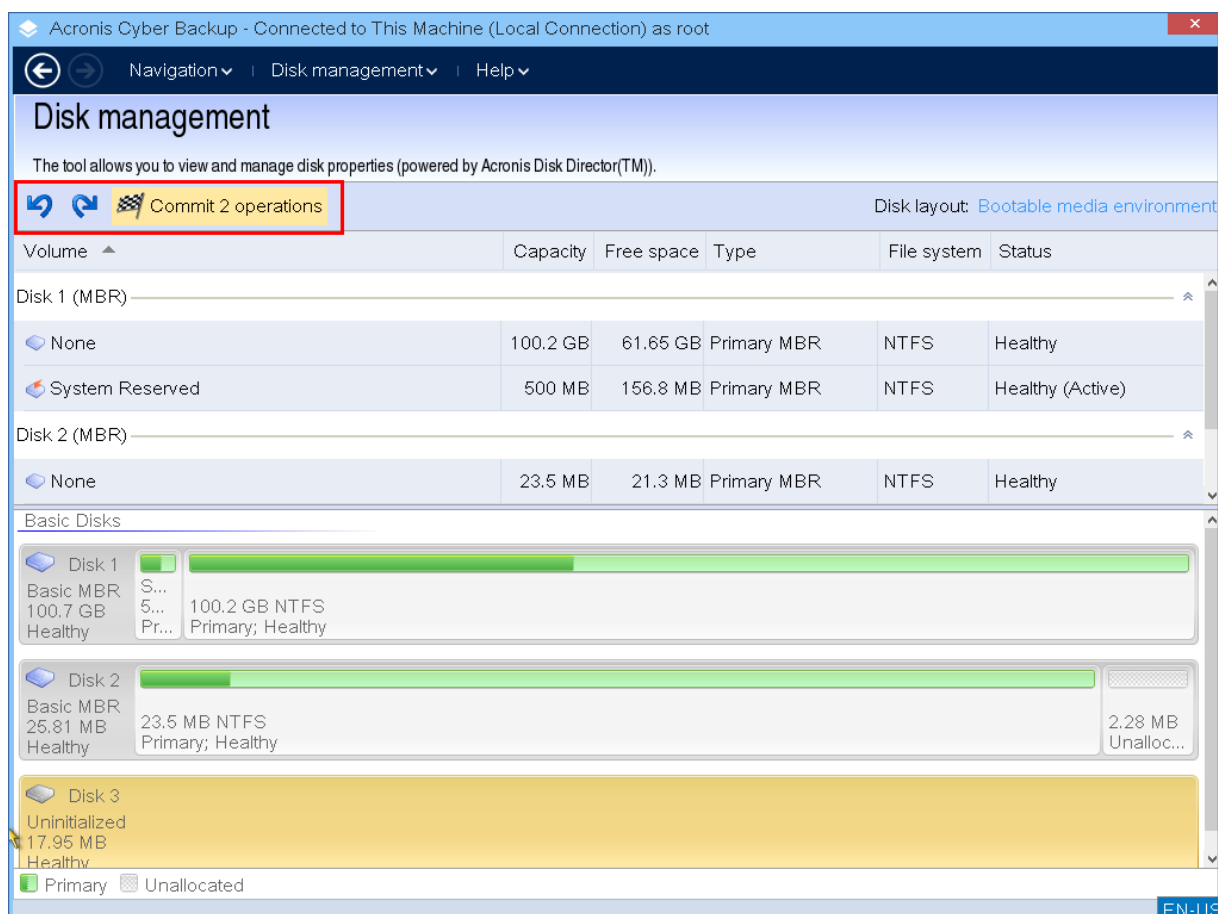
### *To format a volume:*

1. Right-click the desired volume, and then click **Format**.
2. Select the cluster size and file system. The possible file systems options are:
  - FAT16 (disabled if the volume size has been set at more than 2 GB)
  - FAT32 (disabled if the volume size has been set at more than 2 TB)
  - NTFS
3. By clicking **OK**, you will add a pending operation of formatting a volume.
4. To complete the added operation, **commit** it. Exiting the program without committing the operation will effectively cancel it.

## Pending operations

All operations are considered pending until you issue and confirm the **Commit** command. Thus you can control all planned operations, double-check the intended changes, and cancel any operation before it is executed, if necessary.

The **Disk management** view contains the toolbar with icons for **Undo**, **Redo** and **Commit** actions intended for pending operations. These actions might also be launched from the **Disk management** menu.



All planned operations are added to the pending operation list.

The **Undo** action lets you undo the latest operation in the list. While the list is not empty, this action is available.

The **Redo** action lets you reinstate the last pending operation that was undone.

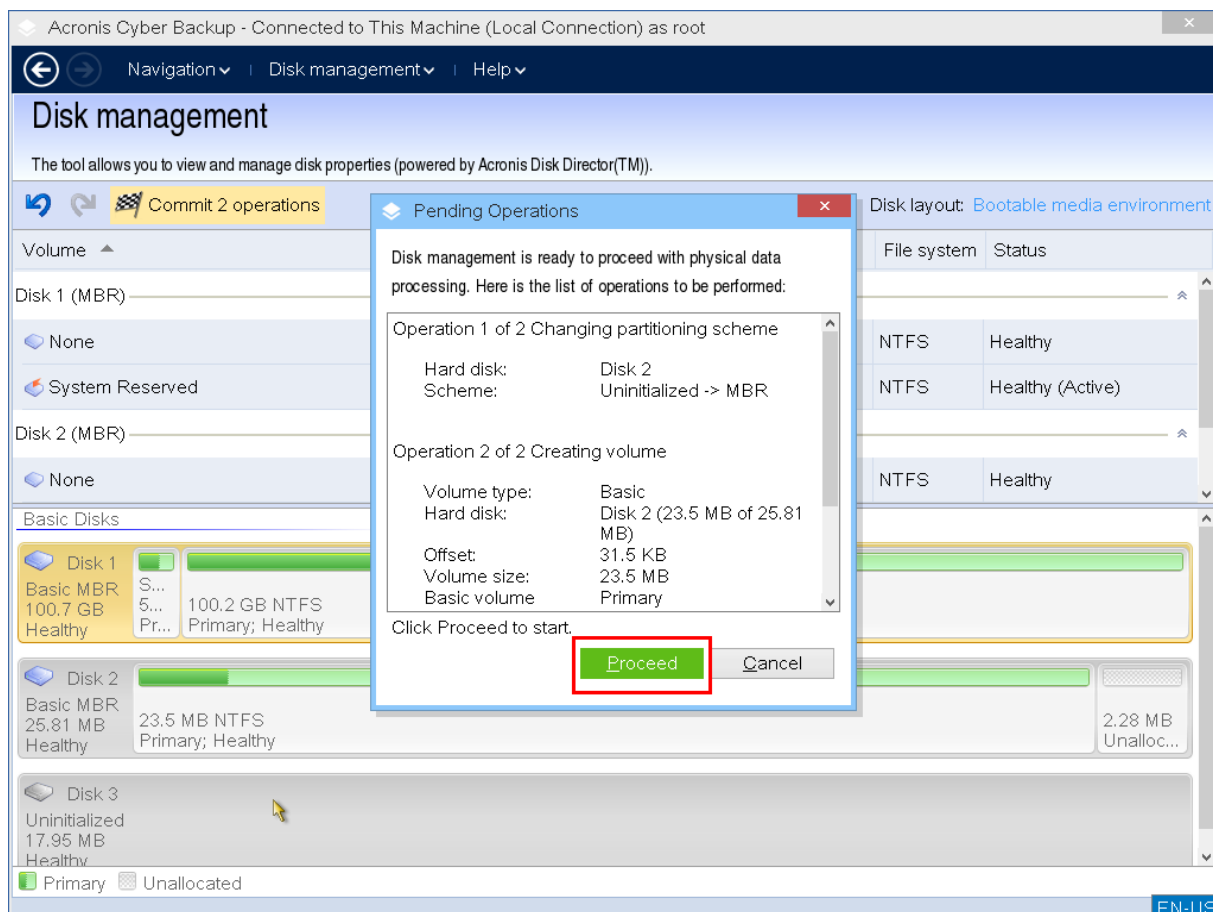
The **Commit** action forwards you to the **Pending Operations** window, where you will be able to view the pending operation list.

To launch their execution, click **Proceed**.

### Note

You will not be able to undo any actions or operations after you choose the **Proceed** operation!

If you don't want to proceed with the commitment, click **Cancel**. Then no changes will be made to the pending operation list. Quitting the program without committing the pending operations also effectively cancels them.



## Remote operations with bootable media

To see the bootable media in the Cyber Protect console, first you need to register it as described in "Registering media on the management server" (p. 388).

After you register the media in the Cyber Protect console, it appears in **Devices > Bootable media**.

By using the web interface, you can manage the media remotely. For example, you can recover data, restart the or shut down the machine booted with the media, or view information, activities, and alerts about the media.

### ***To recover files or folders with bootable media remotely***

1. In the Cyber Protect console, go to **Devices > Bootable media**.
1. Select the media that you want to use for data recovery.
2. Click **Recovery**.
3. Select the location, and then select the backup that you need. Note that backups are filtered by location.
4. Select the recovery point, and then click **Recover files/folders**.
5. Browse to the required folder or use the search bar 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" (p. 287).

6. Click to select the files that you want to recover, and then click **Recover**.
7. In **Path**, select the recovery destination.
8. [Optional] For advanced recovery configuration, click **Recovery options**. For more information, refer to "Recovery options" (p. 339).
9. Click **Start recovery**.
10. Select one of the file overwriting options:
  - **Overwrite existing files**
  - **Overwrite an existing file if it is older**
  - **Do not overwrite existing files**

Choose whether to restart the machine automatically.

11. Click **Proceed** to start the recovery. The recovery progress is shown on the **Activities** tab.

#### ***To recover disks, volumes, or entire machines with bootable media remotely***

1. On the **Devices** tab, go to the **Bootable media** group, and then select the media that you want to use for data recovery.
2. Click **Recovery**.
3. Select the location, and then select the backup that you need. Note that backups are filtered by location.
4. Select the recovery point, and then click **Recover > Entire machine**.  
If necessary, configure the target machine and volume mapping as described in "Recovering a physical machine" (p. 322).
5. For advanced recovery configuration, click **Recovery options**. For more information, refer to "Recovery options" (p. 339).
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.
8. The recovery progress is shown on the **Activities** tab.

#### ***To restart the booted machine remotely***

1. On the **Devices** tab, go to the **Bootable media** group, and then select the media that you want to use for data recovery.
2. Click **Reboot**.
3. Confirm that you want to restart the machine booted with the media.

#### ***To shut down the booted machine remotely***

1. On the **Devices** tab, go to the **Bootable media** group, and then select the media that you want to use for data recovery.
2. Click **Shut down**.
3. Confirm that you want to shut down the machine booted with the media.

### ***To view information about the bootable media***

1. On the **Devices** tab, go to the **Bootable media** group, and then select the media that you want to use for data recovery.
2. Click **Details**, **Activities**, or **Alerts** to see the corresponding information.

### ***To delete bootable media remotely***

1. On the **Devices** tab, go to the **Bootable media** group, and then select the media that you want to use for data recovery.
2. Click **Delete** to delete the bootable media from the Cyber Protect console.
3. Confirm that you want to delete the bootable media.

## Configuring iSCSI devices

This section describes how to configure Internet Small Computer System Interface (iSCSI) 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.

## Startup Recovery Manager

Startup Recovery Manager is a bootable component that resides on your hard drive. With Startup Recovery Manager, you can start the bootable rescue utility without using a separate bootable media.

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 starts and you can perform recovery. On machines with the GRUB boot loader installed, select the Startup Recovery Manager from the boot menu, instead of pressing F11 during a reboot.

You can also back up using Startup Recovery Manager, while on the move.

To use Startup Recovery Manager, you must activate it. Thus, you enable the boot-time prompt **Press F11 for Acronis Startup Recovery Manager** (or add the **Startup Recovery Manager** item to the GRUB menu if you use the GRUB boot loader).

---

### Note

To activate Startup Recovery Manager on a machine with non-encrypted system volume, the machine must have at least 100 MB of free space. Recovery operations that require machine restart need additional 100 MB.

You can activate Startup Recovery Manager on a machine that has a BitLocker-encrypted volume if the machine has at least one other non-encrypted volume. The non-encrypted volume must have at least 500 MB of free space. For recovery operations that require machine restart, the machine must have additional 500 MB of free space.

---

### Important

If Startup Recovery Manager cannot be activated, the backup operations that create One-click recovery backups will fail.

---

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 such boot loaders are installed.

In Linux, when using a boot loader other than GRUB (such as LILO, for example), 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.

## Activating Startup Recovery Manager

On a machine running Agent for Windows or Agent for Linux, you can activate Startup Recovery Manager in the Cyber Protect web console.

### *To activate Startup Recovery Manager in the Cyber Protect web 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.

## Deactivating Startup Recovery Manager

To deactivate Startup Recovery Manager, repeat the activation procedure and select the respective opposite actions. The 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)

## 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](#)".

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.

## Installing Acronis PXE Server

### *To install Acronis PXE Server*

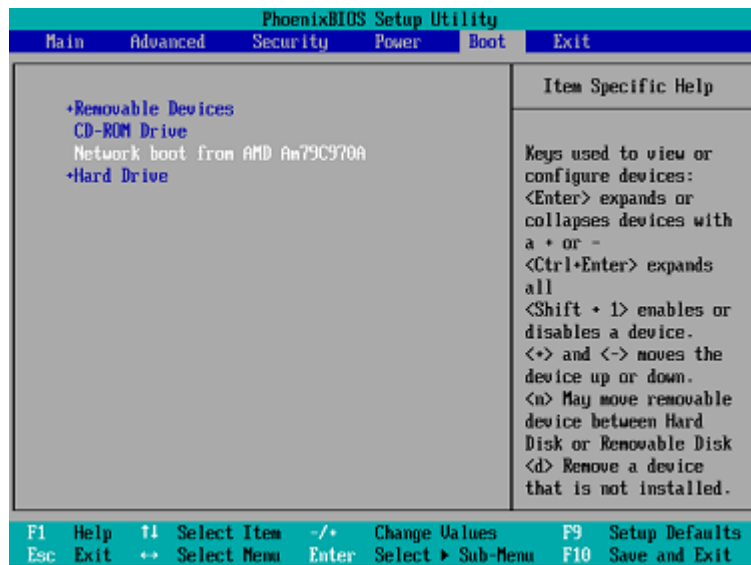
1. Log on as an administrator and start the Acronis Cyber Protect setup program.
2. [Optional] To change the language of the setup program, click **Setup language**.
3. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
4. Click **Customize installation settings**.
5. Next to **What to install**, click **Change**.
6. 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.
7. [Optional] Change other installation settings.
8. Click **Install** to proceed with the installation.
9. 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.

## 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.

## 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://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/boot-from-pxe-server>.

# Protecting mobile devices

The backup app allows you to back up your mobile data to the Cloud storage and then recover it in case of loss or corruption. Note that backup to the cloud storage requires an account and the Cloud subscription.

## Supported mobile devices

You can install the backup app on a mobile device that runs one of the following operating systems:

- iOS 15 to iOS 17 (iPhone, iPod, iPad)
- Android 9 to Android 13

## What you can back up

- Contacts
- Photos
- Videos
- Calendars
- Reminders (only on iOS devices)

## What you need to know

- You can back up the data only to the cloud storage.
- Any time you open the app, you will see the summary of data changes and can start a backup manually.
- The **Continuous backup** functionality is enabled by default. If this setting is turned on:
  - For Android 7.0 or higher, the backup app automatically detects new data on-the-fly and uploads it to the Cloud.
  - For Android 5 and 6, it checks for changes every three hours. You can turn off continuous backup in the app settings.
- The **Use Wi-Fi only** option is enabled by default in the app settings. If this setting is turned on, the backup app will back up your data only when a Wi-Fi connection is available. If the Wi-Fi connection is lost, a backup process does not start. For the app to use cellular connection as well, turn this option off.
- You have two ways to save energy:
  - The **Back up while charging** functionality which is disabled by default. If this setting is turned on, the backup app will back up your data only when your device is connected to a power source. When the device is disconnected from a power source during a continuous backup process, the backup is paused.

- The **Save power mode** which is enabled by default. If this setting is turned on, the backup app will back up your data only when your device battery is not low. When the device battery gets low, the continuous backup is paused. This option is available for Android 8 or higher.
- You can access the backed-up data from any mobile device registered under your account. This helps you transfer the data from an old mobile device to a new one. Contacts and photos from an Android device can be recovered to an iOS device and vice versa. You can also download a photo, video, or contact to any device by using the Cyber Protect web console.
- The data backed up from mobile devices registered under your account is available only under this account. Nobody else can view or recover your data.
- In the backup app, you can recover only the latest data versions. If you need to recover from a specific backup version, use the Cyber Protect web console on either a tablet or a computer.
- [Only for Android devices] If an SD card is present during a backup, the data stored on this card is also backed up. The data will be recovered to an SD card, to the folder **Recovered by Backup** if it is present during recovery, or the app will ask for a different location to recover the data to.

## Where to get the backup app

1. On the mobile device, open a browser and go to <https://backup.acronis.com/>.
2. Sign in with your account.
3. Click **All devices** > **Add**.
4. Under **Mobile devices**, select the device type.  
Depending on the device type, you will be redirected to the App Store or to the Google Play Store.
5. [Only on iOS devices] Click **Get**.
6. Click **Install** to install the backup app.

## How to start backing up your data

1. Open the app.
2. Sign in with your account.

Tap **Set up** to create your first backup.

1. Select the data categories that you want to back up. By default, all categories are selected.
2. [optional step] Enable **Encrypt Backup** to protect your backup by encryption. In this case, you will need to also:
  - a. Enter an encryption password twice.

---

### Note

Make sure you remember the password, because a forgotten password can never be restored or changed.

---

- b. Tap **Encrypt**.
3. Tap **Back up**.

4. Allow the app access to your personal data. If you deny access to some data categories, they will not be backed up.

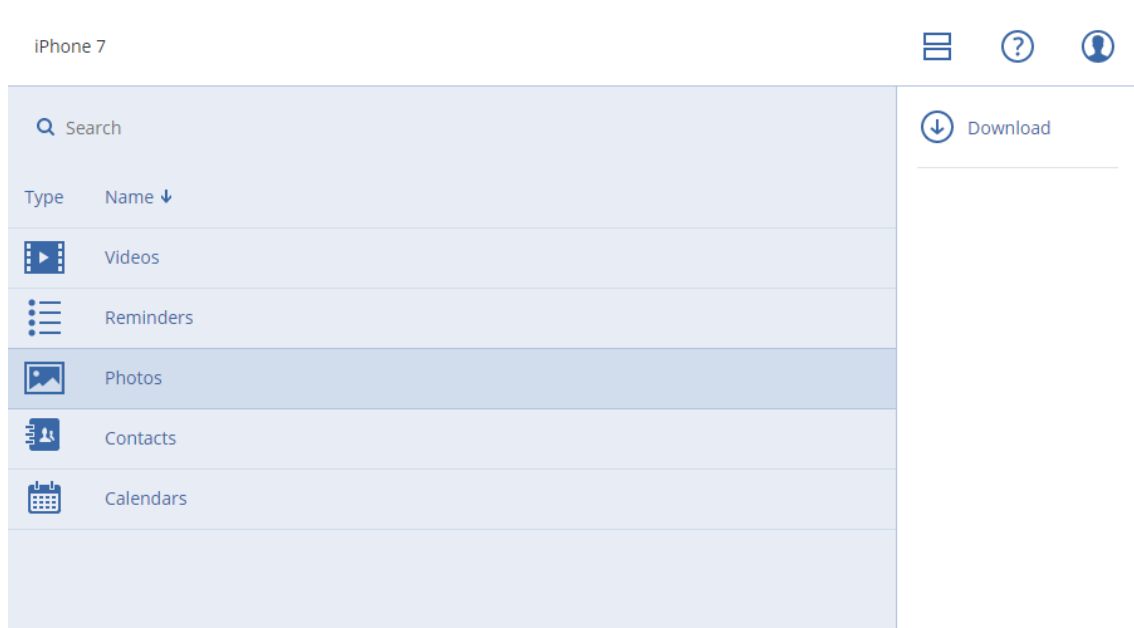
The backup starts.

## How to recover data to a mobile device

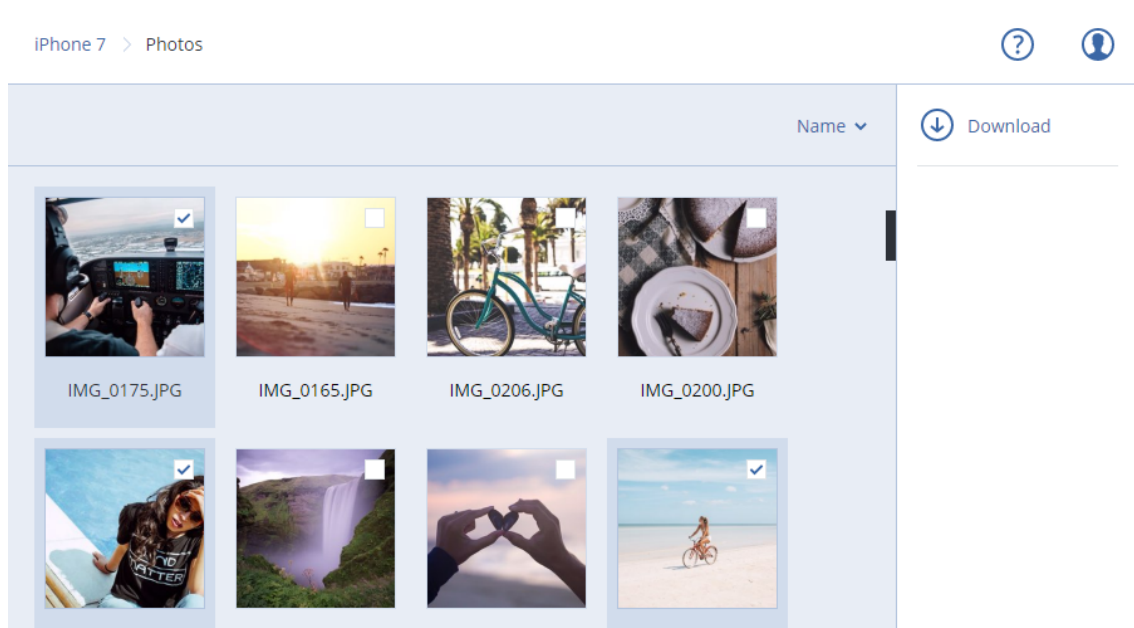
1. Open the backup app.
2. Tap **Browse**.
3. Tap the device name.
4. Do one of the following:
  - To recover all of the backed-up data, tap **Recover all**. No more actions are required.
  - To recover one or more data categories, tap **Select**, and then tap the check boxes for the required data categories. Tap **Recover**. No more actions are required.
  - To recover one or more data items belonging to the same data category, tap the data category. Proceed to further steps.
5. Do one of the following:
  - To recover a single data item, tap it.
  - To recover several data items, tap **Select**, and then tap the check boxes for the required data items.
6. Tap **Recover**.

## How to review data via the Cyber Protect web console

1. On a computer, open a browser and type the Cyber Protect web console URL.
2. Sign in with your account.
3. In **All devices**, click **Recover** under your mobile device name.
4. Do any of the following:
  - To download all photos, videos, contacts, calendars, or reminders, select the respective data category. Click **Download**.



- To download individual photos, videos, contacts, calendars, or reminders, click the respective data category name, and then select the check boxes for the required data items. Click **Download**.



- To preview a photo or a contact, click the respective data category name, and then click the required data item.



# Protecting Microsoft applications

---

## Important

Some of the features described in this section are only available for on-premises deployments.

---

## 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 protection 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 or to Microsoft 365. 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 Databases as files	Entire machine Databases to a live SQL Server instance Databases as files	Entire machine
Microsoft Exchange Server	Databases to a live Exchange Databases as files Granular recovery to a live Exchange or to Microsoft 365*	Entire machine Databases to a live Exchange Databases as files Granular recovery to a live Exchange or to Microsoft 365*	Entire machine
Microsoft SharePoint database servers	Databases to a live SQL Server instance Databases as files Granular recovery by using SharePoint Explorer	Entire machine Databases to a live SQL Server instance Databases as files Granular recovery by using SharePoint Explorer	Entire machine
Microsoft SharePoint front-end web servers	-	-	Entire machine
Active Directory Domain Services	-	Entire machine	-

\* Granular recovery is also available from a mailbox backup.

## 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 \(VSS\)](#) backup option is enabled.
- For virtual machines, the [Volume Shadow Copy Service \(VSS\) for virtual machines](#) 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**).

## Database backup

Before backing up databases, ensure that the requirements listed in "Prerequisites" are met.

Select the databases as described below, and then specify other settings of the protection plan [as appropriate](#).

## 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 [protection plan options](#).

### **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 or individual AAG databases, refer to ["Protecting Always On Availability Groups \(AAG\)"](#).
- If you select a machine running an 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 **Protect**. If prompted, provide credentials to access the SQL Server data.

If you use Windows authentication, 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.

If you use SQL Server authentication, the account must be a member of the **sysadmin** role on each of the instances that you are going to back up.

## 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 <b>Exchange Organization Administrators</b> role group
2010/2013/2016/2019	Databases, Database Availability Groups (DAG)	Membership in the <b>Server Management</b> 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](#)", 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 \(DAG\)](#)".
- 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](#)", you can [select mailboxes for backup](#).

4. If prompted, provide the credentials to access the data.

5. Click **Protect**.

## Protecting Always On Availability Groups (AAG)

### 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.

---

### Note

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 or database set to backup as described in "[Selecting SQL databases](#)".  
You must select the AAG itself to backup all databases of the AAG. To backup a set of databases, define this set of databases in all nodes of the AAG.

---

### Warning!

The database set must be exactly the same in all nodes. If even one set is different, or not defined on all nodes, the cluster backup will not work correctly.

---

3. Configure the "[Cluster backup mode](#)" 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 Backup storage tab](#). The names of AAG backups are based on the following template: <AAG name> - <protection plan name> and have a special icon.

2. To configure recovery, follow the steps described in "[Recovering SQL 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.

---

**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.

---

## Protecting Database Availability Groups (DAG)

### 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

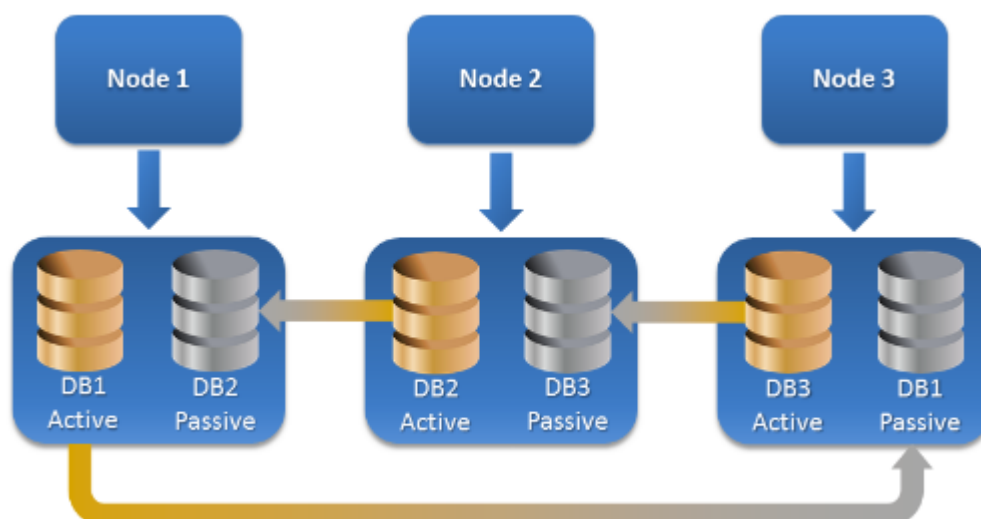
With cluster-aware backup, you back up only one copy of the clustered data. If the data changes its location within the cluster (due to a switchover or a failover), the software will track all relocations of this data and safely back it up.

### 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.

---

### Note

After you install the agent on one of the nodes, the Cyber Protect web 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 protection plan, select the DAG as described in "[Selecting Exchange Server data](#)".
2. Configure the "[Cluster backup mode](#)" backup option.
3. Specify other settings of the protection plan [as appropriate](#).

---

### 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 Backup storage tab](#).

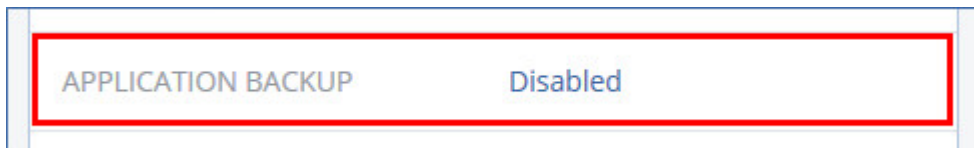
2. Follow the steps described in "Recovering Exchange databases", starting from step 5.

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.

## Application-aware backup

Application-aware disk-level backup is available for physical machines and, ESXi virtual machines, and Hyper-V 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 [protection plan options](#). The Exchange transaction logs are truncated on virtual machines only. You can enable the [VSS full backup option](#) 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) or Agent for Hyper-V.

---

**Note**

For Hyper-V virtual machines that are running Windows Server 2022, application-aware backup is not supported in the agentless mode—that is, when the backup is performed by Agent for Hyper-V. To protect Microsoft applications on these machines, install Agent for Windows inside the guest operating system.

---

Agent for VMware (Virtual Appliance) and Agent for VMware (Linux) can create application-aware backups, but cannot recover application data from them. To recover application data from backups created by these agents, 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 **Backup storage** tab, and then select this machine in **Machine to browse from**.

Other requirements are listed in "Prerequisites" (p. 442) and "Required user rights for application-aware backup" (p. 451).

## Required user rights for application-aware backup

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.

---

**Note**

Only Windows authentication is supported.

---

- 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.

## Additional requirements for machines running Windows

For all Windows versions, you must disable the User Account Control (UAC) policies to allow application-aware backups. If you do not want to disable the UAC policies, you must provide the credentials of a built-in domain administrator (DOMAIN\Administrator) when configuring application-aware backups.

### *To disable the UAC policies in Windows*

1. In the Registry Editor, locate the following registry key:  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
2. Change the **EnableLUA** value to **0**.
3. Restart the machine.

## 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"](#).
10. Click **Add**.

As a result, the mailboxes appear under **Devices > Microsoft Exchange > Mailboxes**.

## Selecting Exchange Server mailboxes

Select the mailboxes as described below, and then specify other settings of the protection plan [as appropriate](#).

### *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**.

## 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>.

## 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.

If you use Windows authentication, 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. If you use SQL Server authentication, you will need to provide credentials for an account that is 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"](#).

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.

System databases are basically recovered in the same way as user databases. The peculiarities of system database recovery are described in ["Recovering system databases"](#).

### ***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 cloud or 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 Backup storage tab](#).

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] [Not available for a database recovered to its original instance as a new database] 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 cloud or 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 Backup storage tab](#).

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.

## 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.

## 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**.

## 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 <b>Exchange Organization Administrators</b> role group.
2010/2013/2016/2019	Databases	Membership in the <b>Server Management</b> 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](#).

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 cloud or 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 Backup storage tab](#).

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 cloud or 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 Backup storage tab](#).

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.

## 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](http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx)

## 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. The mailboxes or mailbox items can be recovered to a live Exchange Server or to Microsoft 365.

The following items can be recovered:

- Mailboxes (except for archive mailboxes)
- Public folders

---

### Note

Available only from database backups. See "Selecting Exchange Server data" (p. 445)

---

- Public folder items
- Email folders
- Email messages
- Calendar events
- Tasks
- Contacts

- Journal entries
- Notes

You can use search to locate the items.

## Recovery to an Exchange Server

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.

## Recovery to Microsoft 365

Recovery can be performed from backups of Microsoft Exchange Server 2010 and later.

When a mailbox is recovered to an existing Microsoft 365 mailbox, the existing items are kept intact, and the recovered items are placed next to them.

When recovering a single mailbox, you need to select the target Microsoft 365 mailbox. When recovering several mailboxes within one recovery operation, the software will try to recover each mailbox to the mailbox of the user with the same name. If the user is not found, the mailbox is skipped. If some mailboxes are skipped, the recovery will succeed with warnings. If all mailboxes are skipped, the recovery will fail.

For more information about recovery to Microsoft 365, refer to "Protecting Microsoft 365 mailboxes" (p. 467).

## Recovering mailboxes

### *To recover mailboxes from an application-aware backup or a database backup*

1. [Only when recovering from a database backup to Microsoft 365] If Agent for Office 365 is not installed on the machine running Exchange Server that was backed up, do one of the following:
  - If there is not Agent for Office 365 in your organization, install Agent for Office 365 on the machine that was backed up (or on another machine with the same Microsoft Exchange Server version).
  - If you already have Agent for Office 365 in your organization, copy libraries from the machine that was backed up (or from another machine with the same Microsoft Exchange Server version) to the machine with Agent for Office 365, as described in "[Copying Microsoft Exchange libraries](#)".
2. 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.
3. Click **Recovery**.
4. 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 cloud or 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 Backup storage tab](#).

The machine chosen for browsing in either of the above actions will perform the recovery instead of the original machine that is offline.
5. Click **Recover > Exchange mailboxes**.
6. Select the mailboxes that you want to recover.

You can search mailboxes by name. Wildcards are not supported.



7. Click **Recover**.
8. [Only when recovering to Microsoft 365]:

- a. In **Recover to**, select **Microsoft Office 365**.
  - b. [If you selected only one mailbox in step 6] In **Target mailbox**, specify the target mailbox.
  - c. Click **Start recovery**.
- Further steps of this procedure are not required.
9. 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 a machine where the **Client Access** role (in Microsoft Exchange Server 2010/2013) or **Mailbox role** (in Microsoft Exchange Server 2016 or later) 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" (p. 453).
  10. [Optional] Click **Database to re-create any missing mailboxes** to change the automatically selected database.
  11. 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 Backup storage tab](#), 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 8-11 of the above procedure.

## Recovering mailbox items

#### ***To recover mailbox items from an application-aware backup or a database backup***

1. [Only when recovering from a database backup to Microsoft 365] If Agent for Office 365 is not installed on the machine running Exchange Server that was backed up, do one of the following:
  - If there is not Agent for Office 365 in your organization, install Agent for Office 365 on the machine that was backed up (or on another machine with the same Microsoft Exchange Server version).
  - If you already have Agent for Office 365 in your organization, copy libraries from the machine that was backed up (or from another machine with the same Microsoft Exchange Server version) to the machine with Agent for Office 365, as described in "[Copying Microsoft Exchange libraries](#)".
2. 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.
3. Click **Recovery**.
  4. 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 cloud or 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 Backup storage tab](#).

The machine chosen for browsing in either of the above actions will perform the recovery instead of the original machine that is offline.
  5. Click **Recover > Exchange mailboxes**.
  6. Click the mailbox that originally contained the items that you want to recover.
  7. 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.

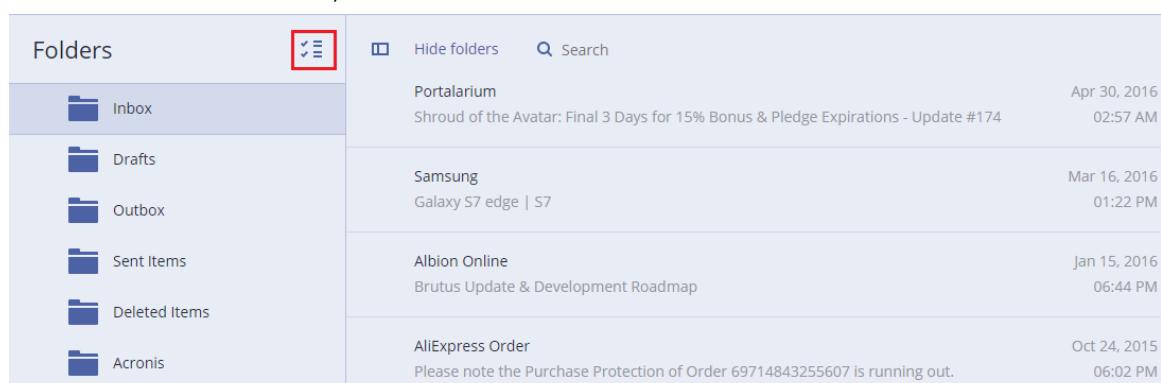
---

### Note

Click the name of an attached file to download it.

---

To be able to select folders, click the recover folders icon.



8. Click **Recover**.
9. To recover to Microsoft 365, select **Microsoft Office 365** in **Recover to**.  
To recover to an Exchange Server, keep the default **Microsoft Exchange** value in **Recover to**.
10. [Only when recovering to an Exchange Server] 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 a machine where the **Client Access** role (in Microsoft Exchange Server 2010/2013) or **Mailbox role** (in Microsoft Exchange Server 2016 or later) 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" (p. 453).

11. 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.

12. [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. Due to Microsoft Exchange limitations, events, tasks, notes, and contacts are restored to their original location regardless of any different **Target folder** specified.

13. 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 Backup storage tab](#), 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.

---

#### **Note**

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 9-13 of the above procedure.



## Copying Microsoft Exchange Server libraries

When [recovering Exchange mailboxes or mailbox items to Microsoft 365](#), you may need to copy the following libraries from the machine that was backed up (or from another machine with the same Microsoft Exchange Server version) to the machine with Agent for Office 365.

Copy the following files, according to the Microsoft Exchange Server version that was backed up.

Microsoft Exchange Server version	Libraries	Default location
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

The libraries should be placed in the folder **%ProgramData%\Acronis\ese**. If this folder does not exist, create it manually.

## 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**.

# Protecting Microsoft 365 mailboxes

---

## Important

This section is valid for on-premises deployments of Acronis Cyber Protect. If you are using a cloud deployment, refer to

<https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html>.

For more information on the licensing options, see [Acronis Cyber Protect for Microsoft 365 Licensing](#).

---

## Why back up Microsoft 365 mailboxes?

Even though Microsoft 365 is a cloud service, regular backups provide an additional layer of protection from user errors and intentional malicious actions. You can recover deleted items from a backup even after the Microsoft 365 retention period has expired. Also, you can keep a local copy of the Microsoft 365 mailboxes if it is required by a regulatory compliance.

## Recovery

The following items can be recovered from a mailbox backup:

- Mailboxes
- Email folders
- Email messages
- Calendar events
- Tasks
- Contacts
- Journal entries
- Notes

You can use search to locate the items.

Recovery can be performed to Microsoft 365 or to a live Exchange Server.

When a mailbox is recovered to an existing Microsoft 365 mailbox, the existing items with matching IDs are overwritten. When a mailbox is recovered to an existing Exchange Server mailbox, the existing items are kept intact. The recovered items are placed next to them.

Recovery of mailbox items does not overwrite anything. Instead, the full path to a mailbox item is recreated in the target folder.

## Limitations

- Applying a protection plan to more than 500 mailboxes may cause backup performance degradation. To protect a large number of mailboxes, create several protection plans and schedule them to run at different times.
- Archive mailboxes (**In-Place Archive**) cannot be backed up.
- A mailbox backup includes only folders visible to users. The **Recoverable items** folder and its subfolders (**Deletions, Versions, Purges, Audits, DiscoveryHold, Calendar Logging**) are not included in a mailbox backup.
- Recovery to a new Microsoft 365 mailbox is not possible. You must first create a new Microsoft 365 user manually, and then recover items to this user's mailbox.
- Recovery to a different Microsoft 365 organization is not supported.
- Some item types or properties supported by Microsoft 365 may not be supported by Exchange Server. They will be skipped during recovery to Exchange Server.

## Adding a Microsoft 365 organization

To add a Microsoft organization, you need to know your application ID, application secret, and Microsoft 365 tenant ID. For more information on how to find these, refer to [Obtaining application ID and application secret](#).

### *To add a Microsoft 365 organization*

1. [Install Agent for Office 365](#) on a Windows machine that is connected to the Internet. There must be only one Agent for Office 365 in an organization.
2. In the Cyber Protect web console, click **Microsoft Office 365**.
3. In the window that opens, enter your application ID, application secret, and Microsoft 365 tenant ID.
4. Click **Sign in**.

As a result, your organization data items appear in the Cyber Protect web console, on the **Microsoft Office 365** tab.

## Obtaining application ID and application secret

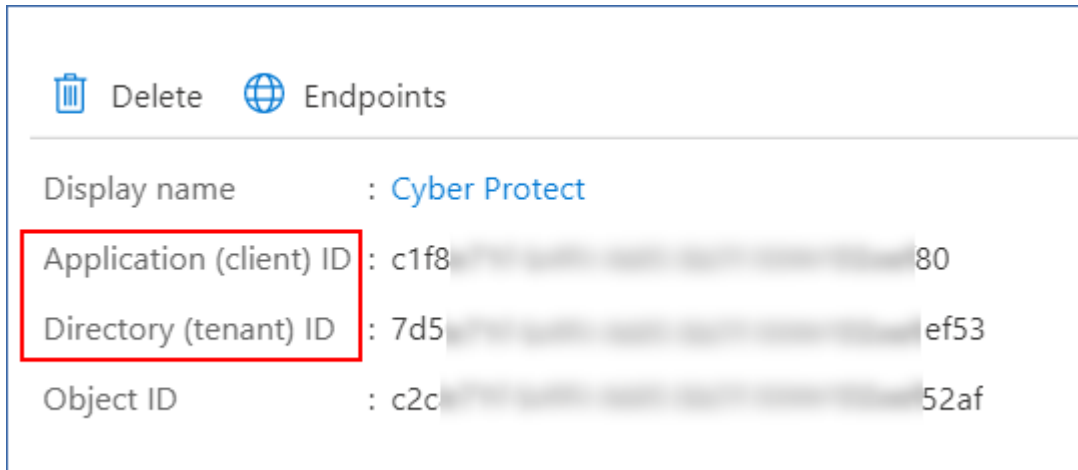
To use the modern authentication for Microsoft 365, you need to create a custom application in the Azure Active Directory and grant it specific API permissions. Thus, you will obtain the **application ID, application secret, and directory (tenant) ID** that you need to [enter in the Cyber Protect web console](#).

### *To create an application in Azure Active Directory*

1. Log in to the [Azure portal](#) as an administrator.
2. Navigate to **Azure Active Directory > App registrations**, and then click **New registration**.

3. Specify a name for your custom application, for example, Cyber Protect.
4. In **Supported Account types**, select **Accounts in this organizational directory only**.
5. Click **Register**.

Your application is now created. In the Azure portal, navigate to the application's **Overview** page and check your application (client) ID and directory (tenant ID).





For more information on how to create an application in the Azure portal, refer to the [Microsoft documentation](#).

#### ***To grant your application the necessary API permissions***

1. In the Azure portal, navigate to the application's **API permissions**, and then click **Add a permission**.
2. Select the **APIs my organization uses** tab, and then search for **Office 365 Exchange Online**.
3. Click **Office 365 Exchange Online**, and then click **Application permissions**.
4. Select the **full\_access\_as\_app** check box, and then click **Add permissions**.
5. In **API permissions**, click **Add a permission**.
6. Select **Microsoft Graph**.
7. Select **Application permissions**.
8. Expand the **Directory** tab, and then select the **Directory.Read.All** check box. Click **Add permissions**.
9. Check all permissions, and then click **Grant admin consent for <your application's name>**.
10. Confirm your choice by clicking **Yes**.

#### ***To create an application secret***

1. In the Azure portal, navigate to your application's **Certificates & secrets > New client secret**.
2. In the dialog box that opens, select Expires: **Never**, and then click **Add**.
3. Check your application secret in the **Value** field and make sure that you remember it.

Client secrets			
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.			
<a href="#">+ New client secret</a>			
Description	Expires	Value	
Password uploaded on Wed Jun 03 2020	12/31/2299	42A... [Redacted]	 

For more information on the application secret, refer to the [Microsoft documentation](#).

## Changing the Microsoft 365 access credentials

You can change access credentials for Microsoft 365 without re-installing the agent.

### ***To change the Microsoft 365 access credentials***

1. In the Cyber Protect web console, go to **Devices > Microsoft Office 365**.
2. Select the Microsoft 365 organization.
3. Click **Specify credentials**.
4. Enter your application ID, application secret, and Microsoft 365 tenant ID. For more information on how to find these, refer to [Obtaining application ID and application secret](#).
5. Click **Sign in**.

## Selecting mailboxes

Select the mailboxes as described below, and then specify other settings of the protection plan [as appropriate](#).

### ***To select mailboxes***

1. In the Cyber Protect web console, go to **Devices > Microsoft Office 365**.
2. Select the mailboxes that you want to back up.
3. Click **Backup**.

## Recovering mailboxes and mailbox items

### Recovering mailboxes

1. [Only when recovering to an Exchange Server] Ensure that there is an Exchange user with the same logon name as the username of the user whose mailbox is being recovered. If not, create the user. See the full list of requirements for this user in "Requirements on user accounts" (p. 460).
2. In the Cyber Protect web console, go to **Devices > Microsoft Office 365**.
3. 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 Backup storage tab](#), and then click **Show backups**.
4. Select a recovery point. Note that recovery points are filtered by location.

5. Click **Recover > Mailbox**.
6. To recover to an Exchange Server, in **Recover to**, select **Microsoft Exchange**. Continue recovery as described in "Recovering mailboxes" (p. 461), starting from step 9. Further steps of this procedure are not required.  
To recover to Microsoft 365, in **Recover to**, keep the default **Microsoft Office 365** value.
7. In **Target mailbox**, view, change, or specify the target mailbox.  
By default, the original mailbox is selected. If this mailbox does not exist, you must specify the target mailbox.
8. Click **Start recovery**.

## Recovering mailbox items

1. [Only when recovering to an Exchange Server] Ensure that there is an Exchange user with the same logon name as the username of the user whose mailbox is being recovered. If not, create the user. See the full list of requirements for this user in "Requirements on user accounts" (p. 460).
2. In the Cyber Protect web console, go to **Devices > Microsoft Office 365**.
3. 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 Backup storage tab](#), and then click **Show backups**.
4. Select a recovery point. Note that recovery points are filtered by location.
5. Click **Recover > Email messages**.
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.

---

### Note

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:



7. Click **Recover**.
8. To recover to an Exchange Server, in **Recover to**, select **Microsoft Exchange**.  
To recover to Microsoft 365, in **Recover to**, keep the default **Microsoft Office 365** value.

9. [Only when recovering to an Exchange Server] To select or change the target machine, click **Target machine with Microsoft Exchange Server**. 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" (p. 453).
10. In **Target mailbox**, view, change, or specify the target mailbox.  
By default, the original mailbox is selected. If this mailbox does not exist, you must specify the target mailbox.
11. [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.
12. Click **Start recovery**.



# Protecting Google Workspace data

This feature is available only in cloud deployments of Acronis Cyber Protect. For a detailed description of this functionality, refer to <https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html>.

# Protecting Oracle Database

Protection of Oracle Database is described in a separate document available at [https://dl.managed-protection.com/u/pdf/AcronisCyberProtect\\_15\\_OracleBackup\\_whitepaper.pdf](https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf).

# Special operations with virtual machines

## Running a virtual machine from a backup (Instant Restore)

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

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 Cyber Protection service.
- The backup can be stored in a network folder, on a storage node, 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 can also be run from a backup stored in the cloud storage, but it works slower because this operation requires intense random-access reading from the backup. 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.
- Backups of both physical and virtual machines can be used. Backups of Virtuozzo *containers* cannot be used.

- Backups that contain Linux logical volumes (LVM) must be created by Agent for VMware or Agent for Hyper-V. The virtual machine must be of the same type as the original machine (ESXi or Hyper-V).

## 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 Backup storage tab](#).
2. Click **Run as VM**.

The software automatically selects the host and other required parameters.

✕ Run 'Windows 8 x64' as VM

TARGET MACHINE
Windows 8 x64_temp on 10.255.154.182
DATASTORE
datastore3
VM SETTINGS
Memory: 2.00 GB
Network adapters: 1
POWER STATE
On ▼
<b>RUN NOW</b>

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](#), 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:



. Such virtual machines cannot be selected for backup.

## 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.

## 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 protection agent.

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.

The location of the final virtual disks is defined in the parameters of the **Run as VM** operation (**Datastore** for ESXi or **Path** for Hyper-V). Prior to starting the finalization, ensure that free space, sharing capabilities, and performance of this datastore are suitable for running the machine in production.

---

### **Note**

Finalization is not supported for Hyper-V running in Windows Server 2008/2008 R2 and Microsoft Hyper-V Server 2008/2008 R2 because the necessary API is missing in these Hyper-V versions.

---

### *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.

## What you need to know about finalization

### 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.

### Finalization of machines running from cloud backups

Because of intensive access to the backed-up data, the finalization speed highly depends on the connection bandwidth between the backup location and the agent. The finalization will be slower for backups located in the cloud as compared to local backups. If the Internet connection is very slow or unstable, the finalization of a machine running from a cloud backup may fail. We recommend to run virtual machines from local backups if you are planning to perform finalization and have the choice.

## Working in VMware vSphere

This section describes operations that are specific for VMware vSphere environments.

### 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](#), 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**

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**

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.


## 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](#).
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: 

## 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.

## 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**  
Stop failover if the original machine was fixed. The replica will be powered off. Replication will be resumed.
- **Perform permanent failover to the replica**  
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**  
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](#).
7. Click **Start recovery**.
8. Confirm your decision.

## 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 \(CBT\)](#)".

### 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](#)".

## Pre/Post commands

This option is similar to the backup option "[Pre/Post commands](#)".

## Volume Shadow Copy Service VSS for virtual machines

This option is similar to the backup option "[Volume Shadow Copy Service VSS for virtual machines](#)".

## 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](#)".

## Performance

This option is similar to the recovery option "[Performance](#)".

## Pre/Post commands

This option is similar to the recovery option "[Pre/Post commands](#)".

## VM power management

This option is similar to the recovery option "[VM power management](#)".

## 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](#).

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.

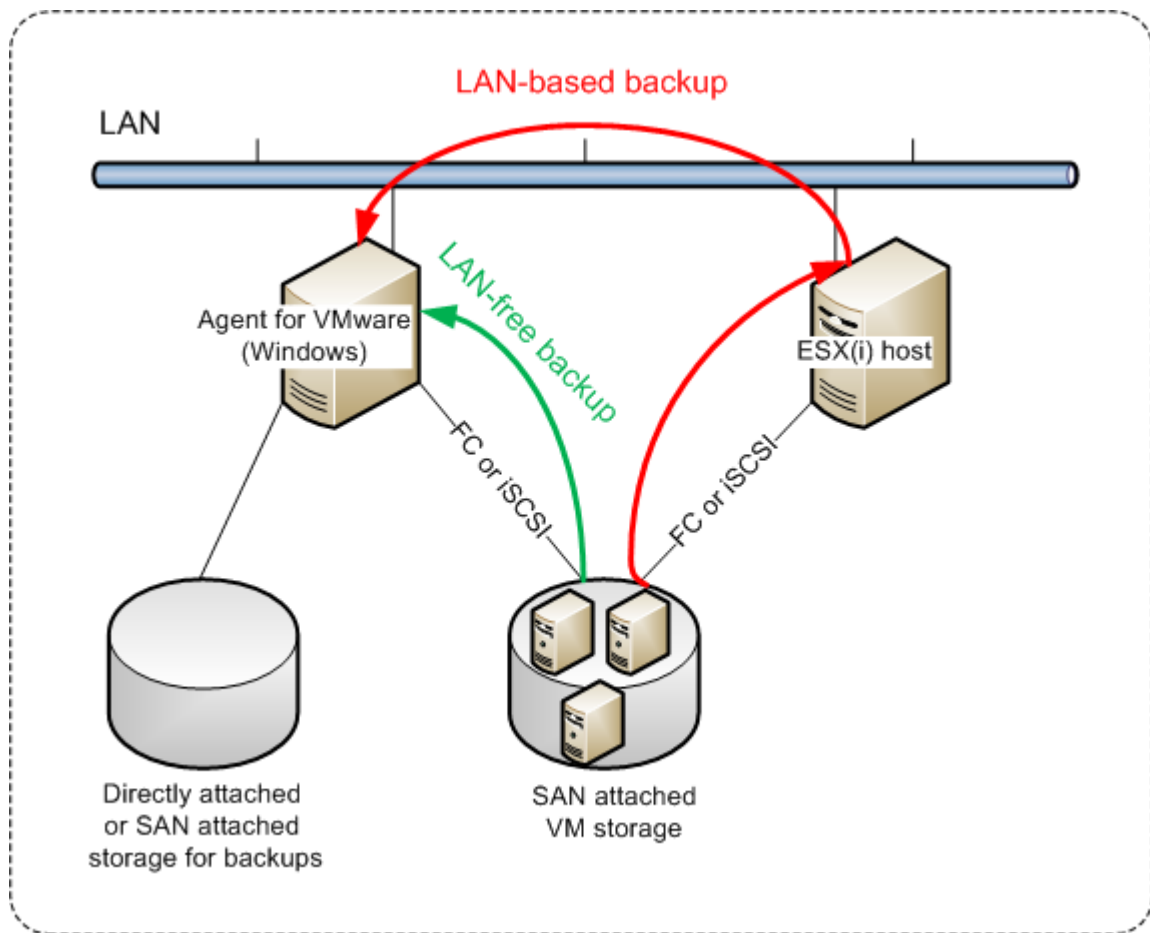
As a result, the software will continue updating the replica. All replications will be incremental.

## 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**.

---

#### **Note**

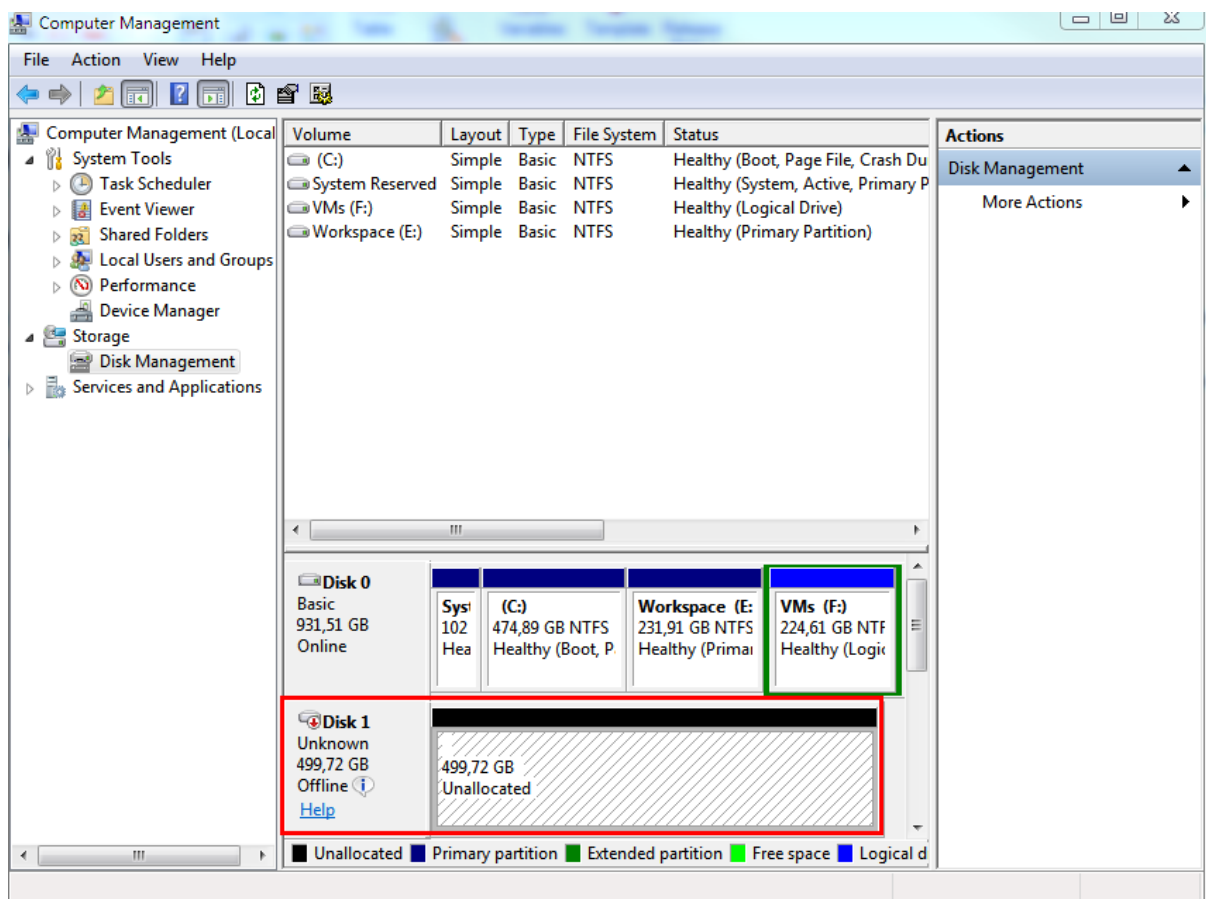
To find the **Administrative Tools** applet, you may need to change the **Control Panel** view to something other than **Home** or **Category**, or use search.

---

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.



## 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](#)".
- The machine running Agent for VMware (Windows) is configured as described in "[Configuring the machine running Agent for VMware](#)".
- The SAN storage is [registered on the management server](#).
- [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](#)".
- The "[SAN hardware snapshots](#)" backup option is enabled in the protection plan options.

## 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.



**Configure Volume Snapshot Copies**

? Snapshot Reserves (%): 5

☒ Make Snapshot directory (.snapshot) visible  
Visibility of .snapshot directory on this volume at the client mount points.

☒ Enable scheduled Snapshot Copies

**Snapshot Policies and Schedules**

Select a Snapshot policy that has desired schedules for Snapshot copies:

Snapshot Policy: default

Schedules of Selected Snapshot Policy:

Schedule...	Retained Sn...	Schedule	SnapMirror Label
hourly	6	Advance cron - {Minu...	-
weekly	2	On weekdays - Sunda...	weekly
daily	2	Daily - Run at 0 hour 1...	daily

Current Timezone: Etc/UTC

[Tell me more about Snapshot configurations](#)

OK Cancel

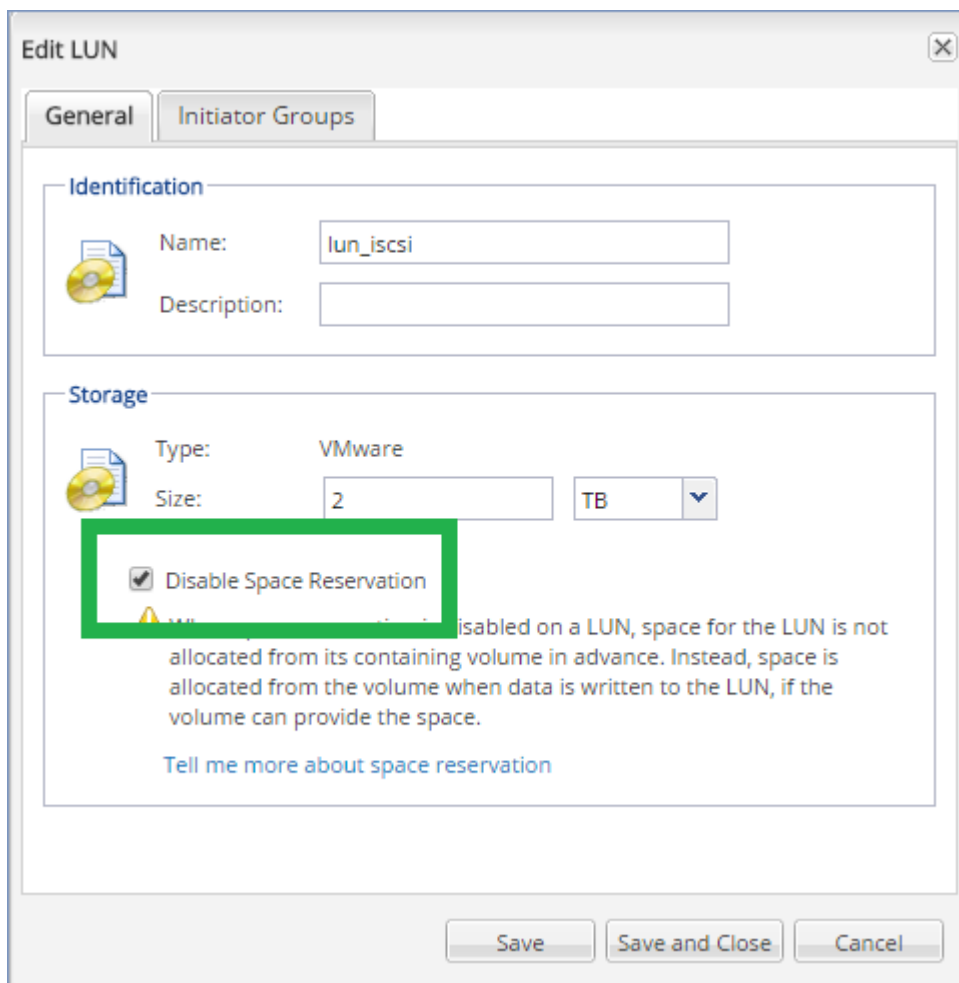
- [For NFS datastores] Access to NFS shares from Windows NFSv3 clients must be enabled on the Storage Virtual Machine (SVM) that was specified when creating the datastore. The access can be enabled by the following command:

```
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.



## 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](#)".

### Configuring NFS Client

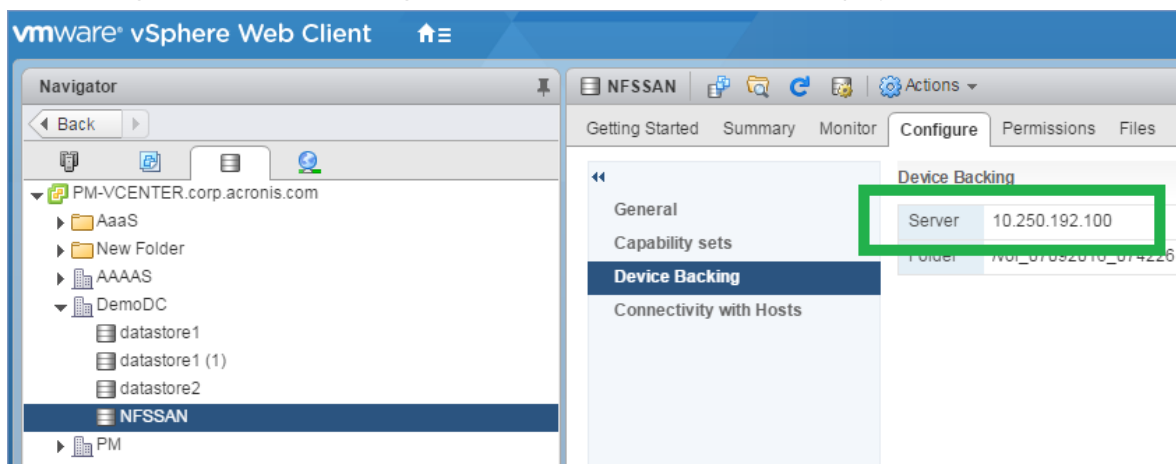
Ensure that all of the following is true:

- 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.

## 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**.

## 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](#) 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](#).

### ***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 protection plan](#), in **Where to back up**, select **Local folders**, and then type the letter corresponding to the locally attached storage, for example, **D:\**.

## 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](#). 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](#).

- 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.

## Support for VM migration

This section informs you about what to expect when virtual machines migrate within a vSphere environment, including migration between ESXi hosts that are part of a vSphere cluster.

### vMotion

vMotion moves a virtual machine's state and configuration to another host while the machine's disks remain in the same location on shared storage.

- vMotion of Agent for VMware (Virtual Appliance) is not supported and is disabled.
- vMotion of a virtual machine is disabled during a backup. Backups will continue to run after the migration is completed.

### Storage vMotion

Storage vMotion moves virtual machine disks from one datastore to another.

- Storage vMotion of Agent for VMware (Virtual Appliance) is not supported and is disabled.
- Storage vMotion of a virtual machine is disabled during a backup. Backups will continue to run after the migration.

## Managing virtualization environments

You can view the vSphere, Hyper-V, and Virtuozzo environments in their native presentation. Once the corresponding agent is installed and registered, the **VMware**, **Hyper-V**, or **Virtuozzo** tab appears under **Devices**.

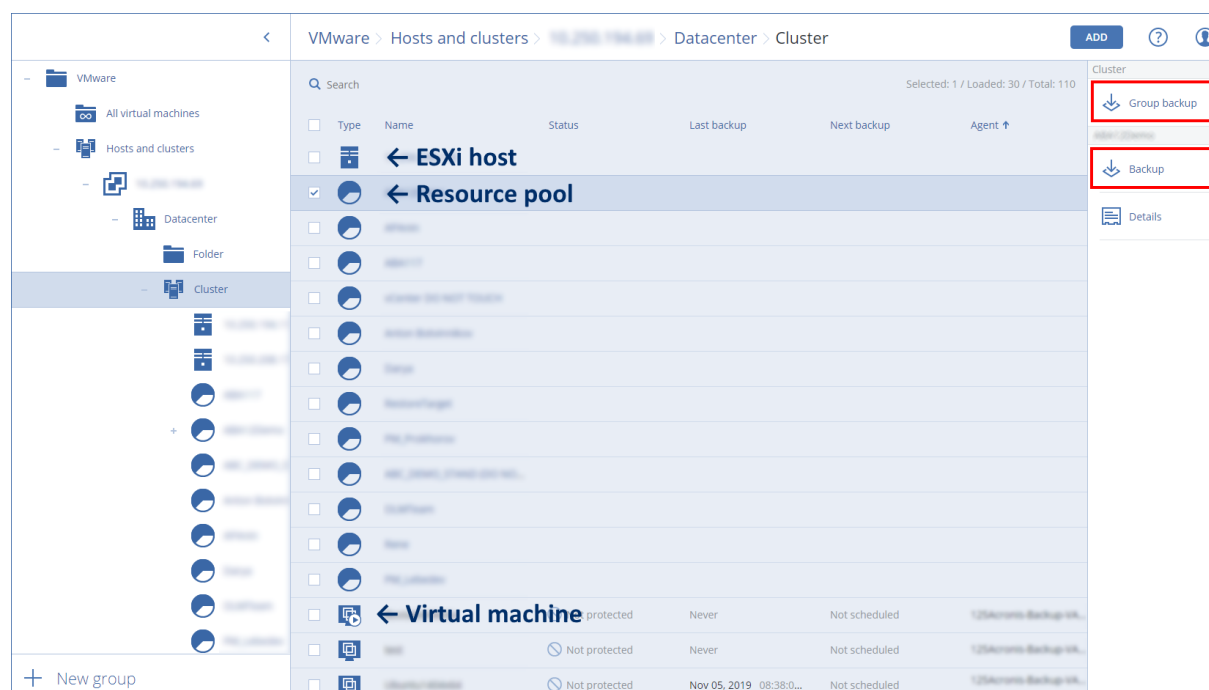
In the **VMware** tab, you can back up the following vSphere infrastructure objects:

- Data center
- Folder
- Cluster
- ESXi host
- Resource pool

Each of these infrastructure objects works 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 machines by clicking **Backup**, or the parent group machines in which the selected group is included by clicking **Group backup**.

For example, you have selected the cluster and then selected a resource pool inside it. If you click **Backup**, all virtual machines included in the selected resource pool will be backed up. If you click **Group backup**, all virtual machines included in the 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**.

## Viewing backup status in vSphere Client

You can view backup status and the last backup time of a virtual machine in vSphere Client.

This information appears in the virtual machine summary (**Summary > Custom attributes/Annotations/Notes**, depending on the client type and vSphere version). You can also enable the **Last backup** and **Backup status** columns on the **Virtual Machines** tab for any host, datacenter, folder, resource pool, or the entire vCenter Server.



To provide these attributes, Agent for VMware must have the following privileges in addition to those described in ["Agent for VMware - necessary privileges"](#):

- **Global > Manage custom attributes**
- **Global > Set custom attribute**

## Agent for VMware – necessary privileges

This section describes the privileges required for operations with ESXi virtual machines and, additionally, for virtual appliance deployment.

---

### Note

vStorage APIs must be installed on the ESXi host to enable virtual machine backups. See <https://kb.acronis.com/content/14931>.

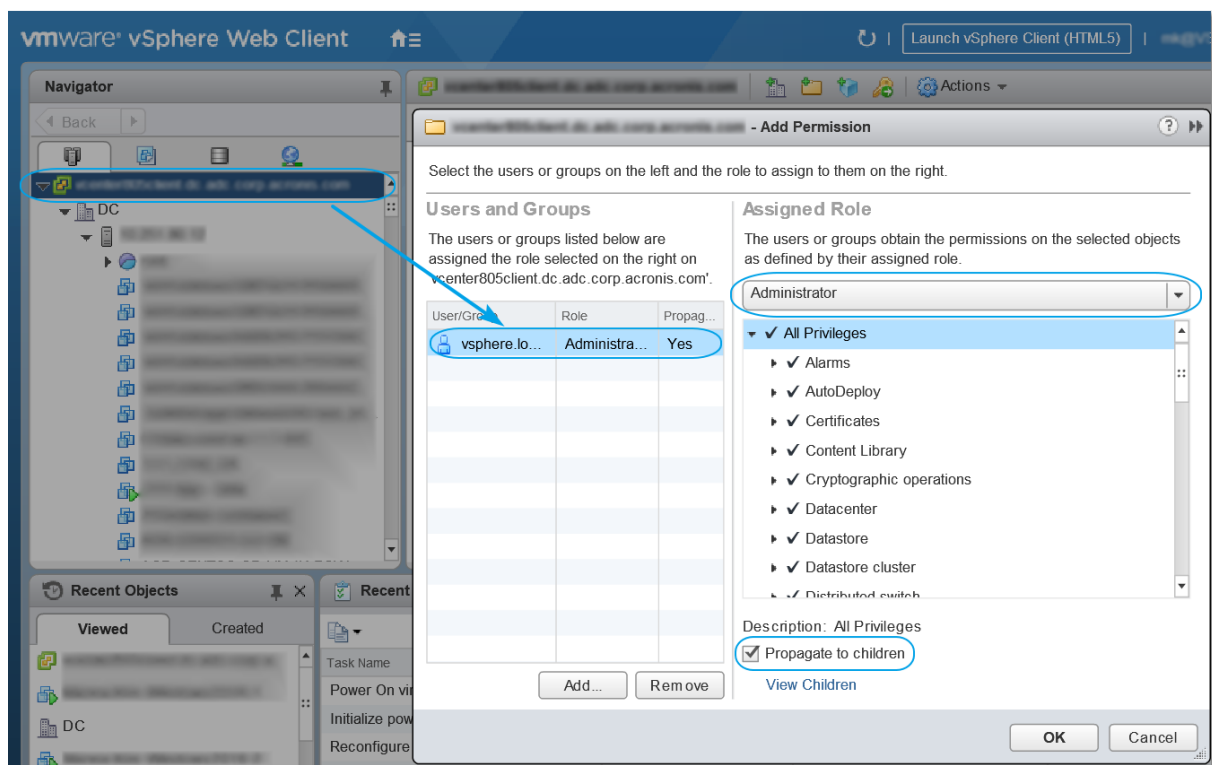
---

To perform any operations with vCenter objects, such as virtual machines, ESXi hosts, clusters, vCenter, and more, Agent for VMware authenticates on vCenter or ESXi host by using the vSphere credentials provided by a user. The vSphere account, used for connection to vSphere by Agent for VMware, must have the required privileges on all levels of vSphere infrastructure starting from the vCenter level.

Specify the vSphere 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 ["Managing virtualization environments"](#) section.

To assign the permissions to a vSphere user on the vCenter level, do the following:

1. Log in to vSphere web client.
2. Right-click on vCenter and then click **Add permission**.
3. Select or add a new user with the required role (the role must include all the required permissions from the table below).
4. Select the **Propagate to children** option.



Object	Privilege	Operation				
		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	+	+	+		
	Manage custom attributes	+	+	+		
	Set custom attribute	+	+	+		
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		+	+	+	+
	Import					+
Virtual machine > Configuration	Add existing disk	+	+		+	
	Add new disk		+	+	+	+
	Add or remove device		+		+	+
	Advanced	+	+	+		+
	Change CPU count		+			
	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	+		+		

	<b>disk access</b>					
	<b>Allow virtual machine download</b>	+	+	+	+	
<b>Virtual machine</b> <b>&gt; State</b>  <b>Virtual machine</b> <b>&gt; Snapshot management</b> (vSphere 6.5 and later)	<b>Create snapshot</b>	+		+	+	+
	<b>Remove snapshot</b>	+		+	+	+
<b>vApp</b>	<b>Add virtual machine</b>				+	

\* This privilege is required for backing up encrypted machines only.

\*\* This privilege is required for application-aware backups only.

## Backing up clustered Hyper-V machines

In a Hyper-V cluster, virtual machines may migrate between cluster nodes. Follow these recommendations to set up a correct backup of clustered Hyper-V machines:

1. A machine must be available for backup no matter what node it migrates to. To ensure that Agent for Hyper-V can access a machine on any node, the [agent service](#) must run under a domain user account that has administrative privileges on each of the cluster nodes. We recommend that you specify such an account for the agent service during the Agent for Hyper-V installation.
2. Install Agent for Hyper-V on each node of the cluster.
3. Register all of the agents on the management server.

## High Availability of a recovered machine

When you recover backed-up disks to an *existing* Hyper-V virtual machine, the machine's High Availability property remains as is.

When you recover backed-up disks to a *new* Hyper-V virtual machine, or do a conversion to a Hyper-V virtual machine [within a protection plan](#), the resulting machine is not highly available. It is considered as a spare machine and is normally powered off. If you need to use the machine in the production environment, you can configure it for High Availability from the **Failover Cluster Management** snap-in.

# Limiting the total number of simultaneously backed-up virtual machines

In the **Scheduling** backup option, you can limit the number of simultaneously backed-up virtual machines per protection plan.

When an agent runs multiple plans at the same time, the number of simultaneously backed-up machines adds up. Multiple backups that are run by the same agent might affect the backup performance and overload the host and the virtual machine storage. That is why you can configure another limitation, on the agent level.

## ***To limit the simultaneous backups on the agent level***

### ***Agent for VMware (Windows)***

1. On the machine with the agent, create a new text document, and then open it in a text editor.
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. Restart the agent.
  - a. In the **Start** menu, click **Run**.
  - b. Type **cmd**, and then click **OK**.
  - c. On the command line, run the following commands:

```
net stop mms
net start mms
```

### ***Agent for Hyper-V***

1. On the machine with the agent, create a new text document, and then open it in a text editor.
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. Restart the agent.
  - a. In the **Start** menu, click **Run**.
  - b. Type **cmd**, and then click **OK**.
  - c. On the command line, run the following commands:

```
net stop mms
net start mms
```

### ***Virtual appliances***

This procedure applies to Agent for VMware (Virtual Appliance), Agent for Scale Computing, Agent for Virtuozzo Hybrid Infrastructure, and Agent for oVirt.

1. In the console of the virtual appliance, press CTRL+SHIFT+F2 to open the command-line interface.
2. Open the /etc/Acronis/MMS.config file in a text editor.
3. Locate the following section:

```
<key name="SimultaneousBackupsLimits">
 <value name="MaxNumberOfSimultaneousBackups" type="Tdwor">"10"</value>
</key>
```

4. Replace 10 with the maximum number of parallel backups that you want to set.
5. Save the file.
6. Restart the agent by running the reboot command.

### ***All-in-One VMware appliance (OVF)***

1. Log in as the root user to the All-in-One VMware appliance .  
Use the same password that you use to log in to the Cyber Protect web console.
2. Open the /etc/Acronis/MMS.config file in a text editor.
3. Locate the following section:

```
<key name="SimultaneousBackupsLimits">
 <value name="MaxNumberOfSimultaneousBackups" type="Tdwor">"10"</value>
</key>
```

4. Replace 10 with the maximum number of parallel backups that you want to set.
5. Save the file.

- Restart the agent by using the following command:

```
sudo service acronis_mms restart
```

### Agent for Virtuozzo

Agent for Virtuozzo is bundled with Agent for Linux.

- Log in as the root user to the machine with the agent.  
Use the password that you use to log in to the Cyber Protect web console.
- Open the `/etc/Acronis/MMS.config` file in a text editor.
- Locate the following section:

```
<key name="SimultaneousBackupsLimits">
 <value name="MaxNumberOfSimultaneousBackups" type="Tdwor">"10"</value>
</key>
```

- Replace 10 with the maximum number of parallel backups that you want to set.
- Save the file.
- Run the following command to restart the agent:

```
sudo service acronis_mms restart
```

## Machine migration

You can perform machine migration by recovering its backup to a non-original 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	Virtuozzo virtual machine*	Virtuozzo container*	Virtuozzo Hybrid Infrastructure virtual machine*	Scale Computing HC3 virtual machine	RHV/o Virt virtual machine*
Physical machine	+	+	+	-	-	+	+	+
VMware ESXi virtual machine	+	+	+	-	-	+	+	+
Hyper-V virtual machine	+	+	+	-	-	+	+	+



Virtuozzo virtual machine*	+	+	+	+	-	+	+	+
Virtuozzo container*	-	-	-	-	+	-	-	-
Virtuozzo Hybrid Infrastructure virtual machine*	+	+	+	-	-	+	+	+
Scale Computing HC3 virtual machine	+	+	+	-	-	+	+	+
Red Hat Virtualization/oVirt virtual machine*	+	+	+	-	-	+	+	+

\* Only available with the cloud deployment.

For instructions on how to perform migration, refer to the following sections:

- Physical-to-virtual (P2V) – "Recovering a physical machine to a virtual machine" (p. 324)
- Virtual-to-virtual (V2V) – "Recovering a virtual machine" (p. 326)
- Virtual-to-physical (V2P) – "[Recovering a virtual machine](#)" (p. 326) or "Recovering disks and volumes by using bootable media" (p. 329)

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.

## Windows Azure and Amazon EC2 virtual machines

To back up a Windows Azure or Amazon EC2 virtual machine, install a protection agent on the machine. The backup and recovery operations are the same as with a physical machine.

Nevertheless, the machine is counted as virtual when you set quotas for the number of machines in a cloud deployment.

The difference from a physical machine is that Windows Azure and Amazon EC2 virtual machines cannot be booted from bootable media. If you need to recover to a new Windows Azure or Amazon EC2 virtual machine, follow the procedure below.

***To recover a machine as a Windows Azure or Amazon EC2 virtual machine***

1. Create a new virtual machine from an image/template in Windows Azure or Amazon EC2. The new machine must have the same disk configuration as the machine that you want to recover.
2. Install Agent for Windows or Agent for Linux on the new machine.
3. Recover the backed-up machine as described in "[Physical machine](#)". When configuring the recovery, select the new machine as the target machine.

## Network requirements

The agents installed on the backed-up machines must be able to communicate with the management server over the network.

## On-premises deployment

- If both the agents and the management server are installed in the Azure/EC2 cloud, all machines are already located in the same network. No additional actions are required.
- If the management server is located outside the Azure/EC2 cloud, the machines in the cloud will not have network access to the local network where the management server is installed. To enable the agents installed on such machines to communicate with the management server, a virtual private network (VPN) connection between the local (on-premises) and the cloud (Azure/EC2) network must be created. For instructions about how to create the VPN connection, refer to the following articles:

Amazon EC2: [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_VPN.html#vpn-create-cgw](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw)

Windows Azure: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

## Cloud deployment

In a cloud deployment, the management server is located in one of the Acronis data centers and is thus reachable by the agents. No additional actions are required.

# Protecting SAP HANA

Protection of SAP HANA is described in a separate document available at [https://dl.managed-protection.com/u/pdf/AcronisCyberProtect\\_15\\_SAP\\_HANA\\_whitepaper\\_en-US.pdf](https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdf).

# Antimalware and web protection

Antimalware protection in Cyber Protect provides you with the following benefits:

- Top protection in all the stages: proactive, active, and reactive.
- Four different antimalware technologies inside to provide the best-of-breed multi-layered protection.
- Management of Microsoft Security Essentials and Windows Defender Antivirus.

## Antivirus & Antimalware protection

The Antivirus and Antimalware protection module allows you to protect your Windows and macOS machines from all recent malware threats. Note that the Active Protection functionality that is part of the antimalware protection is not supported on macOS machines. See the full list of supported antimalware features: [Supported features by operating system](#).

Acronis Cyber Protect is supported and registered in Windows Security Center.

If your machine is already protected with a third-party antivirus solution at the moment of applying the Antivirus and Antimalware protection module to the machine, the system will generate an alert and will stop the Real-time protection in order to prevent potential compatibility and performance issues. You will need to either disable or uninstall the third-party antivirus solution, in order to enable fully functional Acronis Cyber Protect Antivirus and Antimalware protection.

The following antimalware capabilities are available to you:

- Detection of malware in files in the real-time protection and on-demand modes (for Windows, macOS)
- Detection of malicious behavior in processes (for Windows)
- Blocking access to malicious URLs (for Windows)
- Moving dangerous files to the quarantine
- Adding trusted corporate applications to the whitelist

The Antivirus and Antimalware protection module provides you with two types of scanning:

- Real-time protection scan
- On-demand malware scan

## Real-time protection scan

Real-time protection checks all the files that are being executed or opened on a machine to prevent malware threats.

You can choose one of the following types of scanning:

- On-access detection means that the antimalware program runs in the background and actively and constantly scans your machine system for viruses and other malicious threats for the entire duration that your system is powered on. Malware will be detected in both cases when a file is

being executed and during various operations with the file such as opening it for reading/editing.

- On-execution detection means that only executable files will be scanned at the moment they are run to ensure they are clean and will not cause any damage to your machine or data. Copying of an infected file will remain unnoticed.

## On-demand malware scan

Antimalware scanning is performed according to a schedule.

You can monitor the results of antimalware scanning in **Dashboard > Overview > Recently affected** widget.

## Antivirus & Antimalware protection settings

To learn how to create a protection plan with the Antivirus & Antimalware protection module, refer to "[Creating a protection plan](#)".

The following settings can be specified for the Antivirus & Antimalware protection module.

### 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.

In the Cyber Backup editions of Acronis Cyber Protect, Active Protection is a separate module in the [protection plan](#). Thus, it can be configured separately and applied to different devices or group of devices. In the Protect editions of Acronis Cyber Protect, Active Protection is part of the Antivirus & Antimalware protection module.

Active Protection is available for machines running the following operating systems:

- Desktop operating systems: Windows 7 Service Pack 1 and later  
On machines running Windows 7, ensure that [Update for Windows 7 \(KB2533623\)](#) is installed.
- Server operating systems: 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.

Default setting: **Enabled**.

## Active Protection 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**  
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.

Default setting: **Revert using cache**.

## Network folder protection

The **Protect network folders mapped as local drives** option defines whether Antivirus & Antimalware protection protects from local malicious processes network folders that are mapped as local drives.

This option applies to folders shared via SMB or NFS protocols.

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, specify a local folder. Network folders, including folders on mapped drives, are not supported.

Default setting: **Enabled**.

## Server-side protection

This option defines whether Antivirus & Antimalware protection protects network folders that are shared by you from the external incoming connections from other servers in the network that may potentially bring threats.

Default setting: **Disabled**.

## Setting trusted and blocked connections

On the **Trusted** tab, you can specify the connections that are allowed to modify any data. You must define the user name and IP address.

On the **Blocked** tab, you can specify the connections that will not be able to modify any data. You must define the user name and IP address.

## Self-protection

**Self-protection** prevents unauthorized changes to the software's own processes, registry records, executable and configuration files, Secure Zone, and backups located in local folders. We do not recommend disabling this feature.

Default setting: **Enabled**.

## Allowing processes to modify backups

The **Allow specific processes to modify backups** option is effective when **Self-protection** is enabled.

It 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 is useful, for example, if you remove backup files or move them to a different location by using a script.

If this option is disabled, 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 remove 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 enabled, you can allow other processes to modify the backups. Specify the full path to the process executable, starting with the drive letter.

Default setting: **Disabled**.

## Cryptomining process detection

This option defines whether Antivirus & Antimalware protection detects potential cryptomining malware.

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.

Default setting: **Enabled**.

## Cryptomining process detection settings

Select the action that the software will perform when a cryptomining activity is detected, and then click **Done**. You can select one of the following:

- **Notify only**

The software generates an alert about the process suspected of cryptomining activities.

- **Stop the process**

The software generates an alert and stops the process suspected of cryptomining activities.

Default setting: **Stop the process**.

## Quarantine

Quarantine is a folder where to keep suspicious (probably infected) or potentially dangerous files isolated.

**Remove quarantined files after** – Defines the period in days after which the quarantined files will be removed.

Default setting: **30 days**.

## Behavior detection

Acronis Cyber Protect protects your system by using behavioral heuristics to identify malicious processes: it compares the chain of actions performed by a process with the chains of actions recorded in the database of malicious behavior patterns. Thus, a new malware is detected by its typical behavior.

Default setting: **Enabled**.

### Behavior detection settings

In **Action on detection**, select the action that the software will perform when detecting a malware activity, and then click **Done**.

You can select one of the following:

- **Notify only**

The software will generate an alert about the process suspected of malware activity.

- **Stop the process**

The software will generate an alert and stop the process suspected of malware activity.

- **Quarantine**

The software will generate an alert, stop the process, and move the executable file to the quarantine folder.

Default setting: **Quarantine**.



## Real-time protection

**Real-time protection** constantly checks your machine system for viruses and other threats for the entire time that your system is powered on.

Default setting: **Enabled**.

### Configuring the action on detection for Real-time protection

In **Action on detection**, select the action that the software will perform when a virus or other malicious threat is detected, and then click **Done**.

You can select one of the following:

- **Block and notify**  
The software blocks the process and generates an alert about the process suspected of malware activities.
- **Quarantine**  
The software generates an alert, stops the process, and moves the executable file to the quarantine folder.

Default setting: **Quarantine**.

### Configuring the scan mode for Real-time protection

In **Scan mode**, select the action that the software will perform when a virus or other malicious threat is detected, and then click **Done**.

You can select one of the following:

- **Smart on-access** – Monitors all system activities and automatically scans files when they are accessed for reading or writing, or whenever a program is launched.
- **On-execution** – Automatically scans only executable files when they are launched to ensure that they are clean and will not cause any damage to your computer or data.

Default setting: **Smart on-access**.

## Schedule scan

You can define schedule according to which your machine will be checked for malware, by enabling the **Schedule scan** setting.

### Action on detection:

- **Quarantine**  
The software generates an alert and moves the executable file to the quarantine folder.
- **Notify only**  
The software generates an alert about the process that is suspected to be malware.

Default setting: **Quarantine**.

### Scan type:

- **Full**

The full scan takes much longer to finish in comparison to the quick scan because every file will be checked.

- **Quick**

The quick scan only scans the common areas where malware normally resides on the machine.

- **Custom**

The custom scan checks the files/folders that were selected by the administrator to the Protection plan.

You can schedule all three scans **Quick**, **Full**, and **Custom** scan in one protection plan.

Default settings:

- **Quick** and **Full** scan are scheduled.
- **Custom** scan is disabled by default.

### Schedule the task run using the following events:

- **Schedule by time** – The task will run according to the specified time.
- **When user logs in to the system** – By default, a login of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.
- **When user logs off the system** – By default, a logoff of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.

---

#### Note

The task will not run at system shutdown. Shutting down and logging off are different events in the scheduling configuration.

---

- **On the system startup** – The task will run when the operating system starts.
- **On the system shutdown** – The task will run when the operating system shuts down.

Default setting: **Schedule by time**.

### Schedule type:

- **Monthly** – Select the months and the weeks or days of the month when the task will run.
- **Daily** – Select the days of the week when the task will run.
- **Hourly** – Select the days of the week, repetition number, and the time interval in which the task will run.

Default setting: **Daily**.

**Start at** – Select the exact time when the task will run.

**Run within a date range** – Set a range in which the configured schedule will be effective.

**Start conditions** – Define all conditions that must be met simultaneously for the task to run.

Start conditions for antimalware scans are similar to the start conditions for the Backup module that are described in "Start conditions" (p. 255). You can define the following additional start conditions:

- **Distribute task start time within a time window** – This option allows you to set the time frame for the task in order to avoid network bottlenecks. You can specify the delay in hours or minutes. For example, if the default start time 10:00 AM and the delay is 60 minutes, then the task will start between 10:00 AM and 11:00 AM.
- **If the machine is turned off, run missed tasks at the machine startup**
- **Prevent the sleep or hibernate mode during task running** – This option is effective only for machines running Windows.
- **If start conditions are not met, run the task anyway after** – Specify the period after which the task will run, regardless of the other start conditions.

**Scan only new and changed files** – Only newly created and modified files will be scanned.

Default setting: **Enabled**.

When scheduling a **Full scan**, you have two additional options:

- **Scan archive files**

Default setting: **Enabled**.

- **Max recursion depth**

How many levels of embedded archives can be scanned. For example, MIME document > ZIP archive > Office archive > document content.

Default setting: **16**.

- **Max size**

Maximum size of an archive file to be scanned.

Default setting: **Unlimited**.

- **Scan removable drives**

Default setting: **Disabled**.

- **Mapped (remote) network drives**
- **USB storage devices** (such as flash drives and external hard drives)
- **CDs/DVDs**

## Exclusions

To minimize the resources used by the heuristic analysis and to eliminate the so-called false positives when a trusted program is considered as ransomware, you can define the following settings:

On the **Trusted** tab, you can specify:

- Processes that will never be considered as malware. Processes signed by Microsoft are always trusted.
- Folders in which file changes will not be monitored.
- Files and folders in which the scheduled scan will not be performed.

On the **Blocked** tab, you can specify:

- Processes that will always be blocked. These processes will not be able to start as long as Active Protection is enabled on the machine.
- Folders in which any processes will be blocked.

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.

Default setting: No exclusions are defined by default.

## URL Filtering

Please see [URL Filtering](#) for detailed description.

## Active Protection

In the Cyber Backup editions of Acronis Cyber Protect, Active Protection is a separate module in the [protection plan](#). This module has the following settings:

- Action on detection
- Self-protection
- Network folder protection
- Server-side protection
- Cryptomining process detection
- Exclusions

In the Protect editions of Acronis Cyber Protect, Active Protection is part of the Antivirus & Antimalware protection module.

Active Protection is available for machines running the following operating systems:

- Desktop operating systems: Windows 7 Service Pack 1 and later  
On machines running Windows 7, ensure that [Update for Windows 7 \(KB2533623\)](#) is installed.
- Server operating systems: Windows Server 2008 R2 and later.

Agent for Windows must be installed on the machine.

To learn more about Active Protection and its settings, refer to "Antivirus & Antimalware protection settings" (p. 509).

## Windows Defender Antivirus

Windows Defender Antivirus is a built-in antimalware component of Microsoft Windows that is delivered starting from Windows 8.

The Windows Defender Antivirus module allows you to configure Windows Defender Antivirus security policy and track its status via the Cyber Protect web console.

This module is applicable for the machines on which Windows Defender Antivirus is installed.

## Schedule scan

Specify the schedule for scheduled scanning.

### Scan mode:

- **Full** – a full check of all files and folders in addition to the items scanned during a quick scan. It requires more machine resources compared to the quick scan.
- **Quick** – a quick check of the in-memory processes and folders where malware is typically found. It required less machine resources.

Define the time and day of the week when the scan will be performed.

**Daily quick scan** – define the time for the daily quick scan.

You can set the following options depending on your needs:

**Start the scheduled scan when the machine is on but not in use**

**Check for the latest virus and spyware definitions before running a scheduled scan**

**Limit CPU usage during the scan to**

For more details about the Windows Defender Antivirus schedule settings, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings>.

## Default actions

Define the default actions to be performed for the detected threats of different severity levels:

- **Clean** – clean up the detected malware on a machine.
- **Quarantine** – put the detected malware in the quarantine folder but do not remove it.
- **Remove** – remove the detected malware from a machine.
- **Allow** – do not remove or quarantine the detected malware.
- **User defined** – a user will be prompted to specify the action to be performed with the detected malware.
- **No action** – no action will be taken.
- **Block** – block the detected malware.

For more details about the Windows Defender Antivirus default actions settings, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings>.

## Real-time protection

Enable **Real-time protection** to detect and stop malware from installing or running on machines.

**Scan all downloads** – if selected, scanning is performed for all downloaded files and attachments.

**Enable behavior monitoring** – if selected, behavior monitoring will be enabled.

**Scan network files** – if selected, network files will be scanned.

**Allow full scan on mapped network drives** – if selected, mapped network drives will be fully scanned.

**Allow email scanning** – if enabled, the engine will parse the mailbox and mail files, according to their specific format, in order to analyze the mail bodies and attachments.

For more details about the Windows Defender Antivirus real-time protection settings, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings>.

## Advanced

Specify the advanced scan settings:

- **Scan archive files** – include archived files such as .zip or .rar files in the scanning.
- **Scan removable drives** – scan removable drives during full scans.
- **Create a system restore point** – in some cases an important file or registry entry could be removed as "false positive", then you will be able to recover from a restore point.
- **Remove quarantined files after** – define the period after which the quarantined files will be removed.
- **Send file samples automatically when a further analysis is required:**
  - **Always prompt** – you will be asked for confirmation before file sending.
  - **Send safe samples automatically** – most samples will be sent automatically except files that may contain personal information. Such files will require additional confirmation.
  - **Send all samples automatically** – all samples will be sent automatically.
- **Disable Windows Defender Antivirus GUI** – if selected, the Windows Defender Antivirus user interface will not be available to a user. You can manage the Windows Defender Antivirus policies via Cyber Protect web console.
- **MAPS (Microsoft Active Protection Service)** – online community that helps you choose how to respond to potential threats.
  - **I don't want to join MAPS** – no information will be sent to Microsoft about the software that was detected.
  - **Basic membership** – basic information will be sent to Microsoft about the software that was detected.
  - **Advanced membership** – more detailed information will be sent to Microsoft about the software that was detected.

For more details, refer to <https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise>.

For more details about the Windows Defender Antivirus advanced settings, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings>.

## Exclusions

You can define the following files and folders to be excluded from scanning:

- **Processes** – any file that the defined process reads from or writes to will be excluded from scanning. You need to define a full path to the executable file of the process.
- **Files and folders** – the specified files and folders will be excluded from scanning. You need to define a full path to a folder or file, or define the file extension.

For more details about the Windows Defender Antivirus exclusion settings, refer to <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings>.

## Microsoft Security Essentials

Microsoft Security Essentials is a built-in antimalware component of Microsoft Windows that is delivered with Windows versions earlier than 8.

The Microsoft Security Essentials module allows you to configure Microsoft Security Essentials security policy and track its status via the Cyber Protect web console.

This module is applicable for machines on which Microsoft Security Essentials is installed.

The Microsoft Security Essentials settings are almost the same as [Microsoft Windows Defender Antivirus](#) except the absence of the real-time protection settings and inability to define exclusions via the Cyber Protect web console.

## URL filtering

Malware is often distributed by malicious or infected sites and uses the so called "drive-by download" method of infection. URL filtering allows you to protect your machines from threats like malware and phishing coming from the Internet. You can block the access to websites that may have malicious content.

URL filtering also allows you to control the web usage in order to comply with external regulations or internal company policies. You can configure different access policies for more than 40 website categories.

Currently, the HTTP and HTTPS connections from Windows machines are checked by the protection agent.

The URL filtering feature requires an Internet connection to function.

---

**Note**

Conflicts might occur if URL filtering is used in parallel with third-party antivirus solutions that also use URL filtering features. You can determine the statuses of other installed antivirus solutions through Windows Security Center.

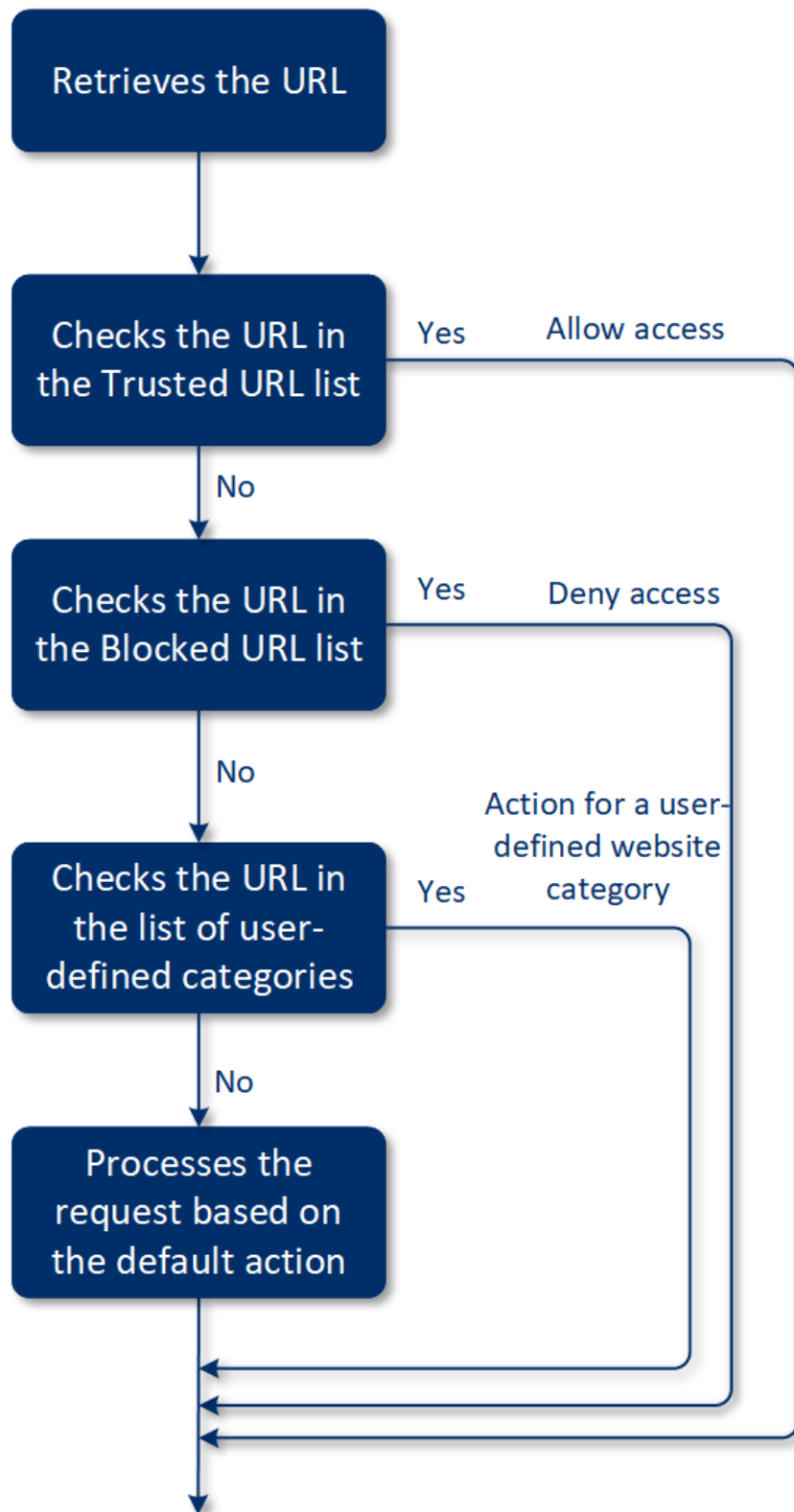
If a compatibility or performance issue occurs, uninstall the third-party solution or disable the URL filtering module in your protection plans

---

## How it works

A user follows a link or enters a URL in the address bar of a browser. The Interceptor fetches the URL and sends it to the protection agent. The protection agent parses the URL, checks the database, and then returns a verdict to the Interceptor. If the URL is forbidden, the Interceptor blocks the access to it and notifies the user that it is not allowed to see this content.





### ***To configure the URL filtering***

1. Create a protection plan with the URL filtering module enabled.
2. Configure the URL filtering settings (see below).
3. Assign the protection plan to the machines that you want.

To check which URLs have been blocked, go to **Dashboard > Alerts**.

## URL filtering settings

The following settings can be configured for the URL filtering module.

### Malicious website access

Specify which action will be performed when a user tries to open a malicious website:

- **Block** – The access to the malicious website will be blocked and an alert will be generated.
- **Always ask user** – The user will be asked to choose whether to proceed to the website or to go back.

### Categories to filter

There are 44 website categories for which you can configure the access policy. By default, the access to websites from all categories is allowed.

	Website category	Description
1	<b>Advertising</b>	This category covers domains whose main purpose is to serve advertisements.
2	<b>Message boards</b>	This category covers forums, discussion boards, and question-answer type websites. This category does not cover the specific sections on company websites where customers ask questions.
3	<b>Personal websites</b>	This category covers personal websites, as well as all types of blogs: individual, group, and even company ones. A blog is a journal published on the World Wide Web. It consists of entries ("posts"), typically displayed in reverse chronological order so that the most recent post appears first.
4	<b>Corporate/business websites</b>	This is a broad category that covers corporate websites that typically do not belong to any other category.
5	<b>Computer software</b>	This category covers websites offering computer software, typically either open-source, freeware, or shareware. It may also cover some online software stores.
6	<b>Medical drugs</b>	This category covers websites related to medicine/alcohol/cigars that have discussions on the use or selling of (legal) medical drugs or paraphernalia, alcohol, or tobacco products.  Note that illegal drugs are covered in the Narcotics category.
7	<b>Education</b>	This category covers websites belonging to official educational institutions, including those that are outside of the .edu domain. It also includes educational websites, such as an encyclopedia.

8	<b>Entertainment</b>	This category covers websites that provide information related to artistic activities and museums, as well as websites that review or rate content such as movies, music, or art.
9	<b>File sharing</b>	This category covers file-sharing websites where a user can upload files and share them with others. It also covers torrent-sharing websites and torrent trackers.
10	<b>Finance</b>	This category covers websites belonging to all banks around the world that provide online access. Some credit unions and other financial institutions are covered as well. However, some local banks may be left uncovered.
11	<b>Gambling</b>	This category covers gambling websites. These are the “online casino” or “online lottery” type website, which typically requires payment before a user can gamble for money in online roulette, poker, blackjack, or similar games. Some of them are legitimate, meaning there is a chance to win; and some are fraudulent, meaning that there is no chance to win. It also detects “beating tips and cheats” websites that describe the ways to make money on gambling and online lottery websites.
12	<b>Games</b>	<p>This category covers websites that provide online games, typically based on Adobe Flash or Java applets. It does not matter for detection whether the game is free or requires a subscription, however, casino-style websites are detected in the Gambling category.</p> <p>This category does not cover:</p> <ul style="list-style-type: none"> <li>• Official websites of companies that develop video games (unless they produce online games)</li> <li>• Discussion websites where games are discussed</li> <li>• Websites where non-online games can be downloaded (some of them are covered in the Illegal category)</li> <li>• Games that require a user to download and run an executable, like World of Warcraft; those can be prevented by different means like a firewall</li> </ul>
13	<b>Government</b>	This category covers government websites, including government institutions, embassies, and office websites.
14	<b>Hacking</b>	This category covers websites that provide the hacking tools, articles, and discussion platforms for hackers. It also covers websites offering exploits for common platforms that facilitate Facebook or Gmail account hacking.
15	<b>Illegal activities</b>	<p>This category is a broad category related to hate, violence and racism, and it is intended to block the following categories of websites:</p> <ul style="list-style-type: none"> <li>• Websites belonging to terrorist organizations</li> <li>• Websites with racist or xenophobic content</li> </ul>

		<ul style="list-style-type: none"> <li>• Websites discussing aggressive sports, and/or promoting violence</li> </ul>
16	<b>Health and fitness</b>	This category covers websites associated with medical institutions, websites related to disease prevention and treatment, websites that offer information or products about weight loss, diets, steroids, anabolic or HGH products, as well as websites providing information on plastic surgery.
17	<b>Hobbies</b>	This category covers websites that present resources related to activities typically performed during an individual's free time, such as collecting, arts and crafts, and cycling.
18	<b>Web hosting</b>	This category covers free and commercial website hosting services that allow private users and organizations to create and publish web pages.
19	<b>Illegal downloads</b>	<p>This category covers websites related to software piracy, including:</p> <ul style="list-style-type: none"> <li>• Peer-to-peer (BitTorrent, emule, DC++) tracker websites that are known in helping to distribute copyrighted content without the copyright holder's consent</li> <li>• Warez (pirated commercial software) websites and discussion boards</li> <li>• Websites providing users with cracks, key generators, and serial numbers to facilitate the use of software illegally</li> </ul> <p>Some of these websites may also be detected as pornography or alcohol/cigars, since they often use porn or alcohol advertisements to earn money.</p>
20	<b>Instant messaging</b>	This category covers instant messaging and chat websites that allow users to chat in real-time. It will also detect yahoo.com and gmail.com since they both contain an embedded instant messenger service.
21	<b>Jobs/employment</b>	This category covers websites presenting job boards, job-related classified advertisements, and career opportunities, as well as aggregators of such services. It does not cover recruiting agencies or the "jobs" pages on regular company websites.
22	<b>Mature content</b>	This category covers the content that was labeled by a website creator as requiring a mature audience. It covers a wide range of websites from the Kama Sutra book and sex education websites, to hardcore pornography.
23	<b>Narcotics</b>	This category covers websites sharing information about recreational and illegal drugs. This category also covers websites covering development or growing drugs.
24	<b>News</b>	This category covers news websites that provide text and video news. It strives to cover both global and local news websites; however, some small local news websites may not be covered.

25	<b>Online dating</b>	<p>This category covers online dating websites – paid and free - where users can search for other people by using some criteria. They may also post their profiles to let others search them. This category includes both free and paid online dating websites.</p> <p>Because most of the popular social networks can be used as online dating websites, some popular websites like Facebook are also detected in this category. It's recommended to use this category with the Social networks category.</p>
26	<b>Online payments</b>	<p>This category covers websites offering online payments or money transfers. It detects popular payment websites like PayPal or Moneybookers. It also heuristically detects the webpages on the regular websites that ask for the credit card information, allowing detection of hidden, unknown, or illegal online stores.</p>
27	<b>Photo sharing</b>	<p>This category covers photo-sharing websites whose primary purpose is to let users upload and share photos.</p>
28	<b>Online stores</b>	<p>This category covers known online stores. A website is considered an online store if it sells goods or services online.</p>
29	<b>Pornography</b>	<p>This category covers websites containing erotic content and pornography. It includes both paid and free websites. It covers websites that provide pictures, stories, and videos, and it will also detect pornographic content on mixed-content websites.</p>
30	<b>Portals</b>	<p>This category covers websites that aggregate information from multiple sources and various domains, and that usually offer features such as search engines, e-mail, news, and entertainment information.</p>
31	<b>Radio</b>	<p>This category covers websites that offer Internet music streaming services, from online radio stations to websites that provide on-demand (free or paid) audio content.</p>
32	<b>Religion</b>	<p>This category covers websites promoting religion or a sect. It also covers the discussion forums related to one or multiple religions.</p>
33	<b>Search engines</b>	<p>This category covers search engine websites, such as Google, Yahoo, and Bing.</p>
34	<b>Social networks</b>	<p>This category covers social network websites. This includes MySpace.com, Facebook.com, Bebo.com, etc. However, specialized social networks, like YouTube.com, will be listed in the Video/Photo category.</p>
35	<b>Sport</b>	<p>This category covers websites that offer sports information, news, and tutorials.</p>
36	<b>Suicide</b>	<p>This category covers websites promoting, offering, or advocating suicide. It does not cover suicide prevention clinics.</p>

37	<b>Tabloids</b>	This category is mainly designed for soft pornography and celebrity gossip websites. A lot of the tabloid-style news websites may have subcategories listed here. Detection for this category is also based on heuristics.
38	<b>Waste of time</b>	This category covers websites where individuals tend to spend a lot of time. This can include websites from other categories such as social networks or entertainment.
39	<b>Traveling</b>	This category covers websites that present travel offers and travel equipment, as well as travel destination reviews and ratings.
40	<b>Videos</b>	This category covers websites that host various videos or photos, either uploaded by users or provided by various content providers. This includes websites like YouTube, Metacafe, Google Video, and photo websites like Picasa or Flickr. It will also detect videos embedded in other websites or blogs.
41	<b>Violent cartoons</b>	<p>This category covers websites discussing, sharing, and offering violent cartoons or manga that may be inappropriate for minors due to violence, explicit language, or sexual content.</p> <p>This category doesn't cover the websites that offer mainstream cartoons such as "Tom and Jerry".</p>
42	<b>Weapons</b>	This category covers websites offering weapons for sale or exchange, manufacture, or usage. It also covers the hunting resources and the usage of air and BB guns, as well as melee weapons.
43	<b>Email</b>	This category covers websites that provide email functionality as a web application.
44	<b>Web proxy</b>	<p>This category covers websites that provide web proxy services. This is a "browser inside a browser" type website when a user opens a web page, enters the requested URL into a form, and clicks "Submit". The web proxy site downloads the actual page and shows it inside the user browser.</p> <p>These are the following reasons this type is detected (and might need to be blocked):</p> <ul style="list-style-type: none"> <li>• For anonymous browsing. Since requests to the destination web server are made from the proxy web server, only its IP address is visible and if the server administrators trace the user, the trace will end on web proxy – which may or may not keep logs necessary to locate the original user.</li> <li>• For location spoofing. User IP addresses are often used for profiling the service by the source location (some national government websites may only be available from local IP addresses), and using those services might help the user to spoof their true location.</li> <li>• For accessing prohibited content. If a simple URL filter is used, it will</li> </ul>

		<p>only see the web proxy URLs and not the actual servers that the user visits.</p> <ul style="list-style-type: none"> <li>• For avoiding company monitoring. A business policy might require monitoring employee Internet usage. By accessing everything through a web proxy, a user might escape monitoring that will not provide correct information.</li> </ul> <p>Since the SDK analyzes the HTML page (if provided), and not just URLs, for some categories the SDK will still be able to detect the content. Other reasons, however, cannot be avoided just by using the SDK.</p>
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

If you enable the **Show all notifications for blocked URLs by categories** check box, the notifications for blocked URLs by categories will be shown in the tray. If a website has several sub-domains, notifications are also generated for them, therefore their number may be significant.

## Exclusions

URLs that are known as safe can be added to the list of the trusted URLs. URLs that represent a threat can be added to the list of the blocked URLs.

### ***To add a URL to a list***

1. In the URL filtering module of a protection plan, click **Exclusions**.
2. Select the desired list: **Trusted** or **Blocked**.
3. Click **Add**.
4. Specify the URL or IP address, and then click the check mark.

### **Examples of URL exclusions:**

- If you add xyz.com as trusted/untrusted, all addresses in the xyz.com domain will be treated as trusted or untrusted depending where you want to add it.
- If you want to add a specific subdomain, you can add **mail.xyz.com** as trusted/untrusted, and this will not cause all the **xyz.com** addresses to be trusted or untrusted.
- If you want to add IPv4 to be trusted/untrusted, the following format has to be used to be valid:  
**20.53.203.50.**
- If you want to add several URL exclusions at the same time, make sure to add each entry on a new line:  
**acronis.com**  
**mail.xyz.com**  
**20.53.203.50**

# Quarantine

**Quarantine** is a special isolated folder on a machine's hard disk where the suspicious files detected by Antivirus & Antimalware protection are placed to prevent further spread of threats.

Quarantine allows you to review suspicious and potentially dangerous files from all machines and decide whether they should be removed or restored. The quarantined files are automatically removed if the machine is removed from the system.

## How do files get into the quarantine folder?

1. You configure the protection plan and define the default action for infected files – to place in Quarantine.
2. The system during the scheduled or on-access scanning detects malicious files, places them in the secure folder - Quarantine.
3. The system updates the quarantine list on machines.
4. Files are automatically cleaned up from the quarantine folder after the time period defined in the **Remove quarantined files after** setting in the protection plan.

## Managing quarantined files

To manage the quarantined files, go to **Anti-malware protection > Quarantine**. You will see a list with quarantined files from all machines.

Name	Description
<b>File</b>	The file name.
<b>Date quarantined</b>	The date and time when the file was placed in Quarantine.
<b>Device</b>	The device on which the infected file was found.
<b>Threat name</b>	The threat name.
<b>Protection plan</b>	The protection plan according to which the suspicious file was placed in Quarantine.

You have two possible actions with quarantined files:

- **Delete** – permanently remove a quarantined file from all machines.
- **Restore** – restore a quarantined file to the original location without any modifications. If currently there is a file with the same name in the original location, then it will be overwritten with the restored file.

## Quarantine location on machines

The default location for quarantined files is:



For a Windows machine: %ProgramData%\%product\_name%\Quarantine

For a Mac/Linux machine: /usr/local/share/%product\_name%/quarantine

## Corporate whitelist

---

### Important

Corporate whitelist requires that Scan Service is installed on the management server.

---

An antivirus solution might identify legitimate corporate-specific applications as suspicious. To prevent these false positives detections, the trusted applications are manually added to a whitelist, which is time consuming.

Cyber Protect can automate this process: backups are scanned by the Antivirus and Antimalware protection module and the scanned data are analyzed, so that such applications are moved to the whitelist, and false positive detections are prevented. Also, the company-wide whitelist improves the further scanning performance.

The whitelist can be enabled and disabled. When it is disabled, the files added to it are temporarily hidden.

### Automatic adding to the whitelist

1. Run a cloud scanning of backups on at least two machines. You can do this by using the "Backup scanning plans" (p. 356).
2. In the whitelist settings, enable the **Automatic generation of whitelist** switch.

### Manual adding to the whitelist

Even when the **Automatic generation of whitelist** switch is disabled, you can add files to the whitelist manually.

1. In the Cyber Protect web console, go to **Antimalware protection > Whitelist**.
2. Click **Add file**.
3. Specify the path to the file, and then click **Add**.

### Adding quarantined files to the whitelist

You can add files that are quarantined to the whitelist.

1. In the Cyber Protect web console, go to **Antimalware protection > Quarantine**.
2. Select a quarantined file, and then click **Add to whitelist**.

### Whitelist settings

When you enable the **Automatic generation of whitelist** switch, you must specify one of the following levels of heuristic protection:

- **Low**

Corporate applications will be added to the whitelist only after a significant amount of time and checks. Such applications are more trusted. However, this approach increases the possibility of false positive detections. The criteria to consider a file as clean and trusted are high.

- **Default**

Corporate applications will be added to the whitelist according to the recommended protection level, to reduce possible false positive detections. The criteria to consider a file as clean and trusted are medium.

- **High**

Corporate applications will be added to the whitelist faster, to reduce possible false positive detections. However, this does not guarantee that the software is clean, and it might later be recognized as suspicious or malware. The criteria to consider a file as clean and trusted are low.

## Viewing details about items in the whitelist

You can click an item in the whitelist to view more information about it and to analyze it online.

If you are unsure about an item that you added, you can check it in the VirusTotal analyzer. When you click **Check on VirusTotal**, the site analyzes suspicious files and URLs to detect types of malware by using the file hash of the item that you added. You can view the hash in the **File hash (MD5)** string.

The **Machines** value represents the number of machines where such hash was found during backup scanning. This value is populated only if an item came from Backup scanning or Quarantine. This field remains empty if the file has been added manually to the whitelist.

## Antimalware scan of backups

To prevent the recovery of infected files, configure a [backup scanning plan](#) and ensure that the backups do not contain malware.

Antimalware scan of backups is available if the Scan Service component is installed with the Cyber Protect Management Server. For more information, see "Scan Service" (p. 92).

Backup scanning plans are supported for **Entire machine** and **Disk/volume** backups of Windows machines. Only volumes with the NTFS file system and GPT or MBR partitioning are scanned.

The following backup storages are supported:

- Cloud storage
- Network folder
- Local folder

Only agents installed on the same workload can access backups in a local folder.

---

**Note**

For security and performance reasons, we recommend that you use a dedicated machine for scanning purposes. This machine must have access to all scanned backups.

---

The backups that you select for scanning can be in one of the following states:

- Not scanned
- No malware
- Malware detected

To check the status, in the Cyber Protect web console, go to **Backup storage > Locations**, and then check the **Status** column. The **Backup scanning details** widget on the **Dashboard > Overview** tab also provides information about this status.

## Limitations

- Recovery points with Continuous data protection (CDP) backups are not scanned. Only non-CDP recovery points of the selected backup set are scanned. For more information about Continuous data protection, see "Continuous data protection (CDP)" (p. 237).
- When you perform safe recovery of an **Entire machine** backup, the data in the CDP recovery point is not automatically recovered. To recover this data, run a **Files/folders** recovery.

# Protection of collaboration and communication applications

Zoom, Cisco Webex Meetings, and Microsoft Teams are now widely used for video/web conferencing and communications. Cyber Protect allows you to protect your collaboration tools.

The protection configuration for Zoom, Cisco Webex Meetings, and Microsoft Teams is similar. In the example below, we will consider configuration for Zoom.

## ***To set up Zoom protection***

1. Install a protection agent on the machine where the collaboration application is installed.
2. Log in to the Cyber Protect web console and [apply a protection plan](#) with one of the following modules enabled:
  - **Antivirus and Antimalware protection** (with the **Self-Protection** and **Active Protection** settings enabled) – if you have one of the Cyber Protect editions.
  - **Active Protection** (with the **Self-Protection** setting enabled) – if you have one of the Cyber Backup editions.
3. [Optional] For automatic update installation, configure the [Patch management module](#) in the protection plan.

As a result, your Zoom application will be under protection that includes the following activities:

- Installing Zoom client updates automatically
- Protecting Zoom processes from code injections
- Preventing suspicious operations by Zoom processes
- Protecting the "hosts" file from adding the domains related to Zoom

# Vulnerability assessment and patch management

**Vulnerability assessment** (VA) is a process of identifying, quantifying, and prioritizing found vulnerabilities in the system. By using the Vulnerability assessment module in a protection plan, you can scan your machines for vulnerabilities and check if the operating systems and installed applications are up-to-date and work properly.

Vulnerability assessment scanning is supported for machines running the following operating systems:

- Windows. For more information, see "Supported Microsoft and third-party products" (p. 534).
- Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure) machines. For more information, see "Supported Linux products" (p. 535).

Use the **Patch management** (PM) functionality to manage patches (updates) for applications and operating systems installed on your machines, and keep your systems up-to-date. In the Patch management module you can automatically or manually approve update installations on your machines.

Patch management is supported for machines running Windows. For more information, see "Supported Microsoft and third-party products" (p. 534).

## Vulnerability assessment

The vulnerability assessment process consists of the following steps:

1. You [create a protection plan](#) with enabled Vulnerability assessment module, specify the [vulnerability assessment settings](#), and assign the plan to machines.
2. The system, by schedule or on demand, sends a command to the protection agents to run the vulnerability assessment scanning.
3. The agents receive the command, start scanning machines for vulnerabilities, and generate the scanning activity.
4. After the vulnerability assessment scanning completes, the agents generate the results and send them to Monitoring Service.
5. Monitoring Service processes the data from the agents and shows the results in the [vulnerability assessment widgets](#) and a list of found vulnerabilities.
6. By using this information, you can decide which of the found vulnerabilities must be fixed.

You can monitor the results of the vulnerability assessment scanning in **Dashboard > Overview > Vulnerabilities / Existing vulnerabilities** widgets.

## Supported Microsoft and third-party products

The following Microsoft products and third-party products for Windows operating systems are supported for vulnerability assessment.

### Supported Microsoft products

#### Desktop operating systems

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

#### Server operating systems

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

#### Microsoft Office and related components

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

#### Windows-related components

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio and Applications
- Components of the operating system

#### Server applications

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017

- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

## Supported third-party products for Windows

Cyber Protect supports vulnerability assessment and patching for a wide range of third-party apps, including collaboration tools and VPN clients that have vital importance in the remote work scenarios.

For the full list of supported third-party products for Windows, refer to <https://kb.acronis.com/content/62853>.

## Supported Linux products

The following Linux distributions and versions are supported for vulnerability assessment:

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronis Storage 2.4.0
- Acronis Storage 2.2.0

## Vulnerability assessment settings

To learn how to create a protection plan with the Vulnerability assessment module, refer to "Creating a protection plan" (p. 218). You can perform vulnerability assessment scanning by schedule or on demand (by using the **Run now** action in a protection plan).

You can specify the following settings in the Vulnerability assessment module.

### What to scan

Define which software products you want to scan for vulnerabilities:

- Windows machines:
  - **Microsoft products**
  - **Windows third-party products**  
For more information about the supported third-party products for Windows, refer to <https://kb.acronis.com/content/62853>.
- Linux machines:
  - **Scan Linux packages**

## Schedule

Define the schedule according to which the vulnerability assessment scan will be performed on the selected machines:

### Schedule the task run using the following events:

- **Schedule by time** – The task will run according to the specified time.
- **When user logs in to the system** – By default, a login of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.
- **When user logs off the system** – By default, a logoff of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.

---

#### Note

The task will not run at system shutdown. Shutting down and logging off are different events in the scheduling configuration.

---

- **On the system startup** – The task will run when the operating system starts.
- **On the system shutdown** – The task will run when the operating system shuts down.

Default setting: **Schedule by time**.

### Schedule type:

- **Monthly** – Select the months and the weeks or days of the month when the task will run.
- **Daily** – Select the days of the week when the task will run.
- **Hourly** – Select the days of the week, repetition number, and the time interval in which the task will run.

Default setting: **Daily**.

**Start at** – Select the exact time when the task will run.

**Run within a date range** – Set a range in which the configured schedule will be effective.

**Start conditions** – Define all conditions that must be met simultaneously for the task to run.

Start conditions for antimalware scans are similar to the start conditions for the Backup module that are described in "Start conditions" (p. 255). You can define the following additional start conditions:

- **Distribute task start time within a time window** – This option allows you to set the time frame for the task in order to avoid network bottlenecks. You can specify the delay in hours or minutes. For example, if the default start time 10:00 AM and the delay is 60 minutes, then the task will start between 10:00 AM and 11:00 AM.
- **If the machine is turned off, run missed tasks at the machine startup**
- **Prevent the sleep or hibernate mode during task running** – This option is effective only for machines running Windows.
- **If start conditions are not met, run the task anyway after** – Specify the period after which the task will run, regardless of the other start conditions.



---

**Note**

Start conditions are not supported for Linux.

---

## Vulnerability assessment for Windows machines

You can scan for vulnerabilities Windows machines and third-party products for Windows.

1. In the Cyber Protect web console, [create a protection plan](#) and enable the **Vulnerability assessment** module.
2. Specify the vulnerability assessment settings:
  - **What to scan** – select **Microsoft products**, **Windows third-party products**, or both.
  - **Schedule** – define the schedule for performing the vulnerability assessment.  
For more information about the **Schedule** options, refer to "Vulnerability assessment settings" (p. 535).
3. Assign the plan to the Windows machines.

After a vulnerability assessment scan, you can see a [list of found vulnerabilities](#). You can process the information and decide which of the found vulnerabilities must be fixed.

To monitor the results of the vulnerability assessment, see **Dashboard > Overview > Vulnerabilities / Existing vulnerabilities** widgets.

## Vulnerability assessment for Linux machines

You can scan Linux machines for application-level and kernel-level vulnerabilities.

### *To configure the vulnerability assessment for Linux machines*

1. In the Cyber Protect web console, [create a protection plan](#) and enable the **Vulnerability assessment** module.
2. Specify the vulnerability assessment settings:
  - **What to scan** – select **Scan Linux packages**.
  - **Schedule** – define the schedule for performing the vulnerability assessment.  
For more information about the **Schedule** options, refer to "Vulnerability assessment settings" (p. 535).
3. Assign the plan to the Linux machines.

After a vulnerability assessment scan, you can see a [list of found vulnerabilities](#). You can process the information and decide which of the found vulnerabilities must be fixed.

To monitor the results of the vulnerability assessment, see **Dashboard > Overview > Vulnerabilities / Existing vulnerabilities** widgets.

## Managing found vulnerabilities

If the vulnerability assessment was performed at least once and some vulnerabilities were found, you can see them in **Software management > Vulnerabilities**. The list of vulnerabilities shows both vulnerabilities for which patches are available, and those without suggested patches. You can use the filter to show only vulnerabilities with available patches.

Name	Description
<b>Name</b>	The name of vulnerability.
<b>Affected products</b>	Software products for which the vulnerabilities were found.
<b>Machines</b>	The number of affected machines.
<b>Severity</b>	The severity of found vulnerability. The following levels can be assigned according to the Common Vulnerability Scoring System (CVSS): <ul style="list-style-type: none"><li>• <b>Critical:</b> 9 - 10 CVSS</li><li>• <b>High:</b> 7 - 9 CVSS</li><li>• <b>Medium:</b> 3 - 7 CVSS</li><li>• <b>Low:</b> 0 - 3 CVSS</li><li>• <b>None</b></li></ul>
<b>Patches</b>	The number of appropriate patches.
<b>Published</b>	The date and time when the vulnerability was published in Common Vulnerabilities and Exposures (CVE).
<b>Detected</b>	The first date when an existing vulnerability was detected on machines.

You can find the description of a found vulnerability by clicking its name in the list.

### ***To start the vulnerability remediation process***

1. In the Cyber Protect web console, go to **Software management > Vulnerabilities**.
2. Select the vulnerabilities in the list, and then click **Install patches**. The vulnerability remediation wizard will open.
3. Select the patches to be installed. Click **Next**.
4. Select the machines on which you want to install patches.
5. Choose whether to reboot the machines after patch installation:
  - **No** – reboot will never be initiated after patch installation.
  - **If required** – reboot is initiated only if it is required for applying the updates.
  - **Yes** – reboot will be always initiated after patch installation. However, you can specify a delay.

**Do not reboot until backup is finished** – if a backup process is running, the machine reboot will be delayed until the backup completes.

6. Click **Install patches**.

As a result, the selected patches are installed on the selected machines.

## Patch management

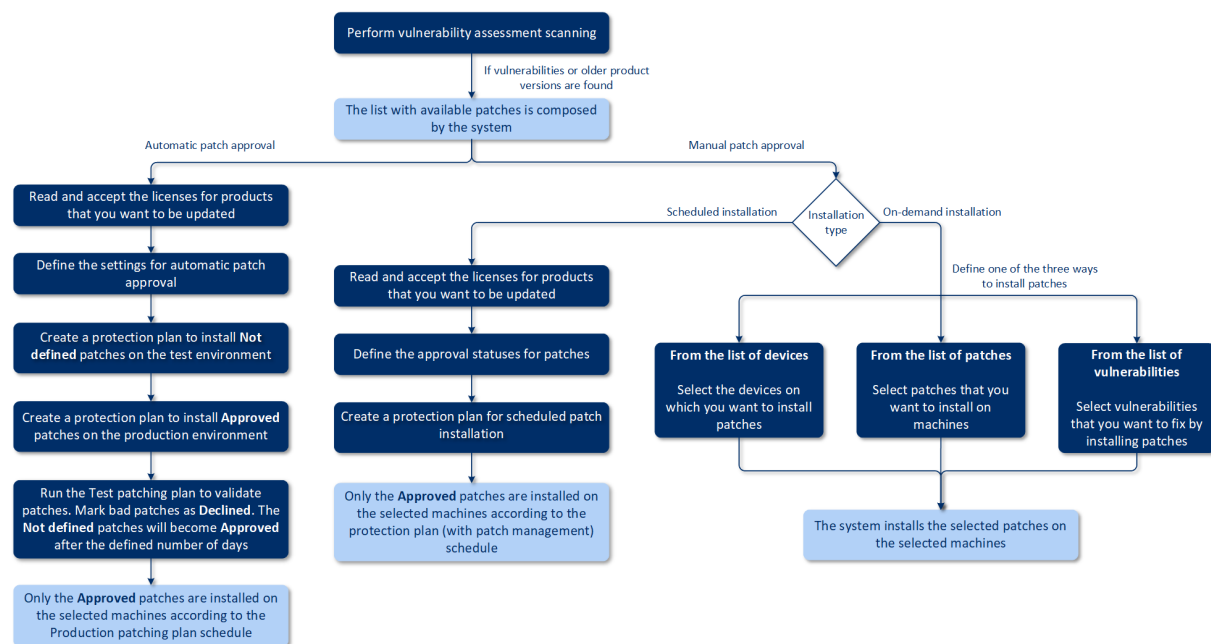
Use patch management functionality to:

- Install OS-level and application level updates
- Approve patches manually or automatically
- Install patches on-demand and according to a schedule
- Precisely define which patches to apply by different criteria: severity, category, and approval status
- Perform pre-update backup in order to prevent possible unsuccessful updates
- Define the reboot option to be applied after patch installation

Cyber Protect introduces peer-to-peer technology to minimize network bandwidth traffic. You can choose one or more dedicated agents that will download updates from the Internet and distribute them among other agents in the network. All agents will also share updates with each other as peer-to-peer agents.

## How it works

You can configure either automatic or manual patch approval. In the scheme below, you can see both automatic and manual patch approval workflows.



1. First, you need to perform at least one [vulnerability assessment scan](#) by using the protection plan with the **Vulnerability assessment** module enabled. After the scan is performed, the lists of [found vulnerabilities](#) and [available patches](#) are composed by the system.
2. Then, you can configure the [automatic patch approval](#) or use [manual patch approval](#) approach.
3. Define how to install patches – according to a schedule or on-demand. On-demand patch installation can be done in three ways according to your preferences:
  - Go to the list of patches (**Software management > Patches**) and install the necessary patches.
  - Go to the list of vulnerabilities (**Software management > Vulnerabilities**) and start the remediation process which includes patch installation as well.
  - Go to the list of devices (**Devices > All devices**), select the particular machines that you want to update, and install patches on them.

You can monitor the results of the patch installation in **Dashboard > Overview > Patch installation history** widget.

## Patch management settings

To learn how to create a protection plan with the Patch management module, refer to "[Creating a protection plan](#)". By using the protection plan, you can specify which updates for Microsoft products and other third-party products for Windows OS to automatically install on the defined machines.

The following settings can be specified for the Patch management module.

### Microsoft products

To install the Microsoft updates on the selected machines, enable the **Update Microsoft products** option.

Select which updates you want to be installed:

- **All updates**
- **Only Security and Critical updates**
- **Updates of specific products:** you can define custom settings for different products. If you want to update specific products, for each product you can define which updates to install by [category](#), [severity](#), or [approval status](#).

Updates of specific products ✕

	Products	Category	Severity	Approval status
<input type="checkbox"/>	Windows Server 2012 R2 L...	Custom	Custom	Custom
<input checked="" type="checkbox"/>	Windows Server 2012 R2	ServicePacks, Upd...	Critical, High, Medi...	Approved
<input checked="" type="checkbox"/>	Windows Server 2012	CriticalUpdates	Critical, High	Approved
<input type="checkbox"/>	Windows Server 2016 and ...	—	—	—
<input checked="" type="checkbox"/>	Windows Server 2016	SecurityUpdates	Critical	Approved

[Reset to default](#)
Cancel
Save

## Windows third-party products

To install the third-party updates for Windows OS on the selected machines, enable the **Windows third-party products** option.

Select which updates you want to be installed:

- **Only major updates** allows you to install the latest available version of the update.
- **Only minor updates** allows you to install the minor version of the update.
- **Updates of specific products:** you can define custom settings for different products. If you want to update specific products, for each product you can define which updates to install by [category](#), [severity](#), or [approval status](#).

Updates of specific products ✕

	Products	Category	Severity	Approval status
<input type="checkbox"/>	Adobe Reader	—	—	—
<input type="checkbox"/>	Adobe Flash Player for Chr...	—	—	—
<input type="checkbox"/>	Adobe Flash Player for Fire...	—	—	—
<input checked="" type="checkbox"/>	Oracle Java Runtime Envir...	Major updates	Critical	Approved
<input checked="" type="checkbox"/>	Mozilla Firefox	Minor updates	All	Approved
<input type="checkbox"/>	Google Chrome	—	—	—

[Reset to default](#)
Cancel
Save

## Schedule

Define the schedule according to which the updates will be installed on the selected machines.

### Schedule the task run using the following events:

- **Schedule by time** – The task will run according to the specified time.
- **When user logs in to the system** – By default, a login of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.
- **When user logs off the system** – By default, a logoff of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.

---

#### Note

The task will not run at system shutdown. Shutting down and logging off are different events in the scheduling configuration.

---

- **On the system startup** – The task will run when the operating system starts.
- **On the system shutdown** – The task will run when the operating system shuts down.

Default setting: **Schedule by time**.

### Schedule type:

- **Monthly** – Select the months and the weeks or days of the month when the task will run.
- **Daily** – Select the days of the week when the task will run.
- **Hourly** – Select the days of the week, repetition number, and the time interval in which the task will run.

Default setting: **Daily**.

**Start at** – Select the exact time when the task will run.

**Run within a date range** – Set a range in which the configured schedule will be effective.

**Start conditions** – Define all conditions that must be met simultaneously for the task to run.

Start conditions for antimalware scans are similar to the start conditions for the Backup module that are described in "Start conditions" (p. 255). You can define the following additional start conditions:

- **Distribute task start time within a time window** – This option allows you to set the time frame for the task in order to avoid network bottlenecks. You can specify the delay in hours or minutes. For example, if the default start time 10:00 AM and the delay is 60 minutes, then the task will start between 10:00 AM and 11:00 AM.
- **If the machine is turned off, run missed tasks at the machine startup**
- **Prevent the sleep or hibernate mode during task running** – This option is effective only for machines running Windows.
- **If start conditions are not met, run the task anyway after** – Specify the period after which the task will run, regardless of the other start conditions.

## Pre-update backup

**Run backup before installing software updates** – the system will create an incremental backup of machine before installing any updates on it. If there were no backups created earlier, then a full

backup of machine will be created. This will allow you to roll back to the previous state in case of patch installation failure. For the **Pre-update backup** option to work, the corresponding machines must have both the Patch management and the Backup module enabled in a protection plan and the items to back up – entire machine or boot+system volumes. If you select inappropriate items to back up, then the system will not allow you to enable the **Pre-update backup** option.

## Managing list of patches

After the vulnerability assessment completes, you will find the available patches in **Software management > Patches**.

Name	Description
<b>Name</b>	The name of the patch
<b>Severity</b>	The severity of the patch: <ul style="list-style-type: none"> <li>• <b>Critical</b></li> <li>• <b>High</b></li> <li>• <b>Medium</b></li> <li>• <b>Low</b></li> <li>• <b>None</b></li> </ul>
<b>Vendor</b>	The vendor of the patch
<b>Product</b>	Product for which the patch is applicable
<b>Installed versions</b>	Product versions that are already installed
<b>Version</b>	Version of the patch
<b>Category</b>	The category to which the patch belongs: <ul style="list-style-type: none"> <li>• <b>Critical update</b> – broadly released fixes for specific problems addressing critical, non-security related bugs.</li> <li>• <b>Security update</b> – broadly released fixes for specific products addressing security issues.</li> <li>• <b>Definition update</b> – updates to virus or other definition files.</li> <li>• <b>Update rollup</b> – cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a specific component, such as Internet Information Services (IIS).</li> <li>• <b>Service pack</b> – cumulative sets of all hotfixes, security updates, critical updates, and updates created since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Tool</b> – utilities or features that aid in accomplishing a task or set of tasks.</li> <li>• <b>Feature pack</b> – new feature releases, usually rolled into products at the next release.</li> <li>• <b>Update</b> – broadly released fixes for specific problems addressing non-critical, non-security related bugs.</li> <li>• <b>Application</b> – patches for an application.</li> </ul>
<b>Microsoft KB</b>	If the patch is for a Microsoft product, the KB article ID is provided
<b>Release date</b>	The date when the patch was released
<b>Machines</b>	Number of affected machines
<b>Approval status</b>	<p>The approval status is mainly needed for automatic approval scenario and to be able to define in the protection plan which updates to install by status.</p> <p>You can define one of the following statuses for a patch:</p> <ul style="list-style-type: none"> <li>• <b>Approved</b> – the patch was installed on at least one machine and validated as ok</li> <li>• <b>Declined</b> – the patch is not safe and may corrupt a machine system</li> <li>• <b>Not defined</b> – the patch status is unclear and should be validated</li> </ul>
<b>License agreement</b>	<ul style="list-style-type: none"> <li>• Read and accept</li> <li>• Disagreed. If you disagree with the license agreement, then the patch status becomes <b>Declined</b> and it will not be installed</li> </ul>
<b>Vulnerabilities</b>	The number of vulnerabilities. If you click on it, you will be redirected to the list of vulnerabilities.
<b>Size</b>	The average size of the patch
<b>Language</b>	The language which is supported by the patch
<b>Vendor site</b>	The official site of the vendor

## Automatic patch approval

Automatic patch approval allows you to make the process of installing updates on machines easier. Let's see the example how it works.

### How it works

You should have two environments: test and production. The test environment is used for testing the patch installation and ensuring that they do not break anything. After you tested patch



installation on the test environment, you can automatically install these safe patches on the production environment.

## Configuring automatic patch approval

### *To configure automatic patch approval*

1. For each vendor whose products you are planning to update, you must read and accept the license agreements. Otherwise, automatic patch installation will not be possible.
2. Configure the settings for automatic approval.
3. [Prepare the protection plan](#) (for example, "Test patching") with the enabled **Patch management** module and apply it to the machines in the test environment. Specify the following condition of patch installation: the patch approval status must be **Not defined**. This step is needed to validate the patches and check whether the machines work properly after patch installation.
4. [Prepare the protection plan](#) (for example, "Production patching") with the enabled **Patch management** module and apply it to the machines in the production environment. Specify the following condition of patch installation: the patch status must be **Approved**.
5. Run the Test patching plan and check the results. The approval status for those machines that have no issues can be preserved as **Not defined** while the status for machines working incorrectly must be set to **Declined**.
6. According to the number of days set in the **Automatic approval** option, those patches that were **Not defined** will become **Approved**.
7. When the Production patching plan is launched, only those patches that are **Approved** will be installed on the production machines.

The manual steps are listed below.

### Step 1. Read and accept the license agreements for the products that you want to update

1. In the Cyber Protect web console, go to **Software management > Patches**.
2. Select the patch, then read and accept the license agreement.

### Step 2. Configure the settings for automatic approval

1. In Cyber Protect web console, go to **Software management > Patches**.
2. Click **Settings**.
3. Enable the **Automatic approval** option and specify the number of days. This means that after the specified number of days starting from the first attempt of patch installation, the patches with the status **Not defined** will become **Approved** automatically.

For example, you specified 10 days. You performed the Test patching plan for test machines and installed patches. Those patches that broke the machines, you marked as **Declined** while the rest of patches stay as **Not defined**. After 10 days, the patches in the **Not defined** status will be automatically switched to **Approved**.

4. Enable the **Automatically accept the license agreements** option. This is needed for automatic license acceptance during patch installation, no confirmation is required from a user.

### Step 3. Prepare the Test patching protection plan

1. In the Cyber Protect web console, go to **Plans > Protection**.
2. Click **Create plan**.
3. Enable the **Patch management** module.
4. Define which updates to install for Microsoft and third-party products, schedule, and pre-update backup. For more details about these settings, refer to "[Patch management settings](#)".

#### Important

For all the products to be updated, define **Approval status** as **Not defined**. When the time to update comes, the agent will install only **Not defined** patches on the selected machines in the test environment.

Updates of specific products

<input checked="" type="checkbox"/>	Products ↓	Category	Severity	Approval status
<input checked="" type="checkbox"/>	Active Directory Rights Ma...	Custom	Custom	Not defined
<input checked="" type="checkbox"/>	Antigen for Exchange/SMTP	CriticalUpdates, Se...	Critical	Not defined
<input checked="" type="checkbox"/>	ASP.NET Web Frameworks	None	All	Not defined
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	Updates	Critical, High, Medi...	Not defined
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	None	All	Not defined
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	None	All	Not defined

[Reset to default](#) [Cancel](#) [Save](#)

### Step 4. Prepare the Production patching protection plan

1. In the Cyber Protect web console, go to **Plans > Protection**.
2. Click **Create plan**.
3. Enable the **Patch management** module.
4. Define which updates to install for Microsoft and third-party products, schedule, and pre-update backup. For more details about these settings, refer to "[Patch management settings](#)".

#### Important

For all the products to be updated, define **Approval status** as **Approved**. When the time to update comes, the agent will install only **Approved** patches on the selected machines in the production environment.

## Note

Updates of specific products

<input checked="" type="checkbox"/>	Products <span>↓</span>	Category	Severity	Approval status
<input checked="" type="checkbox"/>	Products <span>↓</span>	Custom	Custom	Approved
<input checked="" type="checkbox"/>	Active Directory Rights Ma...	CriticalUpdates, Se...	Critical	Approved
<input checked="" type="checkbox"/>	Antigen for Exchange/SMTP	All	All	Approved
<input checked="" type="checkbox"/>	ASP.NET Web Frameworks	Updates	Critical, High, Medi...	Approved
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	All	All	Approved
<input checked="" type="checkbox"/>	Azure File Sync agent upda...	All	All	Approved

[Reset to default](#) [Cancel](#) [Save](#)

## Step 5. Run the Test patching protection plan and check the results

1. Run the Test patching protection plan (by schedule or on-demand).
2. After that, check which of the installed patches are safe and which are not.
3. Go to **Software management > Patches** and set the **Approval status** as **Declined** for those patches that are not safe.

## Manual patch approval

The manual patch approval process is the following:

1. In the Cyber Protect web console, go to **Software management > Patches**.
2. Select the patches that you want to install, then read and accept the license agreements.
3. Set **Approval status** to **Approved** for the patches that you approve for installation.
4. Create a [protection plan with the enabled Patch management](#) module. You can either configure the schedule or launch the plan on-demand by clicking **Run now** in the Patch management module settings.

As a result, only the approved patches will be installed on the selected machines.

## On-demand patch installation

On-demand patch installation can be done in three ways according to your preferences:

- Go to the list of patches (**Software management > Patches**) and install the necessary patches.
- Go to the list of vulnerabilities (**Software management > Vulnerabilities**) and start the remediation process which includes patch installation as well.
- Go to the list of devices (**Devices > All devices**), select the particular machines that you want to update, and install patches on them.

Let's consider patch installation from the list of patches:

1. In the Cyber Protect web console, go to **Software management > Patches**.
2. Accept the license agreements for the patches that you want to install.
3. Select the patches that you want to install and click **Install**.
4. Select the machines on which patches must be installed.
5. Define whether reboot is initiated after installing patches:
  - **Never** – reboot will never be initiated after the patches.
  - **If required** – reboot is done only if it is required for applying the patches.
  - **Always** – reboot will be always initiated after the patches. You can always specify the reboot delay.

**Do not reboot until backup is finished** – if the backup process is running, the machine reboot will be delayed until the backup is completed.
6. Click **Install patches**.

The selected patches will be installed on the selected machines.

## Patch lifetime in the list

To keep the list of patches up-to-date, go to **Software management > Patches > Settings** and specify the **Lifetime in list** option.

The **Lifetime in list** option defines how long will the detected available patch be kept in the list of patches. Generally, the patch is removed from the list if it is successfully installed on all the machines where its absence is detected or the defined time lapses.

- **Forever** – the patch always stays in the list.
- **7 days** – the patch is removed seven days after its first installation.

For example, you have two machines where patches must be installed. One of them is online, another – offline. The patch was installed on the first machine. After 7 days, the patch will be removed from the list of patches even if it is not installed on the second machine because it was offline.
- **30 days** – the patch is removed thirty days after its first installation.

# Smart protection

## Threat feed

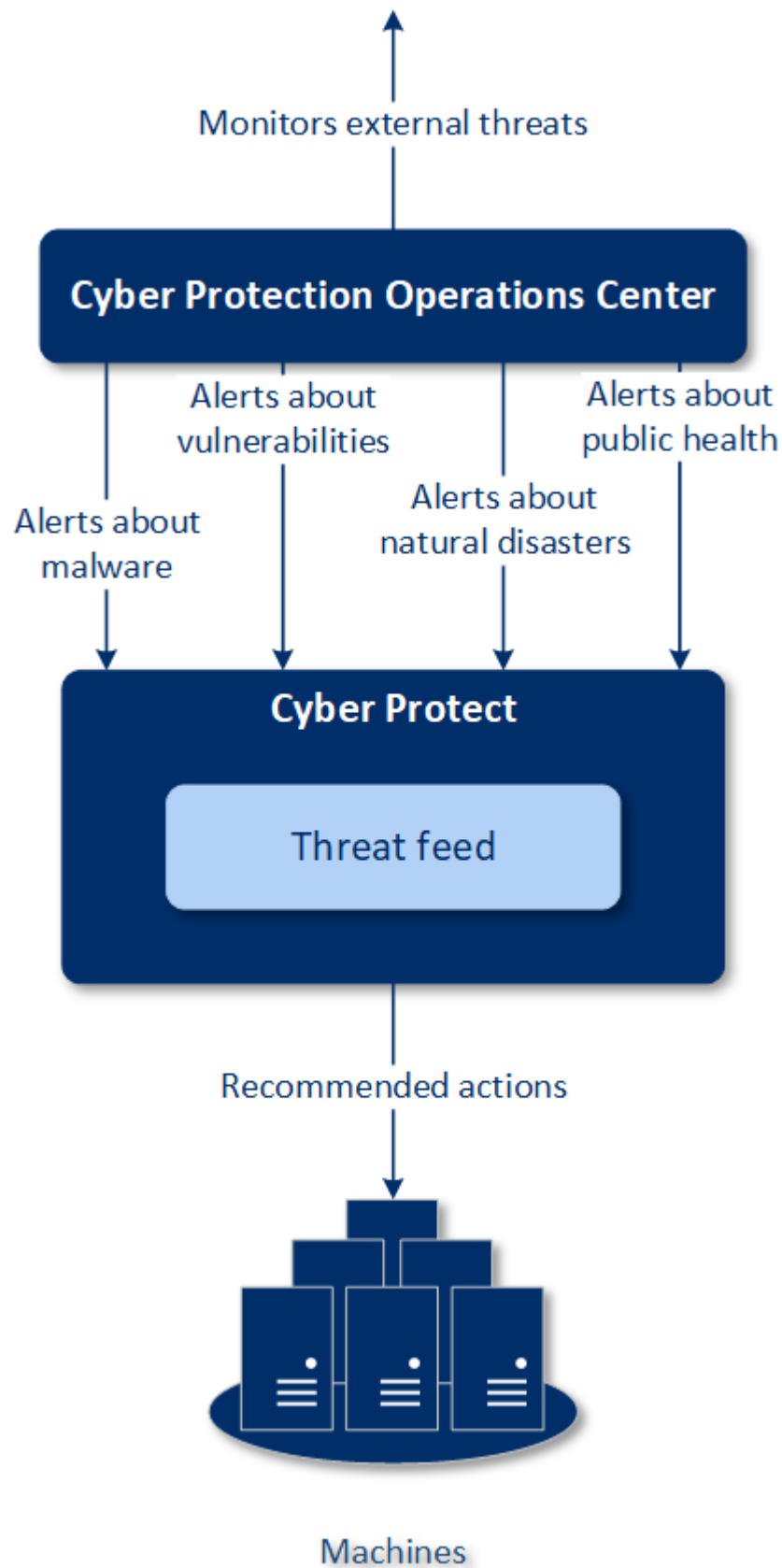
Acronis Cyber Protection Operations Center (CPOC) generates security alerts that are sent only to the related geographic regions. These security alerts provide information about malware, vulnerabilities, natural disasters, public health, and other types of global events that may affect your data protection. The threat feed informs you about all the potential threats and allows you to prevent them.

A security alert can be resolved with the number of specific actions that are provided by the security experts. There are some alerts that are used just for notifying you about the upcoming threats but no recommended actions are available.

## How it works

Acronis Cyber Protection Operations Center monitors external threats and generates alerts about malware, vulnerability, natural disaster, and public health threats. You will be able to see all these alerts in the Cyber Protect web console, in the **Threat feed** section. You can perform respective recommended actions depending on the type of alert.

The main workflow of the threat feed is illustrated in the diagram below.



To run the recommended actions on received alerts from Acronis Cyber Protection Operations Center, do the following:

1. In the Cyber Protect web console, go to **Dashboard > Threat feed** to check whether there are any existing security alerts.
2. Select an alert in the list and review the provided details.
3. Click **Start** to launch the wizard.
4. Enable the actions that you want to be performed and select the machines to which these actions must be applied. The following actions can be suggested:
  - **Vulnerability assessment** – to scan the selected machines for vulnerabilities
  - **Patch management** – to install patches on the selected machines
  - **Anti-malware Protection** – to run full scan of the selected machines
  - **Backup of protected or unprotected machines** – to back up protected/unprotected machines
5. Click **Start**.
6. On the **Activities** page, verify that the activity was successfully performed.

## Deleting all alerts

Threat feed alerts are automatically cleaned up after the following time periods:

- Natural disaster – 1 week
- Vulnerability – 1 month
- Malware – 1 month
- Public health – 1 week

## Data protection map

The Data protection map functionality allows you:

- To get detailed information about the stored data (classification, locations, protection status, and additional information) on your machines.
- To detect whether the data is protected or not. The data is considered protected if it is protected with backup (a protection plan with the Backup module enabled).
- To perform actions for data protection.

## How it works

1. First, you create a protection plan with the [Data protection map](#) module enabled.
2. Then, after the plan is performed and your data is discovered and analyzed, you will get the visual representation of the data protection on the [Data protection map](#) widget.
3. You can also go to **Devices > Data protection map** and find there information about

unprotected files per device.

4. You can take actions to protect the detected unprotected files on devices.

## Managing the detected unprotected files

To protect the important files that were detected as unprotected, do the following:

1. In the Cyber Protect web console, go to **Devices > Data protection map**.

In the list of devices, you can find general information about the number of unprotected files, size of such files per device, and the last data discovery.

To protect files on a particular machine, click the ellipsis icon (...), and then click **Protect all files**. You will be redirected to the list of plans where you can create a protection plan with the Backup module enabled.

To delete the particular device with unprotected files from the list, click **Hide until next data discovery**.

2. To view detailed information about the unprotected files on a particular device, click the name of this device.

You will see a list of unprotected files per file extension and per location. You can filter this list by file extension.

3. To protect all unprotected files, click **Protect all files**. You will be redirected to the list of plans where you can create a protection plan with the Backup module enabled.

To get the information about the unprotected files in the form of report, click **Download detailed report in CSV**.

## Data protection map settings

To learn how to create a protection plan with the Data protection map module, refer to "[Creating a protection plan](#)".

The following settings can be specified for the Data protection map module.

### Schedule

You can define different settings to create the schedule according to which the task for data protection map will be performed.

**Schedule the task run using the following events:**

- **Schedule by time** – The task will run according to the specified time.
- **When user logs in to the system** – By default, a login of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.
- **When user logs off the system** – By default, a logoff of any user will start the task. You can modify this setting so that only a specific user account can trigger the task.



---

**Note**

The task will not run at system shutdown. Shutting down and logging off are different events in the scheduling configuration.

---

- **On the system startup** – The task will run when the operating system starts.
- **On the system shutdown** – The task will run when the operating system shuts down.

Default setting: **Schedule by time**.

**Schedule type:**

- **Monthly** – Select the months and the weeks or days of the month when the task will run.
- **Daily** – Select the days of the week when the task will run.
- **Hourly** – Select the days of the week, repetition number, and the time interval in which the task will run.

Default setting: **Daily**.

**Start at** – Select the exact time when the task will run.

**Run within a date range** – Set a range in which the configured schedule will be effective.

**Start conditions** – Define all conditions that must be met simultaneously for the task to run.

Start conditions for antimalware scans are similar to the start conditions for the Backup module that are described in "Start conditions" (p. 255). You can define the following additional start conditions:

- **Distribute task start time within a time window** – This option allows you to set the time frame for the task in order to avoid network bottlenecks. You can specify the delay in hours or minutes. For example, if the default start time 10:00 AM and the delay is 60 minutes, then the task will start between 10:00 AM and 11:00 AM.
- **If the machine is turned off, run missed tasks at the machine startup**
- **Prevent the sleep or hibernate mode during task running** – This option is effective only for machines running Windows.
- **If start conditions are not met, run the task anyway after** – Specify the period after which the task will run, regardless of the other start conditions.

## Extensions and exception rules

On the **Extensions** tab, you can define the list of file extensions that will be considered as important during the data discovery and checked whether they are protected. Use the following format for defining extensions:

.html, .7z, .docx, .zip, .pptx, .xml

On the **Exception rules** tab, you can define files and folders whose protection status will not be checked during the data discovery.

- **Hidden files and folders** – if selected, hidden files and folders will be skipped during the data examination.
- **System files and folders** – if selected, system files and folders will be skipped during the data examination.

# Remote desktop access

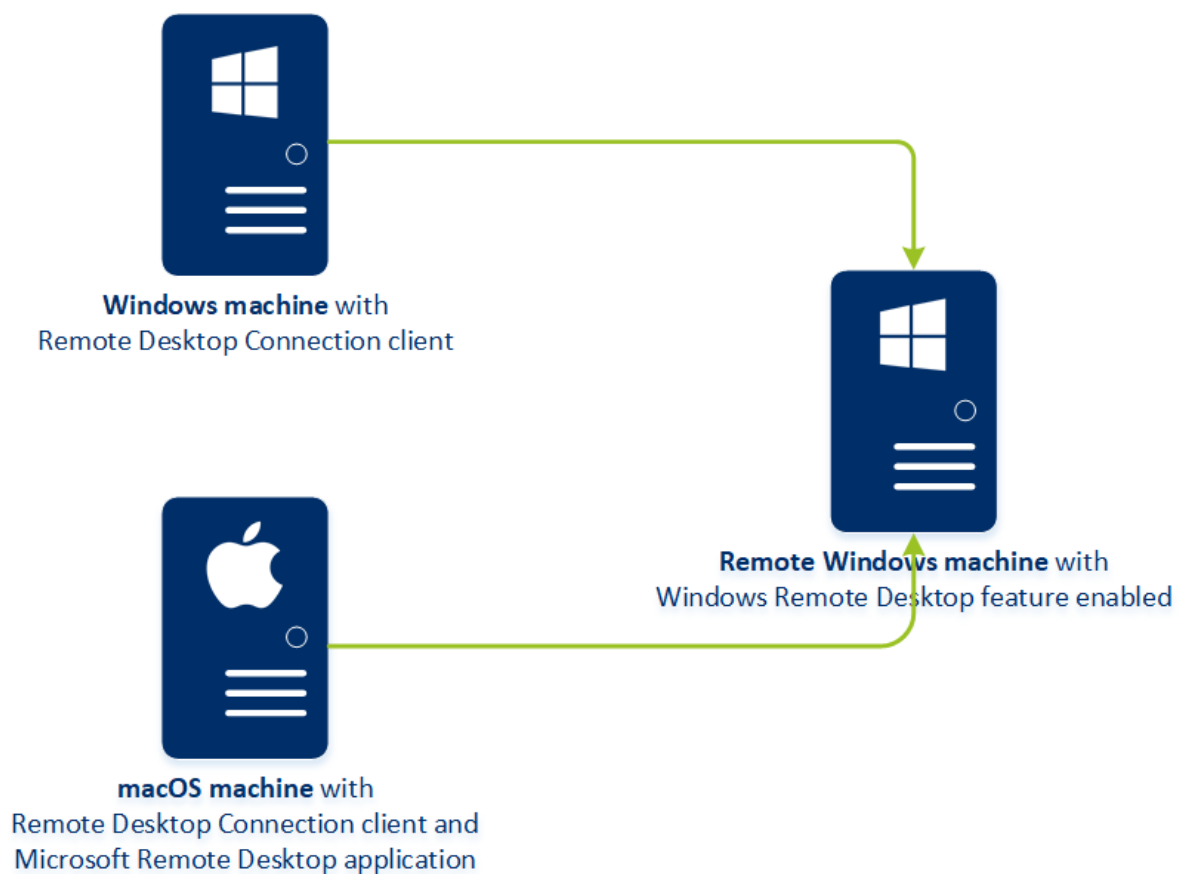
## Remote access (RDP and HTML5 clients)

Cyber Protect provides you with remote access capability. You can remotely connect and manage your user machines right from the web console. This allows you to easily assist to your users in resolving issues on their machines.

Prerequisites:

- A protection agent is installed on the remote machine and is registered on the management server.
- The machine has an appropriate Cyber Protect license assigned.
- The Remote Desktop Connection client is installed on the machine from which the connection is initialized.
- The machine from which the RDP connection is initialized must be able to access the management server by its host name. The DNS settings must be configured properly or the management server host name must be put in the hosts file.

A remote connection can be established from both Windows and macOS machines.



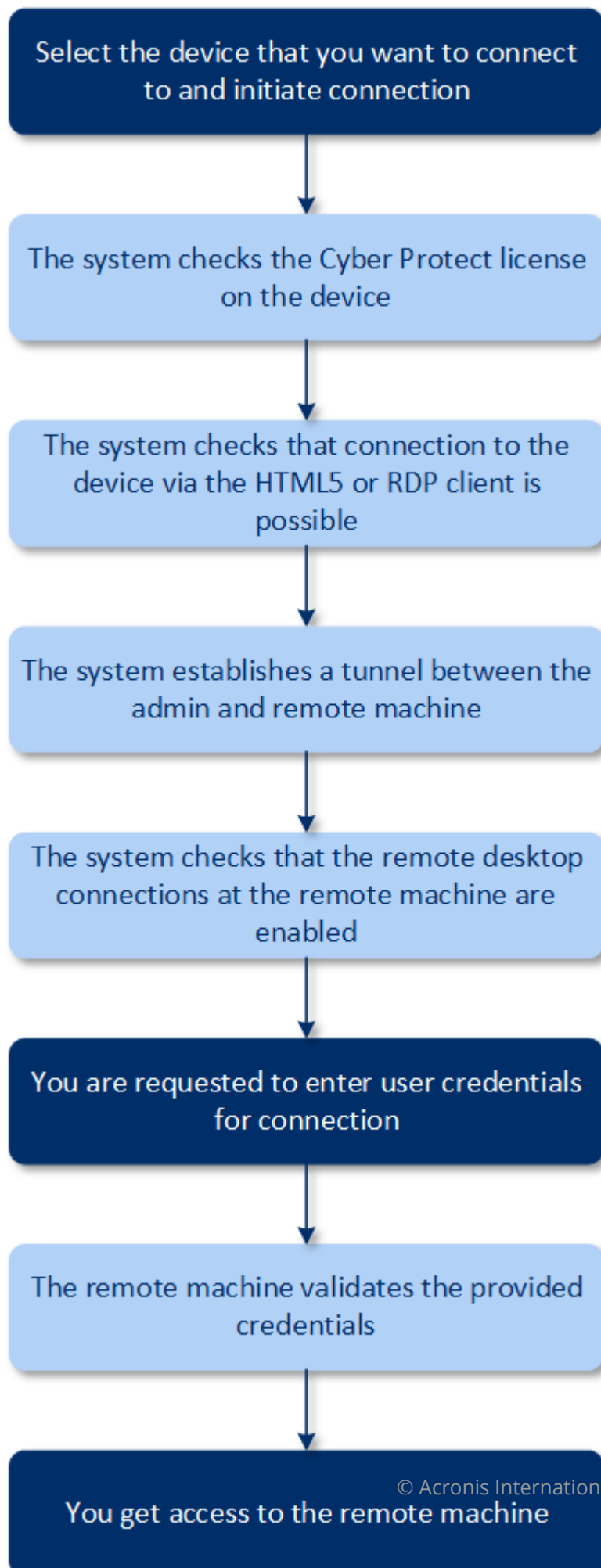
The remote access functionality can be used for connections to Windows machines with the Windows Remote Desktop feature available. That is why a remote access is not possible, for example, to a Windows 10 Home or macOS systems.

To establish a connection from a macOS machine to a remote machine, ensure that the following applications are installed on the macOS machine:

- The Remote Desktop Connection client
- The Microsoft Remote Desktop application

## How it works

When you try to connect to a remote machine, the system first checks whether this machine has a Cyber Protect license. Then, the system checks whether the connection via the HTML5 or RDP client is possible. You initiate a connection via the RDP or HTML5 client. The system establishes a tunnel to the remote machine and checks whether the remote desktop connections are enabled on the remote machine. Then, you enter the credentials and, after their validation, you can access the remote machine.



## How to connect to a remote machine

To connect to a remote machine, do the following:

1. In the Cyber Protect web console, go to **Devices > All devices**.
2. Click on the machine to which you want to connect remotely and then click **Cyber Protection Desktop > Connect via RDP client** or **Connect via HTML5 client**.

---

### Note

Connection via HTML5 client is only available if the management server is installed on a Linux machine.

---

3. [Optional, only for connection via RDP client] Download and install the Remote Desktop Connection client. Initiate the connection to the remote machine.
4. Specify the login and password to access the remote machine, and then click **Connect**.

As a result, you are connected to the remote machine and can manage it.

## Sharing a remote connection

Employees who are working from home may need access to their office computers, but it is possible that your organization may not have a configured VPN or other tools for remote connection. Cyber Protect provides you with the capability to share an RDP link with your users, thus providing them with remote access to their machines.

### *To enable the sharing remote connection functionality*

1. In the Cyber Protect web console, go to **Settings > Protection > Remote connection**.
2. Select the check box **Share remote desktop connection**.

As a result, when you select a device in Cyber Protect web console, a new option **Share remote connection** will appear.

### *To share a remote connection with your users*

1. In the Cyber Protect web console, go to **Devices > All devices**.
2. Select the device to which you want provide a remote connection.
3. Click **Share remote connection**.
4. Click **Get link**. In the opened window, copy the generated link. This link can be shared with a user who needs a remote access to the device. The link is valid for 10 hours.

After getting the link, you can share it via email or other means of communication. The user with whom the link was shared, must click it and then select the connection type:

- Connect via RDP client.  
This connection will prompt for downloading and installing the Remote Connection client.

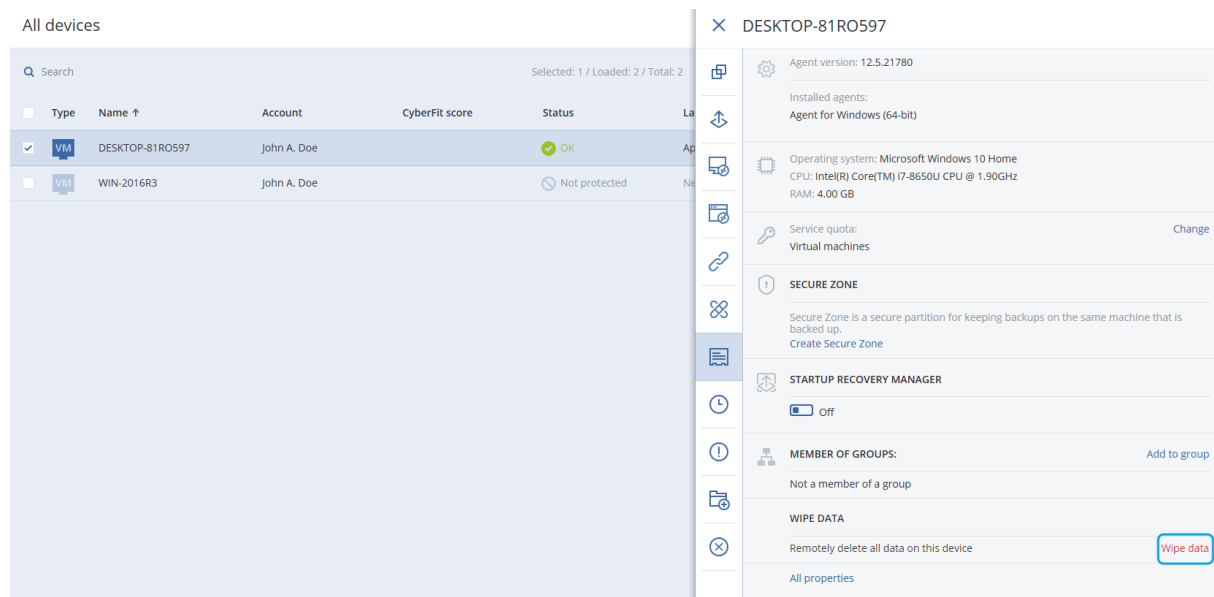
- Connect via HTML5 client.

This connection does not require installation of any RDP client on the user machine. The user will be redirected to a login screen and must enter the credentials for accessing the machine.

# Remote wipe

Remote wipe allows a Cyber Protect service administrator and a machine owner to delete the data on a managed machine – for example, if it gets lost or stolen. Thus, any unauthorized access to sensitive information will be prevented.

Remote wipe is only available for machines running Windows 10. To receive the wipe command, the machine must be turned on and connected to the Internet.



## To wipe data from a machine

1. In the Cyber Protect web console, go to **Devices > All devices**.
2. Select the machine whose data you want to wipe.

### Note

You can wipe data from one machine at a time.

3. Click **Details**, and then click **Wipe data**.  
If the machine that you selected is offline, the **Wipe data** option is inaccessible.
4. Confirm your choice.
5. Enter the credentials of this machine's local administrator, and then click **Wipe data**.

### Note

You can check the details about the wiping process and who started it in **Dashboard > Activities**.



# Device groups

Device groups are designed for convenient management of a large number of registered devices.

You can apply a protection 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 devices**, 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 protection 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 protection 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 protection 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 protection 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 protection 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.

## 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.

## 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**.
  - c. Specify the group name, and then click **OK**.
4. Select the group to which you want to add the device, and then click **Done**.

Another way to add devices to a static group is to select the group and click **Add devices**.

## Creating a dynamic group

1. Click **Devices**, and then select the group which contains the devices for which you want to create a dynamic group.
2. Search for devices by using the search field. You can use multiple attributes and operators described below.
3. Click **Save as** next to the search field.

---

**Note**

Some attributes are not supported for group creation. See the table in section Search query below.

---

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

## Search query

The following table summarizes the available attributes that you can use in your search queries.

Attribute	Meaning	Search query examples	Supported for group creation
name	<ul style="list-style-type: none"><li>• Host name for physical machines</li><li>• Name for virtual machines</li><li>• Database name</li><li>• Email address for mailboxes</li></ul>	<code>name = 'en-00'</code>	Yes
parameters.MacAddress	MAC address.	<code>parameters.MacAddress LIKE '00-22-4D-50-25-E5'</code>	Yes
comment	<p>Comment for a device. It can be specified automatically or manually.</p> <p>Default value:</p> <ul style="list-style-type: none"><li>• For physical machines running Windows, the computer description in Windows is automatically copied as a comment. This value is synchronized every 15 minutes.</li><li>• Empty for other devices.</li></ul>	<code>comment = 'important machine'</code>  <code>comment = ''</code> (all machines without a comment)	Yes

Attribute	Meaning	Search query examples	Supported for group creation
	<p><b>Note</b></p> <p>If you manually add text in the comment field, the automatic synchronization of the Windows description is disabled. To enable it again, clear the comment that you have added.</p> <p>To refresh the automatically synchronized comments for your devices, restart the Managed Machine Service in <b>Windows Services</b> or run the following commands at the command prompt:</p> <pre>net stop mms</pre> <pre>net start mms</pre> <p>To view the comment, under <b>Devices</b>, select the device, click <b>Details</b>, and then locate the <b>Comment</b> section.</p> <p>To add or change the comment, click <b>Add</b> or <b>Edit</b>.</p> <p>For devices on which a protection agent is installed, there are two separate comment fields:</p> <ul style="list-style-type: none"> <li>Agent comment <ul style="list-style-type: none"> <li>For physical machines running</li> </ul> </li> </ul>		

Attribute	Meaning	Search query examples	Supported for group creation
	<p>Windows, the computer description in Windows is automatically copied as a comment. This value is synchronized every 15 minutes.</p> <ul style="list-style-type: none"> <li>◦ Empty for other devices.</li> </ul> <hr/> <p><b>Note</b> If you manually add text in the comment field, the automatic synchronization of the Windows description is disabled. To enable it again, clear the comment that you have added.</p> <hr/> <ul style="list-style-type: none"> <li>• Device comment <ul style="list-style-type: none"> <li>◦ If the agent comment is specified automatically, it is copied as a device comment. Manually added agent comments are not copied as device comments.</li> <li>◦ Device comments are not copied as agent comments.</li> </ul> </li> </ul> <p>A device can have one or the both comments specified, or have them both blank. If the both comments are specified,</p>		

Attribute	Meaning	Search query examples	Supported for group creation
	<p>the device comment has priority.</p> <p>To view an agent comment, under <b>Settings &gt; Agents</b>, select the device with the agent, click <b>Details</b>, and then locate the <b>Comment</b> section.</p> <p>To view a device comment, under <b>Devices</b>, select the device, click <b>Details</b>, and then locate the <b>Comment</b> section.</p> <p>To add or change a comment manually, click <b>Add</b> or <b>Edit</b>.</p>		
ip	IP address (only for physical machines).	ip RANGE ('10.250.176.1', '10.250.176.50')	Yes
cpuArch	CPU architecture.  Possible values: <ul style="list-style-type: none"> <li>'x64'</li> <li>'x86'</li> </ul>	cpuArch = 'x64'	Yes
memorySize	RAM size in megabytes (MiB).	memorySize < 1024	Yes
cpuName	CPU name.	cpuName LIKE '%XEON%'	Yes
insideVm	Virtual machine with an agent inside.  Possible values: <ul style="list-style-type: none"> <li>true</li> <li>false</li> </ul>	insideVm = true	Yes
tzOffset	Machine timezone offset in minutes.	tzOffset = 120	Yes

Attribute	Meaning	Search query examples	Supported for group creation
parameters.Architecture	Operating system architecture.  Possible values: <ul style="list-style-type: none"> <li>'x86'</li> <li>'x64'</li> </ul>	parameters.Architecture = 'x86'	Yes
osName	Operating system name.	osName LIKE '%Windows XP%'	Yes
osType	Operating system type.  Possible values: <ul style="list-style-type: none"> <li>'windows'</li> <li>'linux'</li> <li>'macosx'</li> </ul>	osType IN ('linux', 'macosx')	Yes
osProductType	The operating system product type.  Possible values: <ul style="list-style-type: none"> <li>'dc' Stands for Domain Controller.</li> <li>'server'</li> <li>'workstation'</li> </ul>	osProductType = 'server'	Yes
virtualType	Virtual machine type.  Possible values: <ul style="list-style-type: none"> <li>'vmwesx' VMware virtual machines.</li> <li>'mshyperv' Hyper-V virtual machines.</li> <li>'pcs' Virtuozzo virtual machines.</li> <li>'hci' Virtuozzo Hybrid Infrastructure virtual machines.</li> <li>'scale'</li> </ul>	virtualType = 'vmwesx'	Yes

Attribute	Meaning	Search query examples	Supported for group creation
	Scale Computing HC3 virtual machines. <ul style="list-style-type: none"> <li>'ovirt'</li> </ul> oVirt virtual machines		
osSp	Operating system service pack.	osSp = 1	Yes
osVersionMajor	Major version of the operating system.	osVersionMajor = 1	Yes
osVersionMinor	Minor version of the operating system.	osVersionMinor = 1	Yes
isOnline	Machine availability. Possible values: <ul style="list-style-type: none"> <li>true</li> <li>false</li> </ul>	isOnline = true	No
tenant	The name of the unit to which the device belongs.	tenant = 'Unit 1'	Yes
tenantId	The identifier of the unit to which device belongs.  To get the unit ID, under <b>Devices</b> , select the device, click <b>Details &gt; All properties</b> . The ID is shown in the ownerId field.	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	Yes
state	Device state. Possible values: <ul style="list-style-type: none"> <li>'idle'</li> <li>'interactionRequired'</li> <li>'canceling'</li> <li>'backup'</li> <li>'recover'</li> <li>'install'</li> <li>'reboot'</li> </ul>	state = 'backup'	No



Attribute	Meaning	Search query examples	Supported for group creation
	<ul style="list-style-type: none"> <li>'failback'</li> <li>'testReplica'</li> <li>'run_from_image'</li> <li>'finalize'</li> <li>'failover'</li> <li>'replicate'</li> <li>'createAsz'</li> <li>'deleteAsz'</li> <li>'resizeAsz'</li> </ul>		
status	Resource status. Possible values: <ul style="list-style-type: none"> <li>'notProtected'</li> <li>'ok'</li> <li>'warning'</li> <li>'error'</li> <li>'critical'</li> </ul>	status = 'ok'	No
protectedByPlan	Devices that are protected by a protection plan with a given ID.  To get the plan ID, click <b>Plans &gt; Backup</b> , select the plan, click on the diagram in the <b>Status</b> column, and then click on a status. A new search with the plan ID will be created.	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No
okByPlan	Devices that are protected by a protection plan with a given ID and have an <b>OK</b> status.	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No
errorByPlan	Devices that are protected by a protection plan with a given ID and have an <b>Error</b> status.	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No

Attribute	Meaning	Search query examples	Supported for group creation
warningByPlan	Devices that are protected by a protection plan with a given ID and have a <b>Warning</b> status.	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No
runningByPlan	Devices that are protected by a protection plan with a given ID and have a <b>Running</b> status.	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No
interactionByPlan	Devices that are protected by a protection plan with a given ID and have an <b>Interaction Required</b> status.	interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	No
ou	Machines that belong to the specified Active Directory organizational unit.	ou IN ('RnD', 'Computers')	Yes
id	Device ID.  To get the device ID, under <b>Devices</b> , select the device, click <b>Details</b> > <b>All properties</b> . The ID is shown in the id field.	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Yes
lastBackupTime	The date and time of the last successful backup.  The format is 'YYYY-MM-DD HH:MM'.	lastBackupTime > '2022-03-11'  lastBackupTime <= '2022-03-11 00:15'  lastBackupTime is null	No
lastBackupTryTime	The time of the last backup attempt.  The format is 'YYYY-MM-DD HH:MM'.	lastBackupTryTime >= '2022-03-11'	No
nextBackupTime	The time of the next backup.	nextBackupTime >= '2022-08-11'	No

Attribute	Meaning	Search query examples	Supported for group creation
	The format is 'YYYY-MM-DD HH:MM'.		
agentVersion	Version of the installed protection agent.	agentVersion LIKE '12.0.*'	Yes
hostId	Internal ID of the protection agent.  To get the protection agent ID, under <b>Devices</b> , select the machine, click <b>Details &gt; All properties</b> . Use the "id" value of the agent property.	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Yes
resourceType	Resource type.  Possible values: <ul style="list-style-type: none"> <li>'machine'</li> <li>'virtual_machine.vmwesx'</li> <li>'virtual_machine.mshyperv'</li> <li>'virtual_machine.rhev'</li> <li>'virtual_machine.kvm'</li> <li>'virtual_machine.xen'</li> </ul>	resourceType = 'machine'  resourceType in ('mssql_aag_database', 'mssql_database')	Yes
hasAsz	Protection agent on a physical machine with AcronisSecure Zone.  Possible values: <ul style="list-style-type: none"> <li>true</li> <li>false</li> </ul>	hasAsz=true	Yes
chassis	Machine chassis type.  Possible values: <ul style="list-style-type: none"> <li>unknown</li> <li>laptop</li> <li>desktop</li> </ul>	chassis='laptop'	Yes

Attribute	Meaning	Search query examples	Supported for group creation
	<ul style="list-style-type: none"> <li>server</li> <li>other</li> </ul>		

### Note

If you skip the hour and minutes value, the start time is considered to be YYYY-MM-DD 00:00, and the end time is considered to be YYYY-MM-DD 23:59:59. For example, lastBackupTime = 2020-02-20, means that the search results will include all backups from the interval lastBackupTime >= 2020-02-20 00:00 and lastBackup time <= 2020-02-20 23:59:59

## Operators

The following table summarizes the available operators.

Operator	Meaning	Examples
AND	Logical conjunction operator.	name like 'en-00' AND tenant = 'Unit 1'
OR	Logical disjunction operator.	state = 'backup' OR state = 'interactionRequired'
IN (<value1>,...<valueN>)	This operator is used to test if an expression matches any value in a list of values.	osType IN ('windows', 'linux')
NOT	Logical negation operator.	NOT(osProductType = 'workstation')
NOT IN (<value1>,...<valueN>)	This operator is the opposite of the IN operator.	NOT osType IN ('windows', 'linux')
LIKE 'wildcard pattern'	<p>This operator is used to test if an expression matches the wildcard pattern.</p> <p>The following wildcard operators can be used:</p> <ul style="list-style-type: none"> <li>* or % The asterisk and the percent sign represent zero, one, or multiple characters</li> <li>_ The underscore represents a single character</li> </ul>	<p>name LIKE 'en-00'</p> <p>name LIKE '*en-00'</p> <p>name LIKE '*en-00*'</p> <p>name LIKE 'en-00_'</p>
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')

Operator	Meaning	Examples
= or ==	<i>Equal to operator.</i>	osProductType = 'server'
!= or <>	<i>Not equal to operator.</i>	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'
<	<i>Less than operator.</i>	memorySize < 1024
>	<i>Greater than operator.</i>	diskSize > 300GB
<=	<i>Less than or equal to operator.</i>	lastBackupTime <= '2022-05-11 00:15'
>=	<i>Greater than or equal to operator.</i>	nextBackupTime >= '2022-09-11'

## Applying a protection 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 protection plan.  
The software displays the list of child groups.
2. Select the group to which you want to apply a protection plan.
3. Click **Group backup**.  
The software displays the list of protection plans that can be applied to the group.
4. Do one of the following:
  - Expand an existing protection plan, and then click **Apply**.
  - Click **Create new**, and then create a new protection plan as described in "[Backup](#)".

# Monitoring and reporting

The **Overview** dashboard enables you to monitor the current state of your protected infrastructure.

The **Reports** section enables you to generate on-demand and scheduled reports about your protected infrastructure. This section is only available with an Advanced license.

## The Overview dashboard

The **Overview** dashboard provides a number of customizable widgets that give an overview of your protected infrastructure. You can choose from more than 20 widgets, presented as pie charts, tables, graphs, bar charts, and lists. They have clickable elements that enable you to investigate and troubleshoot issues. The information in the widgets is updated every five minutes.

With an Advanced license, you can also download the current state of the dashboard or send it via email in the .pdf or/and .xlsx format. To send the dashboard via email, ensure that the **Email server** settings are configured.

The available widgets depend on your Cyber Protect edition. The default widgets are listed below:

Widget	Availability	Description
<a href="#">Cyber protection</a>	Not available in Cyber Backup editions	Shows overall information about the size of backups, blocked malware, blocked URLs, found vulnerabilities, and installed patches.
<a href="#">Protection status</a>	Available in all editions	Shows the current protection status for all machines.
Activities	Available in all editions	Shows a summary of the activities that were performed during a specified time period.
Active alerts summary	Available in all editions	Shows a summary of the active alerts by alert type and by severity.
<a href="#">Patch installation status</a>	Not available in Cyber Backup editions	Shows the number of machines grouped by patch installation status.
<a href="#">Missing updates by category</a>	Not available in Cyber Backup editions	Shows the number of missing updates by category.
<a href="#">Disk health status</a>	Not available in Cyber Backup editions	Shows the number of disks by their status.
Devices	Available in all editions	Shows detailed information about the devices in your environment.

Active alerts details	Available in all editions	Shows detailed information about the active alerts.
<a href="#">Existing vulnerabilities</a>	Available in all editions	Shows the existing vulnerabilities for the operating systems and applications in your environment, and the affected machines.
<a href="#">Patch installation history</a>	Not available in Cyber Backup editions	Shows detailed information about the patches that were installed.
<a href="#">Recently affected</a>	Available in all editions	Shows detailed information about the recently infected machines.
Locations summary	Available in all editions	Shows detailed information about the backup locations.

### ***To add a widget***

Click **Add widget**, and then do one of the following:

- Click the widget that you want to add. The widget will be added with the default settings.
- To edit the widget before adding it, click the pencil icon when the widget is selected. After editing the widget, click **Done**.

### ***To rearrange the widgets on the dashboard***

Drag and drop the widgets by clicking their names.

### ***To edit a widget***

Click the pencil icon next to the widget name. Editing a widget enables you to rename it, change the time range, set filters, and group rows.

### ***To remove a widget***

Click the X sign next to the widget name.

## Cyber Protection

This widget shows overall information about the size of backups, blocked malware, blocked URLs, found vulnerabilities, and installed patches.

The upper row shows the current statistics:

- **Backed up today** – the sum of recovery point sizes for the last 24 hours
- **Malware blocked** – the number of currently active alerts about malware blocked
- **URLs blocked** – the number of currently active alerts about URLs blocked
- **Existing vulnerabilities** – the number of currently existing vulnerabilities
- **Patches ready to install** – the number of currently available patches to be installed

The lower row shows the overall statistics:

- The compressed size of all backups
- The accumulated number of blocked malware across all machines
- The accumulated number of blocked URLs across all machines
- The accumulated number of discovered vulnerabilities across all machines
- The accumulated number of installed updates/patches across all machines

## Protection status

### Protection status

This widget shows the current protection status for all machines.

A machine can be in one of the following statuses:

- **Protected** – Machines with applied protection plan.
- **Unprotected** – Machines without applied protection plan. These include both discovered machines and managed machines with no protection plan applied.
- **Managed** – Machines with installed protection agent.
- **Discovered** – Machines without installed protection agent.

If you click on the machine status, you will be redirected to the list of machines with this status for more details.

### Discovered machines

This widget shows the list of discovered machines during the specified time range.

## Disk health monitoring

Disk health monitoring provides information about the current disk health status and a forecast about it, so that you can prevent data loss that might be related to a disk failure. Both HDD and SSD disks are supported.

### Limitations:

- Disk health forecast is supported only for machines running Windows.
- Only disks of physical machines are monitored. Disks of virtual machines cannot be monitored and are not shown in the disk health widgets.
- RAID configurations are not supported.
- On NVMe drives, disk health monitoring is supported only for drives that communicate the SMART data via the Windows API. Disk health monitoring is not supported for NVMe drives that require reading the SMART data directly from the drive.

The disk health is represented by one of the following statuses:

- **OK**  
Disk health is between 70% and 100%.



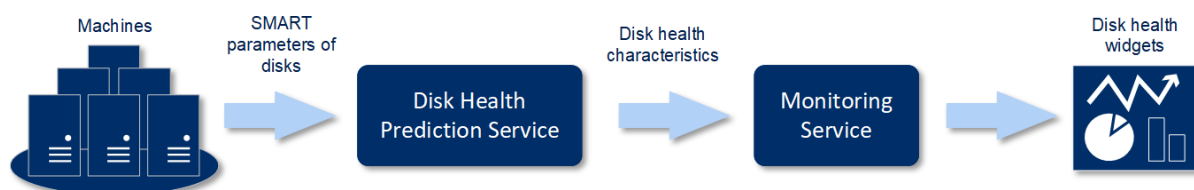
- **Warning**  
Disk health is between 30% and 70%.
- **Critical**  
Disk health is between 0% and 30%.
- **Calculating disk data**  
The current disk status and forecast are being calculated

## How it works

Disk Health Prediction Service uses an AI-based prediction model.

1. The protection agent collects the SMART parameters of the disks and passes this data to Disk Health Prediction Service:
  - SMART 5 – Reallocated sectors count.
  - SMART 9 – Power-on hours.
  - SMART 187 – Reported uncorrectable errors.
  - SMART 188 – Command timeout.
  - SMART 197 – Current pending sector count.
  - SMART 198 – Offline uncorrectable sector count.
  - SMART 200 – Write error rate.
2. Disk Health Prediction Service processes the received SMART parameters, makes forecasts, and provides the following disk health characteristics:
  - Disk health current state: OK, warning, critical.
  - Disk health forecast: negative, stable, positive.
  - Disk health forecast probability in percentage.

The prediction period is always one month.
3. Monitoring Service receives these characteristics, and then shows the relevant information in the disk health widgets in the Cyber Protect web console.

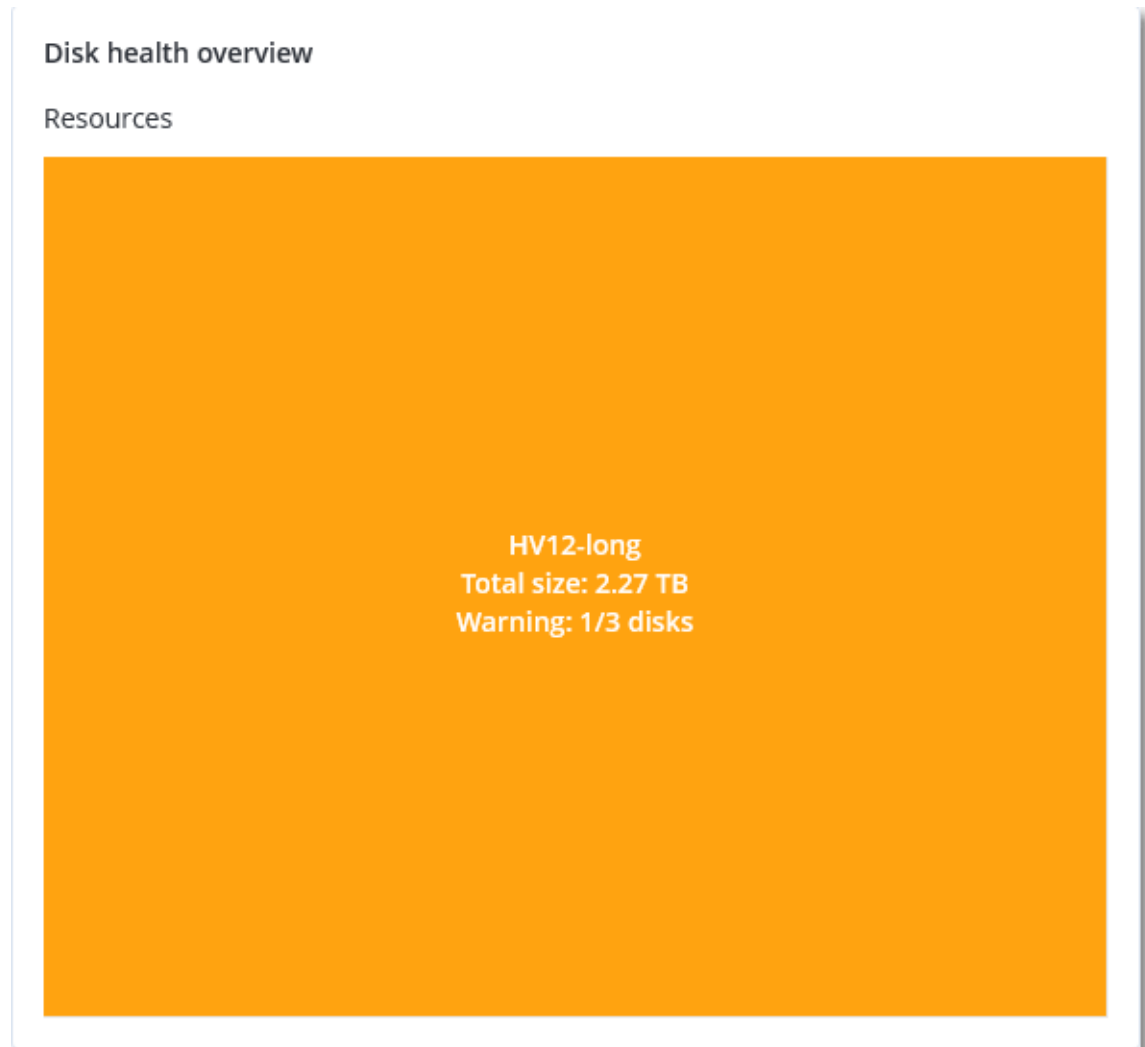


## Disk health widgets

The results of the disk health monitoring are presented in the following widgets that are available in the Cyber Protect web console.

- **Disk health overview** is a treemap widget with two levels of detail that can be switched by drilling down.
  - Machine level  
Shows summarized information about the disk status of all machines in the selected

organizational unit. Only the most critical disk status is shown. The other statuses are shown in a tooltip when you hover over a particular block. The machine block size depends on the total size of all disks of the machine. The machine block color depends on the most critical disk status found.

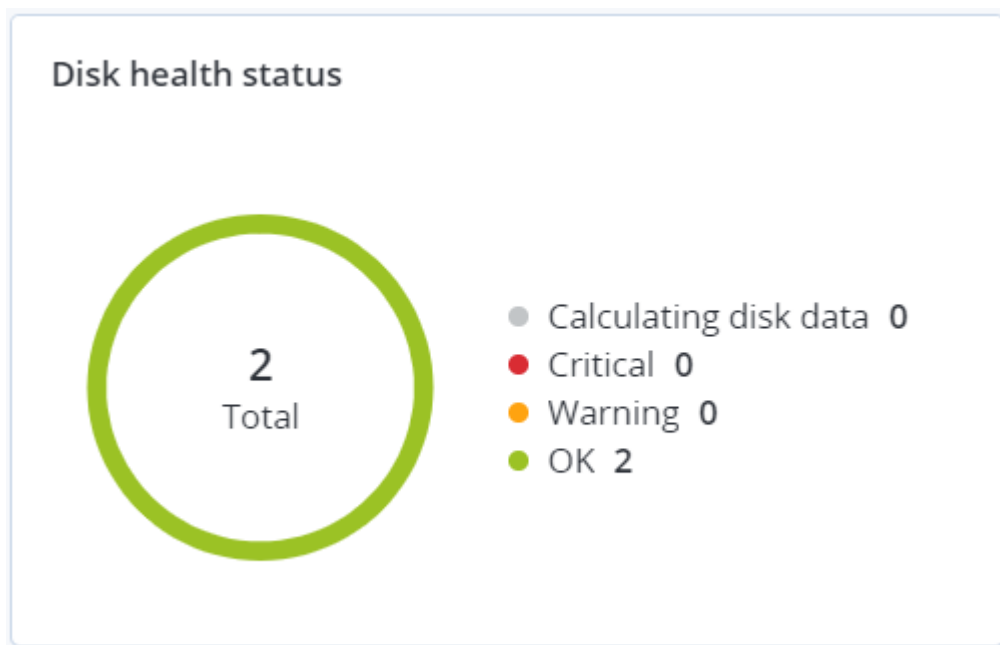


- Disk level  
Shows the current disk health status of all disks for the selected machine. Each disk block shows one of the following disk health forecasts and its probability in percentage:
  - Will be degraded
  - Will stay stable

- Will be improved



- **Disk health status** is a pie chart widget that shows the number of disks for each status.



## Disk health status alerts

The disk health check runs every 30 minutes, while the corresponding alert is generated once a day. When the disk health status changes from **Warning** to **Critical**, an alert is always generated.

Alert name	Severity	Disk health status	Description
Disk failure is possible	Warning	(30 – 70)	The <disk name> disk on this machine is likely to fail in the future. Run a full image backup of this disk as soon as possible, replace it, and then recover the image to the new disk.
Disk failure is imminent	Critical	(0 – 30)	The <disk name> disk on this machine is in a critical state and will most likely fail very soon. An image backup of this disk is not recommended at this point as the added stress can cause the disk to fail. Back up the most important files on this disk immediately and replace it.

## Data protection map

The data protection map feature allows you to discover all data that are important for you and get detailed information about number, size, location, protection status of all important files in a treemap scalable view.

Each block size depends on the total number/size of all important files that belong to an organizational unit/machine.

Files can have one of the following protection statuses:

- **Critical** – there are 51-100% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **Low** – there are 21-50% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **Medium** – there are 1-20% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **High** – all files with the extensions specified by you are protected (backed up) for the selected machine/location.

The results of the data protection examination can be found on the dashboard, in the Data Protection Map widget – a treemap widget that shows details on a machine level.

Hover over the colored block to see more information about the number of unprotected files and their location. To protect them, click **Protect all files**.

## Vulnerability assessment widgets

### Vulnerable machines

This widget shows the vulnerable machines by the vulnerability severity.

The found vulnerability can have one of the following severity levels according to the [Common Vulnerability Scoring System \(CVSS\) v3.0](#):

- Secured: no vulnerabilities are found
- Critical: 9.0 - 10.0 CVSS
- High: 7.0 - 8.9 CVSS
- Medium: 4.0 - 6.9 CVSS
- Low: 0.1 - 3.9 CVSS
- None: 0.0 CVSS

### Existing vulnerabilities

This widget shows currently existing vulnerabilities on machines. In the **Existing vulnerabilities** widget, there are two columns showing timestamps:

- **First detected** – date and time when a vulnerability was detected initially on the machine.
- **Last detected** – date and time when a vulnerability was detected the last time on the machine.

## Patch installation widgets

There are four widgets related to the patch management functionality.

### Patch installation status

This widget shows the number of machines grouped by the patch installation status.

- **Installed** – all available patches are installed on a machine
- **Reboot required** – after patch installation reboot is required for a machine
- **Failed** – patch installation failed on a machine

### Patch installation summary

This widget shows the summary of the patches by their installation status.

### Patch installation history

This widget shows detailed information about the patches that were installed on the machines.

## Missing updates by categories

This widget shows the number of missing updates per category. The following categories are shown:

- Security updates
- Critical updates
- Other

## Backup scanning details

This widget is available only if Scan Service is installed on the management server. The widget shows detailed information about the threats that were detected in the backups.

## Recently affected

This widget shows detailed information about the recently infected machines. Here, you can find information about what threat was detected and how many files were infected.

## No recent backups

This widget shows workloads with applied protection plans, whose last successful backup date was earlier than the time range specified in the widget settings.

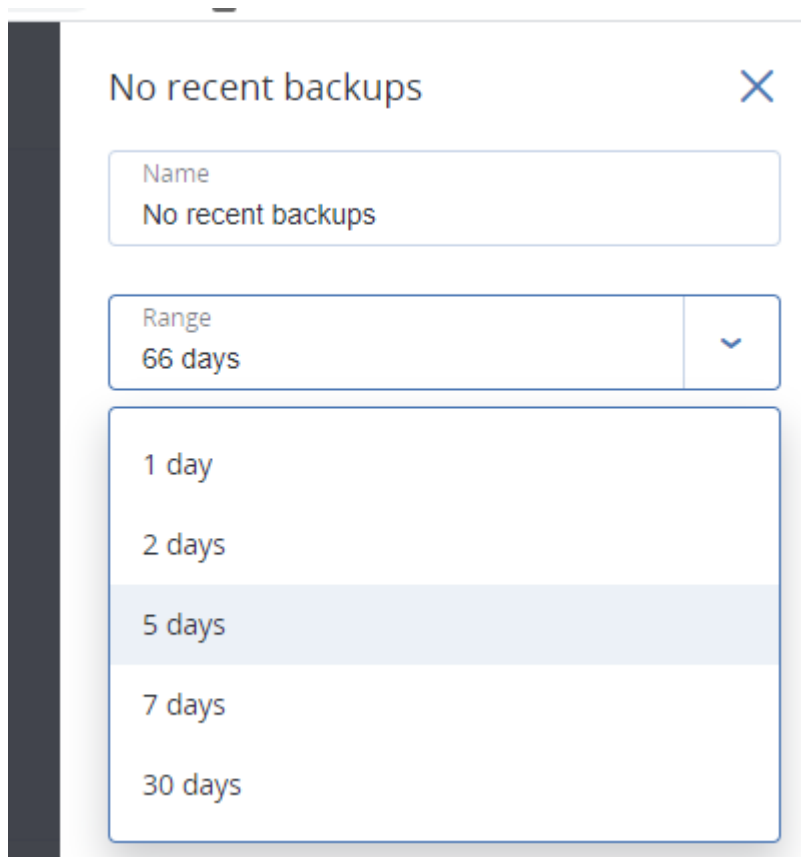
## No recent backups

Total devices: 25

 UbuntuResto...	781 days ago
 vm-Win2012-...	776 days ago
 APanin Cent...	683 days ago
 vm-Win2012-...	665 days ago
 VS-Win2k12-...	649 days ago

[Show all](#)

By default, when you add this widget, it shows information for the last 5 days. You can use the drop-down menu to select another period or enter a number of days manually. The maximum number of days you can enter is 180.



## The Activities tab

The **Activities** tab provides an overview of the activities during the last 90 days.

To customize the view of the **Activities** tab, click the gear icon and select the columns that you want to see. To see the activity progress in real time, select the **Refresh automatically** check box. Note that frequent updates of multiple activities might degrade the performance of the management server.

Activities					
<input type="text" value="Device name"/> search		Any status ▾	Any type ▾	Most recent ▾	<input checked="" type="checkbox"/> Refresh automatically
Status	Description	Device	Start time	Finish time ↓	Duration
✓ Succeeded	Logging in account 'WIN-K2...		Mar 29 10:04:27 PM	Mar 29 10:04:27 PM	0 sec
✓ Succeeded	Logging in account 'WIN-K2...		Mar 29 10:04:27 PM	Mar 29 10:04:27 PM	0 sec
✓ Succeeded	Adding machine 'WIN-K2RL...		Mar 29 05:55:54 PM	Mar 29 05:55:54 PM	0 sec
✓ Succeeded	Logging in account 'WIN-K2...		Mar 29 11:13:48 AM	Mar 29 11:13:48 AM	0 sec
✓ Succeeded	Logging in account 'WIN-K2...		Mar 28 10:38:26 AM	Mar 28 10:38:26 AM	0 sec

You can search the listed activities by the following criteria:

- **Device name**  
This is the machine on which the activity is performed.
- **Started by**  
This is the account who started the activity.

You can also filter the activities by the following properties:



- **Status**

For example, succeeded, failed, in progress, or canceled.

- **Type**

For example, applying plan, deleting backups, installing software updates.

- **Time**

For example, the most recent activities, the activities from the past 24 hours, or the activities during a specific period within the default retention period.

To change the default retention period, edit the `task_manager.yaml` configuration file.

***To change the retention period***

1. On the machine running the management server, open the following configuration file in a text editor:

- In Windows: `%Program Files%\Acronis\TaskManager\task_manager.yaml`
- In Linux: `/usr/lib/Acronis/TaskManager/task_manager.yaml`

2. Locate the following section:

```
database:
 connection-string: ""
 run-cleanup-at: "23:59"
 cleanup-batch-size: 10
 max-cleanup-retries: 10
 log-queries: false
 max-transaction-retries: 10
 shards:
 - connection-string: sqlite://task-manager.sqlite
 days-to-keep: 90
 space: "default"
 key: "00000000-0000-0000-0000-000000000000"
```

3. Edit the `days-to-keep` line as desired.

For example:

```
days-to-keep: 30
```

---

**Note**

You can change the retention period according to your needs. Increasing the retention period degrades the performance of the management server.

---

4. Restart **Acronis Service Manager Service** as described in "To restart Acronis Service Manager Service" (p. 214).

## Reports

You can use predefined reports or create a custom report. A report can include any set of dashboard widgets.

You can only configure reports for the units that you manage.

The reports can be sent via email or downloaded on a schedule. To send the reports via email, ensure that the **Email server** 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.

The available reports depend on your Cyber Protect edition. The default reports are listed below:

Report name	Availability	Description
Alerts	Cyber Backup Advanced Cyber Protect Advanced	Shows the alerts that occurred during a specified time period.
Backup scanning details	Cyber Protect Advanced	Shows detailed information about detected threats in the backups.
Backups	Cyber Backup Advanced Cyber Protect Advanced	Shows details about the current backups and recovery points.
Current status	Cyber Backup Advanced Cyber Protect Advanced	Shows the current status of your environment.
Daily activities	Cyber Backup Advanced Cyber Protect Advanced	Shows a summary about the activities that were performed during a specified time period.
Data protection map	Cyber Protect Advanced	Shows detailed information about the number, size, location, and protection status of all important files on the machines.
Detected threats	Cyber Backup Advanced Cyber Protect Advanced	Shows details about the affected machines by number of blocked threats, and information about the healthy and vulnerable machines.

Discovered machines	Cyber Backup Advanced Cyber Protect Advanced	Shows all machines that were discovered in the organization network.
Disk health prediction	Cyber Protect Advanced	Shows predictions about when your HDD/SSD will break down, and the current disk status.
Existing vulnerabilities	Cyber Backup Advanced Cyber Protect Advanced	Shows the existing vulnerabilities for the operating systems and applications in your environment, and the affected machines.
Licenses	Cyber Backup Advanced Cyber Protect Advanced	Shows a summary of available licenses.
Locations	Cyber Backup Advanced Cyber Protect Advanced	Shows usage statistics for the backup locations, for a specified time period.
Patch management summary	Cyber Protect Advanced	Shows the number of missing patches, installed patches, and applicable patches. You can drill down the report to get the missing/installed patch information and details about all the systems.
Summary	Cyber Backup Advanced Cyber Protect Advanced	Shows a summary of the protected devices, for a specified time period.
Tape activities	Cyber Backup Advanced Cyber Protect Advanced	Shows a list of tapes that were used during the last 24 hours.
Weekly activities	Cyber Backup Advanced Cyber Protect Advanced	Shows a summary of the activities that were performed during a specified time period.

## Basic operations with reports

- To view a report, click its name.
- For additional operations with a report, click the ellipsis icon (...).

The same operations are available from within the report.

### ***To add a report***

1. Click **Add report**.
2. Do one of the following:
  - To add a predefined report, click its name.
  - To add a custom report, click **Custom**. A new report with the name **Custom** is added to the list of reports. Open this report and add widgets to it.
3. [Optional] Drag and drop the widgets to rearrange them.
4. [Optional] Edit the report as described below.

### ***To edit a report***

1. Click the ellipsis icon (...) next to a report name, and then click **Settings**.
2. Edit the report. You can:
  - Rename the report
  - Change the time range for all widgets included in the report
  - Schedule sending the report via email in the .pdf or/and .xlsx format
3. Click **Save**.

### ***To schedule 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 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**.

## 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](#), 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
```

# Advanced storage options

## Tape devices

The following sections describe in detail how to use tape devices for storing backups.

### 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.

## Overview of tape support

Protection agents can back up data to a tape device directly or through a storage node. In either case, fully automatic operation of the tape device is ensured. When a tape device with several drives is attached to a storage node, multiple agents can simultaneously back up to tapes.

## 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)

Protection agents and storage nodes do not use RSM. When [detecting a tape device](#), 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.

## Supported hardware

Acronis Cyber Protect supports external SCSI devices. These are devices connected to Fibre Channel or using the SCSI, iSCSI, Serial Attached SCSI (SAS) interfaces. Also, Acronis Cyber Protect supports USB-connected tape devices.

In Windows, Acronis Cyber Protect 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.

To learn if your specific device is supported, use the Hardware Compatibility Tool as described at <http://kb.acronis.com/content/57237>. You are welcome to send a report about the test results to Acronis. Hardware with confirmed support is listed in the Hardware Compatibility List: <https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl>.

## 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:

- In Windows XP/Server 2003: %ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database.
- In Windows 7 and later versions of Windows: %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database.
- In Linux: /var/lib/Acronis/BackupAndRecovery/ARSM/Database.

The database size depends on the number of backups stored on tapes and equals approximately 10 MB per hundred backups. The database may be large if the tape library contains thousands of backups. In this case, you may want to store the tape database on a different volume.

### ***To relocate the database in Windows:***

1. Stop the Removable Storage Management service.
2. Move all files from the default location to the new location.
3. Find the registry key HKEY\_LOCAL\_MACHINE\SOFTWARE\Acronis\ARSM\Settings.
4. Specify the new location path in the registry value ArsmDm1DbProtocol. The string may contain up to 32765 characters.
5. Start the Removable Storage Management service.

### ***To relocate the database in Linux:***

1. Stop the acronis\_rsm service.
2. Move all files from the default location to the new location.
3. Open the configuration file /etc/Acronis/ARSM.config in a text editor.



4. Locate the line `<value name="ArsmDm1DbProtocol" type="TString">`.
5. Change the path under this line.
6. Save the file.
7. Start the `acronis_rsm` service.

## The TapeLocation folder

The TapeLocation folder contains a cache of the file system metadata from all volumes that are backed up on tapes.

The default TapeLocation folder path is:

- In Windows XP/Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation`
- In Windows 7 and later: `%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`
- In Linux: `/var/lib/Acronis/BackupAndRecovery/TapeLocation`

The TapeLocation folder size is about 0,5-1% of the size of all backups stored on tapes. For disk-level backups with the file recovery option enabled, the TapeLocation folder size might be slightly larger, depending on the number of the backed-up files.

## Parameters for writing to tapes

The tape writing parameters (block size and cache size) allow you to fine-tune the software to achieve the maximum performance. Both parameters are required for writing to tapes, but normally you only need to adjust the block size. The optimal value depends on the tape device type and on the data being backed up, such as the number of files and their size.

---

### Note

When the software reads from a tape, it uses the same block size that was used when writing to the tape. If the tape device does not support this block size, the reading will fail.

---

The parameters are set on each machine that has a tape device attached. It can be a machine where an agent or a storage node is installed. On a machine running Windows, the configuration is performed in the registry; on a Linux machine, it is done in the configuration file

**`/etc/Acronis/BackupAndRecovery.config`.**

In Windows, create the respective registry keys and their DWORD values. In Linux, add the following text at the end of the configuration file, right before the `</registry>` tag:

```
<key name="TapeLocation">
 <value name="WriteCacheSize" type="Dword">
 "value"
 </value>
 <value name="DefaultBlockSize" type="Dword">
 "value"
 </value>
</key>
```

## 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.

## Tape-related backup options

You can configure the **Tape management** backup options to determine:

- Whether to enable file recovery from disk-level backups stored on tapes.
- Whether to return tapes back to slots after protection 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.

## Parallel operations

Acronis Cyber Protect can simultaneously perform operations with various components of a tape device. During an operation that uses a drive (backing up, recovering, **rescanning**, or **erasing**), you can launch an operation that uses a changer (**moving** a tape to another slot or **ejecting** 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** can be performed simultaneously with any other operation. During **inventorying**, no other operation is available except for detecting the new tape devices.

Operations that cannot be performed in parallel are queued.

## 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 the following data types to tapes: Microsoft 365 mailboxes, Microsoft Exchange mailboxes.
3. You cannot create application-aware backups of physical and virtual machines.
4. In macOS, only file-level backup to a managed tape-based location is supported.
5. 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.
6. The deduplication of backups located on tapes is not possible.
7. The software cannot automatically overwrite a tape that contains non-deleted backups or if there are dependent backups on other tapes.

The only exception to this rule is when the option "Overwrite a tape in the stand-alone tape drive when creating a full backup" is enabled.

8. 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.
9. You can [validate](#) any backup stored on tapes, but you cannot select for validation an entire tape-based location or tape device.
10. A managed tape-based location cannot be protected with encryption. Encrypt your backups instead.
11. The software cannot simultaneously write one backup to multiple tapes or multiple backups through the same drive to the same tape.
12. Devices that use the Network Data Management Protocol (NDMP) are not supported.
13. Barcode printers are not supported.
14. Linear Tape File System (LTFS) formatted tapes are not supported.

## Readability of tapes written by older Acronis products

The following table summarizes the readability of tapes written by Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5, 11.7, and 12.5 product families in Acronis Cyber Protect. The table also illustrates the compatibility of tapes written by various components of Acronis Cyber Protect.

You can append incremental and differential backups to rescanned backups that were created by Acronis Backup 11.5, 11.7, and 12.5.

	...is readable on a tape device attached to a machine with...			
	Acronis Cyber Protect Bootable Media	Acronis Cyber Protect Agent for Windows	Acronis Cyber Protect Agent for Linux	Acronis Cyber Protect Storage Node

<b>Tape written on a locally attached tape device (tape drive or tape library) by...</b>	Bootable Media	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	Agent for Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	Agent for Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
<b>Tape written on a tape device through...</b>	Backup Server	9.1	-	-	-	-
		Echo	-	-	-	-
	Storage Node	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+

## Getting started with a tape device

### 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 protection agent is installed on the machine.

## Before backing up

1. Load tapes to the tape device.
2. Log in to the Cyber Protect web 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.

---

### Note

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](#) such tapes to the **Free tapes** pool manually.

---

### Note

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 protection plan as described in the ["Backup"](#) section. When specifying the backup location, select **Tape pool 'Acronis'**.

## Results

- To access the location where backups will be created, click **Backup storage > Tape pool 'Acronis'**.
- Tapes with the backups will be moved to the **Acronis** pool.

## Backing up to a tape device attached to a storage node

### Prerequisites

- A storage node is registered on the management server.
- The tape device is attached to the storage node in accordance with the manufacturer's instructions.

## Before backing up

1. Load tapes to the tape device.
2. Log in to the Cyber Protect web console.
3. Click **Settings** > **Tape management**, expand the node with the storage node name, 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 pools 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.

---

### Note

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](#) such tapes to the **Free tapes** pool manually.

---

### Note

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.

---

- d. Decide whether you want to back up to the **Acronis pool** or to [create a new pool](#).  
**Details.** Having several pools enables you to use a separate tape set for each machine or each department of your company. By using multiple pools, you can prevent backups created via different protection plans from mixing up on one tape.
- e. If the selected pool can take tapes from the **Free tapes** pool when required, skip this step. Otherwise, move tapes from the **Free tapes** pool to the selected pool.  
**Tip.** To learn whether a pool can take tapes from the **Free tapes** pool, click the pool and then click **Info**.

## Backing up

Create a protection plan as described in the "Backup" section. When specifying the backup location, select the created tape pool.

## Results

- To access the location where backups will be created, click **Backups**, and then click the name of the created tape pool.
- Tapes with the backups will be moved to the selected pool.

## Tips for further usage of the tape library

- You do not need to perform full inventorying each time you load a new tape. To save time, follow the procedure described in the "[Inventorying](#)" section under "Combination of fast and full inventorying".
- You can create other pools on the same tape library and select any of them as a destination for backups.

## Recovering under an operating system from a tape device

### *To recover under an operating system from a tape device:*

1. Log in to the Cyber Protect web 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](#) 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](#).
  - 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](#).

---

### **Warning!**

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](#) 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.



## 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"](#).
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](#).
- 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.

## Recovering under bootable media from a tape device attached to a storage node

### *To recover under bootable media from a tape device attached to a storage node:*

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. Click **Recover**.
5. Click **Select data**, and then click **Browse**.
6. In the **Path** box, type `bsp://<storage node address>/<pool name>/`, where `<storage node address>` is the IP address of the storage node that contains the required backup, and `<pool name>` is the name of the tape pool. Click **OK** and specify credentials for the pool.
7. Select the backup, 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.
8. Configure other recovery settings.
9. Click **OK** to start the recovery.
10. 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](#).
  - 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.

## Tape management

### 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.

## 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](#) 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 Cyber Protect in a tape device attached to another storage node or 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.

## Operations with pools

### Creating a pool

#### *To create a pool:*

1. Click **Settings > Tape management**.
2. Select the machine or the storage node 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 or the storage node 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.
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 protection plans that have the pool as the backup location. Otherwise, these protection plans will fail.

---

#### *To delete a pool:*

1. Click **Settings > Tape management**.
2. Select the machine or the storage node 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.

## 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 or the storage node 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 or the storage node 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.
6. Select the pool to move the tapes to.
7. Click **Move** to save the changes.

---

#### Note

If you have restorable backups on the tape and you move the tape to another pool, make sure you refresh the vault under Backup storage once you complete the move operation. The backups will be available in the second pool despite the original backup destination.

---

## 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 or storage node 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 or storage node 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	<b>Imported tapes</b>
	Storage node	<b>Imported tapes</b>
Storage node	The same storage node	Where the tape was before
	Another storage node	<b>Imported tapes</b>
	Agent	<b>Imported tapes</b>
Third-party backup application	Agent or storage node	<b>Unrecognized tapes</b>

Tapes of certain types are sent to specific pools:

Tape type	Tape is sent to pool...
Empty tape	<b>Free tapes</b>
Empty write-protected tape	<b>Unrecognized tapes</b>
Cleaning tape	<b>Unrecognized tapes</b>

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](#) 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](#) 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.

To rescan tapes with a multistreamed or both multistreamed and multiplexed backup, you need at least the same number of drives that were used to create this backup. Such a backup cannot be rescanned through a stand-alone tape drive.

Run the rescanning:

- If the database of a storage node or managed machine is lost or damaged.
- If information about a tape in the database is out of date (for example, a tape contents were modified by another storage node or agent).
- To obtain access to backups stored on tapes when working under bootable media.
- If you have mistakenly **removed** 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** it, **remove** 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 or the storage node 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](#).

---

**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](#). 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 or the storage node 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 or the storage node 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 or the storage node 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](#), 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](#)) tape.

### ***To remove a tape***

1. Click **Settings > Tape management**.
2. Select the machine or the storage node 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](#) 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](#) to detect the tape.

---

#### **Note**

During the inventorying, do *not* enable the **Move unrecognized and imported tapes to the 'Free tapes' pool** switch.

---

3. Perform the [rescanning](#) 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](#), 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 or the storage node 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.

## Storage nodes

A storage node is a server designed to optimize the usage of various resources (such as the corporate storage capacity, the network bandwidth, and the production servers' CPU load) that are required to protect enterprise data. This goal is achieved by organizing and managing the locations that serve as dedicated storage locations of the enterprise backups (managed locations).

The primary purpose of Acronis Storage Node is to enable centralized access to tape drives or libraries, for example, backup and recover data from multiple devices to the same tape drive or library (managed vault on tape).

Another use case is to enable advanced deduplication capabilities where data across multiple devices needs to be deduplicated against each other and stored in a single location (managed vault with enabled deduplication).

## Installing a storage node and a catalog service

Before installing a storage node, ensure that the machine meets the [system requirements](#).

We recommend that you install a storage node and a catalog service on separate machines. The system requirements to a machine running a catalog service are described in "Cataloging best practices" (p. 620).

### ***To install a storage node and/or a catalog service***

1. Log on as an administrator and start the Acronis Cyber Protect setup program.
2. [Optional] To change the language of the setup program, click **Setup language**.
3. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
4. Click **Install a protection agent**.
5. Click **Customize installation settings**.
6. Next to **What to install**, click **Change**.
7. Select the components to install:
  - To install a storage node, select the **Storage Node** check box. The **Agent for Windows** check box is automatically selected.
  - To install a catalog service, select the **Catalog Service** check box.
  - If you do not want to install other components on this machine, clear the corresponding check boxes.Click **Done** to continue.
8. Specify the management server where the components will be registered:
  - a. Next to **Acronis Cyber Protect 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 "Step 1: Generating a registration token" (p. 193).
  - d. Click **Done**.
9. If prompted, select whether the machine with the storage node and/or the catalog service 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](#)".
  10. [Optional] Change other installation settings as described in "[Customizing installation settings](#)".
  11. Click **Install** to proceed with the installation.
  12. After the installation completes, click **Close**.

## Updating the catalog service with Acronis Cyber Protect 15 Update 4

Acronis Cyber Protect 15 Update 4 uses a new version of the catalog service. The new version is not directly compatible with the catalog data that is created by earlier versions.

During the update to Acronis Cyber Protect 15 Update 4, you can manually migrate this data to the new version of the catalog service. Alternatively, you can skip the migration and recreate the catalog data later. Recreating the catalog data takes more time than its migration.

### ***To migrate the catalog data***

1. On the machine where the catalog service is installed, run the Acronis Cyber Protect setup program.
2. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
3. Select the **I understand** check box, and then click **Update**.
4. Select the **Specify a temporary** folder check box.
5. Specify the folder in which the catalog data will be exported.  
The exported data is encrypted. The temporary folder is automatically deleted when the migration completes.
6. Click **Done**.

### ***To skip the migration of the catalog data***

1. On the machine where the catalog service is installed, run the Acronis Cyber Protect setup program.
2. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
3. Select the **I understand** check box, and then click **Update**.
4. Clear the **Specify a temporary folder** check box.
5. Click **Done**.
6. Confirm your choice.

As a result, the existing catalog data will become unavailable after the update to Acronis Cyber Protect 15 Update 4. To recreate the catalog data, run a backup.

---

**Note**

If the catalog service, the storage node, and the management server run on separate machines, ensure that you update all of them to Acronis Cyber Protect 15 Update 4, in this order:

1. Management server
  2. Storage node
  3. Catalog service
- 

## Adding a managed location

A managed location can be organized:

- In a local folder:
  - On a hard drive local to the storage node
  - On a SAN storage that appears to the operating system as a locally attached device
- In a network folder:
  - On an SMB/CIFS share
  - On a SAN storage that appears to the operating system as a network folder
  - On a NAS
- On a tape device that is locally attached to the storage node.

Tape-based locations are created in the form of [tape pools](#). One tape pool is present by default. If necessary, you can create other tape pools, as described later in this section.

### *To create a managed location in a local or network folder*

1. Do one of the following:
  - Click **Backup storage > Add location**, and then click **Storage node**.
  - When creating a protection plan, click **Where to back up > Add location**, and then click **Storage node**.
  - Click **Settings > Storage nodes**, select the storage node that will manage the location, and then click **Add location**.
2. In **Name**, specify a unique name for the location. "Unique" means that there must not be another location with the same name, managed by the same storage node.
3. [Optional] Select the storage node that will manage the location. If you selected the last option in step 1, you will not be able to change the storage node.
4. Select the storage node name or IP address that the agents will use to access the location.  
By default, the storage node 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 access failure. To change this setting at a later time, click **Backup storage > the location > Edit**, and then change the **Address** field value.
5. Enter the folder path or browse to the desired folder.

6. Click **Done**. The software checks the access to the specified folder.
7. [Optional] Enable backup deduplication in the location.

Deduplication minimizes backup traffic and reduces the size of backups stored in the location by eliminating duplicate disk blocks.

For more information about deduplication restrictions, refer to "[Deduplication restrictions](#)".
8. [Only if deduplication is enabled] Specify or change the **Deduplication database path** field value.

This must be a folder on a hard drive local to the storage node. To improve the system performance, we recommend that you create the deduplication database and the managed location on different disks.

For more information about deduplication database, refer to "[Deduplication best practices](#)".
9. [Optional] Select whether to protect the location with encryption. Anything written to the location will be encrypted and anything read from it will be decrypted transparently by the storage node, by using a location-specific encryption key stored on the storage node.

For more information about encryption, refer to "[Location encryption](#)".
10. [Optional] Select whether to catalog the backups stored in the location. The data catalog lets you easily find the required version of data and select it for recovery.

If several cataloging services are registered on the management server, you can select the service that will catalog the backups stored in the location.

Cataloging can be enabled or disabled at a later time, as described in "[How to enable or disable cataloging](#)".
11. Click **Done** to create the location.

#### ***To create a managed location on a tape device***

1. Click **Backup storage > Add location** or, when creating a protection plan, click **Where to back up > Add location**.
2. Click **Tapes**.
3. [Optional] Select the storage node that will manage the location.
4. Follow the steps described in "[Creating a pool](#)", starting from step 4.

---

#### **Note**

By default, agents use the storage node name to access a managed tape-based location. To make the agents use the storage node IP address, click **Backup storage > the location > Edit**, and then change the **Address** field value.

---

# Deduplication

## Deduplication restrictions

### Common restrictions

Encrypted backups cannot be deduplicated. If you want to use deduplication and encryption at the same time, leave the backups unencrypted and direct them to a location where both deduplication and encryption are enabled.

### Disk-level backup

Deduplication of disk blocks is not performed if the volume's allocation unit size—also known as cluster size or block size—is not divisible by 4 KB.

---

#### Note

The allocation unit size on most NTFS and ext3 volumes is 4 KB. This allows for block-level deduplication. Other examples of allocation unit sizes allowing for block-level deduplication include 8 KB, 16 KB, and 64 KB.

---

### File-level backup

Deduplication of a file is not performed if the file is encrypted.

#### Deduplication and NTFS data streams

In the NTFS file system, a file may have one or more additional sets of data associated with it—often called *alternate data streams*.

When such file is backed up, so are all its alternate data streams. However, these streams are never deduplicated—even when the file itself is.

## Deduplication best practices

Deduplication is a complex process that depends on many factors.

The most important factors that influence deduplication speed are:

- The speed of access to the deduplication database
- The RAM capacity of the storage node
- The number of deduplicating locations created on the storage node.

To increase deduplication performance, follow the recommendations below.



## Place the deduplication database and deduplicating location on separate physical devices

The deduplication database stores the hash values of all items stored in the location—except for those that cannot be deduplicated, such as encrypted files.

To increase the speed of access to a deduplication database, the database and the location must be placed on separate physical devices.

It is best to allocate dedicated devices for the location and the database. If this is not possible, at least do not place a location or database on the same disk with the operating system. The reason is that the operating system performs a large number of hard disk read/write operations, which significantly slows down the deduplication.

### Selecting a disk for a deduplication database

- The database must reside on a fixed drive. Please do not try to place the deduplication database on external detachable drives.
- To minimize access time to the database, store it on a directly attached drive rather than on a mounted network volume. The network latency may significantly reduce deduplication performance.
- The disk space required for a deduplication database can be estimated by using the following formula:

$$S = U * 90 / 65536 + 10$$

Here,

S is disk size, in GB

U is the planned amount of unique data in the deduplication data store, in GB

For example, if the planned amount of unique data in the deduplication data store is U=5 TB, the deduplication database will require a minimum of free space, as shown below:

$$S = 5000 * 90 / 65536 + 10 = 17 \text{ GB}$$

### Selecting a disk for a deduplicating location

For the purpose of data loss prevention, we recommend using RAID 10, 5, or 6. RAID 0 is not recommended since it is not fault tolerant. RAID 1 is not recommended because of relatively low speed. There is no preference to local disks or SAN, both are good.

## 40 to 160 MB of RAM per 1 TB of unique data

When the limit is reached, deduplication will stop but backup and recovery will continue to work. If you add more RAM to the storage node, after the next backup, the deduplication will resume. In general, the more RAM you have, the larger volumes of unique data you can store.

## Only one deduplicating location on each storage node

It is highly recommended that you create only one deduplicating location on a storage node. Otherwise, the whole available RAM volume may be distributed in proportion to the number of the locations.

## Absence of applications competing for resources

The machine with the storage node should not run applications that require much system resources; for example, Database Management Systems (DBMS) or Enterprise Resource Planning (ERP) systems.

## Multi-core processor with at least 2.5 GHz clock rate

We recommend that you use a processor with the number of cores not less than four and the clock rate not less than 2.5 GHz.

## Sufficient free space in the location

Deduplication at target requires as much free space as the backed-up data occupies immediately after saving it to the location. Without a compression or deduplication at source, this value is equal to the size of the original data backed up during the given backup operation.

## High-speed LAN

1-Gbit LAN is recommended. It will allow the software to perform 5-6 backups with deduplication in parallel, and the speed will not reduce considerably.

## Back up a typical machine before backing up several machines with similar contents

When backing up several machines with similar contents, it is recommended that you back up one machine first and wait until the end of the backed-up data indexing. After that, the other machines will be backed up faster owing to the efficient deduplication. Because the first machine's backup has been indexed, most of the data is already in the deduplication data store.

## Back up different machines at different times

If you back up a large number of machines, spread out the backup operations over time. To do this, create several protection plans with various schedules.

## Location encryption

If you protect a location with encryption, anything written to the location will be encrypted and anything read from it will be decrypted transparently by the storage node, by using a location-specific encryption key stored on the node. If the storage medium is stolen or accessed by an unauthorized person, the malefactor will not be able to decrypt the location contents without access to the storage node.

This encryption has nothing to do with the backup encryption specified by the protection plan and performed by an agent. If the backup is already encrypted, the storage node-side encryption is applied over the encryption performed by the agent.

### ***To protect the location with encryption***

1. Specify and confirm a word (password) to be used for generating the encryption key.  
The word is case-sensitive. You will be asked for this word only when attaching the location to another storage node.
2. Select one of the following encryption algorithms:
  - **AES 128** – the location contents will be encrypted by using the Advanced Encryption Standard (AES) algorithm with a 128-bit key.
  - **AES 192** – the location contents will be encrypted by using the AES algorithm with a 192-bit key.
  - **AES 256** – the location contents will be encrypted by using the AES algorithm with a 256-bit key.
3. Click **OK**.

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 stored in the location and the more secure the backups will be.

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

## Cataloging

### Data catalog

The data catalog lets you easily find the required version of data and select it for recovery. The data catalog displays the data stored in the managed locations for which cataloging is or was enabled.

The **Catalog** section appears under the **Backup storage** tab only if at least one catalog service is registered on the management server. For information about installing the catalog service, refer to ["Installing a storage node and a catalog service"](#).

The **Catalog** section is visible only to [organization administrators](#).

### Limitations

Cataloging is supported only for disk- and file-level backups of physical machines, and backups of virtual machines.

The following data cannot be displayed in the catalog:

- Data from the encrypted backups
- Data backed up to tape devices
- Data backed up to the cloud storage
- Data backed up by product versions earlier than Acronis Cyber Protect 12.5

## Selecting the backed-up data for recovery

1. Click **Backup storage > Catalog**.
2. If several cataloging services are registered on the management server, select the service that catalogs the backups stored in the location.

---

### Note

To see which service catalogs a location, select the location in **BackupStorage > Locations > Locations**, and then click **Details**.

---

3. The software shows the machines that were backed up to the managed locations cataloged by the selected catalog service.

Select the data to recover by browsing or by using search.

#### • Browsing

Double-click a machine to view the backed-up disks, volumes, folders, and files.

To recover a disk, select the disk marked with the following icon:



To recover a volume, double click the disk that contains the volume, and then select the volume.

To recover files and folders, browse the volume where they are located. You can browse

volumes that are marked with the folder icon:



#### • Search

In the search field, type the information that helps to identify the required data items (this can be a machine name, a file or folder name, or a disk label) and then click **Search**.

You can use the asterisks (\*) and question marks (?) as wildcards.

As a result of the search, you will see the list of backed-up data items whose names fully or partially match the entered value.

4. By default, the data will be reverted to the latest possible point in time. If a single item is selected, you can use the **Versions** button to select a recovery point.
5. Having selected the required data, do one of the following:
  - Click **Recover**, and then configure the parameters of the recovery operation as described in ["Recovery"](#).
  - [Only for files/folders] If you want to save the files as a .zip file, click **Download**, select the location to save the data to, and click **Save**.

## Cataloging best practices

To increase cataloging performance, follow the recommendations below.

## Installation

We recommend that you install a catalog service and a storage node on separate machines. Otherwise, these components will compete for CPU and RAM resources.

If several storage nodes are registered on the management server, one catalog service is sufficient unless the indexing or search performance degrades. For example, if you notice that cataloging is working 24/7 (meaning that there are no pauses between cataloging activities), install one more catalog service on a separate machine. Then, remove some of the managed locations and recreate them with the new catalog service. The backups stored in these locations will be kept intact.

## System requirements

Parameter	Minimum value	Recommended value
Number of CPU cores	2	4 and more
RAM	8 GB	16 GB and more
Hard disk	7200 rpm HDD	SSD
Network connection between the machine with the storage node and the machine with the catalog service	100 Mbps	1 Gbps

## How to enable or disable cataloging

If cataloging is enabled for a managed location, the content of each backup directed to the location is added to the data catalog as soon as the backup is created.

You can enable cataloging when adding a managed location or at a later time. Once cataloging is enabled, all backups that are stored in the location and were not previously cataloged will be cataloged after the next backup to the location.

The cataloging process can be time-consuming, especially if a large number of machines is backed up to the same location. You can disable cataloging at any time. Cataloging of backups that were created prior to disabling will be completed. The newly created backups will not be cataloged.

### *To configure cataloging for an existing location*

1. Click **Backup storage > Locations**.
2. Click **Locations**, and then select the managed location for which you want to configure cataloging.
3. Click **Edit**.
4. Enable or disable the **Catalog service** switch.
5. Click **Done**.

# System settings

These settings are only available in on-premises deployments.

To access these settings, click **Settings** > **System settings**.

The **System settings** section is visible only to [organization administrators](#).

## Email notifications

You can configure the global settings for email notifications that are sent from the management server when an event occurs.

---

### Note

These settings do not affect the email delivery of scheduled reports. See "Reports" (p. 586).

---

In [default backup options](#), 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 protection plan](#), 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 protection plans that use the global settings are affected.

---

Before configuring these settings, ensure that the [Email server](#) 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. [Optional] Select a language that will be used in the email notifications.
6. 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.
7. Click **Save**.

## 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 one of the following:
  - **Custom**
  - **Gmail**
  - **Yahoo Mail**
  - **Outlook.com**
3. [Only for a custom email service] 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. [Only for Gmail, Yahoo Mail, and Outlook.com] Specify the credentials of an account that will be used to send messages.
5. [Only for a custom email service] 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.
6. [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.

## Security

Use these options to enhance security of your Acronis Cyber Protect on-premises deployment.

## 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 Cyber Protect 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.**

## Updates

This option defines whether Acronis Cyber Protect checks for a new version each time an organization administrator signs in to the Cyber Protect web console.

The preset is: **Enabled.**

If this option is disabled, the administrator can check for updates manually as described in ["Checking for software updates"](#).

## Default backup options

The default values of [backup options](#) are common for all protection 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 protection plans created after the change takes place.

When creating a protection 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 Cyber Protect web 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**.

# Protection settings

To configure the protection settings, in the Cyber Protect web console, go to **Settings > Protection**.

For more information about specific settings and procedures, refer to the respective topic in this section.

## Updating the protection definitions

By default, all protection agents can connect to the Internet and download updates for the following components:

- Antimalware
- Vulnerability assessment
- Patch management

## Agents with the Updater role

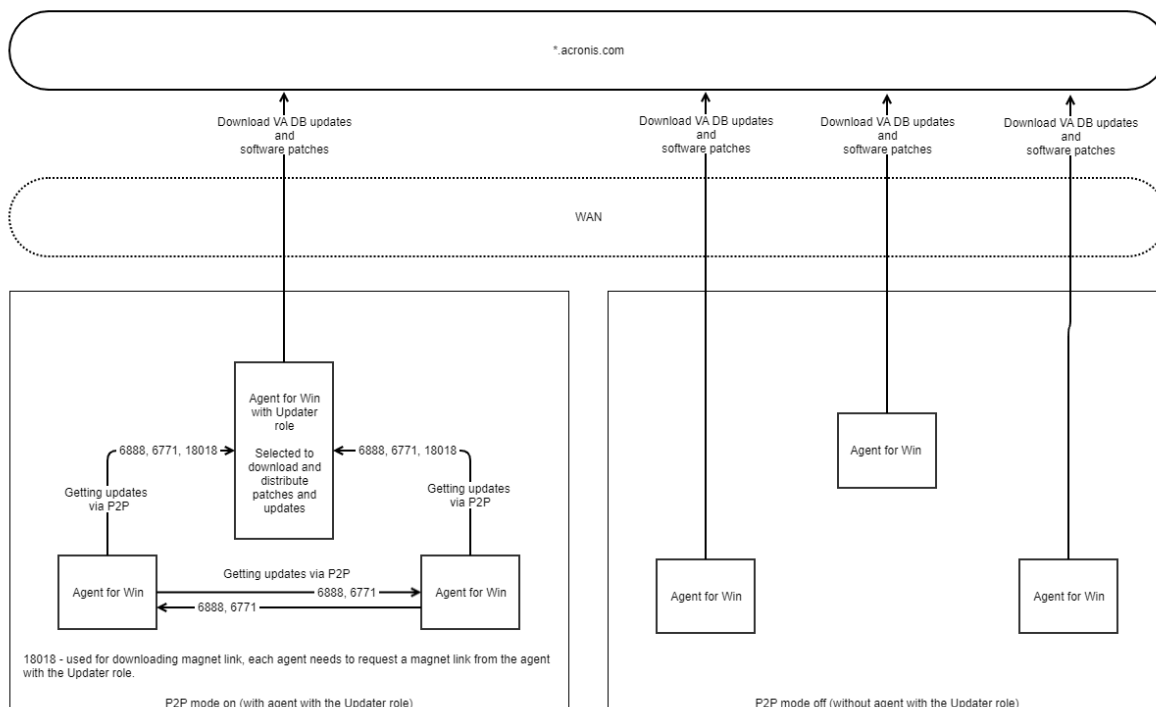
An administrator can minimize the network bandwidth traffic by selecting one or more protection agents in the environment and assigning the Updater role to them. Thus, the dedicated agents will connect to the Internet and download updates. All other agents will connect to the dedicated updater agents by using peer-to-peer technology, and then download the updates from them.

The agents without the Updater role will connect to the Internet if there is no dedicated updater agent in the environment, or if the connection to a dedicated updater agent cannot be established for about five minutes.

Before assigning the Updater role to an agent, ensure that the machine on which the agent runs is powerful enough, and has a stable high-speed Internet connection and enough disk space.

You can assign the Updater role to multiple agents in the environment. Thus, if an agent with the Updater role is offline, other agents with this role can serve as a source of updated protection definitions.

The following diagram illustrates the options for downloading protection updates. To the left, an agent is assigned the Updater role. That agent connects to the Internet to download the protection updates, and its peer agents connect to the Updater agent to obtain the latest updates. To the right, no agent is assigned the Updater role, so all agents connect to the Internet to download protection updates.



### To prepare a machine for the Updater role

- On the machine where an agent with the Updater role will run, apply the following firewall rules:
  - Inbound (incoming) "updater\_incoming\_tcp\_ports": allow connection to TCP ports 18018 and 6888 for all firewall profiles (public, private, and domain).
  - Inbound (incoming) "updater\_incoming\_udp\_ports": allow connection to UDP port 6888 for all firewall profiles (public, private, and domain).
- Restart the Acronis Agent Core Service.
- Restart the Firewall Service.

If you do not apply these rules and the firewall is enabled, peer agents will download the updates from the cloud.

### To assign the Updater role to an agent

- In the Cyber Protect web console, go to **Settings > Agents**.
- Select the machine with the agent to which you want to assign the Updater role.
- Click **Details**, and then enable the **Use this agent to download and distribute patches and updates** switch.

## Scheduling the updates

You can schedule automatic updates of the protection definitions on all agents or manually update them on selected agents.

### To schedule automatic updates

1. In the Cyber Protect web console, go to **Settings > Protection > Protection definitions update**.
2. Select **Schedule**.
3. In **Schedule type**, select one of the following:
  - **Daily**  
Select days of the week on which to update the protection definitions.  
In **Start at**, select the time when the updates start.
  - **Hourly**  
Set a granular schedule for updates.  
In **Run every**, set the periodicity of updates.  
In **From ... To**, set a specific time range for the updates.

#### ***To update the protection definitions manually***

1. In the Cyber Protect web console, go to **Settings > Agents**.
2. Select the machines on whose agents you want to update the protection definitions, and then click **Update definitions**.

## Changing the download location

Protection definitions are downloaded to the default temporary folder on your machine, and then they are stored in the Acronis program folder.

#### ***To change the temporary folder for download***

1. On the management server machine, open the `atp-database-mirror.json` file for editing.  
You can find this file in the following location:
  - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
  - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
2. Change the value for "enable\_user\_config" to true.

```
{
 "sysconfig":
 {
 ...
 "enable_user_config": true
 }
 ...
}
```

3. On the management server machine, open the `config.json` file for editing.  
You can find this file in the following location:
  - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
  - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
4. Add the following line: `"mirror_temp_dir": "<path_to_new_download_location>"`  
For example:

```
{
 "mirror_temp_dir": "C:\\temp"
}
```

The path can be absolute or relative to the AppData folder.

If the folder cannot be created or the management server cannot write to it, the default location will be used.

## Cache storage options

The cached data is stored in the following location:

- Windows: C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache
- Linux: /opt/acronis/var/atp-downloader/Cache
- macOS: /Library/Application Support/Acronis/Agent/var/atp-downloader/Cache

You can configure a schedule for clearing the outdated cached data and set a limit for its size. You can set different limits for machines with non-updater agents and machines with updater agents.

## Source of the latest protection definitions

You can download the latest protection definitions from the following locations:

- **The Cloud**

The protection agents connect to the Internet and download the latest protection definitions from the Acronis Cloud. By default, all agents that are registered on the management server, check for updates and distribute them. For more information about agents with the Updater role, refer to "Updating the protection definitions" (p. 626).

- **Cyber Protect Management Server**

With this option, the agents do not need access to the Internet. They only connect to the management server where the protection definitions are stored. However, the management server needs to be connected to the Internet in order to download the latest protection definitions.

- **Custom web servers**

This option is intended for troubleshooting and testing purposes or for use in air-gapped environments. For more information, refer to "Updating the protection definitions in an air-gapped environment" (p. 630). Usually, you will need to select this option only when instructed to do so by the Acronis support team.

## Remote connection

When you enable the remote connection, the options **Connect via RDP client** and **Connect via HTML5 client** appear in the Cyber Protect web console, under **Cyber Protection Desktop** in the right-hand menu. The right-hand menu opens when you select a workload on the **Devices** tab.

Enabling or disabling the remote connection affects all users of your organization.

### ***To enable the remote connection***

1. In the Cyber Protect web console, go to **Settings > Protection**.
2. Click **Remote connection**, and then enable the **Remote desktop connection** switch.

Additionally, you can enable remote connection sharing. With this option, you can generate a link that allows accessing the selected workload remotely. You can share these links with other users.

### ***To enable remote connection sharing***

1. In the Cyber Protect web console, go to **Settings > Protection**.
2. Select the **Share remote desktop connection** check box.

As a result, the option **Share remote connection** appears in the Cyber Protect web console, under **Cyber Protection Desktop** in the right-hand menu.

## Updating the protection definitions in an air-gapped environment

Acronis Cyber Protect supports updating the protection definitions in air-gapped environments.

### ***To update the protection definitions in an air-gapped environment***

1. Install a second management server that can access the Internet, outside your air-gapped environment.  
For more information on how to do that, refer to "Installing the management server" (p. 85).
2. Copy the protection definitions from the online management server to a removable drive, and then transfer the definitions to an HTTP server in the air-gapped environment.  
For more information on this step, refer to "Downloading the definitions to an online management server" (p. 630) and "Transferring the definitions to an HTTP server" (p. 632).
3. On the air-gapped management server, configure the HTTP server as a source of updated protection definitions.  
For more information on this step, refer to "Configuring the source of definitions on the air-gapped management server" (p. 632).

## Downloading the definitions to an online management server

After installing a second management server that can access the Internet, download the latest protection definitions and copy them to a removable drive, such as a USB flash memory or an external hard drive.

### ***To download and copy the protection definitions***

1. On the machine with the online management server, copy the AtpDatabaseMirror folder to a location by your choice – for example, the desktop or the Temp folder.  
You can find the AtpDatabaseMirror folder in the following location:

- Windows: %ProgramData%\Acronis\
  - Linux: /usr/lib/Acronis/
2. Open the `atp_database_mirror.json` file for editing. You can find the file in the following location:
    - Windows: %Program Files%\Acronis\AtpDatabaseMirror

---

**Note**

In Windows, this folder is not the same as the folder in the previous step.

---

- Linux: /usr/lib/Acronis/AppDatabaseMonitor
3. Edit the `atp_database_mirror.json` file as follows:
    - a. Change the value of "enable\_apdata\_as\_root" to false.
    - b. Change the values of all entries of "local\_path" to the absolute path of the location where you want to save the protection definitions.
  4. Save the changes in the `atp_database_mirror.json` file.
  5. On the machine with the online management server, stop the **Acronis Management Server** service by using the following command:

- Windows (Command Prompt):

```
sc stop AcrMngSrv
```

- Linux (Terminal):

```
sudo systemctl stop acronis_ams.service
```

6. In the `AtpDatabaseMirror` folder that you copied to a location by your choice, start the `AtpDatabaseMirror` tool by using the following command:

- Windows (Command Prompt):

```
atp_database_mirror.exe -config atp_database_mirror.json
```

- Linux (Terminal):

```
sudo ./atp_database_mirror -config atp_database_mirror.json
```

When all updates are downloaded to the folder that you specified in "local\_path", the following line will appear in the Command Prompt or the Terminal window:

```
standing by for 1m0s
```

7. Stop the `AtpDatabaseMirror` tool by pressing CTRL+C.
8. Copy the files from in the folder that you specified in "local\_path" to a removable drive.

Next, you must copy the files from the removable drive to a HTTP server in your air-gapped environment. You can use the air-gapped management server as an HTTP server. For more information, refer to "Transferring the definitions to an HTTP server" (p. 632).

## Transferring the definitions to an HTTP server

To distribute the protection definitions in your air-gapped environment, you need a dedicated HTTP server. You can use your air-gapped management server as an HTTP server.

### ***To transfer the protection definitions to an HTTP server***

1. On the machine where you will run the HTTP server, copy the protection definitions to a folder by your choice.
2. From the folder where you copied the protection definitions, start an HTTP server.

For example, you can use Python and run the following command:

```
python -m http.server 8080
```

---

#### **Note**

You can use any HTTP server that you prefer.

---

3. In the folder where you copied the protection definitions, open the following `update-index.json` files for editing:
  - `./ngmp/update-index.json`
  - `./vapm/update-index.json`
4. In both `update-index.json` files, edit all `products > os > arch > components > versions > url` fields, as follows:
  - a. As IP and port values, set the IP address and the port of your HTTP server.
  - b. Do not change the other part of the path.For example, `"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"`, where 192.168.1.10 is the IP address of the HTTP server, and 8080 is its port. Do not change the `/ngmp/win64/ngmp.zip` part.
5. Save your edits in the both `update-index.json` files.

Next, you must configure the source of the protection definitions on the air-gapped management server. For more information, refer to "Configuring the source of definitions on the air-gapped management server" (p. 632).

## Configuring the source of definitions on the air-gapped management server

After configuring the HTTP server, you must configure it on the air-gapped management server as the source of the protection definitions.

### ***To configure the source of protection definitions on the air-gapped management server***

1. In the Cyber Protect web console of the air-gapped management server, go to **Settings > Protection > Protection definitions update**.



2. Select **Definitions**.
3. Select **Custom**, and then specify the following paths:
  - For **Antivirus and Antimalware definitions**:  
http://<IP address of your HTTP server>:8080/scanner
  - For **Advanced detections definitions**:  
http://<IP address of your HTTP server>:8080/ngmp
  - For **Vulnerability assessment and patch management definitions**:  
http://<IP address of your HTTP server>:8080/vapm

As a result, the agents in the air-gapped environment will download the protection definitions from your HTTP server.

# Administering user accounts and organization units

## On-premises deployment

The functionality described in this section is available only to [organization administrators](#).

To access these settings, click **Settings** > **Accounts**.

## Units and administrative accounts

To manage units and administrative accounts, in the Cyber Protect web console, go to **Settings** > **Accounts**. The **Accounts** panel shows the **Organization** group with the tree of units (if any), as well as the list of administrative accounts on the selected hierarchical level.

### Units

The **Organization** group is automatically created when you install the management server. With the Acronis Cyber Protect Advanced license, you can create child groups called units, which typically correspond to units or departments of the organization, and add administrative accounts to the units. This way, you can delegate the protection 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" (p. 638).

Every unit can have child units. The administrative accounts of the parent unit have the same rights in all child units. The **Organization** group is the top-level parent unit, and administrative accounts on this level have the same rights in all units.

### Administrative accounts

Any account that is able to sign in to the Cyber Protect web console is administrative account.

In the Cyber Protect web console, any administrative account can view or manage anything on or below the hierarchical level of its unit. For example, an administrative account in the *organization* has access to this top level and therefore access to all the units of this organization, while an administrative account in a specific *unit* can access only this unit and its child units.

### Which accounts can be administrative?

If the management server is installed on a Windows machine that is included in an Active Directory domain, you can grant administrative rights to local users, or users and user groups within the Active Directory domain forest.

By default, the management server establishes an SSL/TLS-protected connection to the Active Directory domain controller. If this is not possible, no connection will be established. However, you can allow nonsecure connections, by editing the `auth-connector.json5` file.

To use a secure connection, ensure that LDAP over SSL (LDAPS) is configured for your Active Directory.

### ***To configure LDAPS for Active Directory***

1. On the domain controller, create and install an LDAPS certificate that meets the Microsoft requirements.

For more information on how to perform these operations, refer to [Enable LDAP over SSL with a third-party certification authority](#) in the Microsoft documentation.

2. On the domain controller, open **Microsoft Management Console** and verify that the certificate exists under **Certificates (Local Computer) > Personal > Certificates**.
3. Restart the domain controller.
4. Verify that LDAPS is enabled.

### ***To allow nonsecure connections to the domain controller***

1. Log in to the machine where the management server is installed.
2. Open the auth-connector.json5 file for editing.

The auth-connector.json5 file is located in %ProgramFiles%\Acronis\AuthConnector\Acronis\AuthConnector.

3. Navigate to the **sync** section, and in every "**connectionMode**" line, replace "**ssl\_only**" with "**auto**".

In the **auto** mode, a nonsecure connection is established if a TLS connection is not possible.

4. Restart **Acronis Service Manager Service** as described in "To restart Acronis Service Manager Service" (p. 214).

---

### **Note**

If the management server is not included in an Active Directory domain or if it is installed on a Linux machine, you can grant administrative rights only to local users and groups.

---

To learn how to add an administrative account to the management server, refer to "Adding administrative accounts" (p. 637).

## **Administrative account roles**

Each administrative account is assigned a role with the predefined rights that are necessary for specific tasks. The administrative account roles are the following:

- **Administrator**

This role provides full administrative access to the organization or a unit.

- **Read-only**

This role provides read-only access to the Cyber Protect web console. It only allows gathering diagnostic data, such as system reports. The read-only role does not allow browsing backups or browsing the content of backed-up mailboxes.

- **Auditor**

This role provides read-only access to the **Activities** tab in the Cyber Protect web console. For

more information about this tab, refer to "The Activities tab" (p. 584). This role does not allow gathering or exporting any data, including system information of the management server.

Any changes in the roles are shown on the **Activities** tab.

## Inheritance of roles

Roles in a parent unit are inherited by its child units. If the same user account has different roles assigned in the parent unit and in a child unit, it will have both roles.

Also, roles can be explicitly assigned to a specific user account or inherited from a user group. Thus, a user account can have both a specifically assigned role and an inherited one.

If a user account has different roles (assigned and/or inherited), it can access objects and perform actions allowed by any of these roles. For example, a user account with an assigned read-only role and inherited administrator role will have administrator rights.

---

### Important

In the Cyber Protect web console, only explicitly assigned roles for the current unit are shown. Any possible discrepancies with the inherited roles are not displayed. We strongly recommend that you assign administrator, read-only, and auditor roles to separate accounts or groups, in order to avoid possible issues with the inherited roles.

---

## 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 Cyber Protect web 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.

## Administrative account in multiple units

An account can be granted administrative rights in any number of units. For such an account, as well as for administrative accounts on the organization level, the unit selector is shown in the Cyber Protect web console. By using this selector, this account can view and manage each unit separately.

An account that has permissions for all units in an organization does not have permissions for the organization. Administrative accounts on the organization level must be added to the **Organization** group explicitly.

## How to populate units with machines

When an administrator adds a machine via the web interface, 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, 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.

## Adding administrative accounts

---

### Note

This feature is not available in the Standard and Essentials editions.

---

### *To add accounts*

1. Click **Settings > Accounts**.  
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 account**.
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. Select the role for the account.
8. Repeat steps 4-6 for all users or groups that you want to add.
9. When finished, click **Done**.
10. [Only in Linux] Add the user names to Pluggable Authentication Module (PAM) configuration for Acronis modules as described below.

### ***To add user names to the PAM configuration for Acronis***

This procedure applies to management servers running on Linux machines and in Acronis Cyber Protect All-in-One Appliance.


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.

## Creating units

1. Click **Settings > Accounts**.
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**.

## Cloud deployment

Administering user accounts and organization units is available in the management portal. To access the management portal, click **Management Portal** when logging in to the Cyber Protection

service or click the  icon in the top-right corner, and then click **Management portal**. Only users that have administrative privileges can access this portal.

For information about administering user accounts and organization units, refer to the Management Portal Administrator's Guide. To access this document, click the question mark icon in the management portal.

This section provides additional information related to managing the Cyber Protection service.

## Quotas

Quotas enable you to limit the users' ability to use the service. To set the quotas, select the user on the **Users** tab, and then click the pencil icon in the **Quotas** section.

When a quota is exceeded, a notification is sent to the user's email address. If you do not set a quota overage, the quota is considered "soft". This means that restrictions on using the Cyber Protection service are not applied.

You can also specify the quota overages. An overage allows the user to exceed the quota by the specified value. When the overage is exceeded, restrictions on using the Cyber Protection service are applied.

## Backup

You can specify the cloud storage quota, the quota for local backup, and the maximum number of machines/devices/mailboxes a user is allowed to protect. The following quotas are available:

- **Cloud storage**
- **Workstations**
- **Servers**
- **Windows Server Essentials**
- **Virtual hosts**
- **Universal**

This quota can be used instead of any of the four quotas listed above: Workstations, Servers, Windows Server Essentials, Virtual hosts.

- **Mobile devices**
- **Microsoft 365 mailboxes**
- **Local backup**

A machine/device/mailbox is considered protected as long as at least one protection plan is applied to it. A mobile device becomes protected after the first backup.

When the cloud storage quota overage is exceeded, backups fail. When the overage for a number of devices is exceeded, the user cannot apply a protection plan to more devices.

The **Local backup** quota limits the total size of local backups that are created by using the cloud infrastructure. An overage cannot be set for this quota.

## Disaster recovery

These quotas are applied by the service provider to the entire company. Company administrators can view the quotas and the usage in the management portal, but cannot set quotas for a user.

- **Disaster recovery storage**

This storage is used by primary and recovery servers. If the overage for this quota is reached, it is not possible to create primary and recovery servers, or add/extend disks of the existing primary servers. If the overage for this quota is exceeded, it is not possible to initiate a failover or just start a stopped server. The running servers continue to run.

When the quota is disabled, all of the servers are deleted. The **Cloud recovery site** tab disappears from the Cyber Protect web console.

- **Compute points**

This quota limits the CPU and RAM resources that are consumed by primary and recovery servers during a billing period. If the overage for this quota is reached, all primary and recovery servers are shut down. It is not possible to use these servers until the beginning of the next billing period. The default billing period is a full calendar month.

When the quota is disabled, the servers cannot be used regardless of the billing period.

- **Public IP addresses**

This quota limits the number of public IP addresses that can be assigned to primary and recovery servers. If the overage for this quota is reached, it is not possible to enable public IP addresses for more servers. You can disallow a server to use a public IP address, by clearing the **Public IP address** check box in the server settings. After that, you can allow another server to use a public IP address, which usually will not be the same one.

When the quota is disabled, all of the servers stop using public IP addresses, and thus become not reachable from the Internet.

- **Cloud servers**

This quota limits the total number of primary and recovery servers. If the overage for this quota is reached, it is not possible to create primary or recovery servers.

When the quota is disabled, the servers are visible in the Cyber Protect web console, but the only available operation is **Delete**.

- **Internet access**

This quota enables or disables the Internet access from primary and recovery servers.

When the quota is disabled, the primary and recovery servers are disconnected from the Internet immediately. The **Internet access** switch in the servers' properties becomes cleared and disabled.

## Notifications

To change the notifications settings for a user, select the user on the **Users** tab, and then click the pencil icon in the **Settings** section. The following notifications settings are available:

- **Quota overuse notifications** (enabled by default)

The notifications about exceeded quotas.

- **Scheduled usage reports**

The usage reports described below that are sent on the first day of each month.

- **Failure notifications, Warning notifications, and Success notifications** (disabled by default)

The notifications about the execution results of protection plans and the results of disaster recovery operations for each device.

- **Daily recap about active alerts** (enabled by default)

The recap that informs about failed backups, missed backups, and other problems. The recap is sent at 10:00 (data center time). If there are no problems by this moment, the recap is not sent.

All notifications are sent to the user's email address.



## Reports

The report about using the Cyber Protection service includes the following data about the organization or a unit:

- Size of backups by unit, by user, by device type.
- Number of protected devices by unit, by user, by device type.
- Price value by unit, by user, by device type.
- The total size of backups.
- The total amount of protected devices.
- Total price value.

## Command-line reference

Command-line reference is a separate document available at [https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect\\_15\\_Command\\_Line\\_Reference/index.html](https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html).

# 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 technical support 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.

# 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. 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.

## M

### **Managed location**

A backup location managed by a storage node. Physically, managed locations can reside on a network share, SAN, NAS, on a hard drive local to the storage node, or on a tape library locally attached to the storage node. The storage node performs cleanup and validation (if those are included in a protection plan) for each backup stored in the managed location. You can specify additional operations that the storage node will perform (deduplication, encryption).

## 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.

### **Startup Recovery Manager**

A modification of the bootable agent, residing on the system disk and configured to start at boot time when F11 is pressed. Startup Recovery Manager eliminates the need for rescue media or network connection to start the bootable rescue utility. Startup Recovery Manager is especially useful for mobile users. If a failure occurs, the user reboots the machine, hits F11 on prompt "Press F11 for Startup Recovery Manager..." and performs data recovery in the same way as with ordinary bootable media. Limitation: requires re-activation of loaders other than Windows loaders and GRUB.

# Index

## 3

32- or 64-bit? 365

## 4

40 to 160 MB of RAM per 1 TB of unique data 617

## A

A device plan conflicts with a group plan 220

About Acronis Cyber Infrastructure 248

About Secure Zone 245

About the Physical Data Shipping service 304

Absence of applications competing for resources 618

Accessing the Cyber Protect web console 200

Acronis account, local and cloud consoles 23

Acronis Cyber Protect 15 editions 17

Acronis Cyber Protect appliance 106

Acronis patented technologies 16

Acronis PXE Server 434

Activating a management server 27

Activating Startup Recovery Manager 434

Activating the account 146

Active Protection 509, 516

Active Protection settings 510

Adding a backup location 249

Adding a custom message to the web console 208

Adding a machine running Linux 113

Adding a machine running macOS 113

Adding a machine running Windows 108

Adding a managed location 614

Adding a Microsoft 365 organization 468

Adding a Scale Computing HC3 cluster 116

Adding a vCenter or an ESXi host 113

Adding Acronis Plug-in to WinPE 383

Adding administrative accounts 637

Adding devices to static groups 562

Adding license keys to a management server 41

Adding licenses to your Acronis account 26

Adding machines from the Cyber Protect web console 108

Adding quarantined files to the whitelist 529

Adding the console to the list of local intranet sites 202

Adding the console to the list of trusted sites 204

Adding VLANs 387

Additional parameters 161, 166

Additional requirement for virtual machines 451

Additional requirements for application-aware backups 443

Additional requirements for machines running Windows 452

Additional scheduling options 251

Administering user accounts and organization units 634

Administrative account in multiple units 637

Administrative account roles 635

- Administrative accounts 634
- Advanced 518
- Advanced storage options 244, 591
- Agent for Exchange (for mailbox backup) 54
- Agent for Hyper-V 57
- Agent for Linux 55
- Agent for Mac 56
- Agent for Office 365 55
- Agent for Oracle 55
- Agent for Scale Computing HC3 – required roles 192
- Agent for Scale Computing HC3 (Virtual Appliance) 57
- Agent for SQL, Agent for Exchange (for database backup and application-aware backup), Agent for Active Directory 54
- Agent for VMware – necessary privileges 497
- Agent for VMware (Virtual Appliance) 57
- Agent for VMware (Windows) 57
- Agent for Windows 53
- Agent for Windows XP SP2 60
- Agent installation parameters 127, 130
- Agents 47, 53
- Agents with the Updater role 626
- Alerts 275
- Alerts configuration file 589
- Allocating licenses to a management server 30
- Allowing only HTTPS connections to the web console 207
- Allowing processes to modify backups 511
- Always incremental (single-file) 230
- Amazon 70

- Antimalware and web protection 508
- Antimalware scan of backups 530
- Antivirus & Antimalware protection 508
- Antivirus & Antimalware protection settings 509
- Application-aware backup 450
- Applying a protection plan to a group 573
- Applying several plans to a device 220
- Are the required packages already installed? 71
- Assignment of licenses to workloads 38
- Attaching SQL Server databases 456
- Autodiscovery and manual discovery 177
- Autodiscovery of machines 175
- Automatic adding to the whitelist 529
- Automatic driver search 332
- Automatic patch approval 544
- Availability of the backup options 272
- Availability of the recovery options 339
- Available actions with a protection plan 221

## B

- Back up a typical machine before backing up several machines with similar contents 618
- Back up different machines at different times 618
- Backing up 598-599
- Backing up a machine to a locally attached tape device 597
- Backing up clustered Hyper-V machines 501
- Backing up databases included in an AAG 447
- Backing up the Exchange cluster data 449

- Backing up to a tape device attached to a storage node 598
- Backup 223, 639
- Backup consolidation 276
- Backup file name 276
- Backup file name vs. simplified file naming 279
- Backup format 280
- Backup format and backup files 281
- Backup module cheat sheet 225
- Backup options 272
- Backup replication 356
- Backup scanning details 582
- Backup scanning plans 356
- Backup schemes, operations, and limitations 249
- Backup to and recovery from a network share 372
- Backup to and recovery from the bootable media 372
- Backup to and recovery from the cloud storage 372
- Backup validation 282, 341
- Backup window 301
- Backup with bootable media on-premises 390
- Basic disk cloning 412
- Basic operations with reports 588
- Basic parameters 159, 165
- Basic precautions 410
- Before backing up 598-599
- Before you start 183, 186
- Behavior detection 512
- Behavior detection settings 512

- Boot mode 342
- Bootable media 362
- Bootable Media Builder 364
- Built-in groups 561
- By total size of backups 230

## C

- Cache storage options 629
- calculate hash 295
- Catalog service installation parameters 128
- Cataloging 619
- Cataloging best practices 620
- Categories to filter 522
- Change volume label 428
- Change volume letter 427
- Changed block tracking (CBT) 282
- Changed Block Tracking (CBT) 482
- Changing the backup format to version 12 (TIBX) 281
- Changing the download location 628
- Changing the language 201
- Changing the logon account on Windows machines 156
- Changing the Microsoft 365 access credentials 470
- Changing the ports used by the protection agent 148
- Changing the SQL Server or Exchange Server access credentials 465
- Check access to the drivers in bootable environment 331
- Check device IP address 260
- Checking for software updates 140



- Choosing the operating system for disk management 410
- Citrix 66
- Cleanup 359
- Cloud deployment 45, 146, 195, 201, 506, 638
- Cloud management server 22
- Cloud storage 285
- Cluster-aware backup 448
- Cluster backup mode 283
- Coexistence with third-party software 591
- Command-line reference 642
- Common backup rule 74
- Common installation rule 74
- Common parameters 123, 129
- Common requirements 443
- Common restrictions 616
- Compatibility with Dell EMC Data Domain storages 75
- Compatibility with encryption software 74
- Compatibility with RSM and third-party software 591
- Components 47
- Components for remote installation 112
- Components to install 86
- Compression level 284
- Configuring a web browser for Integrated Windows Authentication 201
- Configuring an already registered Agent for VMware 116
- Configuring automatic patch approval 545
- Configuring iSCSI devices 432
- Configuring iSCSI Initiator 490
- Configuring network settings 387
- Configuring NFS Client 490
- Configuring proxy server settings 149
- Configuring the action on detection for Real-time protection 513
- Configuring the machine running Agent for VMware 490
- Configuring the scan mode for Real-time protection 513
- Configuring the severity of alerts 589
- Configuring the source of definitions on the air-gapped management server 632
- Configuring the virtual appliance 184, 187
- Connecting to a machine booted from media 387
- Considerations for users with the Advanced license 271
- Continuous data protection (CDP) 237
- Control type 376
- Conversion methods 266
- Conversion to a virtual machine 265, 360
- Conversion to a virtual machine in a protection plan 267
- Copying Microsoft Exchange Server libraries 465
- Copyright statement 16
- Corporate whitelist 529
- CPU priority 302
- Create a bootable media or download a ready-made one? 362
- Create a volume 423
- Creating a dynamic group 562
- Creating a pool 604

- Creating a protection plan 218
- Creating a replication plan 479
- Creating a static group 562
- Creating bootable media 321
- Creating the .mst transform and extracting the installation packages 121, 158
- Creating units 638
- Criteria 287
- Cryptomining process detection 511
- Cryptomining process detection settings 512
- Custom groups 561
- Custom pools 603
- Custom scripts 373
- Customizing installation settings 86
- Cyber Protect web console view 216
- Cyber Protection 575

## D

- Data catalog 619
- Data Deduplication 81
- Data protection map 551, 580
- Data protection map settings 552
- Database backup 444
- Database for Scan Service 93
- Database for the management server 89
- Date and time for files 343
- Deactivating Startup Recovery Manager 434
- Decreasing the license quota allocated to an offline management server 34
- Deduplication 616
- Deduplication best practices 616
- Deduplication restrictions 616

- Default actions 517
- Default administrators 636
- Default backup file name 278
- Default backup options 624
- DefaultBlockSize 594
- Delete a volume 426
- Deleting a pool 604
- Deleting all alerts 551
- Deleting backups 354
- Deleting the machine 477
- Deploying Agent for oVirt (Virtual Appliance) 174
- Deploying Agent for Scale Computing HC3 (Virtual Appliance) 186
- Deploying Agent for Virtuozzo Hybrid Infrastructure (Virtual Appliance) 175
- Deploying Agent for VMware (Virtual Appliance) from an OVF template 183
- Deploying Agent for VMware (Virtual Appliance) via the web interface 114
- Deploying agents through Group Policy 192
- Deploying the OVF template 184
- Deploying the virtual appliance 187
- Deployment 248
- Deployment agent 111
- Detecting tape devices 602
- Device groups 561
- Direct selection 231, 234
- Disable automatic DRS for the agent 183
- Disabling automatic assignment for an agent 494
- Disaster recovery 349, 639

- Discovered machines 576
- Disk-level backup 616
- Disk conversion
  - basic to dynamic 420
  - dynamic to basic 421
  - GPT to MBR 420
  - MBR to GPT 419
- Disk health monitoring 576
- Disk health status alerts 580
- Disk health widgets 577
- Disk initialization 411
- Disk management with bootable media 406
- Disk operations 411
- Disk provisioning 482
- Distribution algorithm 493
- Do not show messages and dialogs while processing (silent mode) 286, 343
- Do not start when connected to the following Wi-Fi networks 259
- Do not start when on metered connection 259
- Documentation 249
- Downloading files from the cloud storage 335
- Downloading the definitions to an online management server 630
- Drivers for Universal Restore 381
- Dumping the report data 589
- Dynamic disk conversion
  - MBR to GPT 420

## E

- Editing a pool 604

- Eject tapes after each successful backup of each machine 311
- Ejecting 610
- Email notifications 284, 622
- Email server 623
- Enable file recovery from disk backups stored on tapes 311
- Enable VSS full backup 316
- Encryption 262
- Encryption as a machine property 263
- Encryption in a protection plan 263
- Erasing 610
- Error handling 285, 483
- Event properties 254
- Example 256-261
  - "Bad block" emergency backup 254
  - Installing the packages manually in Fedora 14 73
- Examples 132-134, 162, 168-170
- Exchange Server clusters overview 448
- Exclude hidden files and folders 288
- Exclude system files and folders 288
- Exclusions 515, 519, 527
- Existing vulnerabilities 581
- Exporting and importing the report structure 588
- Exporting backups 353
- Extensions and exception rules 553
- Extracting files from local backups 338

## F

- Failback options 483

- Failing back 482
- Failing over to a replica 481
- Fast incremental/differential backup 286
- File-level backup 616
- File-level backup snapshot 289
- File-level security 344
- File exclusions 344
- File filters 287
- Files of a script 373
- Finalization of machines running from cloud backups 478
- Finalization vs. regular recovery 478
- Finalizing the machine 477
- Fits the time interval 258
- Flashback 344
- Forensic backup process 290
- Forensic data 289
- Format volume 428
- Full path recovery 345
- Further actions 107

## G

- get content 295
- Getting started with a tape device 597
- Getting the certificate for backups with forensic data 292

## H

- High-speed LAN 618
- High Availability of a recovered machine 501
- How autodiscovery works 175
- How creating Secure Zone transforms the

- disk 246
- How do files get into the quarantine folder? 528
- How it works 237, 265, 291, 320, 357, 509, 520, 539, 544, 549, 551, 556, 577
- How many agents are required for cluster-aware backup and recovery? 449
- How many agents are required for cluster data backup and recovery? 447
- How many agents do I need? 183, 187
- How regular conversion to VM works 268
- How the deployment agent works 112
- How the encryption works 264
- How to assign the user rights 157
- How to connect to a remote machine 558
- How to create Secure Zone 246
- How to delete Secure Zone 248
- How to distinguish backups that are protected on continuous basis 241
- How to enable or disable cataloging 621
- How to get forensic data from a backup? 291
- How to populate units with machines 637
- How to recover data to a mobile device 439
- How to recover your entire machine to the latest state 242
- How to review data via the Cyber Protect web console 439
- How to start backing up your data 438
- How to use notarization 265

## I

- If you choose to create the virtual machine on a virtualization server 269

- If you choose to save the virtual machine as a set of files 269
- Ignore bad sectors 286
- In-archive deduplication 281
- In cloud deployments 184
- In Linux 58, 154, 198, 201, 637
- In macOS 155, 198
- In on-premises deployments 184
- In Windows 58, 153, 198, 200, 636
- Include or exclude files matching specific criteria 287
- Information parameters 131, 167
- Inheritance of roles 636
- Installation 44, 60, 94, 115, 119, 621
- Installation in a Docker container 95
- Installation in Linux 94, 119
- Installation in macOS 120
- Installation in Windows 85, 117
- Installation overview 44
- Installation parameters 123, 129, 159, 165
- Installing a storage node and a catalog service 612
- Installing Acronis PXE Server 435
- Installing Agent for VMware (Windows) 114
- Installing agents 153
- Installing agents locally 117
- Installing or uninstalling the product by specifying parameters manually 122, 158
- Installing the management server 85, 95
- Installing the packages from the repository 72
- Installing the packages manually 73

- Installing the product by using the .mst transform 122, 158
- Installing the software 107
- Interaction with Windows Removable Storage Manager (RSM) 591
- Inventorying 606
- Inventorying methods 606

## K

- Kernel parameters 369
- Known issues 39

## L

- LAN-free backup 484
- License issue 221
- License types 21
- Licensing 21
- Licensing in Acronis Cyber Protect 15 Update 2 and earlier 40
- Licensing in Acronis Cyber Protect 15 Update 3 and later 21
- Limitation 94, 107
- Limitations 39, 52, 60, 63, 65, 67, 69, 108, 230, 236, 246, 267, 343, 468, 485, 531, 576, 595, 619
- Limitations for backup file names 277
- Limiting the total number of simultaneously backed-up virtual machines 502
- Linux 233
- Linux-based 364
- Linux-based bootable media 366
- Linux-based or WinPE-based bootable media? 364
- Linux packages 70

- list backups 293
- list content 294
- Local connection 388
- Local operations with bootable media 389
- Location encryption 618
- Location of the OVF template 184
- Log out inactive users after 624
- Log truncation 297
- LVM snapshotting 297

## M

- Mac 234
- Machine migration 504
- Mailbox backup 452
- Malicious website access 522
- Managed location 230
- Management server 378
- Management Server (for on-premises deployment only) 58
- Management server installation parameters 126, 130
- Management server location 45
- Managing discovered machines 181
- Managing found vulnerabilities 538
- Managing licenses 25
- Managing list of patches 543
- Managing perpetual licenses 42
- Managing quarantined files 528
- Managing subscription licenses 41
- Managing the detected unprotected files 552
- Managing virtualization environments 495
- Manual adding to the whitelist 529

- Manual binding 493
- Manual patch approval 547
- Mass storage drivers to install anyway 332
- McAfee Endpoint Encryption and PGP Whole Disk Encryption 75
- Microsoft 64
- Microsoft Azure 70
- Microsoft BitLocker Drive Encryption and CheckPoint Harmony Endpoint 74
- Microsoft Exchange Server 283
- Microsoft products 540
- Microsoft Security Essentials 519
- Microsoft SQL Server 283
- Migrating the management server 141
- Mirrored-Striped Volume 423
- Mirrored Volume 423
- Missing updates by categories 582
- Monitoring and reporting 574
- Mount points 298, 345
- Mounting Exchange Server databases 459
- Mounting volumes from a backup 351
- Move a tape back to the slot after each successful backup of each machine 311
- Moving to another pool 605
- Moving to another slot 605
- Multi-core processor with at least 2.5 GHz clock rate 618
- Multi-volume snapshot 299
- Multiplexing 313
- Multistreaming 312

## N

Names without variables 278  
NetApp SAN storage requirements 488  
Network connection diagram - Cyber Protect processes 82  
Network connection diagram for Acronis Cyber Protect 81  
Network folder protection 510  
Network port 380  
Network requirements 506  
Network settings 379  
NFS 230  
No recent backups 582  
No successful backups for a specified number of consecutive days 275  
Notarization 264  
Notarization of backups with forensic data 291  
Note for Mac users 319  
Notifications 640  
Nutanix 68

## O

Obtaining application ID and application secret 468  
Off-host data processing 355  
Offline on-premises management server 23  
On-demand malware scan 509  
On-demand patch installation 547  
On-premises deployment 44, 85, 200, 506, 634  
On-premises deployments 194  
On-premises management server 22

On Windows Event Log event 254  
One-click recovery 299  
Online on-premises management server 23  
Only one deduplicating location on each storage node 618  
Operations on the source machine 141  
Operations on the target machine 143  
Operations with backups 350  
Operations with pools 604  
Operations with protection plans 221  
Operations with tapes 605  
Operators 572  
Options description 296  
Oracle 68  
Other components 50  
Output speed during backup 303  
Overview of tape support 591  
Overview of the physical data shipping process 304  
Overwrite a tape in the stand-alone tape drive when creating a full backup 312

## P

Parallel operations 595  
Parallels 67  
Parameters 369  
Parameters for legacy features 168  
Parameters for writing to tapes 593  
Passwords with special characters or blank spaces 138  
Patch installation history 581  
Patch installation status 581

- Patch installation summary 581
- Patch installation widgets 581
- Patch lifetime in the list 548
- Patch management 539
- Patch management settings 540
- PE images 382
- Pending operations 428
- Performance 345, 483
- Performance and backup window 300
- Performing a permanent failover 481
- Physical Data Shipping 304
- Place the deduplication database and deduplicating location on separate physical devices 617
- Plan conflicts with already applied plans 220
- Ports 93
- Post-backup command 306
- Post-data capture command 308
- Post-recovery command 346
- Power off target virtual machines when starting recovery 348
- Power on after recovery 348
- Power on the target virtual machine when recovery is complete 348
- Pre-backup command 305
- Pre-configuring multiple network connections 380
- Pre-data capture command 307
- Pre-recovery command 346
- Pre-update backup 542
- Pre/Post commands 305, 345, 483
- Pre/Post data capture commands 306
- Predefined pools 603
- Predefined scripts 372
- Preparation 94, 114, 119, 146, 331
  - WinPE 2.x and 3.x 382
  - WinPE 4.0 and later 383
- Prepare drivers 331
- Prerequisites 95, 100, 103, 141, 175, 192, 195, 208, 236, 300, 442, 475, 597-598
- Prerequisites for remote installation 110
- Privileges required for the logon account 156
- Protecting a domain controller 441
- Protecting Always On Availability Groups (AAG) 446
- Protecting Database Availability Groups (DAG) 448
- Protecting Google Workspace data 473
- Protecting Microsoft 365 mailboxes 467
- Protecting Microsoft applications 441
- Protecting Microsoft SharePoint 441
- Protecting Microsoft SQL Server and Microsoft Exchange Server 441
- Protecting mobile devices 437
- Protecting Oracle Database 474
- Protecting SAP HANA 507
- Protection of collaboration and communication applications 532
- Protection plan and modules 218
- Protection settings 626
- Protection status 576
- Proxy server 93



## Q

Quarantine 512, 528  
Quarantine location on machines 528  
Quotas 638

## R

RAID-5 423  
Re-attempt, if an error occurs 285  
Re-attempt, if an error occurs during VM snapshot creation 286  
Readability of tapes written by older Acronis products 596  
Real-time protection 513, 518  
Real-time protection scan 508  
Recently affected 582  
Recommendations 342  
Recovering a machine 322  
Recovering a machine with One-click recovery 300  
Recovering a physical machine 322  
Recovering a physical machine to a virtual machine 324  
Recovering a virtual machine 326  
Recovering applications 442  
Recovering disks and volumes by using bootable media 329  
Recovering ESXi configuration 338  
Recovering Exchange databases 457  
Recovering Exchange mailboxes and mailbox items 459  
Recovering files 333  
Recovering files by using bootable media 337

Recovering files by using the web interface 333  
Recovering mailbox items 462, 471  
Recovering mailboxes 461, 470  
Recovering mailboxes and mailbox items 470  
Recovering SQL databases 453  
Recovering system databases 456  
Recovering system state 338  
Recovering the Exchange cluster data 449  
Recovering the master database 456  
Recovering under an operating system from a tape device 600  
Recovering under bootable media from a locally attached tape device 601  
Recovering under bootable media from a tape device attached to a storage node 602  
Recovery 319, 467  
Recovery cheat sheet 319  
Recovery from the cloud storage 373  
Recovery of databases included in an AAG 447  
Recovery options 339  
Recovery to an Exchange Server 460  
Recovery to Microsoft 365 460  
Recovery with bootable media on-premises 399  
Recovery with restart 328  
Red Hat and Linux 66  
Redistribution 493  
Registering an already installed Agent for VMware 115  
Registering and unregistering machines manually 135, 171  
Registering media on the management server 388

Registering SAN storage on the management server 491

Registering the media from the media UI 388

Registration 248

Registration parameters 160, 166

Regular conversion to ESXi and Hyper-V vs. running a virtual machine from a backup 267

Remote access (RDP and HTML5 clients) 555

Remote connection 388, 629

Remote desktop access 555

Remote operations with bootable media 430

Remote wipe 560

Removing 610

Removing Agent for VMware (Virtual Appliance) 198

Removing machines from the Cyber Protect web console 199

Renaming 609

Replicating backups between managed locations 271

Replication 269

Replication of virtual machines 478

Replication options 482

Replication vs. backing up 479

Reports 586, 641

Required user rights 453

Required user rights for application-aware backup 451

Required user rights for the service logon account 88

Requirements 329, 338, 351

Requirements for ESXi virtual machines 443

Requirements for Hyper-V virtual machines 444

Requirements on User Account Control (UAC) 111

Requirements on user accounts 460

Rescanning 608

Resolving plan conflicts 220

Restrictions 271, 479

Results 598-599

Retention rules 261

Reverting to the original initial RAM disk 333

Rules for Linux 232

Rules for macOS 233

Rules for Windows 232

Rules for Windows, Linux, and macOS 232

Running a virtual machine from a backup (Instant Restore) 475

Running the machine 476

## S

Safe recovery 320

SAN hardware snapshots 309

Save battery power 258

Save system information if a recovery with reboot fails 343

Scale Computing 66

Scan Service 92

Schedule 249, 536, 541, 552

Schedule by events 252

Schedule scan 513, 517

Scheduling 309

Scheduling the updates 627

- Scripts in bootable media 372
- Search query 563
- Sector-by-sector backup 310
- Secure Zone 230
- Security 623
- Seeding an initial replica 483
- Selecting a destination 242
- Selecting components for installation 180
- Selecting data to back up 231
- Selecting disks/volumes 231
- Selecting entire machine 231
- Selecting ESXi configuration 236
- Selecting Exchange Server data 445
- Selecting Exchange Server mailboxes 453
- Selecting files/folders 234
- Selecting mailboxes 470
- Selecting SQL databases 444
- Selecting the backed-up data for recovery 620
- Selection rules for Linux 235
- Selection rules for macOS 235
- Selection rules for Windows 235
- Self-protection 511
- Sequence of actions 608
- Server-side protection 510
- Service logon account 87
- Set active volume 427
- Setting trusted and blocked connections 511
- Setting up a display mode 390
- Setting up a machine to boot from PXE 435
- SFTP server and tape device 230
- Sharing a remote connection 558
- Show notification about the last login of the current user 624
- SID changing 347
- Signing a file with ASign 336
- Simple Volume 422
- Skip the task execution 316
- Smart protection 549
- Software-specific recovery procedures 74
- Software requirements 52
- Source of the latest protection definitions 629
- Spanned Volume 422
- Special operations with virtual machines 475
- Specifying a tape set 611
- Splitting 310
- SQL Server high-availability solutions overview 446
- SSL certificate settings 211
- Start conditions 255
- Starting a backup manually 272
- Startup Recovery Manager 433
- Step 1 146
  - Generating a registration token 193
- Step 1. Read and accept the license agreements for the products that you want to update 545
- Step 2 147
  - Creating the .mst transform and extracting the installation package 193
- Step 2. Configure the settings for automatic approval 545
- Step 3 147
  - Setting up the Group Policy objects 193

- Step 3. Prepare the Test patching protection plan 546
- Step 4 148
- Step 4. Prepare the Production patching protection plan 546
- Step 5. Run the Test patching protection plan and check the results 547
- Stopping failover 481
- Storage Node (for on-premises deployment only) 59
- Storage node installation parameters 128
- Storage nodes 612
- Storage vMotion 495
- Striped Volume 422
- Structure of autostart.json 374
- Sufficient free space in the location 618
- Support for VM migration 495
- Supported cluster configurations 447-448
- Supported Cyber Protect features by operating system 17
- Supported data sources and destinations for continuous data protection 238
- Supported file systems 78, 410
- Supported hardware 592
- Supported Linux products 535
- Supported locations 243, 270, 356, 358-359
- Supported Microsoft and third-party products 534
- Supported Microsoft Exchange Server versions 61
- Supported Microsoft products 534
- Supported Microsoft SharePoint versions 61
- Supported Microsoft SQL Server versions 61

- Supported mobile devices 437
- Supported operating systems and environments 53
- Supported Oracle Database versions 62
- Supported SAP HANA versions 62
- Supported third-party products for Windows 535
- Supported virtual machine types 266
- Supported virtualization platforms 62
- Supported web browsers 52
- System requirements 76, 621
- System requirements for the agent 183, 186
- System settings 622

## T

- Tape-related backup options 595
- Tape devices 591
- Tape management 310, 347, 602
- Tape management database 592
- Tape pools 603
- Task failure handling 315
- Task start conditions 315
- TCP ports required for backup and replication of VMware virtual machines 148
- Testing a replica 480
- The Activities tab 584
- The backup location's host is available 257
- The Backup storage tab 350
- The Overview dashboard 574
- The Plans tab 355
- The TapeLocation folder 593

- The tool "tibxread" for getting the backed-up data 292
- The way of using Secure Zone 74
- Threat feed 549
- Tip 271
- Tips for further usage of the tape library 600
- Top-level object 374
- Transferring license quota to another management server 33
- Transferring the definitions to an HTTP server 632
- Troubleshooting 181, 329, 643
- Types of dynamic volumes 422
- Types of management servers 22

## U

- Unattended installation and uninstallation in macOS 169
- Unattended installation or uninstallation 121, 157
- Unattended installation or uninstallation in Linux 129, 163
- Unattended installation or uninstallation in macOS 132
- Unattended installation or uninstallation in Windows 121, 157
- Unattended installation or uninstallation parameters 123, 159, 164
- Uninstallation parameters 128, 131, 162, 168
- Uninstalling the product 197
- Units 634
- Units and administrative accounts 634
- Universal Restore in Linux 333
- Universal Restore in Windows 331

- Universal Restore process 332
- Universal Restore settings 332
- Unregistering a management server 39
- Update 60
- Updates 624
- Updating agents 195
- Updating agents on BitLocker-protected workloads 196
- Updating the catalog service with Acronis Cyber Protect 15 Update 4 613
- Updating the management server 100
- Updating the protection definitions 626
- Updating the protection definitions in an air-gapped environment 630
- Updating the software 108
- Updating virtual appliances 194
- Upgrading to Acronis Cyber Protect 15 197
- URL filtering 519
- URL Filtering 516
- URL filtering settings 522
- Usage examples 270, 279, 475, 479, 494
- Usage scenarios 351
- Use a disk cache to accelerate the recovery 347
- Use tape sets within the tape pool selected for backup 314
- Use the following tape devices and drives 312
- User is idle 256
- Users logged off 257
- Using a certificate issued by a trusted certificate authority 212
- Using a locally attached storage 492

- Using a self-signed certificate 211
- Using Acronis Cyber Protect with other security solutions in your environment 52
- Using policy rules 231, 235
- Using SAN hardware snapshots 487
- Using Universal Restore 331
- Using variables 279

## **V**

- Validating backups 352
- Validation 357
- Variable object 374
- Verifying file authenticity with Notary Service 335
- Viewing backup status in vSphere Client 496
- Viewing details about items in the whitelist 530
- Viewing the distribution result 493
- Virtual machine binding 492
- Virtuozzo (only available with the cloud deployment) 68
- Virtuozzo Hybrid Infrastructure (only available with the cloud deployment) 69
- VM power management 348, 483
- vMotion 495
- VMware 62
- Volume operations 422
- Volume Shadow Copy Service (VSS) 316
- Volume Shadow Copy Service (VSS) for virtual machines 317
- Volume Shadow Copy Service VSS for virtual machines 483
- Vulnerability assessment 533

- Vulnerability assessment and patch management 533
- Vulnerability assessment for Linux machines 537
- Vulnerability assessment for Windows machines 537
- Vulnerability assessment settings 535
- Vulnerability assessment widgets 581
- Vulnerable machines 581

## **W**

- Wait until the conditions from the schedule are met 315
- Warn about local or domain password expiration 624
- Weekly backup 317
- What do I need to use application-aware backup? 450
- What do I need to use the SAN hardware snapshots? 488
- What does a disk or volume backup store? 233
- What else you need to know 262
- What if I do not see backups stored on tapes? 600
- What is a backup file? 277
- What is a tape device? 591
- What to do after inventorying 607
- What to scan 535
- What you can back up 437
- What you can do with a replica 479
- What you need to know 437
- What you need to know about conversion 266
- What you need to know about finalization 478

When backing up to cloud storage 250

When backing up to other locations 250

Where can I see backup file names? 277

Where to get the backup app 438

Which accounts can be administrative? 634

Which machine performs the operation? 271

Whitelist settings 529

Why back up Microsoft 365 mailboxes? 467

Why use application-aware backup? 450

Why use SAN hardware snapshots? 487

Why use Secure Zone? 246

Why use the media builder? 365

Windows 233

Windows Azure and Amazon EC2 virtual machines 505

Windows Defender Antivirus 516

Windows event log 318, 348

Windows third-party products 541

WinPE-based 364

WinPE-based bootable media 381

WinRE-based PE images 382

Work across subnets 436

Working in VMware vSphere 478

WriteCacheSize 594