Acronis

acronis.com

Acronis Cyber Protect 17

Update 1

On-premises Deployment

User Guide

REVISION: 7/9/2026

Table of contents

Getting started with Acronis Cyber Protect 17 ..... **19**
Acronis account 19
Editing the company profile 19
Managing company contacts 20
Deleting your Acronis account 22
Acronis Customer portal, cloud console, and local console 23
Acronis Customer portal 23
Cloud console 25
Local console of an on-premises management server 25
On-premises deployment and cloud deployment 26
Components 27
Management Server 27
Centralized Dashboard 27
Agents 28
Other components 32
Types of management servers 33
Workloads 35
Cyber Protect console 36
Agent-based and agentless backup 36
Which backup type do I need? 37
Acronis Cyber Protect 17 editions and licensing **38**
License types 38
Upgrading to Acronis Cyber Protect 17 38
Managing licenses 39
Adding licenses to your Acronis account 40
Activating a management server 42
Allocating licenses to a management server 45
License co-termination 47
Syncing license renewals or co-termination to an offline management server 49
Transferring license quota to another management server 50
Decreasing the license quota of an offline management server 51
Assigning licenses to workloads 54
Unregistering a management server 55
Software requirements **62**
Supported operating systems and environments 62

© Acronis International GmbH, 2003-2026

Supported operating systems for protection agents 62
Supported operating systems for Management Server 68
Supported operating systems for Storage Node 70
Supported operating systems for Cyber Protect Monitor 70
Agent for Windows XP SP2 70
Supported file systems 72
Supported operations with logical volumes 75
Backup 75
Recovery 76
Supported web browsers 76
Supported Microsoft SQL Server versions 77
Supported Microsoft Exchange Server versions 77
Supported Microsoft SharePoint versions 77
Supported Oracle Database versions 78
Supported SAP HANA versions 78
Supported virtualization platforms 78
VMware (Broadcom) 78
Public clouds 81
Microsoft 81
Scale Computing 84
Proxmox VE 84
Citrix Hypervisor/XenServer 85
Red Hat and Linux 85
Parallels 86
Oracle 87
Nutanix 88
Virtuozzo Server 88
Cyber Frame / Virtuozzo Infrastructure 89
Linux packages required for installation of agents and management server in Linux 89
Are the required packages already installed? 90
Installing the packages from the repository 90
Installing the packages manually 91
Compatibility with encryption software 93
Common installation rule 93
The way of using Secure Zone 93
Common backup rule 93
Software-specific recovery procedures 93

© Acronis International GmbH, 2003-2026

Compatibility with Dell EMC Data Domain storages 94
Retention lock 94
Adding the AR_RETENTION_LOCK_SUPPORT variable 95
Installation 97
System requirements 97
Firewall configuration 98
Installing the management server 102
Installing the management server in Windows 102
Installing the management server in Linux 113
Installation in a Docker container 114
Adding machines from the Cyber Protect console 120
Limitations 120
Adding a machine running Windows 120
Adding a machine running Linux 125
Adding a machine running macOS 125
Adding a vCenter or an ESXi host 125
Adding a Scale Computing HC3 cluster 129
Installing agents locally 129
Downloading protection agents 129
Installing protection agents in Windows 129
Installing protection agents in Linux 131
Installing protection agents in macOS 133
Unattended installation or uninstallation 134
Unattended installation or uninstallation in Windows 134
Installing and uninstalling protection agents in Linux 142
Unattended installation or uninstallation in macOS 148
Deploying protection agents through Group Policy 150
Prerequisites 150
Creating the transform file and extracting the installation packages 151
Setting up the Group Policy object 152
Registering and unregistering machines manually 152
Generating a registration token 156
Managing registration tokens 157
Using passwords with special characters or blank spaces 158
Dynamic installation of antimalware components 159
Deploying virtual appliances 160
Deploying Agent for VMware (Virtual Appliance) from an OVF template 160

 © Acronis International GmbH, 2003-2026

Deploying Agent for Scale Computing HC3 (Virtual Appliance) 163
Agent for oVirt (Virtual Appliance) 170
Agent for Nutanix (Virtual Appliance) 175
Agent for Synology 181
Updating virtual appliances 190
SSH connections to a virtual appliance 190
Migrating the management server 192
Prerequisites 192
Operations on the source machine 192
Operations on the target machine 194
Registering a management server to the Centralized Dashboard 197
Unregistering a management server from the Centralized Dashboard 200
Device discovery 201
Discovering multiple devices 202
Device discovery by using Device Sense ™ 208
Remote installation of agents 212
Excluding devices from discovery 219
Connecting to discovered devices remotely 219
Troubleshooting device discovery 220
Checking for software updates 221
Updating agents 222
Updating protection agents on BitLocker-encrypted workloads 223
Uninstalling the product 223
In Windows 224
In Linux 224
In macOS 224
Removing Agent for VMware (Virtual Appliance) 225
Removing machines from the Cyber Protect console 225
Ports, services, and processes used by Acronis Cyber Protect 225
Supported Cyber Protect features by operating system 226
Managing workloads in the Cyber Protect console 229
Accessing the Cyber Protect console 229
On-premises deployment 229
Cloud deployment 230
Changing the language 230
Configuring a web browser for Integrated Windows Authentication 230
Allowing only HTTPS connections to the web console 235

 © Acronis International GmbH, 2003-2026

Adding a custom message to the web console 236
SSL certificate settings 239
Protection plans and modules 242
Creating a protection plan 243
Actions with protection plans 244
Disabling browsing of the folder tree 248
Resolving plan conflicts 250
The Plans tab 251
Compatibility issues with plans 252
Resolving compatibility issues 253
Device groups 254
Built-in groups 254
Custom groups 255
Creating a static group 255
Adding devices to static groups 256
Creating a dynamic group 256
Applying a protection plan to a group 266
Monitoring and reporting 267
The Overview dashboard 267
The Activities tab 277
Cyber Protect Monitor 279
Reports 282
Configuring the severity of alerts 285
SIEM log forwarding 286
Creating a SIEM log forwarding plan 287
Renaming the SIEM log forwarding plan 289
Editing the SIEM log forwarding plan 289
Deleting the SIEM log forwarding plan 289
SIEM forwarding methods 290
SIEM data format and examples 300
SIEM troubleshooting 307
System settings 317
Email notifications 317
Email server 318
Security 319
Updates 320
Default backup options 320

 © Acronis International GmbH, 2003-2026

Protection settings 320
Updating the protection definitions 320
Scheduling the updates 322
Changing the download location 323
Cache storage options 324
Source of the latest protection definitions 324
Remote connection 324
Updating the protection definitions in an air-gapped environment 325
Administering user accounts and organization units 330
Units and administrative accounts 330
Adding administrative accounts 334
Creating units 338
Viewing the last logged-in user 338
Backup 339
Backup module cheat sheet 341
Limitations 343
Selecting data to back up 344
Selecting entire machine 344
Selecting disks/volumes 344
Selecting files/folders 347
Selecting ESXi configuration 350
Continuous data protection (CDP) 350
Selecting a destination 357
Supported locations 357
Advanced storage options 358
About Secure Zone 360
About Acronis Cyber Infrastructure 363
Backup schedule 364
Backup schemes 364
Backup types 366
Running a backup on a schedule 367
Running a backup manually 379
Retention rules 380
Important tips 381
Retention rules according to the backup scheme 382
Configuring retention rules 384
Encryption 385

 © Acronis International GmbH, 2003-2026

Configuring encryption in the protection plan 386
Configuring encryption as a machine property 386
Conversion to a virtual machine 388
Conversion plans 388
Alternative options 389
Limitations 389
Types of conversion to virtual machine 390
Conversion to a virtual machine with the protection plan 391
Conversion to a virtual machine with a separate conversion plan 394
Replication 398
Usage examples 398
Supported locations 398
Considerations for users with the Advanced license 399
Backup options 400
Availability of the backup options 400
Alerts 403
Backup consolidation 403
Backup file name 404
Backup format 408
Backup validation 410
Changed block tracking (CBT) 410
Cluster backup mode 411
Compression level 412
Email notifications 412
Error handling 413
Fast incremental/differential backup 414
File filters 415
File-level backup snapshot 417
Forensic data 417
Log truncation 425
LVM snapshotting 426
Mount points 426
Multi-volume snapshot 427
One-click recovery 428
Performance and backup window 432
Physical Data Shipping 436
Pre/Post commands 437

 © Acronis International GmbH, 2003-2026

Pre/Post data capture commands 439
Scheduling 441
Sector-by-sector backup 442
Splitting 442
Tape management 443
Task failure handling 447
Task start conditions 447
Volume Shadow Copy Service (VSS) 448
Volume Shadow Copy Service (VSS) for virtual machines 450
Weekly backup 451
Windows event log 452
Operations with backups 452
The Backup storage tab 452
Mounting volumes from a backup 453
Validating backups 455
Exporting backups 455
Deleting backups 456
Understanding the detection of bottlenecks 458
Off-host data protection plans 462
Backup scanning plans 463
Backup replication 464
Validation 465
Cleanup 467
Special operations with virtual machines 468
Running a virtual machine from a backup (Instant Restore) 468
Working in VMware vSphere 472
Using locally attached storage 497
Backing up clustered Hyper-V machines 498
Limiting the total number of simultaneously backed-up virtual machines 498
Windows Azure and Amazon EC2 virtual machines 500
Recovery 502
Recovery cheat sheet 502
Cross-platform recovery 503
Cross-platform recovery via bootable media 509
Recovery of physical machines 510
Recovering a physical machine as a physical machine 510
Recovering a physical machine as a virtual machine 511

 © Acronis International GmbH, 2003-2026

Recovery of virtual machines 521
Recovering a virtual machine as a physical machine 521
Recovering a virtual machine as a virtual machine 523
Recovering containers 531
Recovering workloads by using bootable media 533
Creating bootable media 533
Recovering files 534
Recovering files by using the Cyber Protect console 534
Downloading files from the cloud storage 535
Signing a file with ASign 537
Recovering files by using bootable media 538
Extracting files from local backups 538
Recovering ESXi configuration 539
Recovery with restart 540
Recovery environments 541
Changing the recovery environment 542
Using Universal Restore 543
Universal Restore in Windows 543
Universal Restore in Linux 545
Safe recovery 546
How it works 546
Automatic domain rejoin 547
Recovery options 548
Availability of the recovery options 548
Backup validation 550
Boot mode 550
Date and time for files 551
Error handling 552
File exclusions 552
File-level security 552
Flashback 553
Full path recovery 553
Mount points 553
Performance 554
Pre/Post commands 554
Tape management 556
SID changing 556

 © Acronis International GmbH, 2003-2026

VM power management 556
Windows event log 557
Power on after recovery 557
Disaster recovery 558
Bootable media 559
Create a bootable media or download a ready-made one? 559
Linux-based or Windows-based bootable media? 561
Linux-based 561
Windows-based 561
Operations with bootable media 561
Creating backups by using bootable media locally 562
Recovering backups by using bootable media locally 571
Managing disks by using bootable media locally 577
Supported file systems 581
Basic precautions 581
Choosing the operating system for disk management 581
Disk operations 582
Volume operations 593
Pending operations 599
Registering bootable media on the management server 601
Registering the media from the media UI 601
Recovering backups by using bootable media remotely 602
Additional remote operations with bootable media 604
Bootable Media Builder 605
Why use the media builder? 605
32-bit or 64-bit? 606
Linux-based bootable media 606
Top-level object 615
Variable object 616
Control type 617
Windows-based bootable media 623
Connecting to a machine booted from media 628
Configuring network settings 628
Local connection 629
Remote connection 629
Configuring the display mode for Linux-based bootable media 629
NIC teaming support 629

 © Acronis International GmbH, 2003-2026

Configuring iSCSI devices 631
Acronis PXE Server 632
Installing Acronis PXE Server 632
Setting up a machine to boot from PXE 633
Work across subnets 634
Startup Recovery Manager 635
Disk space requirements 635
Limitations 636
Activating Startup Recovery Manager 636
Deactivating Startup Recovery Manager 637
Protecting mobile devices 638
Supported mobile devices 638
What you can back up 638
What you need to know 638
Where to get the Acronis Cyber Protect app 639
How to start backing up your data 639
How to recover data to a mobile device 640
How to review data via the Cyber Protect console 640
Protecting Microsoft applications 642
Protecting Microsoft SQL Server and Microsoft Exchange Server 642
Protecting Microsoft SharePoint 642
Protecting a domain controller 642
Recovering applications 643
Requirements for application-aware backups 644
Common requirements 644
Additional requirements for application-aware backups 644
Database backup 646
Selecting SQL databases 646
Selecting Exchange Server data 647
Protecting Always On Availability Groups (AAG) 648
Protecting Database Availability Groups (DAG) 649
Application-aware backup 651
Why use application-aware backup? 651
What do I need to use application-aware backup? 652
Configuring application-aware backup of virtual machines running Windows Server 2022 and later 652
Required user rights for application-aware backups 653

 © Acronis International GmbH, 2003-2026

Mailbox backup 654
Selecting Exchange Server mailboxes 655
Required user rights 655
Recovering SQL databases 656
Recovering system databases 658
Attaching SQL Server databases 658
Recovering Exchange databases 659
Mounting Exchange Server databases 661
Recovering Exchange mailboxes and mailbox items 661
Recovery to an Exchange Server 662
Recovery to Microsoft 365 663
Recovering mailboxes 663
Recovering mailbox items 664
Copying Microsoft Exchange Server libraries 667
Changing the SQL Server or Exchange Server access credentials 668
Protecting Microsoft 365 mailboxes 669
Why back up Microsoft 365 mailboxes? 669
Recovery 669
Limitations 669
Adding a Microsoft 365 organization 670
Obtaining application ID and application secret 670
Changing the Microsoft 365 access credentials 672
Selecting mailboxes 672
Recovering mailboxes and mailbox items 672
Recovering mailboxes 672
Recovering mailbox items 673
Protecting Google Workspace data 675
Protecting Oracle Database 676
Protecting SAP HANA 677
Protecting Proxmox virtual machines and containers 678
Limitations for Proxmox workloads 678
Installing Agent for Proxmox 679
Backing up Proxmox workloads 679
Recovering Proxmox workloads 680
Antimalware and web protection 681
Supported operating systems for antivirus and antimalware protection 681
Antivirus and antimalware protection 685

 © Acronis International GmbH, 2003-2026

Antimalware features 685
Scanning types 685
Antivirus & Antimalware protection settings 686
Active Protection 693
Windows Defender Antivirus 694
Schedule scan 694
Default actions 694
Real-time protection 695
Advanced 695
Exclusions 696
Microsoft Security Essentials 696
URL filtering 696
How it works 697
URL filtering settings 699
Quarantine 705
How do files get into the quarantine folder? 705
Managing quarantined files 705
Quarantine location on machines 705
Self-service custom folder on-demand 706
Corporate whitelist 706
Automatic adding to the whitelist 706
Manual adding to the whitelist 706
Adding quarantined files to the whitelist 707
Whitelist settings 707
Viewing details about items in the whitelist 707
Antimalware scan of backups 707
Limitations 708
Protection of collaboration and communication applications 708
Using Acronis Cyber Protect with other security solutions in your environment 709
Managing your hardware inventory 710
Enabling or disabling the hardware inventory scanning 710
Starting a hardware inventory scan manually 711
Browsing the hardware inventory 711
Viewing the hardware of a single device 713
Managing software 716
Managing your software inventory 716
Enabling or disabling the software inventory scanning 716

 © Acronis International GmbH, 2003-2026

Starting a software inventory scan manually ... 717
Browsing the software inventory ... 717
Viewing the software inventory of a single device ... 719
Assessing vulnerabilities and managing patches ... 720
Vulnerability assessment ... 720
Patch management ... 728
Connecting to workloads for remote desktop or remote assistance ... 746
Supported operating systems for remote desktop and assistance ... 747
Remote connection protocols ... 748
NEAR ... 748
RDP ... 749
Apple Screen Sharing ... 749
Remote sound redirection ... 749
Granting the required system permissions to the Connect Agent ... 750
Connections to remote workloads for remote desktop or remote assistance ... 751
Remote management plans ... 752
Creating a remote management plan ... 752
Adding a workload to a remote management plan ... 760
Removing workloads from a remote management plan ... 760
Additional actions with remote management plans ... 761
Workload credentials ... 763
Adding credentials ... 763
Assigning credentials to a workload ... 764
Deleting credentials ... 764
Unassigning credentials from a workload ... 765
Working with managed workloads ... 765
Configuring RDP settings ... 765
Connecting to managed workloads for remote desktop or remote assistance ... 766
Connecting to a managed workload via a web client ... 769
Transferring files ... 769
Sharing clipboard content between workloads ... 771
Performing control actions on managed workloads ... 772
Monitoring workloads via screenshot transmission ... 775
Observing multiple managed workloads simultaneously ... 776
Using the toolbar in the Viewer window ... 778
Recording and playing remote sessions ... 781
Configuring the Connect Client settings ... 782

 © Acronis International GmbH, 2003-2026

The remote desktop notifiers 783
Smart protection 785
Threat feed 785
How it works 785
Deleting all alerts 787
Data protection map 787
How it works 788
Managing the detected unprotected files 788
Data protection map settings 788
Remote wipe 791
Working with the Centralized Dashboard 792
Centralized Dashboard user roles 792
Assigning Centralized Dashboard user roles 793
Logging in to the Centralized Dashboard 794
Viewing data from multiple management servers 794
Viewing licensing information from multiple management servers 795
Navigating to the web console of a connected management server 796
Downloading the Centralized Dashboard data 796
Centralized Dashboard configuration 797
Centralized Dashboard database queries 799
Basic queries in the Centralized Dashboard database 799
Centralized Dashboard database views and tables 800
Materialized Aggregates schema 800
Views schema 801
Raw data schema 804
Configuring the retention period of the backup data from a local management server 816
Advanced storage options 817
Tape devices 817
What is a tape device? 817
Overview of tape support 817
Getting started with a tape device 823
Tape management 828
Storage nodes 838
Installing a storage node and a catalog service 838
Adding a managed location 839
Deduplication 841
Location encryption 844

 © Acronis International GmbH, 2003-2026

Cataloging 844
Immutable storage 847
Immutable storage modes 847
Supported storages and agents 848
Enabling immutable storage 848
Disabling immutable storage 849
Finding the storage ID 850
Accessing deleted backups in immutable storage 851
Compatibility with Advanced Format (4K-sector) hard disks 852
Command-line reference 854
Troubleshooting 855
Glossary 856
Index 858

© Acronis International GmbH, 2003-2026

Copyright statement

© Acronis International GmbH, 2003-2026. 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.

Getting started with Acronis Cyber Protect 17

To start using Acronis Cyber Protect

1. Add one or more licenses to your account in Acronis Customer Portal (`https://account.acronis.com`).

   Licenses that you purchase online are automatically added to this account.

   Note
   For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

2. [For on-premises deployments] Install and activate your management server.
3. Allocate one or more license to the management server.

   If there is only one management server in your Acronis account, all your licenses are automatically allocated to this server.
4. In the Cyber Protect console, add one or more workloads to the management server.

   Depending on the workload type, you might need to install a protection agent on it.
5. Apply a protection plan to the workloads that you want to protect.

Acronis account

You must have an Acronis account to use Acronis Cyber Protect, manage your licenses and their usage, access the latest product builds, and request technical support.

All licenses and management servers are registered in that account. When you create an Acronis account for a business customer, you also create a company profile and an administrator user profile.

With the administrator credentials, you can access the following consoles:

- Acronis Customer portal

  Note
  For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

- Cyber Protect Cloud console (Cloud console)
- Cyber Protect console (Local console of an on-premises management server)

For more information, see "Acronis Customer portal, cloud console, and local console" (p. 23).

Editing the company profile

The company profile contains information that you provided when you created the Acronis account.

© Acronis International GmbH, 2003-2026

Note
For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

To edit the company profile

Cloud console

1. Log in to the Cyber Protect Cloud console (https://cloud.acronis.com) as administrator.
2. Go to **Company management** > **Company profile**.
3. In the **Company information** section, click **Edit**.
4. Edit the company information, and then click **Save**.

Account.acronis.com

1. Log in to the Acronis Customer portal (https://account.acronis.com) with your Acronis account credentials.
2. In the navigation menu, click **Profile**.
3. In the **General information** section, click **Edit**.
4. Edit the profile information, and then click **Save**.

Managing company contacts

By default, the company administrator that you create with your Acronis account is the user who receives billing, technical, and business-related information from Acronis.

You can create additional company contacts and assign them one or more of the following contact types:

- Billing
- Technical
- Business

You can create a contact from an existing user profile in Cyber Protect Cloud or a contact that is not associated to a user profile.

For more information about how to create a user profile in Cyber Protect Cloud, see "Adding administrative accounts" (p. 334).

Note
For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

To add a company contact

Cloud console

 © Acronis International GmbH, 2003-2026

1. Log in to the Cyber Protect Cloud console (https://cloud.acronis.com) as administrator.
2. Go to **Company management** > **Company profile**.
3. In the **Company contacts** section, click **Add**.
4. [To create a contact from existing user profile] Select **Select an existing user**.
   a. Select a user profile from the drop-down list.
      The drop down-list shows the user profiles in Cyber Protect Cloud. These user profiles are different from the user profiles that you create in the local console.
   b. Select one or more contact types.
5. [To create a contact that is not associated to a user profile] Select **Create a new contact**.
   a. Specify the first name, the last name, and the email address of the contact.
   b. [Optional] Specify the phone number and the job title of the contact.
   c. Select one or more contact types.
6. Click **Add**.

Account.acronis.com

1. Log in to the Acronis Customer portal (https://account.acronis.com) with your Acronis account credentials.
2. In the navigation menu, click **Profile**.
3. [To add a technical contact] Go to **Technical Contact**, and then click **Add contact**
4. [To add a billing contact] Go to **Billing Contact**, and then click **Add contact**.
5. Specify the first name, the last name, and the email address of the contact.
6. [Optional] Specify the phone number and the job title of the contact.
7. Click **Save**.

As a result, a confirmation email will be sent to the email address of the contact.

After the email address is confirmed, it will be used for technical or billing information related to your Acronis account.

To edit a company contact

Cloud console

1. Log in to the Cyber Protect Cloud console (https://cloud.acronis.com) as administrator.
2. Go to **Company management** > **Company profile**.
3. In the **Company contacts** section, select the contact, and then click the ellipsis icon (...) > **Edit**.
4. Edit the contact information, and then click **Save**.

Account.acronis.com

1. Log in to the Acronis Customer portal (https://account.acronis.com) with your Acronis account credentials.
2. In the navigation menu, click **Profile**.
3. [To edit a technical contact] Go to **Technical Contact**, and then click **Edit**.

© Acronis International GmbH, 2003-2026

4. [To edit a billing contact] Go to **Billing Contact**, and then click **Edit**.
5. Edit the contact information, and then click **Save**.

To delete a company contact

Cloud console

1. Log in to the Cyber Protect Cloud console (https://cloud.acronis.com) as administrator.
2. Go to **Company management** > **Company profile**.
3. In the **Company contacts** section, select the contact, and then click the ellipsis icon (...) > **Delete**.
4. Click **Proceed** to confirm your choice.

As a result, the contact is deleted.

Note
When you delete a contact, the user profile that is associated to the contact in Cyber Protect Cloud is not deleted.

Account.acronis.com

1. Log in to the Acronis Customer portal (https://account.acronis.com) with your Acronis account credentials.
2. In the navigation menu, click **Profile**.
3. [To delete a technical contact] Go to **Technical Contact**, and then click the ellipsis icon (...) > **Delete**.
4. [To delete a billing contact] Go to **Billing Contact**, and then click the ellipsis icon (...) > **Delete**.

As a result, the contact is deleted.

Deleting your Acronis account

Warning!
This operation is irreversible. After you delete the account, your company profile, the serial numbers of registered products, and the data that is stored in Acronis Cloud will be permanently lost.

Note
For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

To delete your Acronis account

Cloud console

1. Log in to the Cyber Protect Cloud console (https://cloud.acronis.com) as administrator.
2. Go to **Company management** > **Company profile**.
3. In the **Delete account** section, click **Delete account**.

© Acronis International GmbH, 2003-2026

4. In the conformation wizard, read the warning, and then click **Next**.
5. Select the check box **I acknowledge that all data will be lost and I want to delete my account**, and then click **Next**.
6. In the drop-down menu, select the reason why you want to delete you profile.
7. [Optional] Leave an additional comment.
8. Click **Confirm**.
9. In the confirmation window, click **Done**.

   A confirmation email is sent to your email address. You must confirm the deletion within 24 hours.
10. In the confirmation email, click **Confirm deletion**.

As a result, your Acronis account is deleted. After the deletion completes, a notification will be sent to your email address.

Account.acronis.com

1. Log in to the Acronis Customer portal (https://account.acronis.com) with your Acronis account credentials.
2. In the navigation menu, click **Profile**.
3. In the **Delete account** section, click **Delete account**.
4. In the confirmation wizard, read the warning, and then click **Proceed to deletion**.
5. In the drop-down menu, select the reason why you want to delete you profile.
6. [Optional] Leave an additional comment.
7. Specify your password, and then select the check box **Yes, I acknowledge that all data will be lost and I want to delete my account**.
8. Click **Confirm deletion**.
9. In the confirmation window, select the check box **I confirm that I want to delete my account**, and then click **Delete**.

The deletion process might take up to 24 hours. After the deletion completes, a notification will be sent to your email address.

Acronis Customer portal, cloud console, and local console

With the administrator credentials for your Acronis account, you can access the following consoles:

- Acronis Customer portal
- Cyber Protect Cloud console (Cloud console)
- Cyber Protect console (Local console of an on-premises management server)

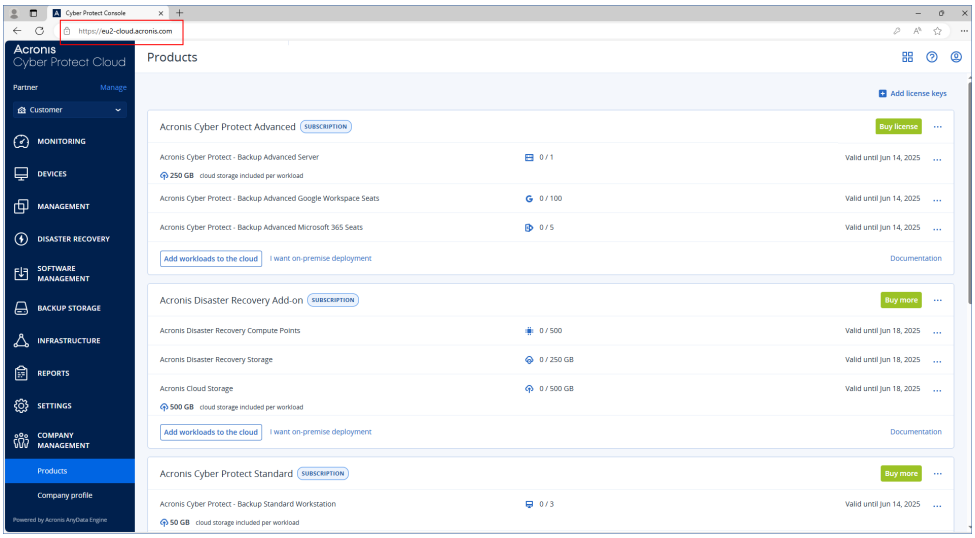
Acronis Customer portal

Acronis Customer portal is available at https://account.acronis.com.

© Acronis International GmbH, 2003-2026

For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

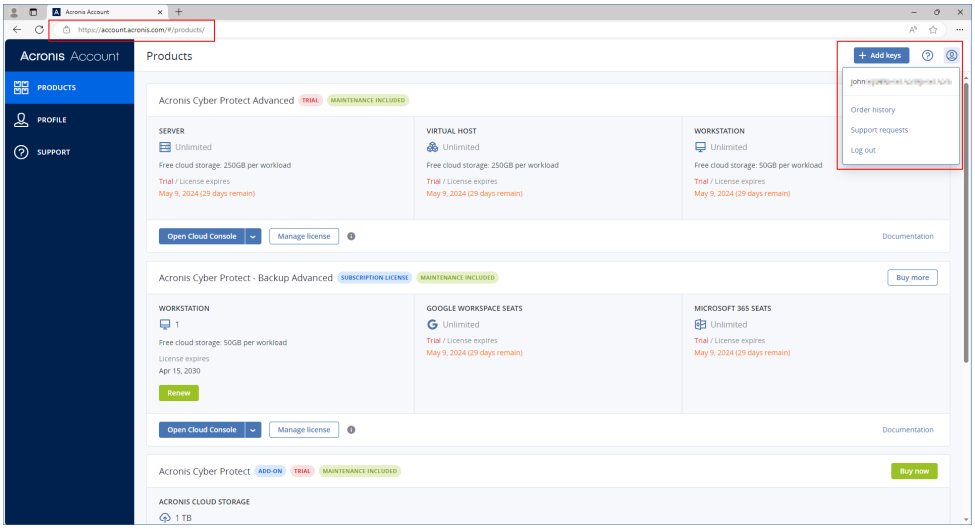
Cloud console



On the **Company management** > **Products** tab in the cloud console, you can check the expiration date of a subscription, add new license keys, register license renewals, and download the product installation files.

On the **Company management** > **Company profile** tab in the cloud console, you can edit the information in the company profile, manage the company contacts, and delete your account.

Account.acronis.com



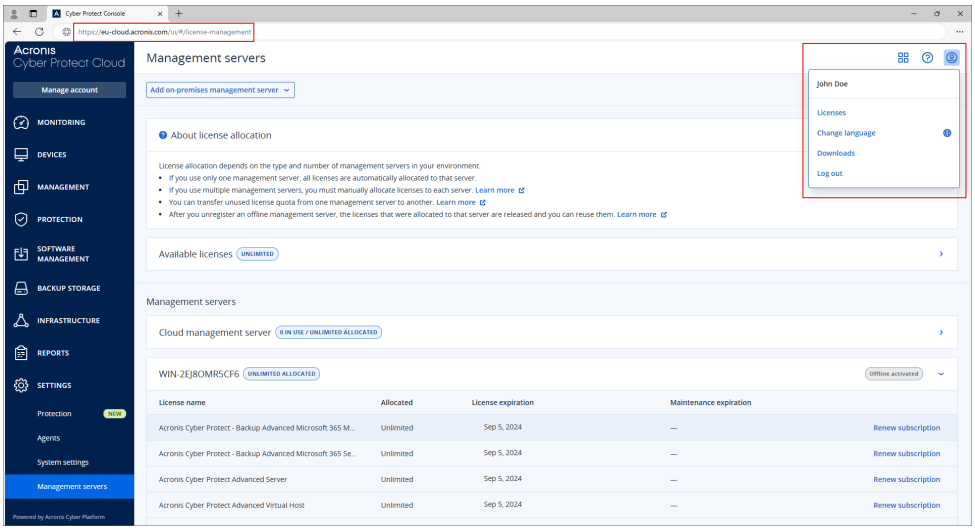
In Acronis Customer portal, you can check the expiration date of a subscription, add new license keys, and register license renewals. You can also contact the Support team, download the product installation files, and access the product documentation.

© Acronis International GmbH, 2003-2026

Cloud console

The cloud console is available at https://cloud.acronis.com.

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

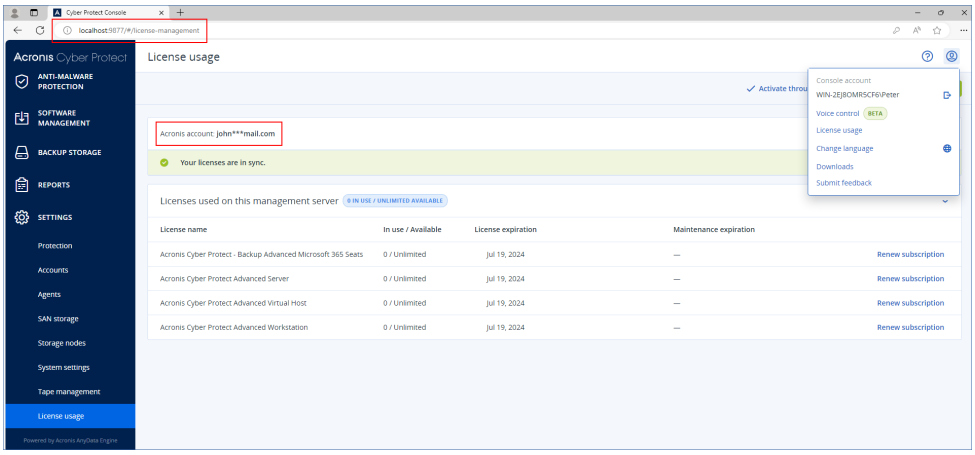


The cloud console is the main location where you can manage your licenses. On the **Settings** > **License usage** tab, you can allocate available licenses and license quota to a specific management server, reallocate license quota to another management server, or finalize the registration of an offline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

Local console of an on-premises management server

The local console is available at `https://<IP>:<port>`.

`IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.



In the local console, you can check the allocated licenses, their quota and usage, and their expiration date.

© Acronis International GmbH, 2003-2026

You must use the local console, together with the cloud console, when you activate an offline management server or allocate licenses to it.

On-premises deployment and cloud deployment

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 the Cyber Protect console.

The management server is responsible for the communication with the protection agents and the management of the protection plans. Before every protection activity, agents see 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.

On-premises deployment

In an on-premises deployment, all product components are installed in your local network.

You must use this deployment if your environment is not connected to the Internet (air-gapped environment).

Perpetual licenses are only available with the on-premises deployment.

The following options are available for installing the management server:

- On a machine running Windows
  With this option, you can install protection agents directly from the management server. If you use an Advanced license, you can create organizational units and delegate their management to unit administrators whose permissions are limited to the corresponding units.
- On a machine running Linux
  This option is recommended for Linux-only environments. You can install protection agents only locally, on the workloads that you want to back up.
- In a Docker container

Cloud deployment

In a cloud deployment, 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 a cyber protection service provided to you by Acronis.

© Acronis International GmbH, 2003-2026

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. Users can access the Cyber Protect console, download agents, and install them on their machines.

You can create administrator accounts on the organization level or on a unit level. Each account has a view scoped to their area of control. Users have access only to their own backups.

Components

Acronis Cyber Protect consists of a management server, agents that are installed on the workloads and communicate with the management server, and other components that enable additional functionalities.

Management Server

Management server is the central point for managing all of your backups. It manages the agents and provides the web interface to users.

The management server is responsible for the communication with the protection agents and for performing general plan management functions. Before every protection activity, agents see 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.

For more information about the management server, see "Types of management servers" (p. 33).

Centralized Dashboard

The Centralized Dashboard component is the central point for monitoring multiple management servers. It is available with the on-premise deployment only on machines on which the management server is installed, or together with the installation of the management server.

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-premises 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.	+	-

© Acronis International GmbH, 2003-2026

	Management Server requires a PostgreSQL database in addition to the SQLite or Microsoft SQL Server database. For more information, see "Configuring a PostgreSQL instance" (p. 109).			
Centralized Dashboard	Centralized Dashboard is the central point for monitoring multiple management servers. With the on-premise deployment, it is installed in your local network. Centralized Dashboard requires a Microsoft SQL Server database. To check the supported versions, see "Supported Microsoft SQL Server versions" (p. 77).	On a machine running Windows.	+	-
Components for Remote Installation	Saves agent installation packages to a local folder.	On the Windows machine running the management server.	+	-

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.

© Acronis International GmbH, 2003-2026

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 machines running macOS	Agent for Mac		+	+
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	Agent for Office	On a Windows	+	+

© Acronis International GmbH, 2003-2026

mailboxes	365	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.	+	-
Antimalware and URL filtering features				
Physical Windows machines	Agent for Antimalware protection	On the machine that you want to protect.	+	+
Physical Windows machines	Agent for URL filtering	On the machine that you want to protect.	+	+
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 (Virtual Appliance)	On the Scale Computing HC3 host.	+	+
Nutanix virtual machines	Agent for Nutanix AHV (Virtual appliance)	On the Nutanix AHV host.	+	+
Proxmox virtual machines	Agent for Proxmox	On the Proxmox VE host.	+	+

© Acronis International GmbH, 2003-2026

	(Bundled into the Agent for Linux (64-bit) installation file)			
Virtuozzo Server virtual machines and containers***	Agent for Virtuozzo (Bundled into the Agent for Linux (64-bit) installation file)	On the Virtuozzo Server 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				
Network-attached storage				
Synology	Agent for Synology	On the Synology NAS device	+	+
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.

© Acronis International GmbH, 2003-2026

**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, see "LAN-free backup" (p. 481).

***For Virtuozzo 7, only ploop containers are supported. Virtual machines are not supported.

****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
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 Builder	Creates bootable media.	On a machine running Windows or Linux.	+	-
Command-Line Tool	Supports the command-line interface with the **acrocmd** utility. **acrocmd** does not contain any tools that physically execute the	On a machine running Windows, Linux, or macOS.	+	+

© Acronis International GmbH, 2003-2026

	commands. It only provides the command-line interface to Cyber Protect components - agents and the management server.			
Cyber Protect 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, Cyber Protect 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 nodes.	On a machine running Windows.	+	-
PXE Server	Enables booting machines into bootable media through the network.	On a machine running Windows.	+	-

Types of management servers

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

© Acronis International GmbH, 2003-2026

- On-premises management server
  - Online management server
  - Offline management server
- Cloud 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, see "Transferring license quota to another management server" (p. 50).

On-premises management server

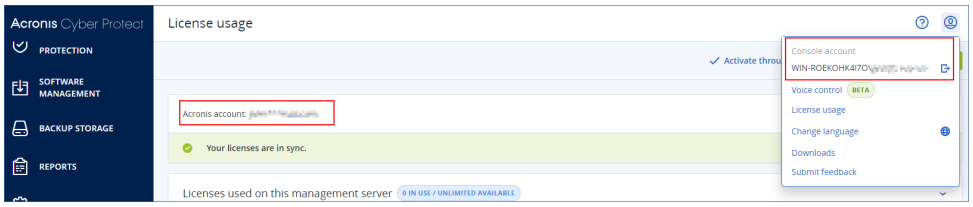
With on-premises deployment, you can install both the management server and the protection agents in your network. You can have an offline management server that is not connected to the Internet or an online management server that has access to the Internet.

On-premises management servers require activation. For more information about the activation, see "Activating a management server" (p. 42).

Online on-premises management server

You can 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.

Note
Two different accounts are shown in the local console of an online 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.



Offline on-premises management server

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

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.

© Acronis International GmbH, 2003-2026

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.

Workloads

A workload is any type of protected resource − for example, a physical machine, a virtual machine, a mailbox, or a database instance. In the Cyber Protect console, the workload is shown as an object to which you can apply a plan (protection plan, backup plan, or scripting plan).

Some workloads require installing a protection agent or deploying a virtual appliance. You can install agents by using the graphical user interface or by using the command-line interface (unattended installation). You can use the unattended installation to automate the installation procedure. For more information about how to install protection agents, see "Installation" (p. 97).

A virtual appliance (VA) is a ready-made virtual machine that contains a protection agent. With a virtual appliance, you can back up other virtual machines in the same environment without installing a protection agent on them (agentless backup). The virtual appliances are available in hypervisor-specific formats, such as .ovf, .ova, or .qcow. For more information about which virtualization platforms support agentless backup, see "Supported virtualization platforms" (p. 78).

The table below summarizes the workload types and their respective agents.

Workload type	Agent	Examples (non-exhaustive list)
Physical machines	A protection agent is installed on every protected machine.	Workstation Laptop Server
Virtual machines	Depending on the virtualization platform, the following backup methods might be available: • Agent-based backup − A protection agent is installed on every protected machine. • Agentless backup − A protection agent is installed only on the hypervisor host, on a dedicated virtual machine, or is deployed as a virtual appliance. This agent backs up all virtual machines in the environment.	VMware virtual machine Hyper-V virtual machine Kernel-based virtual machine (KVM) managed by oVirt VMware Cloud Director (vCD) virtual machines*
Microsoft 365 Business	These workloads are backed up by a cloud agent for which no installation is required.	Microsoft 365 mailbox

© Acronis International GmbH, 2003-2026

Workload type	Agent	Examples (non-exhaustive list)
workloads Google Workspace workloads (available in the cloud deployment)	To use the cloud agent, you need to add your Microsoft 365 or Google Workspace organization to the Cyber Protect console. Additionally, a local Agent for Office 365 is available. It requires installation and can only be used to back up Exchange Online mailboxes. For more information about the differences between the local and the cloud agent, see the Acronis Cyber Protect Cloud documentation.	Microsoft 365 OneDrive Microsoft Teams SharePoint site Google mailbox Google Drive
Applications	The data of specific applications is backed up by dedicated agents, such as Agent for SQL, Agent for Exchange, or Agent for Active Directory.	SQL Server databases Oracle databases Active Directory

Cyber Protect console

In the Cyber Protect console, you can manage workloads and plans, change the protection settings, configure reports, and check the backup storage.

The Cyber Protect console provides access to additional services or features, such as Antivirus and Antimalware protection, Patch management, and Vulnerability assessment. The type and number of these services and features vary according to your Cyber Protect license.

The **Devices** section is available in simple and table view. You can switch the view from the icon in the top right corner.

The simple view shows only a few workloads. The table view is enabled automatically when the number of machines becomes larger. Both views provide access to the same features and operations. This document describes access to operations from the table view.

When a workload goes online or offline, it takes some time for its status to change in the Cyber Protect console.

The status of the workloads is checked every minute. If the agent installed on a workload is not transferring data, and there is no answer to five consecutive checks, the workload is shown as offline. The workload will be shown as online again when it answers a status check or starts transferring data.

Agent-based and agentless backup

Agent-based backup requires that a protection agent is installed on each protected machine. Agent-based backup is supported on all physical and virtual machines.

© Acronis International GmbH, 2003-2026

Agentless backup is supported by some virtualization platforms and it is not available for physical machines. Agentless backup requires only one protection agent, which is installed on a dedicated machine in the virtual environment. This agent backs up all other virtual machines in this environment. For more information about the supported backup types per virtualization platform, see "Supported virtualization platforms" (p. 78).

For some virtualization platforms, virtual appliances are available. A virtual appliance (VA) is a ready-made virtual machine that contains a protection agent. The virtual appliances are available in hypervisor-specific formats, such as .ovf, .ova, or .qcow.

Which backup type do I need?

We recommend the agent-based backup if you need the following:

- Additional protection functionality, such as antivirus and antimalware, patch management, or remote desktop connection.
- Separate virtual machines at the tenant level. For example, because you want to provide the users in the tenant with access only to their own backups.
- File-level backups that you can recover to the guest operating systems.

We recommend the agentless backup if you need the following:

- Only backup, without any additional protection features.
- Simplified management—you can back up multiple virtual machines by installing and configuring only one agent.
- Minimal resource usage—one dedicated agent uses less CPU and RAM than multiple agents installed on each virtual machine in your environment.
- Specific backup setups, such as LAN-free backup. For more information about this feature, see "LAN-free backup" (p. 481).
- Less configuration overhead. The dedicated agent backs up the virtual machines on the hypervisor level, regardless of guest operating systems.

 © Acronis International GmbH, 2003-2026

Acronis Cyber Protect 17 editions and licensing

Acronis Cyber Protect 17 is available in the following editions:

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

For more information about these editions, see the Acronis website.

Note
Some of the features that are described in the User guide may not be available in your edition.

License types

The following license types are available:

- Subscription licenses

  Unlimited updates and free technical support are available within the validity period of a subscription license. When the validity period ends, the existing protection plans stop working and new protection plans cannot be created. The validity period starts on the date of purchase.
- Perpetual licenses (legacy)

  Using the product is not time-limited. However, technical support and free updates to newer versions are accessible only within the maintenance period. The maintenance period is subject to renewal. Cloud deployment and some features, such as cloud-to-cloud backups, are not available with a perpetual license.
- Trial license

  All features are available for 30 days after license activation.

The Acronis licensing policy is available at https://www.acronis.com/company/licensing.html.

Upgrading to Acronis Cyber Protect 17

You can upgrade older versions of Acronis Cyber Protect to version 17, as follows.

Component	Version that you can upgrade
Agents	Acronis Cyber Protect 16 Acronis Cyber Protect 15
Management Server	Acronis Cyber Protect 16 **Important** This upgrade is only available if Management Server is running on an operating system that is supported by Acronis Cyber Protect 17. See "Supported operating systems for Management Server" (p. 68).

© Acronis International GmbH, 2003-2026

Note

- To upgrade from Acronis Cyber Protect 16, you must have an active subscription license or a perpetual license with an active maintenance period.
- 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.
- AcronisCyber Protect 17 requires a PostgreSQL database for the management server, in addition to the existing database. During the upgrade, a new PostgreSQL instance is installed automatically, or you can configure the connection to an existing instance. For more information, see "Configuring a PostgreSQL instance" (p. 109).

To start the upgrade

- Run the installer and follow the on-screen instructions.

Important

Acronis Storage Node version 17 requires agents version 17. It does not work with older agents, such as v16, v15, and v12.5. Do not install the storage node component if you still have older agents running on protected workloads.

The management server in Acronis Cyber Protect 17 is backward compatible and supports protection agents version 15 and version 16.

Upgrading the protection agents does not interfere with the existing backup archives and their settings.

Managing licenses

An Acronis Cyber Protect license is required for every protected workload. A license is not required to install Acronis Cyber Protect.

Licenses that you buy are added to your account in Acronis Customer portal (https://account.acronis.com).

For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

You can allocate the licenses to one or more management servers in your environment. Then, the management server distributes the license quota to the workloads that are registered on that server.

A license is automatically assigned when you apply a protection plan to a workload for the first time. If more than one license is available, the most appropriate license is assigned automatically. For example, a workload might be assigned an Acronis Cyber Protect Advanced – Server license, while another workload might take an Acronis Cyber Protect Standard. The automatic assignment depends on the workload's type, operating system, and required level of protection.

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

 © Acronis International GmbH, 2003-2026

Operation	Location
Adding licenses to your account	You can add licenses in Acronis Customer portal. Licenses that you purchased online are automatically added there.
Activating a management server	You can activate a management server by registering it in your account. You can activate online management servers in their local console (`https://<IP>:<port>`), by signing in to your Acronis account. For this operation, you must use both the cloud and the local consoles. To access the cloud console, you need a second machine that is connected to the Internet.
Allocating licenses to a management server Modifying an existing license allocation	On online management servers, you can allocate licenses by using the cloud console (https://cloud.acronis.com). The allocated licenses are automatically synced to the management server. On offline management servers, you can allocate licenses through an activation file. This procedure requires that you use both the local console of the management server (`https://<IP>:<port>`) and the cloud console (https://cloud.acronis.com).
Assigning licenses to workloads	This operation is automatic, but you can manually change the assignment.
Unregistering a management server from your account	You can unregister online management servers by using the cloud console (https://cloud.acronis.com). You can unregister offline management servers through a deactivation file. This procedure requires that you use both the local console of the offline management server (`https://<IP>:<port>`) and the cloud console (https://cloud.acronis.com). To unregister an offline management server to which you do not have access, you must use only the cloud console.

Adding licenses to your Acronis account

You can only use licenses that are added to your Acronis account.

Licenses that you buy online are automatically added to your account. Licenses that you buy offline must be manually added to your account.

Note
For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

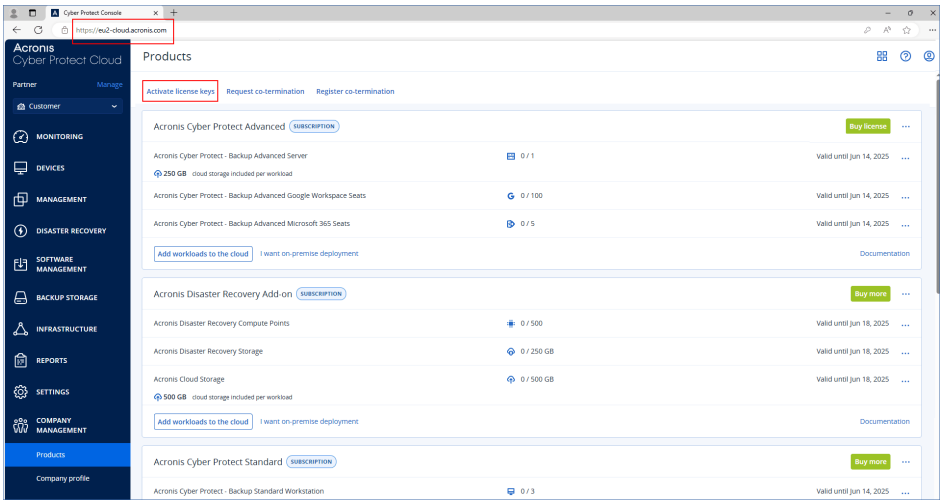
To add a license in your Acronis account

Cloud console

© Acronis International GmbH, 2003-2026

1. Log in to the Cyber Protect Cloud console (https://cloud.acronis.com) as administrator.

   Alternatively, log in to your account at https://account.acronis.com. You will be redirected to the cloud console.
2. Go to **Company management** > **Products**.



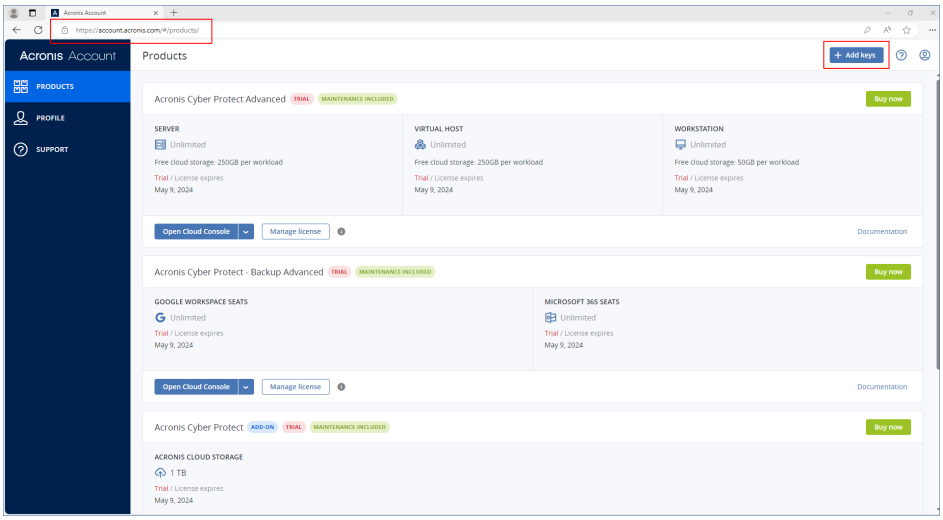
3. Click **Activate license keys**.
4. [To add individual license keys] Click **Enter license keys**.
   a. Enter one or more license keys, one per line.
   b. Click **Add**.
5. [To add a file with multiple license keys] Click **Upload license key file**.
   a. Click **Browse**, and then select the TXT file that contains the license keys.
   b. Click **Add**.

The licenses are now added to your account and you can manage their usage on the **Settings** > **License usage** tab.

Account.acronis.com

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

© Acronis International GmbH, 2003-2026



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 on the **Settings** > **License usage** tab in the cloud console (https://cloud.acronis.com).

Activating a management server

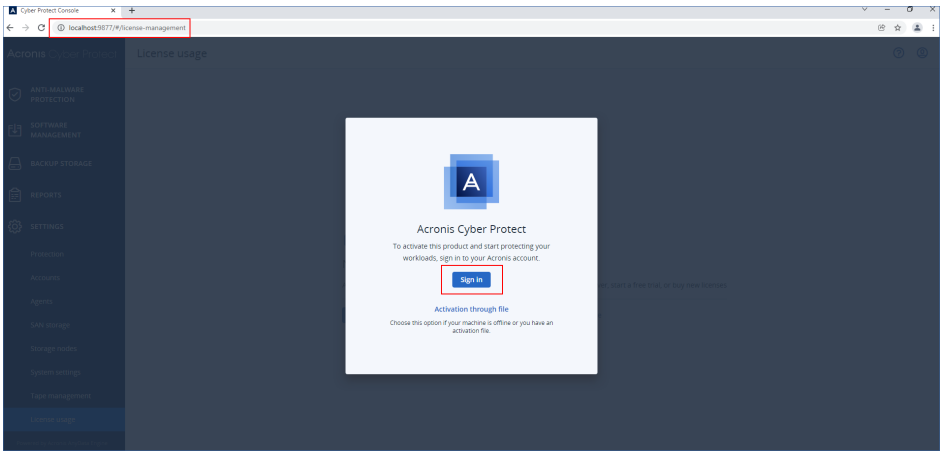
You must activate a management server by registering it in your Acronis account.

To activate an online management server

1. After installing Acronis Cyber Protect management server, open the local console (`https://<IP>:<port>`).

   `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.

2. In the dialog that opens, click **Sign in**.



3. Sign in to your Acronis account.

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

© Acronis International GmbH, 2003-2026

To start protecting your workloads, allocate one or more licenses to this server. For more information, see "Allocating licenses to a management server" (p. 45).

Note

Online management servers require Internet access to sync the licensing information to your Acronis account. If a management server is 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.

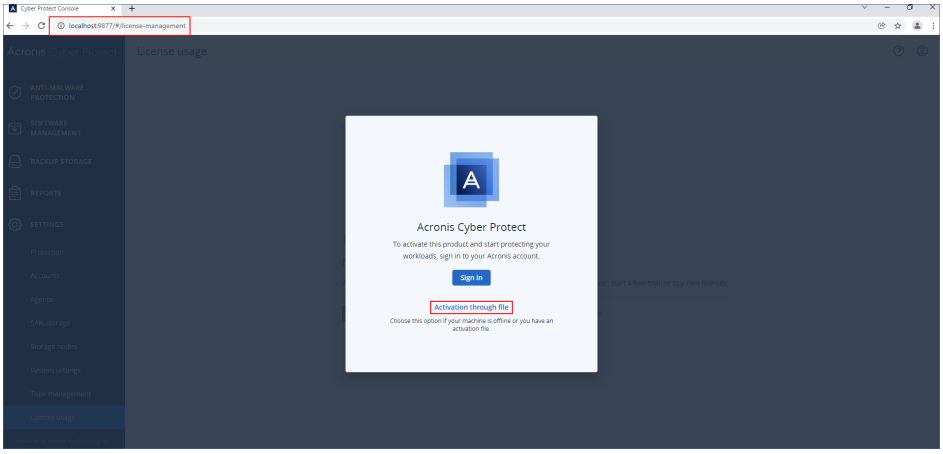
To activate an offline management server

For this operation, you must use both the cloud and the local consoles.

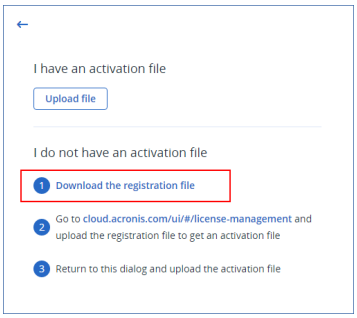
To access the cloud console, you need a second machine that is connected to the Internet.

1. After installing Acronis Cyber Protect management server, open the local console (`https://<IP>:<port>`).

   `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.
2. In the dialog that opens, click **Activation through file**.



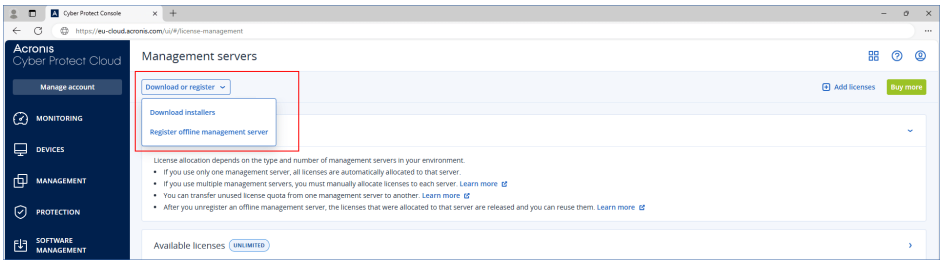
3. Under **I do not have an activation file**, click **Download the registration file**.



   The registration file is downloaded to your machine.
4. Keep the **Activation through file** dialog open.

© Acronis International GmbH, 2003-2026

5. Copy the downloaded registration file to a drive that you can use on the machine that is connected to the Internet. For example, you can use a USB flash drive.
6. On the machine that is connected to the Internet, log in to the cloud console (https://cloud.acronis.com), and then go to **Settings** > **Management servers**.
7. Click **Download or register**, and then click **Register offline management server**.



8. In the dialog that opens, click **Browse**, and then select the registration file that you downloaded from your offline management server.
9. In the dialog 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.

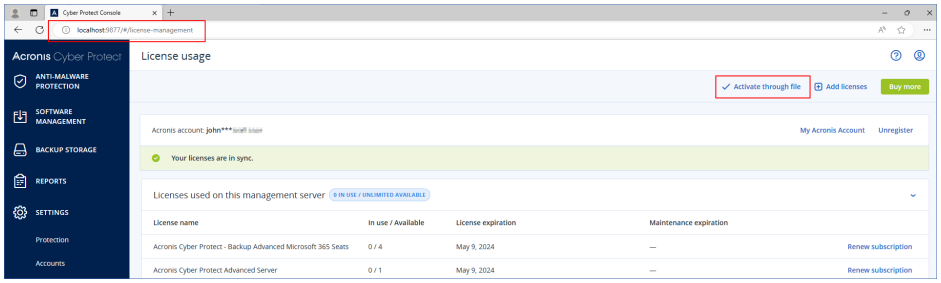
If this is not the only management server in your environment, after the activation, you must allocate licenses by following the procedure in "Allocating licenses to a management server" (p. 45).

10. Copy the downloaded activation file to a drive that you can use on the offline management server. For example, you can use a USB flash drive.
11. In the local console of the offline management server (`https://<IP>:<port>`), go to the **Activation through file** dialog.

    `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.

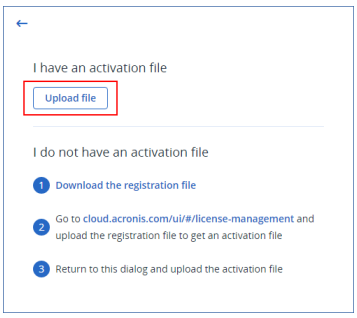
Note

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



© Acronis International GmbH, 2003-2026

12. 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 is running on a virtual machine if the UUID of the virtual machine is not unique. For example, the UUID might be duplicated when you clone a virtual machine or convert it with VMware vCenter Converter. If you face this issue, contact the Support team.

For more information about how to avoid UUID duplication and how to set a unique UUID on a VMware virtual machine, see Changing or keeping a UUID for a moved virtual machine (1541) in the VMware knowledge base.

Allocating licenses to a management server

To use a license, you must allocate its quota or part 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 parts 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, see "Transferring license quota to another management server" (p. 50).

If you have more than one management server in your Acronis account, you can view the new licenses in the cloud console (https://cloud.acronis.com), under **Available licenses**. You must 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, see "Types of management servers" (p. 33).

To allocate licenses to a management server

Online management server

© Acronis International GmbH, 2003-2026

1. In the cloud console (https://cloud.acronis.com), click **Settings** > **Management servers**.
2. Go to the management server to which you want to allocate a license.
3. Click **Add/remove licenses**.
4. In the dialog that opens, specify the license and the license quota that you want to allocate to this server.
5. Click **Confirm**.

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 allocation procedure.

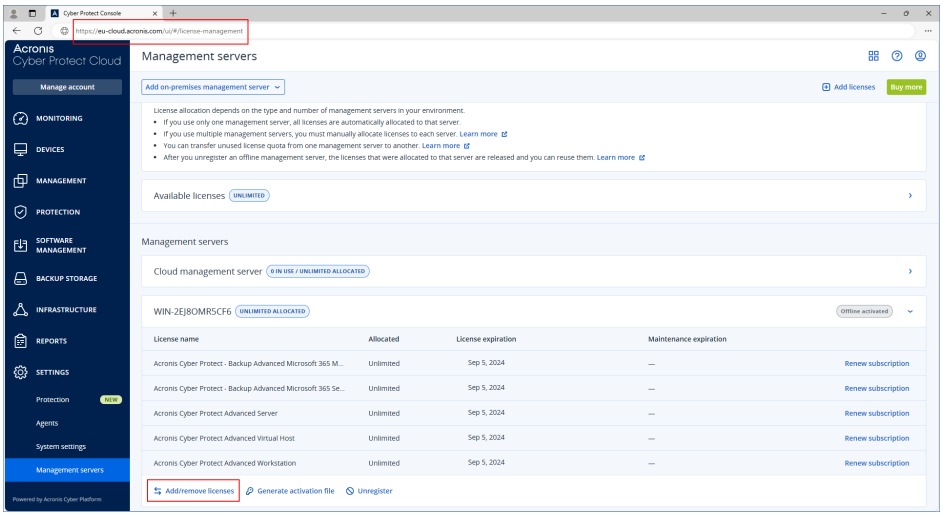
Important
If the modified license quota is smaller than the number of protection agents, the least-loaded agents will stop working. This selection is automatic. If it does not fit your needs, reassign the available licenses manually.

Offline management server

For this operation, you must use both the cloud and the local consoles.

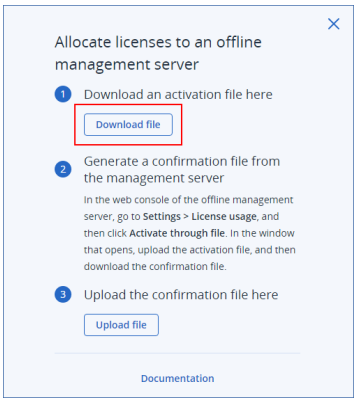
To access the cloud console, you need a second machine that is connected to the Internet.

1. On the machine that is connected to the Internet, log in to the cloud console (https://cloud.acronis.com), and then go to **Settings** > **Management servers**.
2. Go to the management server to which you want to allocate a license.
3. Click **Add/remove licenses**.



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

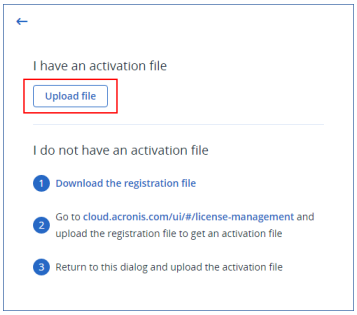
© Acronis International GmbH, 2003-2026



The activation file is downloaded to your machine.

7. Copy the downloaded activation file to a drive that you can use on the offline management server. For example, you can use a USB flash drive.
8. In the local console of the offline management server (`https://<IP>:<port>`), go to **Settings** > **License usage**, and then click **Activate through file**.

   `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.
9. In the dialog that opens, 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 licensing information is synced between your Acronis account and the offline management server.

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

To decrease the allocated license quota, see "Decreasing the license quota of an offline management server" (p. 51).

License co-termination

You can use license co-termination to align the expiration dates of multiple licenses in your account or choose a different expiration date for a single license. By using co-termination, you can change only the license term. You cannot change the license quota.

Co-termination applies to subscription licenses and the active maintenance period of the legacy perpetual licenses.

Aligning the expiration dates of licenses includes the following procedures:

© Acronis International GmbH, 2003-2026

1. Requesting license co-termination from your service provider.
2. Registering the co-terminated (aligned) licenses in your account.
3. [For offline management servers] Synchronizing the licensing information between your account and the offline management server.

Requesting license co-termination

You can request license co-termination in the cloud console.

Important
To avoid incorrect billing, disable the automatic renewal of online purchased licenses by canceling your subscription. For more information, see this knowledge base article.

To request license co-termination

Required role: Company administrator or Protection administrator

1. In the Cyber Protect cloud console, go to **Company management** > **Products**.
2. Click **Request co-termination**.
3. Select one or more licenses whose expiration date you want to change.
   You can select licenses with active subscription or licenses that expired up to 30 days ago.
4. Select a new expiration date.
   You can select a date after the expiration date of the license that has the longest term.
5. Click **Continue**.
6. [If co-termination is not available for all selected licenses] Remove the affected licenses from your selection.
   The licenses for which co-termination is not available are highlighted.
   a. Click **Remove affected licenses**.
   b. Click **Continue**.
7. Specify an email address, and then click **Co-terminate**.

As a result, a co-termination request is created.

When your co-termination order is processed, a sales representative will contact you. If you need to contact the Sales team earlier, click **Contact Sales**. After your co-termination order is completed, you will receive a purchase order, invoice, or a certificate number via email.

Next, you must register the co-terminated (aligned) licenses in your account. For more information, see "Registering license co-termination" (p. 48).

Registering license co-termination

After receiving a purchase order, invoice, or a certificate number via email, you must register the co-terminated (aligned) licenses in your account.

To register license co-termination

Required role: Company administrator or Protection administrator

 © Acronis International GmbH, 2003-2026

1. In the Cyber Protect cloud console, go to **Company management** > **Products**.
2. Click **Register co-termination**.
3. Specify your billing email address and one of the following:
   - Purchase order number
   - Invoice number
   - License certificate number

   You can find these numbers in the PDF document that was sent to your email address.
4. Click **Register**.

As a result, the license information in your account is updated.

Important
If you use an offline management server, you must sync the updated license information with it. For more information, see "Syncing license renewals or co-termination to an offline management server" (p. 49).

Syncing license renewals or co-termination to an offline management server

For offline management servers, you must manually sync the licensing information from your Acronis account with the management server after you do any of the following:

- renew a subscription license
- renew a maintenance period
- co-terminate licenses

For online management servers, syncing is automatic.

Prerequisites

- You have renewed your subscription license or maintenance period, or you have co-terminated licenses.
- The updated licensing information is shown in the Customer portal.

  Note
  For new customers, Acronis Customer portal is part of the cloud console. These customers are redirected to the cloud console when they log in to their account at https://account.acronis.com.

To sync license renewals or co-termination

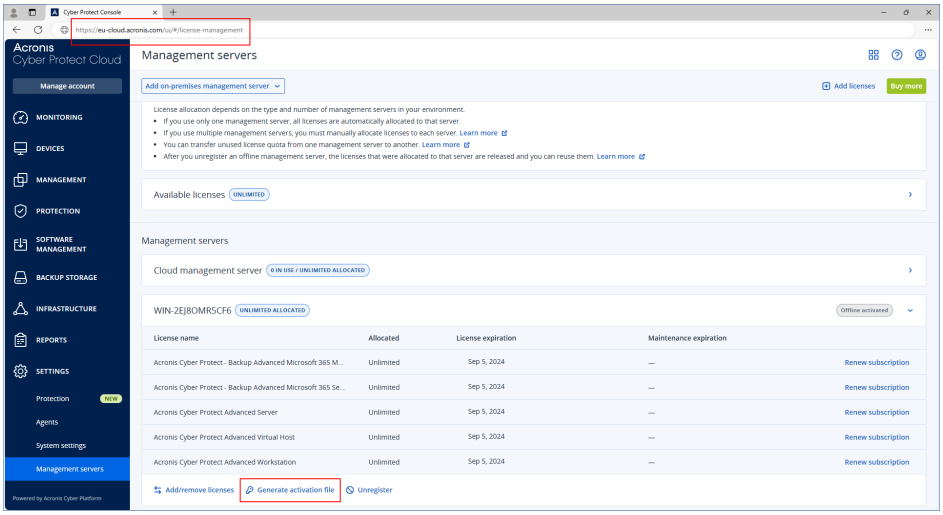
For this operation, you must use both the cloud and the local consoles.

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

1. On the machine that is connected to the Internet, log in to the cloud console (https://cloud.acronis.com), and then go to **Settings** > **Management servers**.

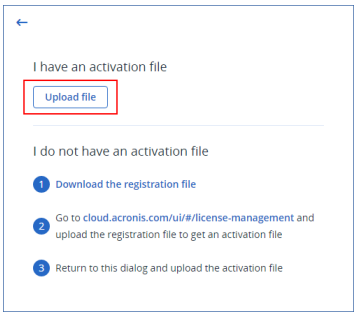
© Acronis International GmbH, 2003-2026

2. Go to the offline management server with which you want to sync the updated licensing information.
3. Click **Generate activation file**.



   The activation file is downloaded to your machine.
4. Copy the downloaded activation file to a drive that you can use on the offline management server. For example, you can use a USB flash drive.
5. In the local console of the offline management server (`https://<IP>:<port>`), go to **Settings** > **License usage**, and then click **Activate through file**.

   `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.
6. In the dialog that opens, 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 licensing information is synced between your Acronis account and the offline management server.

Transferring license quota to another management server

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

© Acronis International GmbH, 2003-2026

Note

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

If you have more than one management server in your Acronis account, you can view the new licenses in the cloud console (https://cloud.acronis.com), under **Available licenses**. You must 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.

   For more information, see the following topics:

   - [For online management servers] "Allocating licenses to a management server" (p. 45)
   - [For offline management servers] "Decreasing the license quota of an offline management server" (p. 51)

   As a result, the released license quota appears in the **Available licenses** section in the cloud console.
2. Allocate the license quota to another management server by following the procedure in "Allocating licenses to a management server" (p. 45).

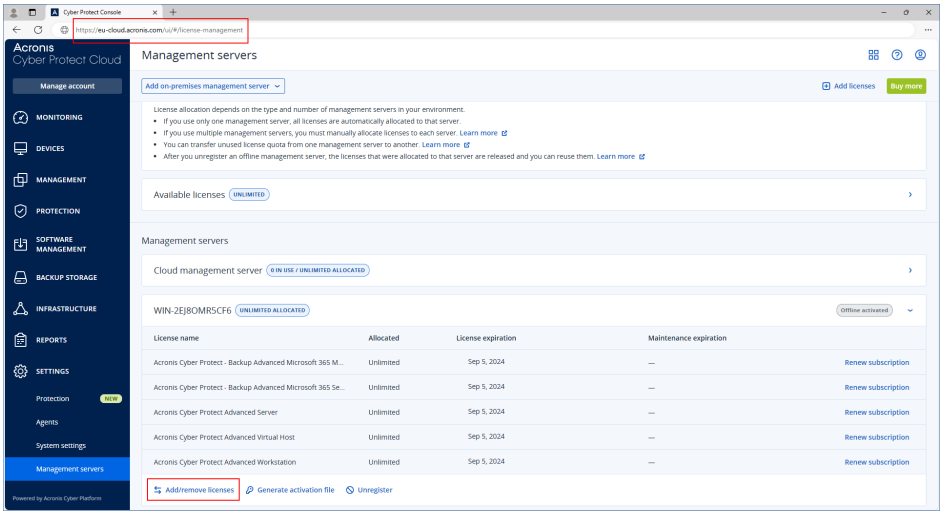
Decreasing the license quota of an offline management server

For this operation, you must use both the cloud and the local consoles.

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

To decrease the license quota

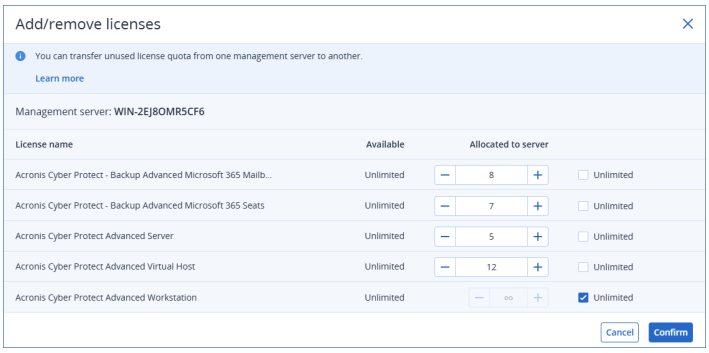
1. On the machine that is connected to the Internet, log in to the cloud console (https://cloud.acronis.com), and then go to **Settings** > **Management servers**.
2. Go to the management server for which you want to decrease the license quota, and then click **Add/remove licenses**.



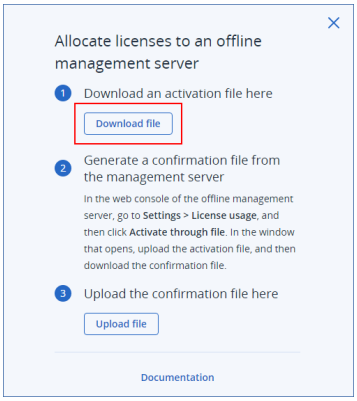
© Acronis International GmbH, 2003-2026

3. In the dialog that opens, modify the license quota, and then click **Confirm**.

   Allocating license quota equal to zero will remove the license from the server.



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

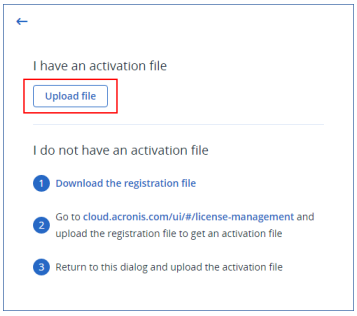


   The activation file is downloaded to your machine.

5. Copy the downloaded activation file to a drive that you can use on the offline management server. For example, you can use a USB flash drive.
6. In the local console of the offline management server (`https://<IP>:<port>`), go to **Settings** > **License usage**, and then click **Activate through file**.

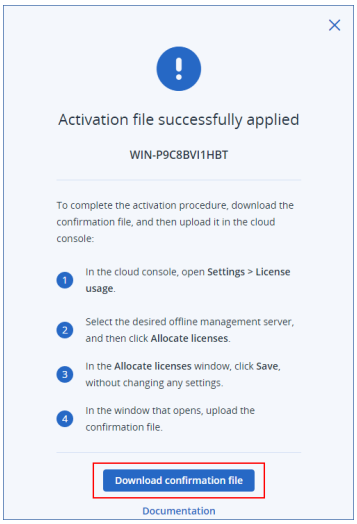
   `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.

7. In the dialog that opens, under **I have an activation file**, click **Upload file**, and then select the activation file that you downloaded from the cloud console.



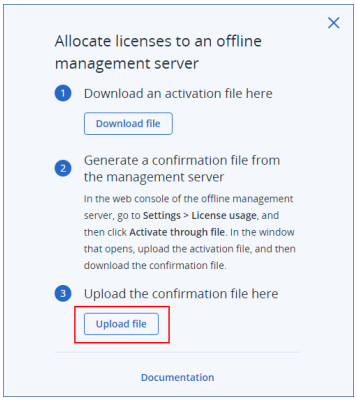
8. In the dialog that opens, click **Download confirmation file**.

© Acronis International GmbH, 2003-2026



The confirmation file is downloaded to your machine.

9. Copy the downloaded confirmation file to a drive that you can use on the machine that is connected to the Internet. For example, you can use a USB flash drive.
10. On the machine that is connected to the Internet, log in to the cloud console (https://cloud.acronis.com), and then go to **Settings** > **Management servers**.
11. Go to the management server for which you want to decrease the license quota, and then click **Add/remove licenses**.
12. In the dialog that opens, click **Confirm**, without changing any settings.
13. In the **Allocate licenses to an offline management server** dialog, click **Upload file**, and then select the confirmation file that you downloaded from the offline management server.



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.

© Acronis International GmbH, 2003-2026

Assigning licenses to workloads

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

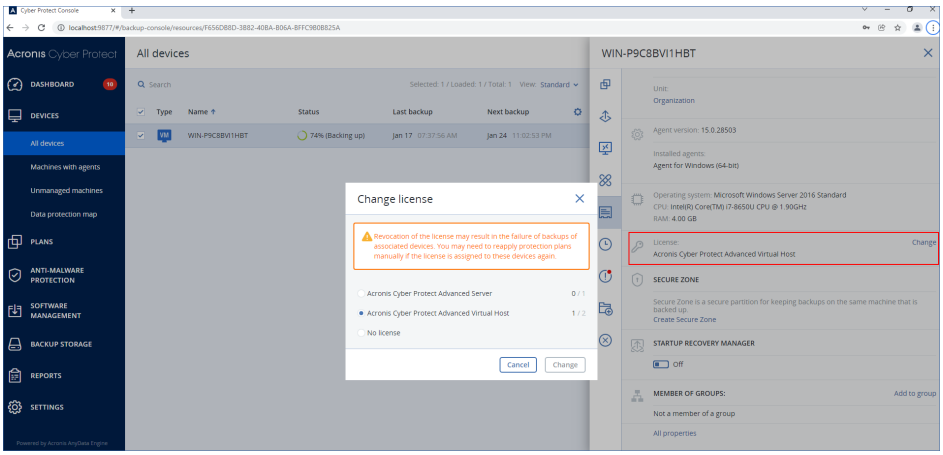
The management server assigns a license to a workload when you apply a protection plan to the workload for the first time. If more than one license is allocated to the management server, it assigns the most appropriate license, depending on the type of the workload, the operating system, and the required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

You can see the workload's license on the **Details** tab of the workload.

You can manually change an automatically assigned license. Manual operations with licenses are available only to organization administrators.

To change an automatically assigned license

1. In the Cyber Protect console, click **Devices**, and then select the workload.
2. Click **Details**.
3. [For on-premises management servers] Go to the **License** section, and then click **Change**.
4. [For cloud management servers] Go to the **Service quota** section, and then click **Change**.
5. Select the license (service quota) that you want to assign to the workload, 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, see this knowledge base article.

© Acronis International GmbH, 2003-2026

Unregistering a management server

You can unregister a management server and reuse the allocated licenses on another management server in your account.

After unregistering, the allocated licenses are released and you can manage them in the cloud console. The licenses are available on the **Settings** > **Management servers** tab, in the **Available licenses** section.

Unregistering an online management server

You can unregister an online management server by using the local console or the cloud console. Both procedures result in removing the management server from your account.

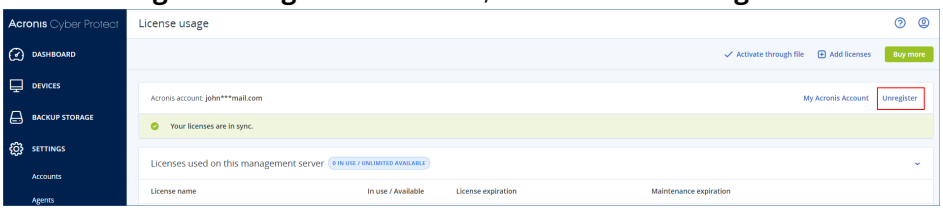
To unregister an online management server

From the local console

1. Log in to the local console of the management server that you want to unregister (`https://<IP>:<port>`).

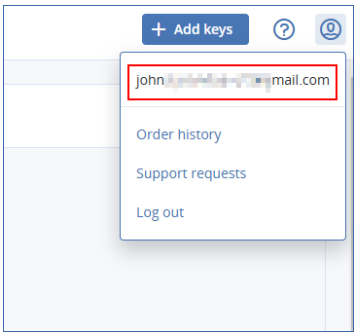
   `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.

2. Go to **Settings** > **Management servers**, and then click **Unregister**.



3. Specify the login for your Acronis account, and then click **Unregister**.

   This login is the email that you use to log in to your account at https://account.acronis.com and https://cloud.acronis.com.



As a result, all licenses that are allocated to this 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.

From the cloud console

© Acronis International GmbH, 2003-2026

1. Log in to the cloud console (https://cloud.acronis.com) as administrator.
2. Go to **Settings** > **Management servers**.
3. Navigate to the management server that you want to unregister, and then click **Unregister**.
4. Click **Unregister** to confirm your choice.

As a result, all licenses that are allocated to this 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.

Unregistering an offline management server

For this operation, you must use both the cloud and the local consoles.

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

To unregister an offline management server

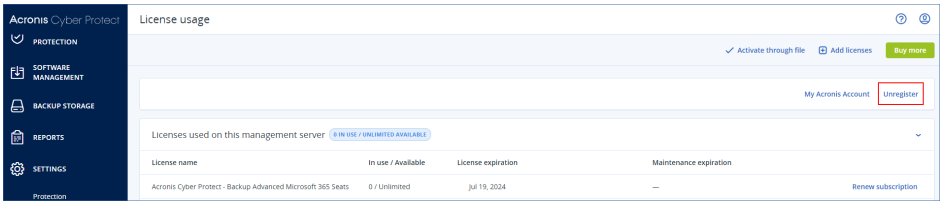
You can start the unregistration procedure from the local console or from the cloud console. Both procedures remove the management server from your account.

These procedures apply only to offline management servers that you can access. For more information, see "Unregistering an inaccessible offline management server" (p. 60).

From the local console

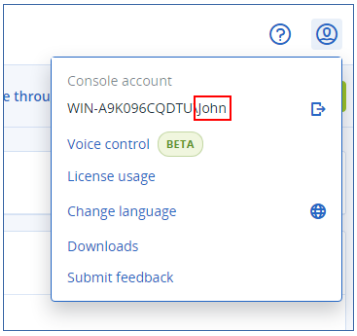
1. Log in to the local console of the management server that you want to unregister (`https://<IP>:<port>`).

   `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.
2. Go to **Settings** > **License usage**, and then click **Unregister**.



3. Specify your console account login, and then click **Unregister**.

   This login is the name that you use to log in to the local console.

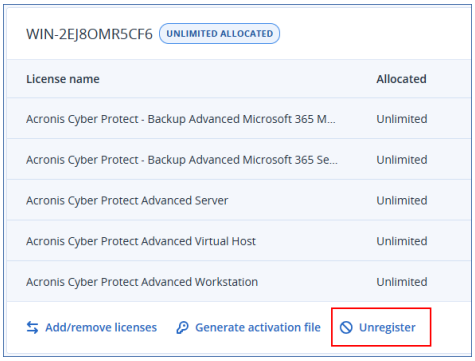


4. In the **Unregistration is successful** dialog, click **Download unregistration file**.

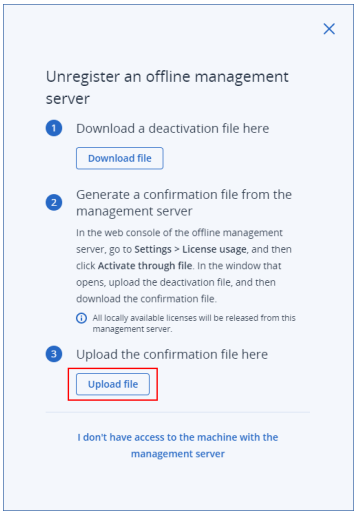
© Acronis International GmbH, 2003-2026

The `forced_deactivation_file.bin` file is downloaded to your machine.

5. Copy the `forced_deactivation_file.bin` file to a drive that you can use on the machine that is connected to the Internet. For example, you can use a USB flash drive.
6. On the machine that is connected to the Internet, log in to the cloud console (https://cloud.acronis.com).
7. Go to **Settings** > **Management servers**, and then find the management server that you want to unregister.
8. Click **Unregister**.



9. In the **Unregister an offline management server** dialog, under **Upload the confirmation file here**, click **Upload file**.



10. Upload the `forced_deactivation_file.bin` file.
11. In the **Management server has been unregistered** dialog, click **Close**.

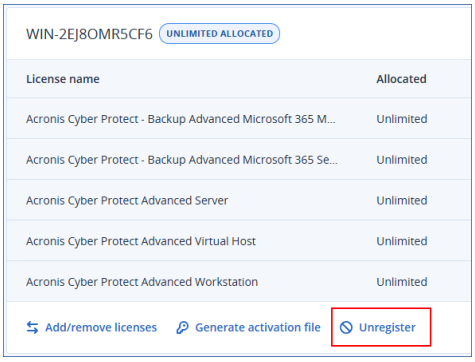
As a result, all licenses that are allocated to this server are released and can be allocated to another management server in your account. In the local console of the unregistered management server, the licenses are reset to zero.

From the cloud console

1. On the machine with Internet access, log in to the cloud console (https://cloud.acronis.com) as administrator.
2. Go to **Settings** > **Management servers**.

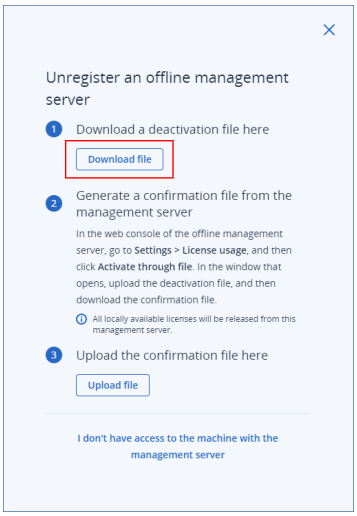
© Acronis International GmbH, 2003-2026

3. Go to the management server that you want to unregister, and then click **Unregister**.



4. In the **Unregister an offline management server** dialog, under **Download a deactivation file here**, click **Download file**.

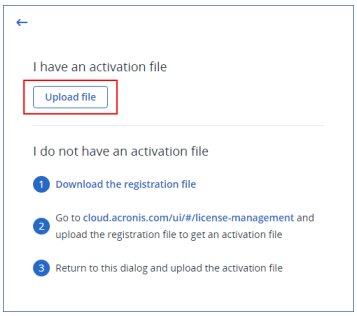
   The `deactivation_file.bin` file is downloaded to your machine.



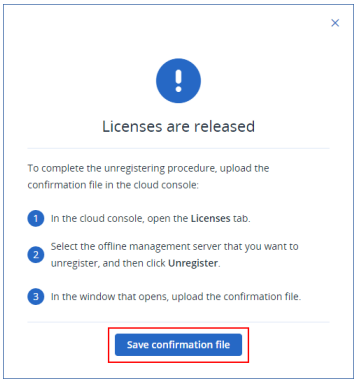
5. Keep the **Unregister an offline management server** dialog open.
6. Copy the `deactivation_file.bin` file to a drive that you can use on the offline management server. For example, you can use a USB flash drive.
7. On the offline management server that you want to unregister (`https://<IP>:<port>`), log in to the local console.

   `IP` is the address of your management server, and `port` is the port on which the Cyber Protect console is available. By default, this port is 9877.
8. Go to **Settings** > **License usage**, and then click **Activate through file**.
9. In the dialog that opens, under **I have an activation file**, click **Upload file**, and then select the `deactivation_file.bin` file.

© Acronis International GmbH, 2003-2026

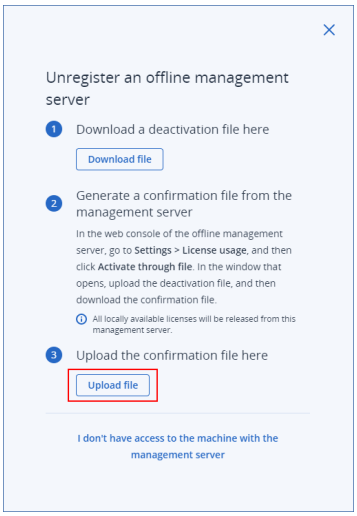


10. In the dialog that opens, click **Save confirmation file**.



The `confirmation_file.bin` file is downloaded to your machine.

11. Copy the `confirmation_file.bin` file to a drive that you can use on the machine that is connected to the Internet. For example, you can use a USB flash drive.
12. On the machine that is connected to the Internet, log in to the cloud console (https://cloud.acronis.com) as administrator.
13. [If the **Unregister an offline management server** dialog is not open] Go to **Settings** > **Management servers**, find the management server that you want to unregister, and then click **Unregister**.
14. In the **Unregister an offline management server** dialog, under **Upload the confirmation file here**, click **Upload file**.



15. Upload the `confirmation_file.bin` file.
16. In the **Management server has been unregistered**, click **Close**.

© Acronis International GmbH, 2003-2026

As a result, all licenses that are allocated to this 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.

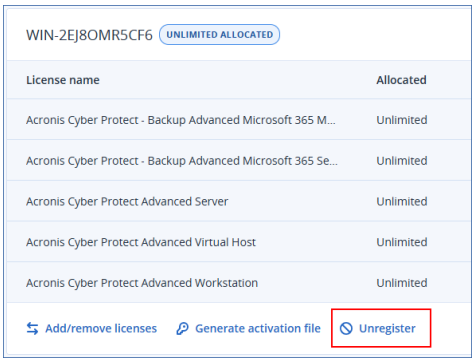
Unregistering an inaccessible offline management server

You can unregister an offline management server to which you do not have access.

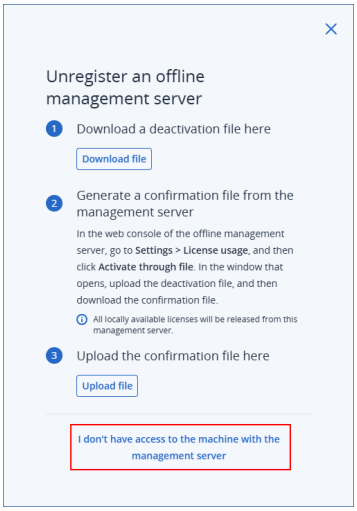
Warning!
This server will be permanently removed from your account and you will not be able to add it again.

To unregister an inaccessible offline management server

1. Log in to the cloud console (https://cloud.acronis.com) as administrator.
2. Go to **Settings** > **Management servers**, and then find the management server that you want to unregister.
3. Click **Unregister**.



4. In the **Unregister an offline management server** dialog, click **I don't have access to the machine with the management server**.



5. Specify your login for confirmation, and then click **Permanently block**.
   This login is the email that you use to log in to your account at https://account.acronis.com and https://cloud.acronis.com.
6. In the **Management server has been unregistered** dialog, click **Close**.

© Acronis International GmbH, 2003-2026

As a result, all licenses that are allocated to this 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.

This server is now blocked and you cannot add it to your account again.

© Acronis International GmbH, 2003-2026

Software requirements

Supported operating systems and environments

Supported operating systems for protection agents

The information below applies to backup and recovery.

Agent for Windows

- Windows 10 version 1809 and later – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server
  A server with up to 10 CPU cores takes a Windows Server Essentials license.
- Windows Server 2025 – all installation options, except for Nano Server
  A server with up to 10 CPU cores takes a Windows Server Essentials license.

Important
Before you upgrade the operating system of a protected workload where a protection agent or the management server is installed, note the following:

- In the case of a major version upgrade (for example, from Windows 7 to Windows 10), you must reinstall the agent or management server after the upgrade, to ensure its proper operation.
- In the case of a minor update within a major version (for example, Windows 10 version 20H2 to Windows 10 version 21H1), you do not need to reinstall the agent after updating the operating system.

Agent for Windows (Legacy)

- 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. To check the details and limitations of this support, see "Agent for Windows XP SP2" (p. 70).
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 and later – Standard and Enterprise editions (x86, x64)

© Acronis International GmbH, 2003-2026

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, see 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 and later – all editions (x86, x64)

Note
Before installing a protection agent, ensure that the following updates from Microsoft are installed:

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

For more information on the required updates, see 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 version 1803 and earlier – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2016 – all installation options, except for Nano Server

Note
* To use Cyber Protect with this version of Windows, you must install the SHA2 code signing support update from Microsoft (KB4474419) before installing the protection agent.

For information on issues related to the SHA2 code signing support update, see this knowledge base article.

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

These agents are delivered as part of Agent for Windows and Agent for Windows (Legacy).

© Acronis International GmbH, 2003-2026

Each of these agents is supported on the same Windows versions as Agent for Windows and Agent for Windows (Legacy), and can be installed on a machine running a supported version of the respective application, with the following exceptions:

- Agent for SQL is not supported for on-premises deployment on Windows 7 Starter and Home editions (x86, x64).
- Agent for SQL does not support Always On Availability Groups (AAG) on Windows Server 2025.
- Agent for Exchange does not support Database Availability Groups (DAG) on Windows Server 2025.

Agent for Exchange (for mailbox backup)

This agent is delivered as part of Agent for Windows and Agent for Windows (Legacy). 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
- Windows Server 2025 – all installation options, except for Nano Server

Agent for Office 365

This agent is delivered as part of Agent for Windows and Agent for Windows (Legacy).

- 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

© Acronis International GmbH, 2003-2026

- 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
- Windows Server 2025 – all installation options, except for Nano Server

Agent for Oracle

This agent is delivered as part of Agent for Windows, Agent for Windows (Legacy), and Agent for Linux (64-bit).

- 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

Cyber Protect supports 32-bit and 64-bit Linux distributions that use the following components:

- Kernel version from 2.6.9 to 7.0

  Supported kernel versions are listed according to the releases in www.kernel.org. Some distributions, such as Red Hat Enterprise Linux, backport new features to older kernel versions. Such distribution-specific kernels might not be supported even though their version is within the supported range.
- The GNU C library (glibc) 2.3.4 or later

The following distributions have been specifically tested. However, even if your Linux distribution or kernel version is not listed below, it might still work correctly in all required scenarios, due to the specifics of the Linux operating systems. If you encounter issues while using Cyber Protect with your combination of distribution and kernel version, contact the Support team for further investigation.

- 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*, 8.8*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*, 10*
- 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, 22.10, 23.04, 23.10, 24.04, 24.10, 25.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38, 39, 40, 41, 42
- 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.

© Acronis International GmbH, 2003-2026

- 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, 12
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*,9*
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.7*, 8.8*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6* – 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*, 8.6*, 8.7*, 8.8*, 8.10*, 9.4*, 9.5*, 9.6*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*
- Rocky Linux 8.0, 8.1, 8.2, 8.3, 8.4*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*
- 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.

* Starting from version 8.4, supported only with kernels 4.18 and later.

Important

Before you upgrade the operating system of a protected workload where the Cyber Protect agent or a management server is installed, note the following.

- In the case of a major version upgrade, you must reinstall the agent or the management server after the upgrade to ensure its proper operation.
- Before you install a new kernel version, check the "Agent for Linux" (p. 65) section to verify that the version is supported.

Agent for Mac

Both the x64 architecture and the ARM architecture (used in Apple silicon processors, such as Apple M1 or M2) are supported.

- 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
- macOS Sequoia 15

© Acronis International GmbH, 2003-2026

Note
The agent also supports all minor versions of the operating systems listed above, for example, macOS Sonoma 14.5.

Agent for VMware (Virtual Appliance)

This agent is delivered as a virtual appliance that runs 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 part of Agent for Windows and Agent for Windows (Legacy). This agent is supported on the same Windows versions as Agent for Windows and Agent for Windows (Legacy) with the following limitations:

- 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

This agent is delivered as part of Agent for Windows and Agent for Windows (Legacy).

- 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 11 – 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
- Windows Server 2025 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 runs on a Scale Computing HC3 host.

Scale Computing HyperCore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6

© Acronis International GmbH, 2003-2026

Agent for oVirt

This agent is delivered as a virtual appliance that runs on a KVM hypervisor host managed by oVirt.

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agent for Nutanix

This agent is delivered as a virtual appliance that runs in a Nutanix AHV cluster.

Nutanix Acropolis Operating System (AOS) 6.5, 6.6, 6.7, 6.8, 6.10

Agent for Synology

This agent is delivered as a virtual appliance that runs on a Synology NAS.

DiskStation Manager 6.2.x, 7.x

Agent for Synology supports only NAS devices with x86_64 processors. ARM processors are not supported. See the Synology knowledge center.

Agent for Virtuozzo

This agent is delivered as part of Agent for Linux (64-bit).

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Server 7.5

Supported operating systems for Management Server

Windows

- Windows 10 version 1809 and later – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server
  A server with up to 10 CPU cores takes a Windows Server Essentials license.
- Windows Server 2025 – all installation options, except for Nano Server
  A server with up to 10 CPU cores takes a Windows Server Essentials license.

© Acronis International GmbH, 2003-2026

Important
Before you upgrade the operating system of a protected workload where a protection agent or the management server is installed, note the following:

- In the case of a major version upgrade (for example, from Windows 7 to Windows 10), you must reinstall the agent or management server after the upgrade, to ensure its proper operation.
- In the case of a minor update within a major version (for example, Windows 10 version 20H2 to Windows 10 version 21H1), you do not need to reinstall the agent after updating the operating system.

Linux

Management Server can be installed on 64-bit Linux distributions that use the following components:

- Kernel version from 3.2 to 7.0

  Supported kernel versions are listed according to the releases in www.kernel.org. Some distributions, such as Red Hat Enterprise Linux, backport new features to older kernel versions. Such distribution-specific kernels might not be supported even though their version is within the supported range.
- The GNU C library (glibc) 2.3.4 or later

Management Server cannot be installed on 32-bit distributions.

The following distributions have been specifically tested. However, even if your Linux distribution or kernel version is not listed below, it might still work correctly in all required scenarios, due to the specifics of the Linux operating systems. If you encounter issues while using Cyber Protect with your combination of distribution and kernel version, contact the Support team for further investigation.

- Red Hat Enterprise Linux 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*, 10*
- Ubuntu 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, 22.10, 23.04, 23.10, 24.04, 24.10, 25.04
- Fedora 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38, 39, 40, 41, 42
- SUSE Linux Enterprise Server 12, 15

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

- Debian 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, 12
- CentOS 7.x, 8.x*
- CentOS Stream 8*,9*

© Acronis International GmbH, 2003-2026

- Oracle Linux 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.7*, 8.8*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6* – both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel
- CloudLinux 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.10*, 9.5*, 9.6*
- ClearOS 7.x
- AlmaLinux 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*, 8.8*, 8.9*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*
- Rocky Linux 8.0, 8.1, 8.2, 8.3, 8.4*, 8.10*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*, 9.6*
- 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, Acronis Cyber Protect will use the default location for storing secure keys, because the operating system does not provide D-Bus compatible location.

* Starting from version 8.4, supported only with kernels 4.18 and later.

Supported operating systems for Storage Node

- Windows 10 version 1809 and later – Home, Pro, Education, Enterprise, IoT Enterprise, and LTSC (formerly LTSB) editions
- Windows Server 2019 – all installation options, except for Nano Server
- Windows 11 – all editions
- Windows Server 2022 – all installation options, except for Nano Server
  A server with up to 10 CPU cores takes a Windows Server Essentials license.
- Windows Server 2025 – all installation options, except for Nano Server
  A server with up to 10 CPU cores takes a Windows Server Essentials license.

Supported operating systems for Cyber Protect Monitor

- With Agent for Windows
  - Windows 10 version 1809 and later
  - Windows Server 2019 and later
- With Agent for Windows (Legacy)
  - Windows 7 and later
  - Windows Server 2008 R2 and later
- With Agent for Mac
  - All macOS versions that are supported by Agent for Mac, except macOS 10.x and macOS 11.x.

Agent for Windows XP SP2

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

© Acronis International GmbH, 2003-2026

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. Newer 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. . 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:

© Acronis International GmbH, 2003-2026

- 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 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	All agents	+	+	+	
ext2/ext3/ext4	All agents	+	+	-	
HFS+	Agent for Mac	-	-	+	
APFS	Agent for Mac	-	-	+	• 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.

© Acronis International GmbH, 2003-2026

JFS	Agent for Linux	-	+	-	• File filters are not supported • Fast incremental/ differential backup cannot be enabled
ReiserFS3	Agent for Linux	-	+	-	
ReiserFS4	Agent for Linux	-	+	-	• File filters are not supported • Fast incremental/ differential backup cannot be enabled • Volumes cannot be resized during a recovery
ReFS	All agents	+	+	+	• File filters are not supported • Fast incremental/ differential backup cannot be enabled • Volumes cannot be resized during a recovery • During a file recovery from a ReFS backup, only the content is recovered. Access-control lists (ACL) and alternate streams are not recovered. Sparse files are recovered as regular files.

© Acronis International GmbH, 2003-2026

XFS	All agents	+	+	+	• File filters are not supported • 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 • Recovery of a machine that has XFS volumes completes with the "Failed to process the boot loader configuration" warning. The machine is bootable despite the warning.
Linux swap	Agent for Linux	-	+	-	No limitations
exFAT	All agents	+	+ Bootable media cannot be used for recovery if the backup *is stored on* exFAT	+	• Only disk/volume backup is supported • File filters are not supported • Individual files cannot be recovered from a backup

© Acronis International GmbH, 2003-2026

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.

Supported operations with logical volumes

Backup and recovery of workloads with logical volumes, such as LDM in Windows (dynamic disks) and LVM in Linux, are supported with the following limitations.

Backup

Agent-based backup is a backup created by a protection agent that is installed on the workload or by a bootable media.

Agentless backup is available only for virtual machines. The agentless backup is performed on the hypervisor level by agent that can back up and recover all virtual machines in the environment. No individual agents are installed on the protected virtual machines.

For more information about the differences between agent-based and agentless backup, see "Agent-based and agentless backup" (p. 36).

Agent-based backup	Agentless backup
• Logical volumes are backed on per volume basis. • File filters (Inclusions/Exclusions) are supported.	• When a logical volume is detected on a disk, the disk is backed up in the sector-by-sector (RAW) mode. The partition structure of the disk is not analyzed and no volume images are stored separately.

© Acronis International GmbH, 2003-2026

Agent-based backup	Agentless backup
	• Individual LDM or LVM volumes cannot be selected as backup source – neither by direct selection nor by using policy rules. Only **Entire machine** is available in the **What to back up** section of a protection plan. • File filters (Inclusions/Exclusions) are not supported. Any configured inclusions or exclusions will be ignored.

Recovery

Agent-based recovery is a recovery performed by an agent that is installed on the workload or by a bootable media.

Agentless recovery supports only virtual machines as targets. The agentless recovery is a performed on the hypervisor level by agent that can back up and recover all virtual machines in the environment. You do not have to create manually a target machine to which the backup is recovered.

	From agent-based backup	From agentless backup
Agent-based recovery	• Per-volume recovery is available. • File and folder recovery is available.	• Per-volume recovery is not available. • File and folder recovery is available.

Agentless recovery	• Machine migration (P2V, V2P, and V2V) is not supported. To recover data from an agent-based backup, use bootable media.
	• The **Run as VM** operation is not supported.
	• File and folder recovery is available.
		• Per-volume recovery is not available.
		• Entire machine recovery is available.
		• File and folder recovery is available.
		• The **Run as VM** operation is supported. To make the virtual machine bootable, you might need to change the boot order. For more information, see this knowledge base article.
		• Conversion to the following types of virtual machine is supported:
		  ◦ VMware ESXi
		  ◦ Microsoft Hyper-V
		  ◦ Scale Computing HC3

Supported web browsers

The web interface supports the following web browsers:

- Google Chrome 109 or later
- Microsoft Edge 109 or later

© Acronis International GmbH, 2003-2026

- Mozilla Firefox 115 or later
- Opera 95 or later

In other web browsers, the user interface might be displayed incorrectly or some functions might be unavailable.

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 Subscription Edition (SE)
- 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

The following Microsoft SharePoint versions are supported:

- 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.

© Acronis International GmbH, 2003-2026

Supported Oracle Database versions

- Oracle Database version 11g, all editions
- Oracle Database version 12c, all editions
- Oracle Database version 19c, all editions
- Oracle Database version 21c, 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.
- HANA 2.0 SPS 03 installed in SUSE 15 with XFS file system.

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 tables summarize how various virtualization platforms are supported.

For more information about the differences between the agent-based and agentless backup, see "Agent-based and agentless backup" (p. 36).

Note
If you use a virtualization platform or version that is not listed below, the **Agent-based backup (Backup from inside a guest OS)** method should still work correctly in all required scenarios. If you encounter issues with the agent-based backup, contact the Support team for further investigation.

VMware (Broadcom)

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based 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* VMware vSphere Essentials Plus* VMware vSphere Standard*	Supported **Devices** > **Add** > **Virtualization hosts** > **VMware ESXi** > **Agent for installation in Windows** or	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

 © Acronis International GmbH, 2003-2026

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	**Devices** > **Add** > **Virtualization hosts** > **VMware ESXi** > **Virtual appliance (OVF)**	
VMware vSphere Hypervisor (Free ESXi)**	Not supported	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
VMware Server (VMware Virtual server) VMware Workstation VMware ACE VMware Player	Not supported	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

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

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

Note

Cyber Protect 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. That is, vSphere 8.0 Update 1 is also supported along with originally released vSphere 8.0.

Support for specific VMware vSphere version means that vSAN of the corresponding version is also supported. For example, support for vSphere 8.0 means that vSAN 8.0 is also supported.

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.

© Acronis International GmbH, 2003-2026

- **Independent disks and RDM**

  Agent for VMware does not back up Raw Device Mapping (RDM) disks in physical compatibility mode or independent disks. The agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding independent disks and RDMs in physical compatibility mode from the 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 a backup without a warning. If you want to back up these volumes or data on these volumes, install an agent in the guest operating system.
- **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**
  - VMware virtual machines: (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. This limitation applies to VMware.
  - Hyper-V virtual machines: For all Generation 2 virtual machines, Secure Boot is disabled after the machine is recovered to both new virtual machine or an existing virtual machine.
- **ESXi configuration backup** is not supported for VMware vSphere 7.0 or later.
- **Virtual machines with empty Instance UUID do not appear in the Cyber Protect console**

  VMware virtual machines with an empty `Instance UUID` vSphere property (`vc.uuid`) are not listed in the Cyber Protect console. For more information on how to resolve this issue, see this knowledge base article.
- **Network settings on the protection agent**

  A backup of a VMware virtual machine can fail if the protection agent cannot resolve the name of the ESXi host registered in vCenter to an IP address, even if the vCenter host name can be resolved. The following error is shown: "You do not have access rights to this file."

© Acronis International GmbH, 2003-2026

To resolve the issue, edit the network settings of the protection agent, by configuring the DNS or modifying the `/etc/hosts` file. To verify the fix, on the machine with the protection agent, run the following command:

```
ping <ESXi host name>
```

- **Supported operations for machines with logical volumes**

  Backup and recovery of workloads with logical volumes, such as LDM in Windows (dynamic disks) and LVM in Linux, are supported with some limitations. For more information about the limitations, see "Supported operations with logical volumes" (p. 75).

Public clouds

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Amazon EC2 instances	Not supported	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Microsoft Azure virtual machines	Supported only with the cloud deployment mode **Devices** > **Add** > **Microsoft Azure virtual machines**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

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	Agentless backup (Backup at the hypervisor level)	Agent-based 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	Supported **Devices** > **Add** > **Virtualization hosts** > **Hyper-V**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

© Acronis International GmbH, 2003-2026

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) with Hyper-V Windows 10 with Hyper-V Windows 11 with Hyper-V 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 Windows Server 2025 with Hyper-V – all installation options, except for Nano Server		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	Not supported	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Microsoft Virtual Server 2005	Not supported	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

Note
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.

© Acronis International GmbH, 2003-2026

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 a backup without a warning. If you want to back up these volumes or data on these volumes, install an agent in the guest operating system.
- **Dependency on the Microsoft WMI subsystem**
  Agentless backups of Hyper-V virtual machines depend on the Microsoft WMI subsystem, and in particular on the `Msvm_VirtualSystemManagementService` class. If the WMI queries fail, the backups will also fail. For more information about the `Msvm_VirtualSystemManagementService` class, see the Microsoft documentation.
- **Virtual machines with PMEM disks**
  Backup of Hyper-V virtual machines that have persistent memory (PMEM) disks is not supported.
- **Cross-platform recovery**
  If Agent for Hyper-V recovers a backup, which is created by another agent, as a new Hyper-V virtual machine, the resulting machine is Generation 1.
- **Secure Boot**
  To guarantee the booting up of Generation 2 Hyper-V virtual machines that are recovered to their original location, Secure Boot is disabled. You can re-enable it manually in the Hyper-V management tool. For more information about Secure Boot and Generation 2 virtual machines, see the Microsoft documentation.
- **Crash-consistent backups of Linux virtual machines**
  Backups of Linux virtual machines running on a Hyper-V 2019 host fail over to crash-consistent snapshots, due to a Microsoft limitation (inability to create production checkpoints for Linux virtual machines). To avoid warnings during a backup, disable the VSS for Virtual Machines backup option in the protection plan.
- **Running a virtual machine from a backup**
  Running a virtual machine from a backup on a Hyper-V host fails if the backup is located on the same volume as the path selected for the mounted VM disks. To resolve the issue, select a

© Acronis International GmbH, 2003-2026

different volume for the path of the mounted VM disks. The space will be used only for changes generated inside the mounted virtual machine, and will not take the entire size of the virtual disk.

- **Supported operations for machines with logical volumes**

  Backup and recovery of workloads with logical volumes, such as LDM in Windows (dynamic disks) and LVM in Linux, are supported with some limitations. For more information about the limitations, see "Supported operations with logical volumes" (p. 75).

Scale Computing

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Scale Computing HyperCore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6	Supported **Devices** > **Add** > **Virtualization hosts** > **Scale Computing HC3**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

Limitations

- Backup of replicated virtual machines

  Virtual machines that are replicated by the native Scale Computing VM replication feature cannot be backed up.

- **Supported operations for machines with logical volumes**

  Backup and recovery of workloads with logical volumes, such as LDM in Windows (dynamic disks) and LVM in Linux, are supported with some limitations. For more information about the limitations, see "Supported operations with logical volumes" (p. 75).

Proxmox VE

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Proxmox VE 7.x, 8, and 8.1	Not supported	Supported only for fully virtualized (HVM) guests. Paravirtualized (PV) guests are not supported. **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Proxmox VE 8.2, 8.3, 8.4, 9.0	Supported	Supported only for fully

© Acronis International GmbH, 2003-2026

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
	Devices > **Add** > **Virtualization hosts** > **Proxmox VE**	virtualized (aka HVM) guests. Paravirtualized (aka PV) guests are not supported. **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

Citrix Hypervisor/XenServer

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Citrix Hypervisor/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, 8.0, 8.1, 8.2	Not supported	Supported only for fully virtualized (aka HVM) guests. Paravirtualized (aka PV) guests are not supported. **Devices** > **Add** > **Virtualization hosts** > **Citrix Hypervisor/XenServer** > **Windows** or **Linux**

Red Hat and Linux

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based 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	Not supported	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Red Hat Virtualization (managed by oVirt) 4.2, 4.3, 4.4, 4.5	Supported **Devices** > **Add** > **Virtualization hosts** > **Red Hat Virtualization (oVirt)**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

© Acronis International GmbH, 2003-2026

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Kernel-based Virtual Machines (KVM)	Not supported	Supported **Devices** > **Add** > **KVM** > **Windows** or **Linux**
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	Supported **Devices** > **Add** > **Virtualization hosts** > **Red Hat Virtualization (oVirt)**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Kernel-based Virtual Machines (KVM) managed by oVirt 4.4 running on Red Hat Enterprise Linux 8.x or CentOS Stream 8.x	Supported **Devices** > **Add** > **Virtualization hosts**> **Red Hat Virtualization (oVirt)**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Kernel-based Virtual Machines (KVM) managed by oVirt 4.5 running on Red Hat Enterprise Linux 8.x or CentOS Stream 8.x	Supported **Devices** > **Add** > **Virtualization hosts** > **Red Hat Virtualization (oVirt)**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

Limitations

Supported operations for machines with logical volumes

Backup and recovery of workloads with logical volumes, such as LDM in Windows (dynamic disks) and LVM in Linux, are supported with some limitations. For more information about the limitations, see "Supported operations with logical volumes" (p. 75).

Parallels

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Parallels Workstation	Not supported	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Parallels Server 4 Bare Metal	Not supported	Supported **Devices** > **Add** > **Workstations**

© Acronis International GmbH, 2003-2026

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
		or **Servers** > **Windows** or **Linux**

Oracle

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Oracle Linux Virtualization Manager (based on oVirt)* 4.3	Supported only with the cloud deployment mode **Devices** > **Add** > **Virtualization hosts** > **Oracle LVM (oVirt)**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Oracle VM Server 3.0, 3.3, 3.4	Not supported	Supported only for fully virtualized (aka HVM) guests. Paravirtualized (aka PV) guests are not supported. **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Oracle VM VirtualBox 4.x	Not supported	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

*Oracle Linux Virtualization Manager is supported by Agent for oVirt.

Limitations

Supported operations for machines with logical volumes

Backup and recovery of workloads with logical volumes, such as LDM in Windows (dynamic disks) and LVM in Linux, are supported with some limitations. For more information about the limitations, see "Supported operations with logical volumes" (p. 75).

© Acronis International GmbH, 2003-2026

Nutanix

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Nutanix Acropolis Operating System (AOS) 6.5, 6.6, 6.7, 6.8, 6.10	Supported **Devices** > **Add** > **Virtualization hosts** > **Nutanix AHV**	Supported **Devices** > **Add** > **Virtualization hosts** > **Nutanix AHV** > **Windows** or **Linux**

Virtuozzo Server

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Supported **Devices** > **Add** > **Virtualization hosts** > **Virtuozzo**	Supported for virtual machines only. Containers are not supported. **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Virtuozzo 7.0.13, 7.0.14	Supported for ploop containers only. Virtual machines are not supported. **Devices** > **Add** > **Virtualization hosts** > **Virtuozzo**	Supported for virtual machines only. Containers are not supported. **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**
Virtuozzo Server 7.5	Supported **Devices** > **Add** > **Virtualization hosts** > **Virtuozzo**	Supported for virtual machines only. Containers are not supported. **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

Limitations

Supported operations for machines with logical volumes

© Acronis International GmbH, 2003-2026

Backup and recovery of workloads with logical volumes, such as LDM in Windows (dynamic disks) and LVM in Linux, are supported with some limitations. For more information about the limitations, see "Supported operations with logical volumes" (p. 75).

Cyber Frame / Virtuozzo Infrastructure

Platform	Agentless backup (Backup at the hypervisor level)	Agent-based backup (Backup from inside a guest OS)
Cyber Frame / Virtuozzo Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0, 6.1, 6.2, 6.3, 7.0, 7.1, 7.2, 7.3	Supported only with the cloud deployment mode **Devices** > **Add** > **Virtualization hosts** > **Cyber Frame**	Supported **Devices** > **Add** > **Workstations** or **Servers** > **Windows** or **Linux**

Limitations

- **Agentless backup of VMs with disks on an external iSCSI storage**
  You can back up virtual machines from Virtuozzo Infrastructure even when virtual disks are stored on external iSCSI volumes that are attached to the VHI cluster. Because Change Block Tracking (CBT) is not supported for these disks and each disk must be read to detect changes, incremental backups might take longer. However, the resulting backup size remains small.
- **Supported operations for machines with logical volumes**
  Backup and recovery of workloads with logical volumes, such as LDM in Windows (dynamic disks) and LVM in Linux, are supported with some limitations. For more information about the limitations, see "Supported operations with logical volumes" (p. 75).

Linux packages required for installation of agents and management server in Linux

To add the necessary modules to the Linux kernel, the agent installer 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.

 © Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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

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

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

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

For other Linux distributions, see 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:

© Acronis International GmbH, 2003-2026

- 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.

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

When recovering an encrypted machines, a restart is required. For more information, see "Recovery with restart" (p. 540).

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

You can use Dell EMC Data Domain devices as backup storage.

With this storage, we recommend that you use a backup scheme that regularly creates full backups, for example **Always full**. To learn more about the available backup schemes, see "Backup schemes" (p. 364).

Retention lock

Retention lock (Governance mode) is supported. If retention lock is enabled on the Data Domain storage, you must add the `AR_RETENTION_LOCK_SUPPORT` environment variable to the machine with the protection agent that uses this storage as a backup destination. For more information, see "Adding the AR_RETENTION_LOCK_SUPPORT variable" (p. 95).

 © Acronis International GmbH, 2003-2026

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

If retention lock is enabled on the Data Domain storage, the backups on the storage will not be deleted by the retention rules in the protection plan. No error will be shown. The backups will be deleted when the retention lock expires and the retention rules are applied again.

Depending on the configuration of the protection plan, retention rules are applied to an archive before or after a backup.

Adding the AR_RETENTION_LOCK_SUPPORT variable

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

To add the `AR_RETENTION_LOCK_SUPPORT` environment variable

In Windows

1. Log in as administrator to the machine with the protection agent.
2. In **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.

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.

In a virtual appliance

1. Log in as administrator to the virtual appliance.
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:

© Acronis International GmbH, 2003-2026

```
export AR_RETENTION_LOCK_SUPPORT=1
```

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

© Acronis International GmbH, 2003-2026

Installation

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	1.2 GB	150 MB
Agent for Windows and one of the following agents: • Agent for SQL • Agent for Exchange	1.3 GB	170 MB
Agent for Windows and one of the following agents: • Agent for VMware (Windows) • Agent for Hyper-V	1.5 GB	180 MB
Agent for Office 365	0.5 GB	170 MB
Agent for Linux	2 GB	130 MB
Agent for Mac	1 GB	150 MB
For on-premises deployments only		
Management Server in Windows	10.5 GB	700 MB + 2.3 MB per connected agent
Management Server in Linux	4 GB	700 MB + 2.3 MB per connected agent
Management Server and Agent for Windows	11 GB	860 MB + 2.3 MB per connected agent
Management Server and Agent for Linux	6 GB	840 MB + 2.3 MB per connected agent

© Acronis International GmbH, 2003-2026

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 archives (4 TB and more).

On x64 systems, operations with bootable media and disk recovery with restart require at least 1.5 GB of memory.

A management server with one registered agent uses about 702 MB of memory. Each additional agent adds about 2.3 MB. Thus, a server with 100 registered agents consumes approximately 930 MB above the operating system and running applications.

You can register up to 1000 agents on a management server that uses the embedded SQLite database.

You can register up to 8000 agents without significant performance degradation on a management server that uses an external Microsoft SQL Server database. With 8000 registered agents, the SQL Server instance will consume about 8 GB of RAM.

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

Firewall configuration

If your environment is protected by a firewall, the following network ports must be open.

If an outbound port is opened on machine with an Acronis component, ensure that the same port is opened as inbound on the destination machine. For example, if you back up data to a NAS device, TCP port 445 must be open for outbound connections on the machine with the protection agent. On the NAS device, TCP port 445 must be open for inbound connections.

If not stated otherwise, all ports are TCP. Local ports that are used by the Cyber Protect services are not listed.

Inbound ports

Common scenarios		
Scenario	**Machine with Management Server**	**Machine with protection agent**
Base scenario (Required for all other scenarios)	9877, 7780	-

© Acronis International GmbH, 2003-2026

Common scenarios		
Scenario	**Machine with Management Server**	**Machine with protection agent**
Patch management	-	18018, 6888
Remote commands via `acrocmd`	9861	9860

Remote installation of agents		
Machine with Management Server	**Machine with the deployment agent**	**Machine on which the protection agent will be installed**
No additional ports are required. Ports 9877 and 7780 from the base scenario are used.	No additional ports are required.	445

VMware scenarios	
Scenario	**Machine with protection agent**
Running a virtual machine from a backup (Instant Restore)	2029
VM replication (when Agent for VMware (Virtual Appliance) is running on the ESXi host or cluster that is the target for VM replication)	3333

PXE server scenario	
Scenario	**Machine with the Acronis PXE component**
Booting a machine by using bootable media from a PXE server	24399 (TCP and UDP), 67, 69, 4011

Acronis Storage Node scenarios	
Scenario	**Machine with Acronis Storage Node**
Backup to Acronis Storage Node	9876, 9862
Remote commands via `acrocmd`	9862

© Acronis International GmbH, 2003-2026

Acronis Cyber Infrastructure scenario	
Scenario	**Machine with Acronis Cyber Infrastructure**
Backup to locally deployed Acronis Cyber Infrastructure	44445, 8888, 44440

Centralized Dashboard scenario	
Scenario	**Machine with Centralized Dashboard**
Management server on which Centralized Dashboard is installed with default configuration	9877

Outbound ports

Management scenarios		
Scenario	**Machine with Management Server**	**Machine with protection agent**
Base scenario (Required for all other scenarios)	443	9877, 7780
Send email notifications	Ports used by your SMTP server, such as 25, 465, 587	-
Syncing subscriptions Syncing vulnerability assessment and patch management databases Syncing anti-malware definitions Downloading and installing components Threat feed alerts	443, 80	80, 443 – Syncing vulnerability assessment and patch management databases 80 – Updating Active protection configuration 443 – Syncing anti-malware definitions

Remote installation of agents		
Machine with Management Server	**Machine with the deployment agent**	**Machine on which the protection agent will be installed**
No additional ports are required.	445 (to the machine on which the agent will be installed)	No additional ports are required. Ports 9877 and 7780 from the base scenario are used.

© Acronis International GmbH, 2003-2026

VMware scenarios		
Scenario	**Machine with Management Server**	**Machine with protection agent**
Deploying Agent for VMware (Virtual appliance)	443, 902	-
Backup of VMware data	-	443, 902
Management operations, such as create, update, and delete virtual machines on vSphere during backup, recovery, and VM replication	-	443
Read/write data on VM disks during backup, recovery, and VM replication (for NFC connections)	-	902
Running a virtual machine from a backup (Instant Restore)	-	2029
VM replication (when Agent for VMware (Virtual Appliance) is running on the ESXi host or cluster that is the target for VM replication)	-	3333

Backup destination scenarios			
Scenario	**Machine with Management Server**	**Machine with protection agent**	**Machine with Acronis Storage Node**
Backup to Acronis Storage Node	-	9876, 9862	9877, 7780
Backup to an Acronis Storage Node vault on a network share or NAS	-	9876, 9862	9877, 7780, 445
Backup to a network share or NAS	-	445	-
Backup to a NFS server	-	TCP, UDP 111 TCP, UDP 2049	-
Backup to a SFTP server	44445, 8888	22	-
Backup to Acronis Cloud or locally deployed Acronis Cyber Infrastructure	443	44445, 443	-
Backup to public clouds	-	80, 443	-

© Acronis International GmbH, 2003-2026

Centralized Dashboard scenario	
Scenario	**Management server that is registered to Centralized Dashboard**
Management server which is registered to Centralized Dashboard with default configuration	9877

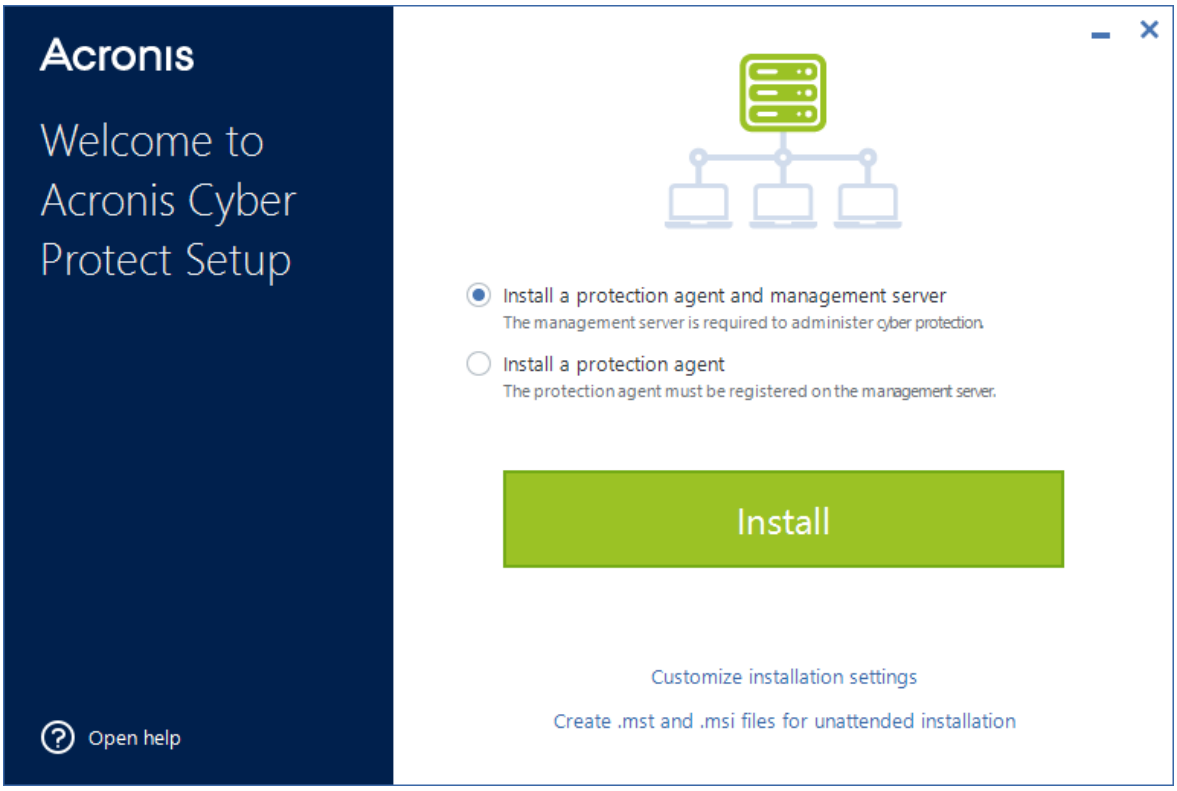
Installing the management server

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

Installing the management server 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:

© Acronis International GmbH, 2003-2026

- 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, see "Customizing installation settings" (p. 103).
- 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, see "Deploying protection agents through Group Policy" (p. 150).

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. See "Activating a management server" (p. 42).

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:

Component	Management server and protection agent	Protection agent only
Management Server	+	-
Components for Remote Installation	+	-
Agent for Windows	+	+

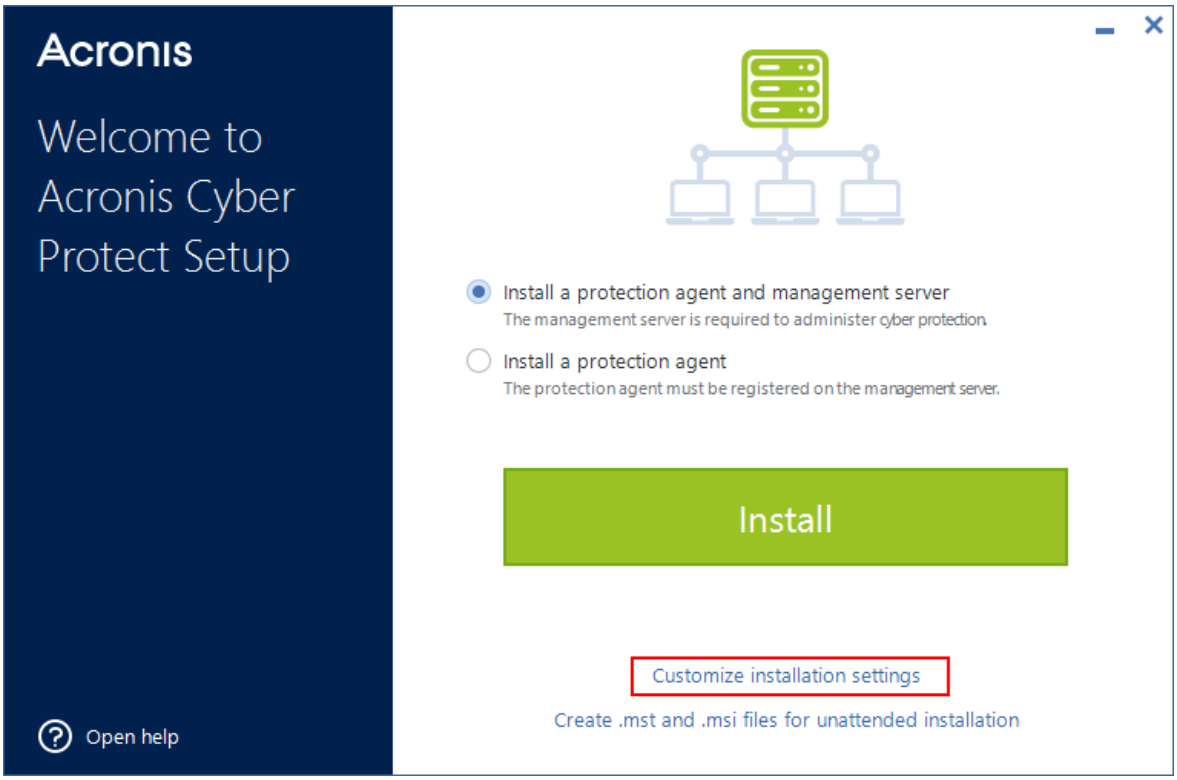
© Acronis International GmbH, 2003-2026

Component	Management server and protection agent	Protection agent only
Bootable Media Builder	+	+
Command-Line Tool	+	+
Cyber Protect Monitor	+	+

For the full list of available components, see "Components" (p. 27).

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:

© Acronis International GmbH, 2003-2026

- **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, see 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.

© Acronis International GmbH, 2003-2026

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

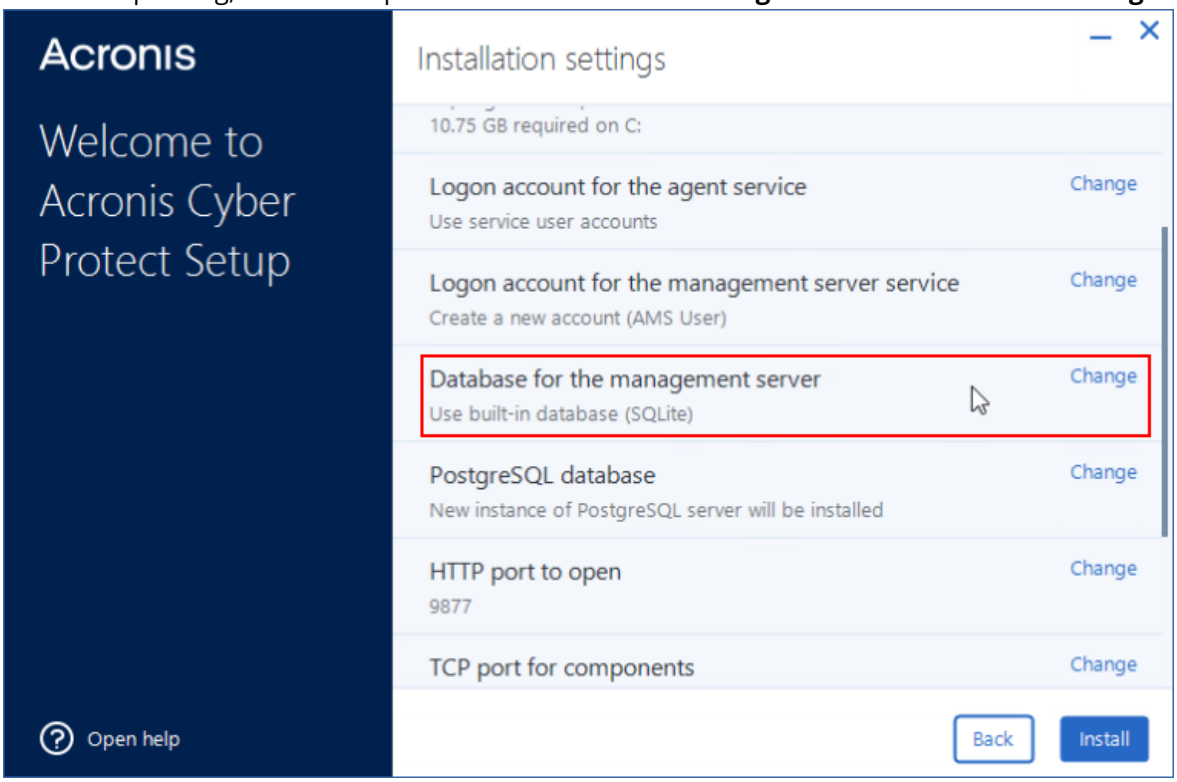
  Microsoft SQL allows registering up to 8000 workloads on the management server, without significant performance degradation. The same Microsoft SQL instance can be used by the management server, by the Scan Service, and by other programs.

  The following MS SQL Server versions are supported:
  - Microsoft SQL Server 2022 (running in Windows)
  - 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

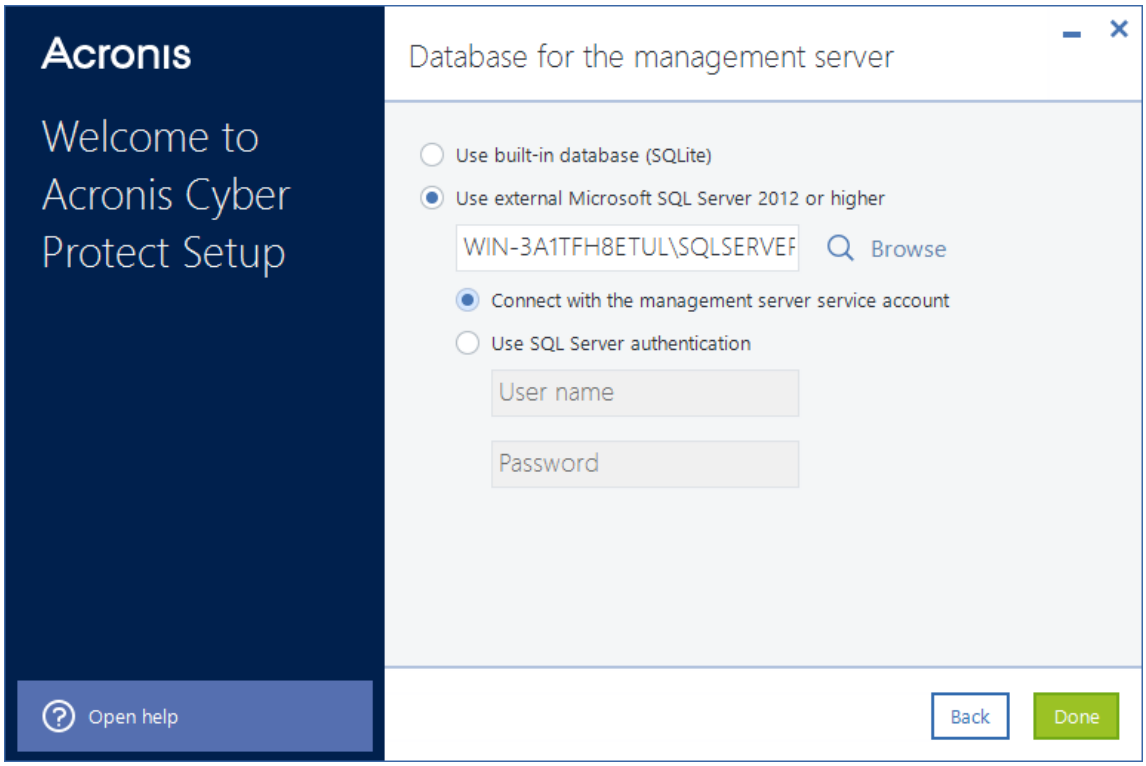
© Acronis International GmbH, 2003-2026

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

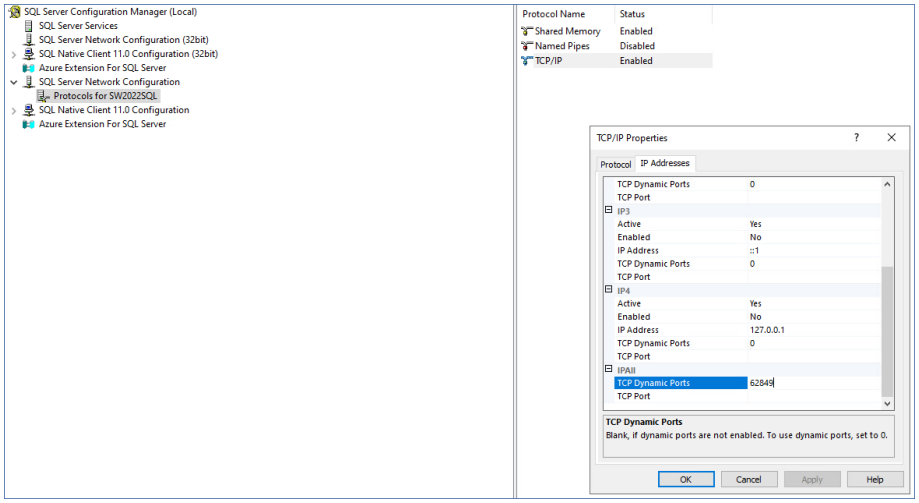


2. Select **Use external Microsoft SQL Server 2012 or higher** and specify the domain name or address of the Microsoft SQL server.
   - If you are connecting to the default Microsoft SQL instance on the server (**MSSQLSERVER**), you can specify only the domain name of the machine where it runs. If the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

© Acronis International GmbH, 2003-2026



- 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, see 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

© Acronis International GmbH, 2003-2026

specified account must follow the format `<MACHINE NAME>\Administrator` and must have the **sysadmin** role in Microsoft SQL Server.

For more information about the logon account, see "Service logon account" (p. 104).

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

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

Configuring a PostgreSQL instance

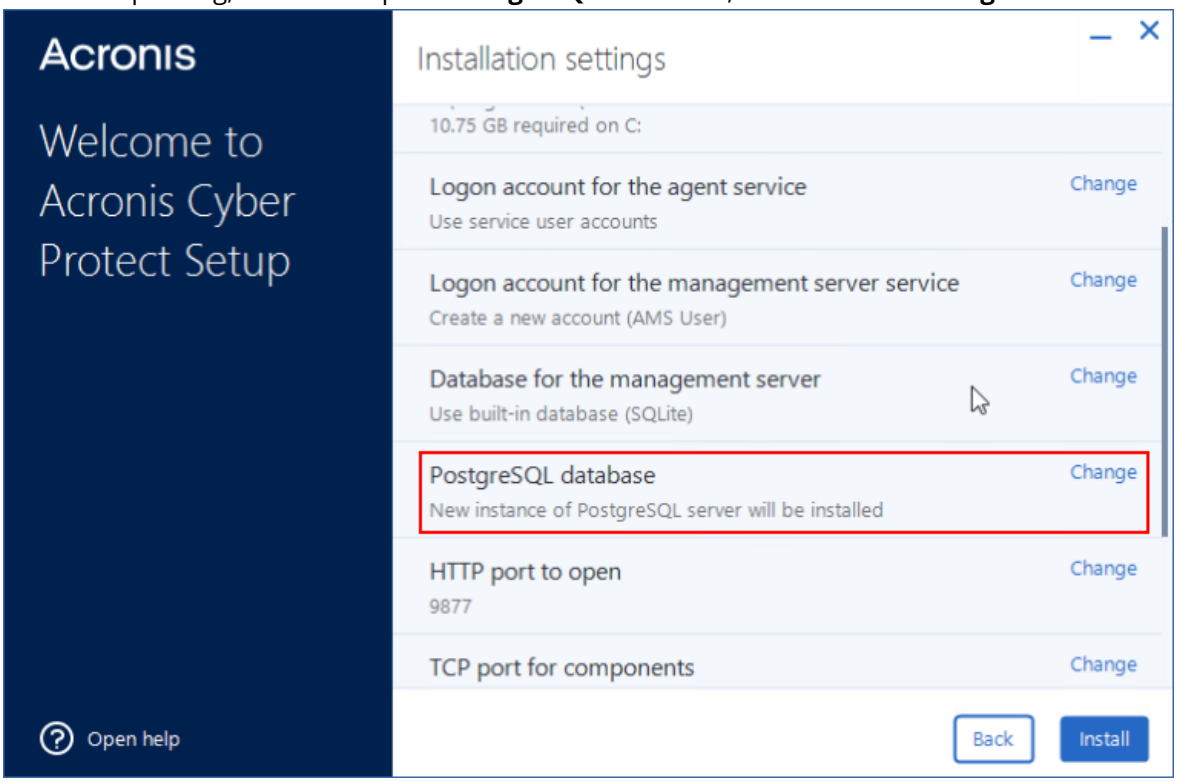
Acronis Cyber Protect 17 requires a PostgreSQL instance, which is used by the Settings Service and the DeviceSense component.

By default, a new instance of PostgreSQL version 16 is installed and automatically configured during the management server installation.

Alternatively, you can use an existing instance of PostgreSQL 14 or later. In this case, it is your responsibility to configure the database, configure high availability, and monitor the system.

To use the management server with an existing PostgreSQL instance

1. In the setup dialog, locate the option **PostgreSQL database**, and then click **Change**.



2. Select **Use existing PostgreSQL instance**, and then specify the following:
   - IP address or hostname of the instance, and its port.
   - Credentials for the account that will be used to connect to the database.

   Important
   This account must have the CREATEDB and CREATEROLE privileges.

© Acronis International GmbH, 2003-2026

3. Click **Done**.
4. Finish the installation of the management server as described in "Installing the management server in Windows" (p. 102).

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, see "To install optional components" (p. 104).

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 PostgerSQL database. For more information about how to choose one, see "Database for Scan Service" (p. 110).

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.

© Acronis International GmbH, 2003-2026

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.

Installing the Centralized Dashboard component

With Centralized Dashboard, you can monitor the management servers of your organization from a single console.

The Centralized Dashboard component is not installed if you run the setup program with default installation settings, and requires a Microsoft SQL Server database. Therefore, to install this component, you must customize the installation settings. You can do that together with the installation of the Management Server component, or separately after the Management Server component is already installed on the machine.

Prerequisites

- The machine on which you will install the Centralized Dashboard component is running a Windows Server 64-bit operating system.

To install the Central Dashboard component

© Acronis International GmbH, 2003-2026

1. In the installation wizard, in the **Installation settings** window, in the **What to install** section, click **Change**.
2. Select **Centralized Dashboard**, and then click **Done**.
3. In **Database for the management server**:
   a. Click **Specify**.
   b. Select **Use external Microsoft SQL Server 2012 or higher**.
   c. Enter the machine name and instance, or click **Browse** to select the database instance.

      If the Microsoft SQL instance is the default one, **MSSQLSERVER**, you can specify only the 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`.

      Note
      Ensure that 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, see http://msdn.microsoft.com/en-us/library/ms189093.aspx. You can enable the TCP/IP protocol by using a similar procedure.

   d. Select an authentication method to connect to the specified Microsoft SQL Server 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 by using the **Use the following account** option, for example by specifying `<MACHINE NAME>\Administrator`. The specified account must have the **dbcreator** or **sysadmin** role in Microsoft SQL Server.

        For more information about the logon account, see "Service logon account" (p. 104).
      - SQL Server authentication

        You can always use this method. The specified account must have the **dbcreator** or **sysadmin** role in Microsoft SQL Server.
   e. Click **Done**.
4. Click **Install**.

   The Centralized Dashboard is installed. You can access the web console by using the URL https://<domain_name_or_ip_address>:<port>/superset, or by using the shortcut icon on the Desktop. By default, the Centralized Dashboard component uses port 9877 for incoming traffic.

   The widgets of the Centralized Dashboard will be empty until you connect at least one management server to the Centralized Dashboard. For more information about connecting a management server to the Central Dashboard, see "Registering a management server to the Centralized Dashboard" (p. 197).

© Acronis International GmbH, 2003-2026

Installing the management server in Linux

Preparation

1. If you want to install Agent for Linux together 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, see this knowledge base article.

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. Select the components that you want to install, and then click **Next**.

   By default, the following components are installed:

   - Management Server
   - Agent for Linux
   - Bootable Media Builder
4. Install a new PostgreSQL instance or configure the connection to an existing instance.
   - [To install a new instance] Click **Install PostgreSQL**.

     Note
     PostgreSQL installation is not supported on Fedora 40 and earlier. On these operating systems, you can only configure the management server with an existing PostgreSQL instance that runs on a different machine.

     - [If prompted to download additional packages] Click **Continue**.
     - Specify the port for the PostgreSQL instance, and then click **Next**.
     - The default port is 5433.

© Acronis International GmbH, 2003-2026

- [To use an existing instance] Click **Select a cluster**.
  - Specify the following:
    - IP address or hostname of the instance, and its port.
    - Credentials for the account that will be used to connect to the database.

      Important
      This account must have the CREATEDB and CREATEROLE privileges.

  - Click **Next**.

5. Specify the port that will be used by a web browser to access the management server, and then click **Next**.

   The default port is 9877.
6. Specify the port that will be used for communication between the product components, and then click **Next**.

   The default port is 7780.
7. After the installation completes, select **Open web console**, and then click **Exit**.

   The Cyber Protect console opens.

To start using your management server, activate it by signing in to your Acronis account or through an activation file. See "Activating a management server" (p. 42).

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 server

  The procedure below uses `acronisbackup17ams_41023.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

 © Acronis International GmbH, 2003-2026

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

Input example

```
sudo docker load -i ./acronisbackup17ams_41023.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, `acronisbackup17ams:41023`.

```
1 #! /bin/bash
2
3 DOCKER_IMAGE=acronisbackup17ams:41023
```

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
```

5. Start a new Docker service to create the container with Acronis Management Server.

   Input template

```
sudo docker service create -p 9877:9877 -p 7780:7780 --ulimit nofile=50000:50000 --
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" --mount
target="/usr/pgsql-15",source="AcronisAMS_usr_pgsql"   --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 --ulimit nofile=50000:50000 --
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_
```


© Acronis International GmbH, 2003-2026

```
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --mount
target="/usr/pgsql-15",source="AcronisAMS_usr_pgsql"   --secret src=ams_
masterkey,target="/var/lib/Acronis/CredStore/masterkey.local" --secret="ams_
masterkey" "acronisbackup17ams:41023"
```

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 `acronisbackup17ams:41023`. To check them for your image, run the `docker images` command, and then see the `REPOSITORY` and `TAG` columns.

Input example

```
sudo docker images
```

Output example

```
# REPOSITORY            TAG     IMAGE ID        CREATED       SIZE
# acronisbackup17ams    41023   2deb8b4b25f9    About an hour ago 3.05GB
```

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     acronisbackup17ams:41023   "/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
      ```


© Acronis International GmbH, 2003-2026

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.
   In this example, the credentials are `root/MyPassword`.

Upgrading the management server

You can upgrade the management server from Cyber Protect version 16 to Cyber Protect version 17.

Prerequisites

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

- AB_AMS_upgrade_to_P17.sh
- AB_AMS_prepare_env_ams.sh
- The Docker image of the management server
  The procedure below uses `acronisbackup17ams_41023.image` as an example.

To upgrade 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. Stop the AMS docker service for version 16.
   You can use the service name or service ID in this command.
   Input example

```
sudo docker service rm ams
```

2. Verify that the container for Acronis Cyber Protect 16 is not listed as a running container.
   Input example

```
sudo docker ps
```

3. 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 ./acronisbackup17ams_41023.image
```

4. Check the ID of the loaded image.
   Input example

© Acronis International GmbH, 2003-2026

```
sudo docker image ls
```

Output example

```
# REPOSITORY            TAG     IMAGE ID        CREATED       SIZE
# acronisbackup17ams    41023   2deb8b4b25f9    About an hour ago  3.05 GB
```

5. Assign the execute permission to the `AB_AMS_upgrade_to_P17.sh` file, and then run it.

   Input template

```
chmod +x /<path>/AB_AMS_upgrade_to_P17.sh
```

```
/<path>/AB_AMS_upgrade_to_P17.sh -u backup_dir -i <image ID>
```

   Input example

```
sudo chmod +x ./AB_AMS_upgrade_to_P17.sh
```

```
sudo ./AB_AMS_upgrade_to_P17.sh -u backup_dir -i 2deb8b4b25f9
```

Note

A backup copy of the version 16 volumes is saved in the `backup_dir` directory. You can use the backup to roll back the changes if the update fails, by running the following command:

```
sudo ./AB_AMS_upgrade_to_P17.sh -r backup_dir
```

6. 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. Start a new Docker service to create the container with Acronis Management Server.

   Input template

```
sudo docker service create -p 9877:9877 -p 7780:7780 --ulimit nofile=50000:50000 --
name="ams"       --mount target="/var/log",source="AcronisAMS_var_log" --mount
```


© Acronis International GmbH, 2003-2026

```
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" --mount
target="/usr/pgsql-15",source="AcronisAMS_usr_pgsql"    --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 --ulimit nofile=50000:50000 --
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" --mount
target="/usr/pgsql-15",source="AcronisAMS_usr_pgsql"    --secret src=ams_
masterkey,target="/var/lib/Acronis/CredStore/masterkey.local" --secret="ams_
masterkey" "acronisbackup17ams:41023"
```

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 `acronisbackup17ams:41023`. To check them for your image, run the `docker images` command, and then see the `REPOSITORY` and `TAG` columns.

Input example

```
sudo docker images
```

Output example

```
# REPOSITORY            TAG     IMAGE ID        CREATED       SIZE
# acronisbackup17ams    41023   2deb8b4b25f9    About an hour ago 3.05GB
```

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     acronisbackup17ams:41023   "/bin/bash -c'/opt/..."   2 minutes
      ago   Up 2 minutes  7780/tcp, 9877/tcp  ams.1.ko7xklvta28rasyukn6kic1ka
      ```

   b. Enter the container.

© Acronis International GmbH, 2003-2026

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.
   In this example, the credentials are `root/MyPassword`.

Adding machines from the Cyber Protect 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, see "Installing protection agents in Windows" (p. 129). 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, see "Service logon account" (p. 104).

Adding a machine running Windows

You can add a Windows machine in the following ways:

- by installing a protection agent remotely, from the Cyber Protect console
- by downloading and running the setup program locally

To install an agent remotely

© Acronis International GmbH, 2003-2026

Important
Before starting the installation, ensure that the prerequisites for remote installation are met. See "Prerequisites for remote installation" (p. 122).

At least one online agent is required in your environment. This agent will be used as a deployment agent. See "Deployment agent" (p. 123).

For more information about remotely installing or updating a protection agent on a 32-bit machine, see this knowledge base article.

1. In the Cyber Protect 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 groupand 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, see "Mailbox backup" (p. 654).

To install an agent locally

 © Acronis International GmbH, 2003-2026

1. In the Cyber Protect 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, see "Installing protection agents in Windows" (p. 129).

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, see "To disable UAC" (p. 206).
- 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, see "To disable UAC" (p. 206).
- 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**.
- Remote installation of protection agents requires TCP port **445** to be open on the target machine for both incoming and outgoing requests. Port 445 is automatically opened when you enable File and Printer Sharing. For detailed information about ports used during remote installation, see "Firewall configuration" (p. 98).

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, see "Installing protection agents in Windows" (p. 129). 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, see "Service logon account" (p. 104).

Requirements on User Account Control (UAC)

On a machine that is running Windows 7 or later and is not a member of an Active Directory domain, centralized management operations (including remote installation) require that UAC and UAC remote restrictions be disabled.

To disable UAC

 © Acronis International GmbH, 2003-2026

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, we recommend that after finishing the management operation (for example, remote installation), you revert both settings to their original state: **EnableLUA**=**1** and **LocalAccountTokenFilterPolicy** = **0**

Deployment agent

To install protection agents on remote machines from the Cyber Protect 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.

© Acronis International GmbH, 2003-2026

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\{build}\{architecture}\modern`

  `%Program Files%\Acronis\RemoteInstallationFiles\installation_files\{build}\{architecture}\legacy`

  For example: `C:\Program Files\Acronis\RemoteInstallationFiles\installation_files\17.0.41224\x64\modern`
- Linux:

  `/usr/lib/Acronis/RemoteInstallationFiles/installation_files/{build}/{architecture}/modern`

  `/usr/lib/Acronis/RemoteInstallationFiles/installation_files/{build}/{architecture}/legacy`

  For example: `/usr/lib/Acronis/RemoteInstallationFiles/installation_files/17.0.41224/x64/modern`

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 architecture of your operating system. In most cases, you will need the **Windows 64-bit** installation file. For more information about remotely installing or updating a protection agent on a 32-bit machine, see this knowledge base article.

© Acronis International GmbH, 2003-2026

2. On the machine on which 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 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 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, see "Installing protection agents in Linux" (p. 131).

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 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, see "Installing protection agents in macOS" (p. 133).

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.

 © Acronis International GmbH, 2003-2026

- **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, see "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). 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 that you use a dedicated account for accessing vCenter Server or the ESXi host, instead of using an existing account with the Administrator role. For more information, see "Required privileges for Agent for VMware" (p. 488).
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**.

 © Acronis International GmbH, 2003-2026

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 that you use a dedicated account for accessing vCenter Server or the ESXi host, instead of using an existing account with the Administrator role. For more information, see "Required privileges for Agent for VMware" (p. 488).
9. Click **Install** to install the agent.

Registering an already installed Agent for VMware

This section describes registering Agent for VMware from the Cyber Protect console.

Alternative registration methods:

- You can register Agent for VMware (Virtual Appliance) by specifying the management server in the virtual appliance UI. For more information, see "Configuring the virtual appliance" (p. 161).
- You can register Agent for VMware (Windows) during its installation. For more information, see "Installing protection agents in Windows" (p. 129).

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.

© Acronis International GmbH, 2003-2026

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.
6. [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.
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 **Connect**.
9. Specify the host name or IP address of the vCenter Server or the ESXi host, and credentials to access it.

   We recommend that you use a dedicated account for accessing vCenter Server or the ESXi host, instead of using an existing account with the Administrator role. For more information, see "Required privileges for Agent for VMware" (p. 488).
10. Click **Connect**.
11. Click **Register**.

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 that you use a dedicated account for accessing vCenter Server or the ESXi host, instead of using an existing account with the Administrator role. For more information, see

 © Acronis International GmbH, 2003-2026

"Required privileges for Agent for VMware" (p. 488).

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

Downloading protection agents

Before you install an agent, you must download its installation file from the Cyber Protect console.

To download an agent while adding a workload to protect

1. In the Cyber Protect console, navigate to **Devices** > **All devices**.
2. In the upper right, click **Add device**.
3. Select the agent that corresponds to the operating system of the workload that you are adding.
   The **Save As** dialog opens.
4. [Only for Macs with Apple silicon processors, such as M1 and M2] Click **Cancel**. In the **Add Mac** panel that opens, click **Download ARM installer**.
5. Select a location to save the agent installation file and click **Save**.

To download an agent for later use

1. In the upper right corner of the Cyber Protect console, click the **User** icon.
2. Click **Downloads**.
3. Scroll the list of available installers to locate the agent installer that you need and click the download icon at the end of its row.
   The **Save As** dialog opens.
4. Select a location to save the agent installation file and click **Save**.

Installing protection agents 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:

© Acronis International GmbH, 2003-2026

- 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, see "Customizing installation settings" (p. 103).

  Note

  On Windows workloads, antimalware protection and URL filtering require Agent for Active Protection and Agent for Antimalware protection and URL filtering. For more information, see "Dynamic installation of antimalware components" (p. 159).

- 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 protection agents through Group Policy" (p. 150).

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, see "Generating a registration token" (p. 156).
   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, see "Units and administrative accounts" (p. 330).
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 console, click **Add** > **Microsoft Exchange Server** > **Exchange mailboxes**, and then specify the machine where the **Client**

© Acronis International GmbH, 2003-2026

Access server role (CAS) of Microsoft Exchange Server is enabled. For more information, see "Mailbox backup" (p. 654).

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, see "Generating a registration token" (p. 156).
   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, see "Units and administrative accounts" (p. 330).
9. [Optional] Change other installation settings as described in "Customizing installation settings" (p. 103).
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. 128).
13. [Only when installing Agent for Exchange] Open the Cyber Protect 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, see "Mailbox backup" (p. 654).

Installing protection agents in Linux

Prerequisites

© Acronis International GmbH, 2003-2026

- You downloaded the installation file for Agent for Linux. See "Downloading protection agents" (p. 129).

  The 64-bit installation package contains additional agents, such as Agent for Virtuozzo, Agent for Oracle, and Agent for Proxmox. These agents depend on Agent for Linux and are installed together with it.
- You installed the required Linux packages.
- At least 2 GB of free disk space is available on the machine on which you want to install the agent.
- 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 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).

Limitations

- Some Linux distributions do not allow the installation of packages that are signed with SHA-1. In such cases, the installation fails with the following message: 'Cannot find package Backup and Recovery Agent.' For more information about how to resolve this issue, see this knowledge base article.

To install Agent for Linux

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. 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 Virtuozzo**
      - **Agent for Oracle**
      - **Agent for Proxmox**

      Agent for Virtuozzo, Agent for Oracle, and Agent for Proxmox require that Agent for Linux (64-bit) is also installed.
   c. Click **Next**.
4. Specify the management server where the machine with the agent will be registered.

© Acronis International GmbH, 2003-2026

- To register under a user account:
  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**.
- To register by using a token:
  a. Specify the host name or IP address of the machine where the management server is installed.
  b. Specify the registration token.
     For more information on how to obtain a token, see "Generating a registration token" (p. 156).
  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

Installing protection agents 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.

 © Acronis International GmbH, 2003-2026

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 protection agents through Group Policy" (p. 150).

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, see "Generating a registration token" (p. 156).
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.

 © Acronis International GmbH, 2003-2026

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, see 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 "Unattended installation or uninstallation parameters" (p. 136).

Examples

© Acronis International GmbH, 2003-2026

- 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.

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-	Web Console

© Acronis International GmbH, 2003-2026

		bit	
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
ActiveProtection	AgentsCoreComponents	32-bit/64-bit	Agent for Active Protection
AmpAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Antimalware protection and URL filtering
ArxAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for SQL
ARADAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32-bit/64-bit	Agent for Oracle
ArxOnlineAgentFeature	AgentsCoreComponents	32-bit/64-bit	Agent for Office 365

© Acronis International GmbH, 2003-2026

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 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>`

© Acronis International GmbH, 2003-2026

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`.

`SKIP_SHA2_KB_CHECK={0,1}`

Use this parameter to either check or to skip the check for the installation of the Microsoft update for SHA2 code signing support (KB4474419) on a machine. The check only runs on operating systems that require this update. To see if it is required for your operating system, see "Supported operating systems and environments" (p. 62).

To skip the check, set the parameter value to `1`.

If you do not specify the parameter or set its value to `0`, and the SHA2 code signing support update is not found on the machine, the installation fails.

`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 console as described in "Deploying protection agents through Group Policy" (p. 150).

`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 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}`

 © Acronis International GmbH, 2003-2026

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.

 © Acronis International GmbH, 2003-2026

- `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" (p. 128).

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

© Acronis International GmbH, 2003-2026

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.

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.

Installing and uninstalling protection agents 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.

Prerequisites

- You downloaded the installation file for Agent for Linux. See "Downloading protection agents" (p. 129).

  The 64-bit installation package contains additional agents, such as Agent for Virtuozzo, Agent for Oracle, and Agent for Proxmox. These agents depend on Agent for Linux and are installed together with it.
- You installed the required Linux packages.
- At least 2 GB of free disk space is available on the machine on which you want to install the agent.
- 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 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).

Limitations

- Some Linux distributions do not allow the installation of packages that are signed with SHA-1. In such cases, the installation fails with the following message: 'Cannot find package Backup and

© Acronis International GmbH, 2003-2026

Recovery Agent.' For more information about how to resolve this issue, see this knowledge base article.

To install an 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 (32-bit or 64-bit). See the available parameters and their values in "Unattended installation or uninstallation parameters" (p. 144).
   - 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 do not 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 value for that parameter. For example:

     ```
     --ams=192.168.11.10
     --login=johndoe
     --password=johnspassword
     --auto
     ```

     or

     ```
     -C
     192.168.11.10
     -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 prompted to restart the system after the installation. When prompted for a password, use the password for the root user. If this password is not accepted, use the word "acronis" as a password. During the system restart, opt for MOK (Machine Owner Key) management, select **Enroll MOK**, and then enroll the key by using the

© Acronis International GmbH, 2003-2026

recommended password.

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

To uninstall an agent

1. Open Terminal.
2. Do one of the following:
   - To uninstall the agent and remove all logs, tasks, and configuration settings, run the following command:

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a
     ```

   - To uninstall the agent but keep its ID (for example, if you plan to install the agent later), run the following command:

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a --no-purge
     ```

   - To uninstall the agent by using the installation file, run the following command:

     ```
     <package name> -a -u
     ```

     Here, `<package name>` is the name of the installation package (32-bit or 64-bit). See the available parameters and their values in "Unattended installation or uninstallation parameters" (p. 144).

     Note
     Use this command only when the installation package is the same version as the installed agent and if `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` is corrupted or inaccessible.

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 you installation.

Installation parameters

Basic parameters

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

The components to be installed. Separate the list items with commas, without spaces.

© Acronis International GmbH, 2003-2026

The following components are available in the 64-bit installation package. The additional agents, such as Agent for Virtuozzo, Agent for Oracle, and Agent for Proxmox, depend on Agent for Linux and are installed with it.

Component	Component description
`AcronisCentralizedManagementServer`	Management Server
`BackupAndRecoveryAgent`	Agent for Linux
`AgentForPCS`	Agent for Virtuozzo
`AgentForProxmox`	Agent for Proxmox
`AtpScanService`	Scan Service
`OracleAgentFeature`	Agent for Oracle
`BackupAndRecoveryBootableComponents`	Bootable Rescue Media Builder

Without this parameter, all available 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>`

© Acronis International GmbH, 2003-2026

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 console as described in "Deploying protection agents through Group Policy" (p. 150).

`{-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 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 *not* `https`, the check uses the system CA, or the CA bundle delivered with the product or the pinned public key, correspondingly.

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

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

© Acronis International GmbH, 2003-2026

- `--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_16_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Installing Management Server, specifying custom ports.

```
./AcronisCyberProtect_16_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.

© Acronis International GmbH, 2003-2026

```
./AcronisCyberProtect_16_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_16_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), see "Adding a machine running macOS" (p. 125).

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_16_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_16_MAC.dmg -mountpoint mydirectory
  ```

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

  ```
  hdiutil detach mydirectory
  ```

 © Acronis International GmbH, 2003-2026
  ```

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 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, see "Administering user accounts and organization units" (p. 330).

- 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 console, as described in "Deploying protection agents through Group Policy" (p. 150).

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.

 © Acronis International GmbH, 2003-2026

- ```
  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
  ```

Deploying protection 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 Windows 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

- Active Directory domain with a domain controller running Microsoft Windows Server 2003 or later.
- You must be a member of the **Domain Admins** group in this domain.
- You have downloaded the **All agents for Windows** setup program.

 © Acronis International GmbH, 2003-2026
  ```

To download the setup program, in the Cyber Protect console, click the account icon in the top-right corner, and then click **Downloads**. The download link is also available in the **Add devices** pane.

To deploy agents through Group Policy

1. Generate a registration token as described in "Generating a registration token" (p. 156).
2. Create the .mst file, the .msi file, and the .cab files, as described in "Creating the transform file and extracting the installation packages" (p. 151).
3. Set up the Group Policy object as described in "Setting up the Group Policy object" (p. 152).

Creating the transform file and extracting the installation packages

To deploy protection agents via Windows Group Policy, you need a transform file (.mst), and the installation packages (.msi and .cab files).

Note
The procedure below uses the default registration option, which is registration by token. To learn how to generate a registration token, refer to "Generating a registration token" (p. 156).

To create the .mst file and extract the installation packages (.msi and .cab files)

1. Log in as an administrator on any machine in the Active Directory 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. Run the agent setup program.
4. Click **Create .mst and .msi files for unattended installation**.
5. In **What to install**, select the components that you want to include in the installation, and then click **Done**.
6. In **Registration settings**, click **Specify**, enter a registration token, and then click **Done**.
   You can change the registration method from **Use registration token** (default) to **Use credentials** or **Skip registration**. The **Skip registration** option presumes that you will register the workloads manually later.
7. Review or modify the installation settings, which will be added to the .mst file, and then click **Proceed**.
8. In **Save the files to**, specify the path to the shared folder that you created.
9. Click **Generate**.

As a result, the .mst file, the .msi file, and the .cab files are created and copied to the shared folder that you specified.

Next, set up the Windows Group Policy object. To learn how to do it, refer to "Setting up the Group Policy object" (p. 152).

© Acronis International GmbH, 2003-2026

Setting up the Group Policy object

In this procedure you use the installation packages that you created in "Creating the transform file and extracting the installation packages" (p. 151) to set up a Group Policy object (GPO). The GPO will deploy the agents onto the machines in your domain.

To set up the Group Policy object

1. Log in to the domain controller as a domain administrator.

   If the domain has more than one domain controller, log in to any of them as a domain administrator.
2. [If you deploy agents in an organizational unit] Ensure that the organizational unit in which you want to deploy the agents exists in this domain.
3. In the Windows **Start** menu, point to **Administrative Tools**, and then click **Group Policy Management** (or **Active Directory Users and Computers** for Windows Server 2003).
4. [For 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. [For 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**.
6. Name the new Group Policy object **Agent for Windows.**
7. Open the **Agent for Windows** Group Policy object for editing:
   - [In Windows Server 2008 or later] Under **Group Policy Objects**, right-click the Group Policy object, and then click **Edit**.
   - [In Windows Server 2003] Click the Group Policy object, and then click **Edit**.
8. In the Group Policy object editor snap-in, expand **Computer Configuration**.
9. [For Windows Server 2012 or later] Expand **Policies** > **Software Settings**.
10. [For Windows Server 2003 and Windows Server 2008] Expand **Software Settings**.
11. Right-click **Software installation**, point to **New**, and then click **Package**.
12. Select the agent's .msi installation package in the shared folder that you created, and then click **Open**.
13. In the **Deploy Software** dialog box, click **Advanced**, and then click **OK**.
14. On the **Modifications** tab, click **Add**, and then select the .mst file in the shared folder that you created.
15. Click **OK** to close the **Deploy Software** dialog box.

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 console.

© Acronis International GmbH, 2003-2026

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\Acronis\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
```


© Acronis International GmbH, 2003-2026

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 "Using passwords with special characters or blank spaces" (p. 158).

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\Acronis\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
```

 © Acronis International GmbH, 2003-2026

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 "Using passwords with special characters or blank spaces" (p. 158).

To check the unit ID, in the Cyber Protect 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. 330).

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\Acronis\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>
```

 © Acronis International GmbH, 2003-2026

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\Acronis\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
```

Generating a registration token

A registration token is a series of 12 characters, separated by hyphens in three segments. The registration token passes the identity of a user to the agent setup program, without storing the user credentials for the Cyber Protect console. This enables users to register workloads under their account or apply protection plans to workloads without logging in to the console.

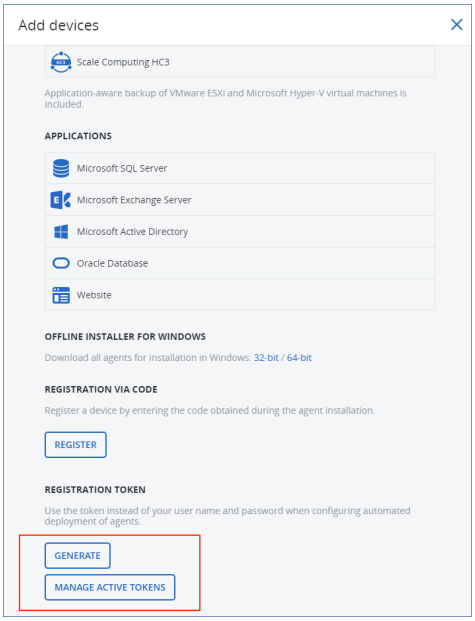
© Acronis International GmbH, 2003-2026

Note
Protection plans are not applied automatically during workload registration. Applying a protection plan is a separate task.

For security reasons, the tokens have limited lifetime, which you can adjust. The default lifetime is 3 days.

To generate a registration token

1. Log in to the Cyber Protect console.
2. Click **Devices** > **All devices** > **Add**.
   The **Add devices** pane opens on the right.
3. Scroll down to **Registration token**, and then click **Generate**.



4. Specify the token lifetime.
5. Click **Generate token**.
6. Click **Copy** to copy the token to your device clipboard, or write the token down manually.

Managing registration tokens

You can view and delete the active registration tokens.

To view the registration tokens

1. Log in to the Cyber Protect console.
2. Click **Devices** > **All devices** > **Add**.
3. Scroll down to **Registration token**, and then click **Manage active tokens**.
   A list with the active tokens that are generated for the tenant opens on the right.

© Acronis International GmbH, 2003-2026

Note
For security reasons, in the **Token** column, only the first two characters of the token value are shown.

To delete a registration token

1. Log in to the Cyber Protect console.
2. Click **Devices** > **All devices** > **Add**.
3. Scroll down to **Registration token**, and then click **Manage active tokens**.
   A list with the active tokens that are generated for the tenant opens on the right.

   Note
   For security reasons, in the **Token** column, only the first two characters of the token value are shown.

4. Select the token, and then click **Delete**.

Using passwords with special characters or blank spaces

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

For example, in Windows, run this command in Command Prompt:

Command template

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

Command examples

- 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"
```


© Acronis International GmbH, 2003-2026

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.

For example, in Windows, run this command in Command Prompt:

Command template

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

Command examples

- 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==
```

Dynamic installation of antimalware components

- Agent for Antimalware protection and URL filtering – required for antimalware protection and URL filtering.
- Agent for Active Protection – required for antimalware protection.

By default, these components are not installed. The respective component is automatically installed if a workload becomes protected by a plan in which any of the following modules is enabled:

- **Antivirus & Antimalware protection**
- **URL filtering**

Similarly, if no protection plan requires antimalware protection or URL filtering, the respective component is automatically uninstalled.

Dynamic installation or uninstallation of components might take up to 10 minutes after you apply, revoke, edit, or delete a protection plan. If any of the following operations is running, dynamic installation or uninstallation will start after the operation completes:

- Backup
- Recovery
- Backup replication

© Acronis International GmbH, 2003-2026

- Virtual machine replication
- Testing a replica
- Running a virtual machine from backup (including finalization)
- Disaster recovery failover (for cloud deployment)
- Disaster recovery failback (for cloud deployment)
- Patch installation
- ESXi configuration backup

Deploying virtual appliances

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
To enable backups of virtual machines, install vStorage APIs on the ESXi host. For more information, see this knowledge base article.

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.

 © Acronis International GmbH, 2003-2026

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 locally attached storage" (p. 497).

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 tempate

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 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.

 © Acronis International GmbH, 2003-2026

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="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>
        ```

      - 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.

© Acronis International GmbH, 2003-2026

Specify the credentials that the agent will use to connect to the vCenter Server or ESXi.

We recommend that you use a dedicated account for accessing vCenter Server or the ESXi host, instead of using an existing account with the Administrator role. For more information, see "Required privileges for Agent for VMware" (p. 488).

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 drive letter and label for it. The label length is limited to 16 characters, due to file system restrictions.

   The disk size must be at least 10 GB.

   Warning!
   If you use a disk that contains data, the data will be deleted.

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.

© Acronis International GmbH, 2003-2026

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. Specify the IP address or the host name of the Scale Computing HC3 cluster.
4. Specify credentials of an account that has the **VM Create/Edit** role assigned in this cluster.
5. Select the number of virtual appliances that you want to deploy.
6. Click **Deploy**.

After the deployment completes, configure the virtual appliance.

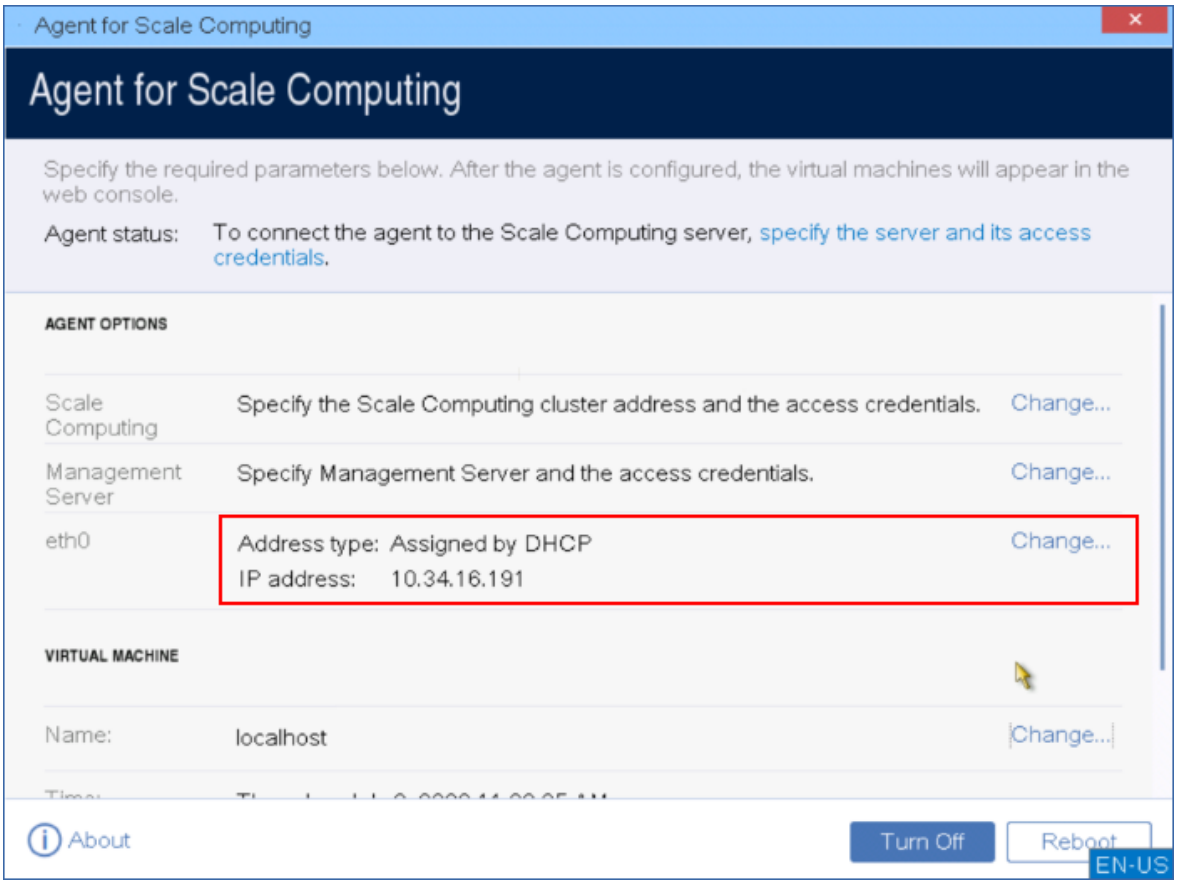
© Acronis International GmbH, 2003-2026

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.



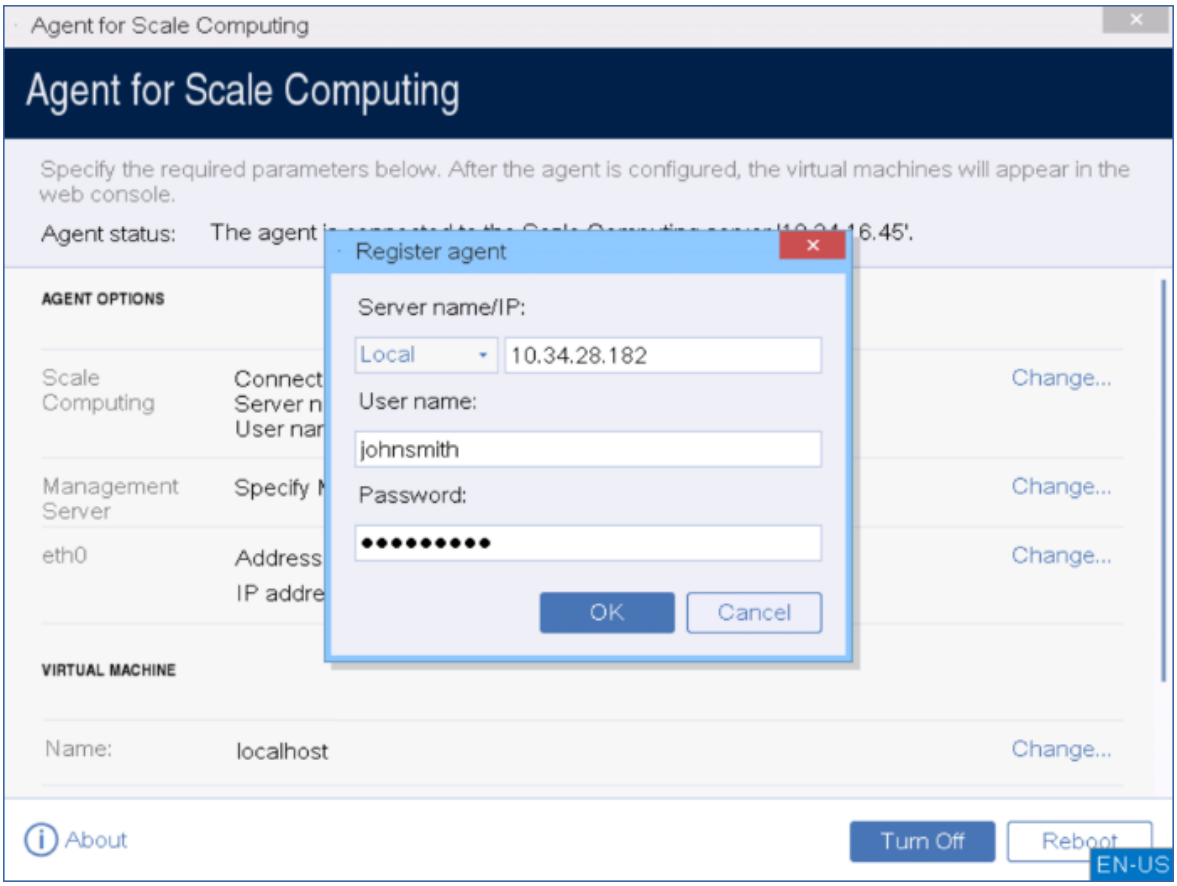
4. Specify the Scale Computing HC3 cluster address and credentials:
   - DNS name or IP address of the cluster.
   - In the **User name** and **Password** fields, enter the credentials for the Scale Computing HC3 account that has the appropriate roles assigned.

   You can click **Check connection** to ensure the access credentials are correct.

© Acronis International GmbH, 2003-2026

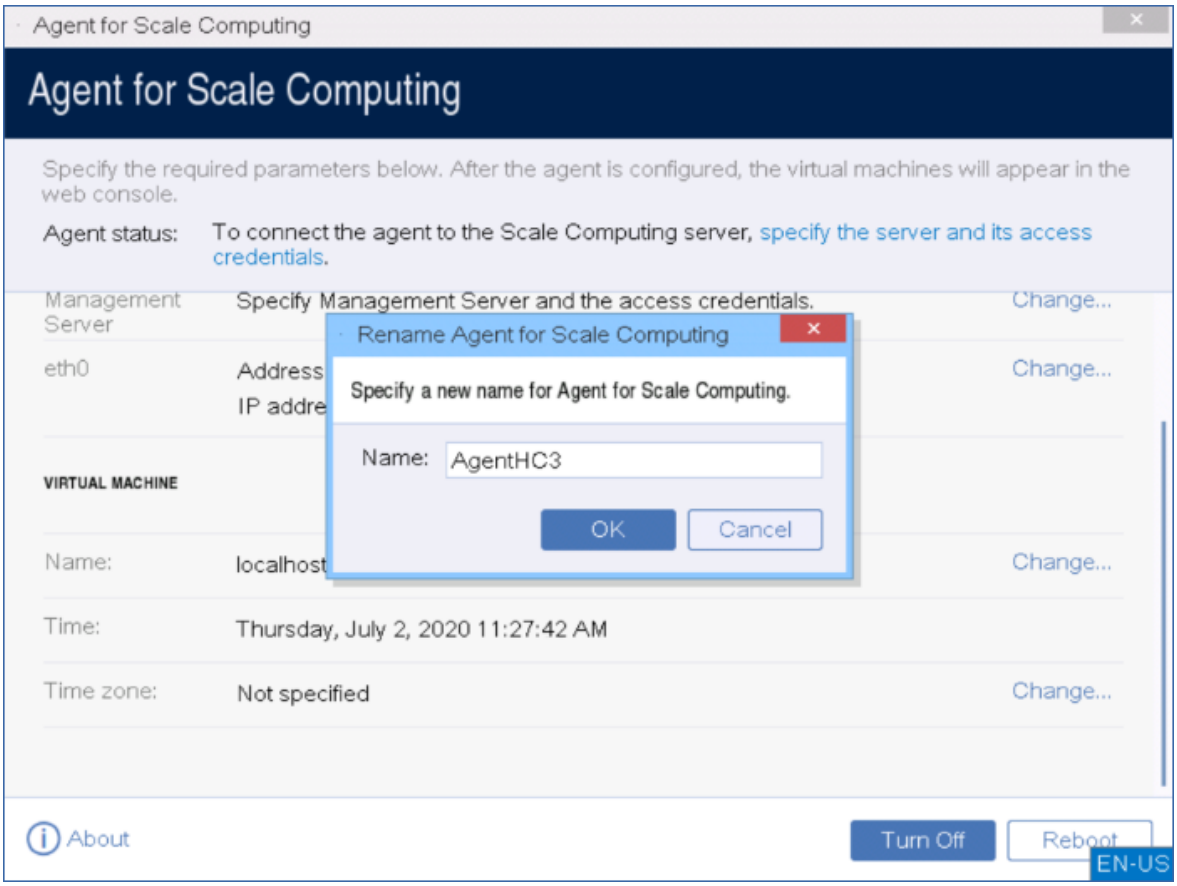
5. Specify the Cyber Protect management server address and credentials for accessing it.

© Acronis International GmbH, 2003-2026



6. [Optional] Specify a name for the agent. This name will be shown in the Cyber Protect console.

© Acronis International GmbH, 2003-2026



7. [Optional] Select the time zone of your location to ensure that the scheduled operations run at the appropriate time.
8. [Optional] Add local backup storage to the virtual appliance.
   a. In your virtual machine environment, select the virtual appliance, and then open its settings for editing.
   b. Add a new hard disk to the virtual appliance.
      The disk size must be at least 10 GB.

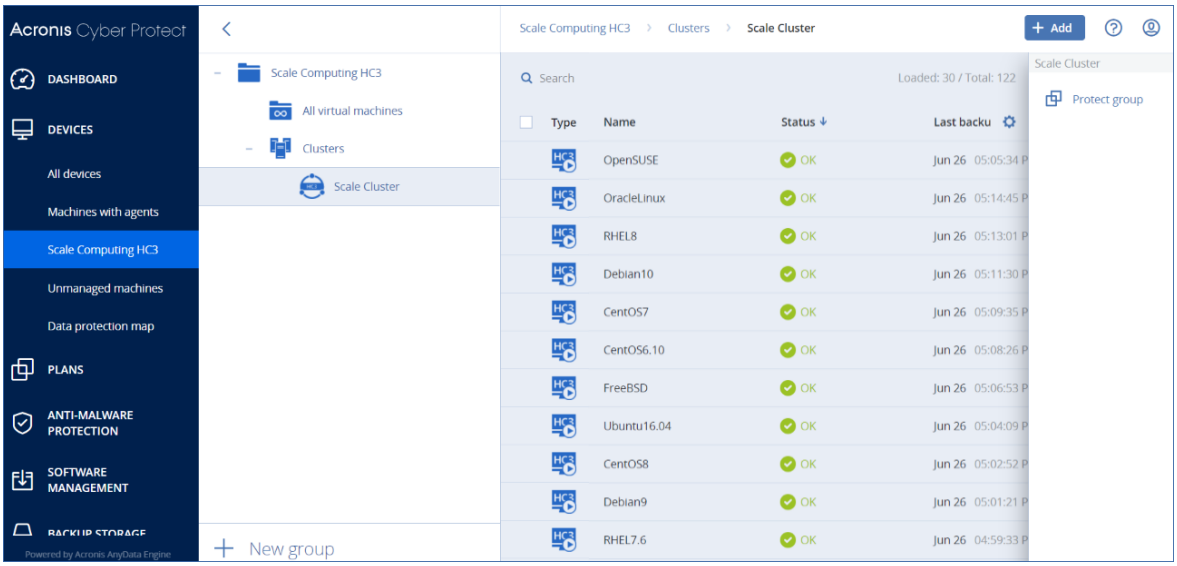
      Warning!
      If you use a disk that contains data, the data will be deleted.

   c. In your virtual machine environment, open the console of the virtual appliance.
   d. Under **Local storages**, click **Refresh**.
      The **Create storage** button becomes active.
   e. Click **Create storage**, and then select the disk that you added to the virtual appliance.
      - Select a drive letter.
      - [Optional] Specify a disk label.
        The label length is limited to 16 characters, due to file system restrictions.
   f. Click **OK**.
   g. Click **Yes**.

To protect the virtual machines in the Scale Computing HC3 cluster

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

Agent for oVirt (Virtual Appliance)

Before you start

This appliance is a preconfigured virtual machine that you deploy in a Red Hat Virtualization/oVirt environment. The appliance contains a protection agent that can back up and recover the virtual machines in the environment.

System requirements for the agent

By default, the virtual appliance uses 2 vCPUs and 4 GiB of RAM. These settings are sufficient for most operations.

To improve the backup performance and avoid failures related to insufficient RAM, you can increase the number of vCPUs to four, and the RAM to 8 GiB in more demanding cases. For example, when you expect the backup traffic to exceed 100 MB per second (as in 10-Gigabit networks) or if you simultaneously back up multiple virtual machines with large hard drives (500 GiB or more).

The size of the appliance virtual disk is 8 GiB.

How many agents do I need?

One virtual appliance can back up and recover all virtual machines in the environment. You can use multiple virtual appliances if you want to distribute the bandwidth load of the backup traffic.

If more than one virtual appliance is deployed in the environment, the automatic redistribution of the backed-up virtual machines occurs when the load imbalance among the appliances reaches 20 percent.

When you deploy an additional virtual appliance, the management server assigns the most appropriate virtual machines to the new appliance, and the load of the existing appliance decreases. When you remove a virtual appliance, the backed-up virtual machines are redistributed among the remaining appliances. Redistribution occurs only if you remove the virtual appliance from the Cyber Protect console. Redistribution will not start if you remove the virtual appliance from the Red Hat Virtualization/oVirt Administration Portal or if the appliance gets corrupted.

To check which agent manages a specific machine

1. In the Cyber Protect console, click **Devices**, and then select **oVirt**.
2. Click the gear icon in the upper-right corner of the table, and under **System**, select the **Agent** checkbox.
3. Check the name of the agent in the column that appears.

Limitations

The following operations are not supported for Red Hat Virtualization/oVirt virtual machines:

© Acronis International GmbH, 2003-2026

- Application-aware backup
- Running a virtual machine from a backup
- Replication of virtual machines
- Changed block tracking

Deploying Agent for oVirt (Virtual Appliance)

You can deploy the oVirt virtual appliance by creating a virtual machine in the Red Hat Virtualization/oVirt environment and deploying the QCOW template that you download from the Cyber Protect console.

If you need more than one virtual appliance in your environment, deploy additional virtual appliances. Do not clone an existing virtual appliance by using the **Clone VM** option in Red Hat Virtualization/oVirt Administration Portal.

To deploy Agent for oVirt (Virtual Appliance)

1. Log in to the Cyber Protect console.
2. Click **Devices** > **All devices** > **Add** > **Red Hat Virtualization (oVirt)**.
   A ZIP archive is downloaded to your machine.
3. Unpack the ZIP archive and extract the OVA image file.
4. Upload the OVA file to a host in the Red Hat Virtualization/oVirt environment that you want to protect.
5. Log in to Red Hat Virtualization/oVirt Administration Portal as an administrator. For more information about the roles required for operations with virtual machines, see "Agent for oVirt (Virtual Appliance) – required roles and ports" (p. 175).
6. From the navigation menu, select **Compute** > **Virtual machines**.
7. Click the vertical ellipsis icon ⋮ above the main table, and then click **Import**.
8. In the **Import Virtual Machine(s)** window, do the following:
   a. In **Data center**, select the data center that you want to protect.
   b. In **Source**, select **Virtual Appliance (OVA)**.
   c. In **Host**, select the host on which you uploaded the OVA file.
   d. In **File Path**, specify the path to the directory that contains the OVA file.
   e. Click **Load**.
      The oVirt virtual appliance template from the OVA file appears in the **Virtual Machines on Source** panel.
      If the template does not appear in this panel, ensure that you have specified the correct path to the file, the file is not damaged, and the host can be reached.
   f. In **Virtual Machines on Source**, select the oVirt virtual appliance template, and then click the right arrow.
      The template appears in the **Virtual machines to import** panel.
   g. Click **Next**.
9. In the new window, click the appliance name, and then configure the following settings:

 © Acronis International GmbH, 2003-2026

- On the **Network interfaces** tab, configure the network interfaces.
- On the **General** tab, change the default name of the virtual machine with the agent.

10. [Optional] To hide the virtual appliance in the Cyber Protect console, assign the tag `acronis_virtual_appliance` to the virtual appliance.

    This will prevent you from accidentally applying protection plans to the appliance itself and including it in dynamic groups.

The deployment is now complete. Next, you must configure the appliance. See "Configuring Agent for oVirt (Virtual Appliance)" (p. 172).

Note

If you use an oVirt virtual appliance with Oracle Linux Virtualization Manager, you might receive the following error: "VM <name of the virtual appliance> is down with error. Exit message: unsupported configuration: domain configuration does not support video model 'qxl'." To resolve this error, change the graphics adapter of the virtual appliance to **CIRRUS**. See "Changing the graphics adapter for Agent for oVirt (Virtual Appliance)" (p. 174).

Configuring Agent for oVirt (Virtual Appliance)

After deploying the virtual appliance, you need to configure it so that it can reach both the oVirt Engine and the Cyber Protect service.

To configure Agent for oVirt (Virtual Appliance)

1. Log in to Red Hat Virtualization/oVirt Administration Portal.
2. Select the virtual appliance that you want to configure, and then click the **Console** icon.
3. In the **eth0** field, configure the network interfaces of the appliance.

   Ensure that automatically assigned DHCP addresses (if any) are valid within the networks that your virtual machine uses or assign them manually. Depending on the number of networks that the appliance uses, there may be one or more interfaces to configure.
4. In the **oVirt** field, click **Change** to specify the oVirt Engine address and credentials for accessing it:
   a. In the **Server name/IP** field, enter the DNS name or IP address of the engine.
   b. In the **User name** and **Password** fields, enter the administrator credentials for this engine.

      Ensure that this administrator account has the roles required for operations with Red Hat Virtualization/oVirt virtual machines. For more information about these roles, refer to "Agent for oVirt (Virtual Appliance) – required roles and ports" (p. 175).

      If Keycloak is the Single-Sign-On (SSO) provider for the oVirt Engine (default in oVirt 4.5.1), use the Keycloak format when specifying the user name. For example, specify the default administrator account as `admin@ovirt@internalsso` instead of `admin@internal`.
   c. [Optional] Click **Check connection** to ensure that the provided credentials are correct.
   d. Click **OK**.
5. Register the appliance in the Cyber Protect service by using one of the following methods.

 © Acronis International GmbH, 2003-2026

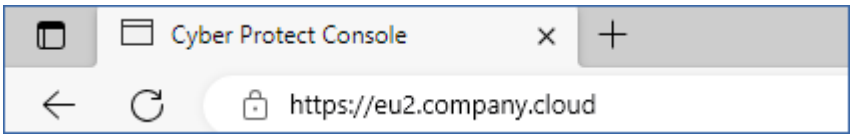
- Register the appliance in its graphical interface.
  a. Under **Agent options**, in the **Management Server** field, click **Change**.
  b. In the **Server name/IP** field, select **Cloud**.
     The Cyber Protect service address appears. Do not change this address unless instructed otherwise.
  c. In the **User name** and **Password** fields, specify the credentials for your Cyber Protect account. The virtual appliance and the virtual machines that the appliance manages are registered under this account.
  d. [Only if two-factor authentication is enabled] Enter the TOTP code from your authenticator app, and then click **OK**.
  e. Click **OK**.
- Register the appliance in the command-line interface.

  Note
  With this method, you need a registration token. For more information about how to generate one, see "Generating a registration token" (p. 156).

  a. Press CTRL+SHIFT+F2 to open the command-line interface.
  b. Run the following command:

```
register_agent -o register -t cloud -a <service address> --token <registration
token>
```

     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 console. For example, `https://eu2.company.cloud`.



     Do not use `https://company.cloud` here.

  c. To return to the graphical interface of the appliance, press ALT+F1.

6. [Optional] In the **Name** field, click **Change** to edit the default name for the virtual appliance, which is **localhost**. This name is shown in the Cyber Protect console.
7. [Optional] In the **Time** field, click **Change**, and then select the time zone of your location to ensure that the scheduled operations run at the appropriate time.
8. [Optional] [If a proxy server is enabled in your network] Configure the proxy server.
   a. Press CTRL+SHIFT+F2 to open the command-line interface.
   b. Open the file `/opt/acronis/etc/aakore.yaml` in a text editor.
   c. Locate the **env** section or create it and add the following lines:

© Acronis International GmbH, 2003-2026

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

d. 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.

e. Run the `reboot` command.

Note

To be able to update a virtual appliance deployed behind a proxy, edit the appliance `config.yaml` file (`/opt/acronis/etc/va-updater/config.yaml`), by adding the following line to the bottom of that file, and then entering values specific to your environment:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

For example:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

To protect virtual machines in the Red Hat Virtualization/oVirt data center

1. Log in to your Cyber Protect account.
2. Navigate to **Devices** > **oVirt** > <your cluster> or find your machines in **Devices** > **All devices**.
3. Select machines and apply a protection plan to them.

Changing the graphics adapter for Agent for oVirt (Virtual Appliance)

If you use Agent for oVirt (Virtual Appliance) with Oracle Linux Virtualization Manager, you might receive the following error: "VM <name of the virtual appliance> is down with error. Exit message: unsupported configuration: domain configuration does not support video model 'qxl'."

To resolve this error, change the graphics adapter of the virtual appliance to **CIRRUS**.

To change the graphics adapter of a virtual appliance

1. Log in to Oracle Linux Administration Portal as an administrator.
2. Go to **Compute** > **Virtual machines**.
3. [If the virtual appliance is powered on] Right-click the virtual appliance, and then select **Shutdown**.
4. Right-click the virtual appliance, and then select **Edit**.
5. [If you see only the **General** tab] Click **Show Advanced Options**.
6. Click **Console**.
7. In **Graphical Console**, for **Video Type**, select **CIRRUS**.
8. Click **OK**.
9. In Oracle Linux Administration Portal, power on the virtual appliance.

© Acronis International GmbH, 2003-2026

Agent for oVirt (Virtual Appliance) – required roles and ports

Required roles

For its deployment and operation, Agent for oVirt requires an administrator account with the following roles assigned.

oVirt/Red Hat Virtualization 4.2 and 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4, 4.5

- SuperUser

Required ports

Agent for oVirt connects to the oVirt Engine by using the URL that you specify when you configure the virtual appliance. Usually, the engine URL has the following format: `https://ovirt.company.com`. In this case, the HTTPS protocol and port 443 are used.

Non-default oVirt settings may require another port. You can find the exact port by analyzing the URL format. For example:

oVirt Engine URL	Port	Protocol
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

No additional ports are required for disk Read/Write operations, because the backup is performed in the HotAdd mode.

Agent for Nutanix (Virtual Appliance)

This appliance is a pre-configured virtual machine that you can deploy to a Nutanix cluster. The appliance contains a protection agent that can back up and recover the virtual machines in the cluster.

You can deploy the virtual appliance from the Cyber Protect console – the console connects to the Nutanix cluster and deploys the virtual appliance automatically.

© Acronis International GmbH, 2003-2026

If the remote deployment fails, you can deploy the virtual appliance manually by using a QCOW2 image. This method requires additional configuration after deployment. For more information, see "Configuring Agent for Nutanix (Virtual Appliance)" (p. 178).

Before you start

This appliance is a pre-configured virtual machine that you can deploy to a Nutanix cluster. The appliance contains a protection agent that can back up and recover the virtual machines in the cluster.

System requirements for the virtual appliance

We recommend that you configure the virtual appliance with 4 vCPUs (4 single-core vCPUs or 2 vCPUs with 2 cores each) and 8 GiB of RAM. These settings are sufficient for most operations.

To improve the backup performance and avoid failures related to insufficient RAM memory, you can increase the RAM memory to 16 GiB in more demanding cases. For example, when you expect the backup traffic to exceed 100 MB per second (as in 10-Gigabit networks) or if you back up simultaneously multiple virtual machines with large hard drives (500 GiB or more).

The size of the appliance virtual disk is 8 GiB.

How many virtual appliances do I need?

One virtual appliance can back up and recover all virtual machines in the cluster. You can use multiple virtual appliances per cluster if you want to distribute the bandwidth load of the backup traffic.

If more than one virtual appliance is deployed in the cluster, the automatic redistribution of the backed-up virtual machines occurs when the load imbalance among the appliances reaches 20 percent.

When you deploy an additional virtual appliance, the management server assigns the most appropriate virtual machines to the new appliance, and the load of the existing appliance decreases. When you remove a virtual appliance, the backed-up virtual machines are redistributed among the remaining appliances. Redistribution occurs only if you remove the virtual appliance from the Cyber Protect console. Redistribution will not start if you remove the virtual appliance from the Nutanix Prism Element console or if the appliance gets corrupted.

Limitations

The following operations are not supported:

- Application-aware backup
- Running a virtual machine from a backup
- Replication of virtual machines
- Backups of Nutanix volume groups

 © Acronis International GmbH, 2003-2026

Deploying Agent for Nutanix from the Cyber Protect console

You can deploy Agent for Nutanix from the Cyber Protect console, without manually creating a virtual machine in the Nutanix cluster.

You must deploy at least one virtual appliance per cluster.

To deploy Agent for Nutanix from the Cyber Protect console

1. In the Cyber Protect console, go to **Devices** > **All devices** > **Add** > **Nutanix AHV**.
2. Specify the connection details for the Nutanix cluster:
   - In the **Host** field, enter the IP address or host name of the Nutanix Prism Element.
   - In the **User name** and **Password** fields, enter the credentials for a Nutanix administrator account. This account must have the **User Admin** and **Cluster Admin** roles in the Nutanix cluster.
3. In the **Management server address** field, select the IP address that the Nutanix cluster will use to connect to the management server.
4. Click **Settings** to review or change the network and storage settings for the virtual appliance:
   - In the **Network** field, select the network to which the virtual appliance will be connected.
   - In the **Storage** field, select the storage container where the virtual appliance disk will be placed.

   The fields are pre-filled with default values.
5. Click **Deploy**.

   The deployment progress is shown in **Activities**.

   When the deployment completes, the virtual appliance appears under **Devices** and the Nutanix virtual machines in the cluster become available for protection.

   If the deployment fails, you can deploy the virtual appliance manually by using a QCOW2 image. For more information, see "Deploying Agent for Nutanix from a QCOW2 template" (p. 177).

Deploying Agent for Nutanix from a QCOW2 template

If the remote deployment of Agent for Nutanix fails, you can deploy the virtual appliance manually by creating a virtual machine in the Nutanix cluster and deploying a QCOW2 image.

You must deploy at least one virtual appliance per cluster.

To deploy Agent for Nutanix from a QCOW2 template

1. Obtain the ZIP file with the QCOW2 image by using one of the following methods:
   - If the automatic download completed successfully, find the ZIP file on the management server machine:
     - In Windows: `C:\ProgramData\Acronis\VaDeployer\va-images`
     - In Linux: `/var/lib/Acronis/VaDeployer`
   - If the automatic download failed, download the ZIP file from the URL that is shown in the error message.

 © Acronis International GmbH, 2003-2026

2. Unpack the ZIP file and extract the QCOW2 image file.
3. Log in to the Nutanix Prism Element console as an administrator.
4. Upload the QCOW2 image file to the Nutanix Prism Element console.
   a. Go to **Settings** and then, under **General**, select **Image configuration**.
   b. Click **Upload image**.
   c. Specify a name for the image.
   d. In **Image Type**, select **Disk**.
   e. Click **Upload a file**, and then click **Choose file**.
   f. Select the QCOW2 image that you extracted from the ZIP file.
   g. Click **Save**.
5. In the Nutanix Prism Element console, create a new virtual machine by using the QCOW2 image.
   a. Go to **VM**, and then click **Create VM**.
   b. Specify a name for the virtual machine.
   c. In **Compute Details**, specify 4 vCPUs (single core) or 2 vCPUs with 2 cores each, and 8 GiB of memory.
   d. In **Disks**, click **Add New Disk**.
   e. In **Operation**, select **Clone from Image Service**.
   f. In **Image**, select the image that you uploaded to the Nutanix Prism Element console.
   g. Click **Add**.
   h. In **Network adapters (NIC)**, click **Add New NIC**.
   i. Configure the network settings, and then click **Add**.
   j. [Optional] To hide the virtual appliance in the Cyber Protect console, in **Description**, specify the following:

      ```
      {AB53A0F1-AD54-480f-80BB-FC72DC41DF53}
      ```

      This will prevent you from accidentally applying protection plans to the appliance itself and including it in dynamic groups.
   k. Click **Save**.
6. On the **VM** > **Table tab**, right-click the virtual machine that you created, and then select **Power on**.

   As a result, the virtual appliance is deployed and powered on.

   Next, configure the virtual appliance. See "Configuring Agent for Nutanix (Virtual Appliance)" (p. 178).

Configuring Agent for Nutanix (Virtual Appliance)

After using a QCOW2 image and the Nutanix Prism Element console to deploy the virtual appliance, you must configure its access to the Nutanix cluster and the Cyber Protect console.

 © Acronis International GmbH, 2003-2026

Note
This procedure is only required if you deployed the virtual appliance manually by using the QCOW2 image. If you deployed the virtual appliance from the Cyber Protect console, no additional configuration is required. For more information, see "Deploying Agent for Nutanix from the Cyber Protect console" (p. 177).

Prerequisites

- You deployed and powered on the Nutanix virtual appliance. See "Deploying Agent for Nutanix from a QCOW2 template" (p. 177).

To configure Agent for Nutanix (Virtual Appliance)

1. Log in to the Nutanix Prism Element console as an administrator.
2. Go to **VM** > **Table**.
3. Right-click the virtual machine that you deployed, and then select **Launch Console**.
4. In the **eth0** field, configure the network interfaces of the appliance.
   If there are automatically assigned DHCP addresses, ensure that they are either valid within the networks that your virtual machine uses or assign them manually. Depending on the number of networks that the appliance uses, there might be one or more interfaces to configure.
5. Specify the IP address of the Nutanix cluster (Nutanix Prism Element) and credentials for accessing it.

   Note
   You cannot configure Agent for Nutanix AHV with the IP address of Nutanix Prism Central. Even if you manage the cluster through Nutanix Prism Central, Agent for Nutanix AHV can only access it through Nutanix Prism Element.

   a. Under **Agent options**, in the **Nutanix** field, click **Change**.
   b. In the **Server name/IP** field, enter the IP address of the cluster.
   c. In the **User name** and **Password** fields, enter the credentials for a Nutanix administrator account.
      This account must have the **User Admin** and **Cluster Admin** roles in the Nutanix cluster.
   d. To verify that the settings are correct, click **Check connection**.
   e. Click **OK**.
6. Register the appliance by using one of the following methods.
   - Register the appliance in its graphical interface.
     a. Under **Agent options**, in the **Management Server** field, click **Change**.
     b. In **Server name/IP**, do one of the following:
        - [For on-premises deployments] Select **Local**, and then specify the host name or IP address of the machine where the management server is installed.
        - [For cloud deployments] Select **Cloud**.

 © Acronis International GmbH, 2003-2026

The Cyber Protect service address appears. Do not change this address unless instructed otherwise.

c. In **User name** and **Password**, do one of the following:
   - [For on-premises deployments] Specify the user name and password of a management server administrator.
   - [For cloud deployments] Specify the credentials for your Cyber Protect account. The virtual appliance and the virtual machines that the appliance manages are registered under this account.

d. [If two-factor authentication is enabled] Enter the TOTP code from your authenticator app, and then click **OK**.

e. Click **OK**.

- Register the appliance in the command-line interface.

Note
With this method, you need a registration token. For more information about how to generate one, see "Generating a registration token" (p. 156).

a. Press CTRL+SHIFT+F2 to open the command-line interface.

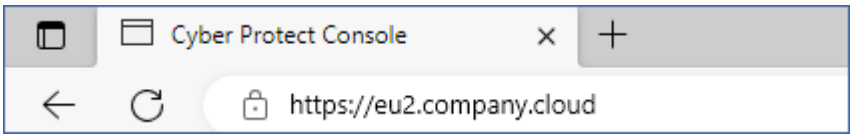
b. Run the following command:
   - [For on-premises deployments]

```
register_agent -o register -a <management server address:port> --token
<registration token>
```

   - [For cloud deployments]

```
register_agent -o register -t cloud -a <service address> --token
<registration token>
```

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 console. For example, `https://eu2.company.cloud`.



Do not use `https://company.cloud` here.

c. To return to the graphical interface of the appliance, press ALT+F1.

7. [Optional] Edit the default name for the virtual appliance, which is **localhost**.
   This name is shown in the Cyber Protect console.
   a. Under **Virtual machine**, in the **Name** field, click **Change**.
   b. Edit the name, and then click **OK**.

 © Acronis International GmbH, 2003-2026

8. [Optional] Configure the time zone of the virtual appliance.
   a. Under **Virtual machine**, in the **Time zone** field, click **Change**.
   b. To ensure that the scheduled operations run at the correct time, select the time zone of your location.
9. [If a proxy server is enabled in your network] Configure the proxy server.
   a. Press CTRL+SHIFT+F2 to open the command-line interface.
   b. Open the file `/opt/acronis/etc/aakore.yaml` in a text editor.
   c. 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
```

   d. 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.
   e. Run the `reboot` command.

Note

To be able to update a virtual appliance deployed behind a proxy, edit the appliance `config.yaml` file (`/opt/acronis/etc/va-updater/config.yaml`), by adding the following line to the bottom of that file, and then entering values specific to your environment:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

For example:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Backing up Nutanix virtual machines

Prerequisites

- You have deployed and configured the Nutanix virtual appliance.

To protect Nutanix virtual machines

1. Log in to the Cyber Protect console.
2. Go to **Devices** > **Nutanix** > <your cluster>.
3. Select virtual machines and apply a protection plan to them.

Agent for Synology

Before you start

With Agent for Synology, you can back up files and folders from and to Synology NAS devices. The NAS-specific properties and access permissions for shares, folders, and files are preserved.

© Acronis International GmbH, 2003-2026

Agent for Synology runs on the NAS device. Thus, you can use the resources of the device for off-host data processing operations, such as backup replication, validation, and cleanup. To learn more about these operations, refer to "Off-host data protection plans" (p. 462).

Note
Agent for Synology supports only NAS devices with x86_64 processors. ARM processors are not supported. See the Synology knowledge center.

You can recover a backup to the original or a new location on the NAS device, and to a network folder that is accessible through that device. Backups in the cloud storage can also be recovered to a non-original NAS device on which Agent for Synology is installed.

The table below summarizes the available backup sources and destinations.

What to backup	Items to backup (Backup source)	Where to backup (Backup destination)
Files/folders	Local folder*	Cloud storage
		Local folder*
	Network folder (SMB)**	Network folder (SMB)**
		NFS folder
		Public clouds***

* Including USB drives that are attached to the NAS device.

Note
Encrypted folders are not supported. These folders are not shown in the Cyber Protect graphical user interface.

** Using external network shares as backup source or backup destination via the SMB protocol is only available for agents running on Synology DiskStation Manager 6.2.3 and later. The data hosted on the Synology NAS itself, including in hosted network shares, can be backed up without limitations.

*** Backup to public clouds, such as Microsoft Azure, Amazon, or S3-compatible storages, is supported only by Agent for Synology 7.x. Agent for Synology 6.x does not support this backup destination due to limitations of the Linux kernel of Synology DSM 6.x.

Limitations

- Agent for Synology supports only NAS devices with x86_64 processors. ARM processors are not supported. See the Synology knowledge center.
- Backed-up encrypted shares are recovered as non-encrypted.

 © Acronis International GmbH, 2003-2026

- Backed-up shares for which the **File compression** option is enabled are recovered with this option disabled.
- You can recover to a Synology NAS device only backups that are created by Agent for Synology.

Downloading the setup program

The setup program for Agent for Synology is available as an SPK file.

Agent for Synology 7.x

To download the setup program

1. In the Cyber Protect console, navigate to **Devices** > **All devices**.
2. In the upper-right corner, click **Add**.
3. Under **Network attached storage (NAS)**, click **Synology**.
   The setup program is downloaded to your machine.

Agent for Synology 6.x

To download the setup program

1. In the Cyber Protect console, navigate to **Devices** > **All devices**.
2. In the upper-right corner, click **Add**.
3. Under **Network attached storage (NAS)**, click **Synology**.
   The setup program for Agent for Synology 7.x is downloaded to your machine.
   You can safely stop the download process or ignore the downloaded file.
4. Click **Download Agent for Synology 6.x**.
   The setup program for Agent for Synology 6.x is downloaded to your machine.

Installing Agent for Synology

Note
Agent for Synology supports only NAS devices with x86_64 processors. ARM processors are not supported. See the Synology knowledge center.

Agent for Synology 7.x

Prerequisites

- The NAS device runs DiskStation Manager 7.x.

  Note
  Only stand alone NAS configurations are supported. Synology Highly Available (HA) configurations are not supported.

- You are a member of the **administrators** group on the NAS device.
- There are at least 200 MB of free space on the NAS volume on which you want to install the

© Acronis International GmbH, 2003-2026

agent.

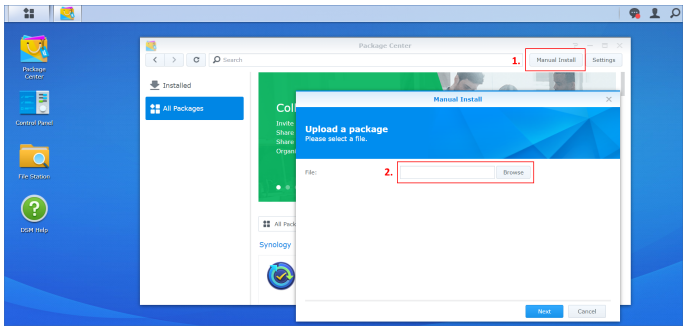
- An SSH client is available on your machine. This document uses Putty as an example.

Limitations

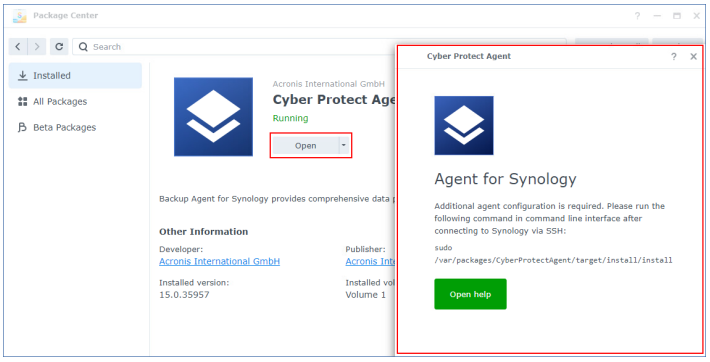
- You cannot register Agent for Synology via QuickConnect. To register the agent, access the NAS device directly.

To install Agent for Synology

1. Log in to Synology DiskStation Manager.
2. Open **Package Center**.
3. Install the agent package:
   a. Click **Manual Install**, and then click **Browse**.



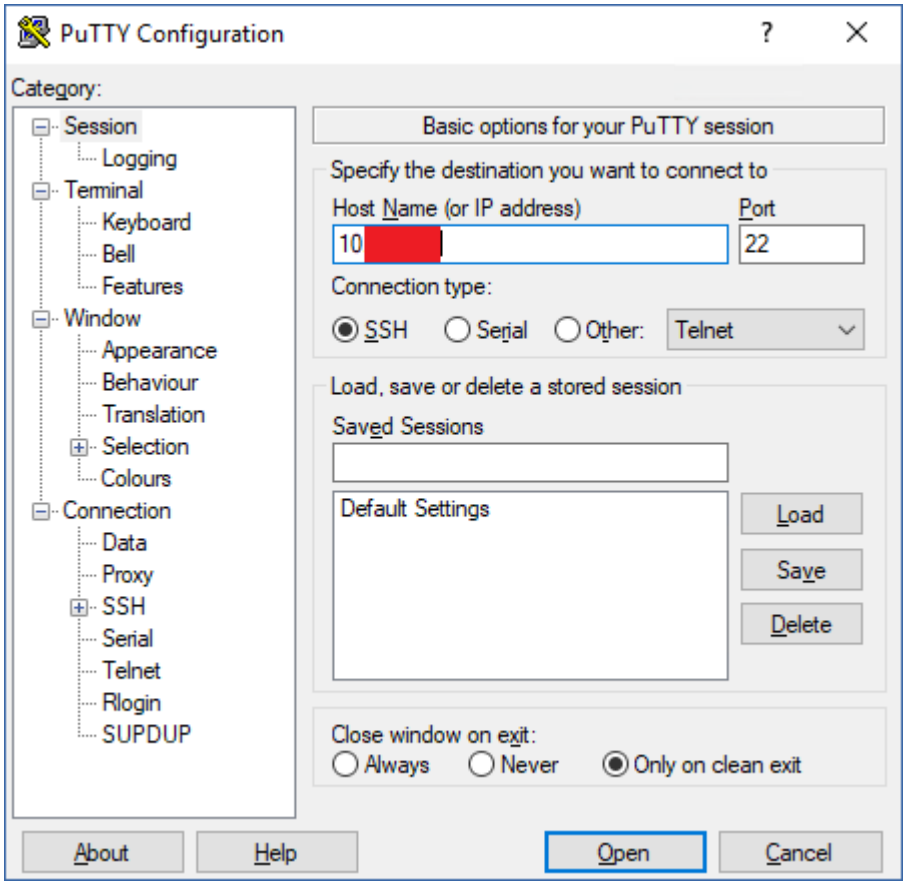
   b. Select the SPK file that you downloaded from the Cyber Protect console, and then click **Next**.
   A warning that you will install a third-party software package is shown. This message is part of the standard installation procedure.
   c. To confirm that you want to install the package, click **Agree**.
4. Select the volume on which you want to install the agent, and then click **Next**.
5. Check the settings, and then click **Done**.
6. In **Package Center**, open **Cyber Protect Agent for Synology**, and then verify that you see the following screen.



7. In Synology DiskStation Manager **Control Panel**, go to **Terminal & SNMP**, and then enable the SSH access to the NAS device.
8. Run the `install` script on the NAS device by using an SSH client (in this example, Putty).
   The script enables the root access to DSM 7.0 or later, which is required to configure the agent.

© Acronis International GmbH, 2003-2026

a. Start Putty, and then specify the IP address or host name of your Synology NAS device.



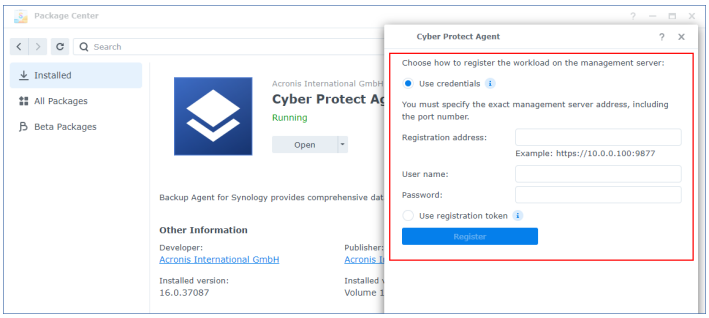
b. Click **Open**, and then log in as a Synology DSM administrator.

c. Run the following command.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

After the script starts, wait for 15 seconds during which the Cyber Protect services initialize.

9. In Synology DiskStation Manager **Control Panel**, go to **Terminal & SNMP**, and then disable the SSH access to the NAS device. The SSH access is no longer required.
10. In Synology DiskStation Manager **Package Center**, open **Cyber Protect Agent for Synology**.
11. Select the registration method.



© Acronis International GmbH, 2003-2026

- [To register the agent by using credentials]
  - In **Registration address**, specify the management server address and port.
  - In the **User name** and **Password** fields, specify credentials for the account under which the agent will be registered. This account cannot be a partner administrator account.
- [To register the agent by using a registration token]
  - In **Registration address**, specify the management server address.
  - In the **Token** field, specify the registration token.

    For more information on how to generate a registration token, see "Generating a registration token" (p. 156).

12. Click **Register**.

Agent for Synology 6.x

Prerequisites

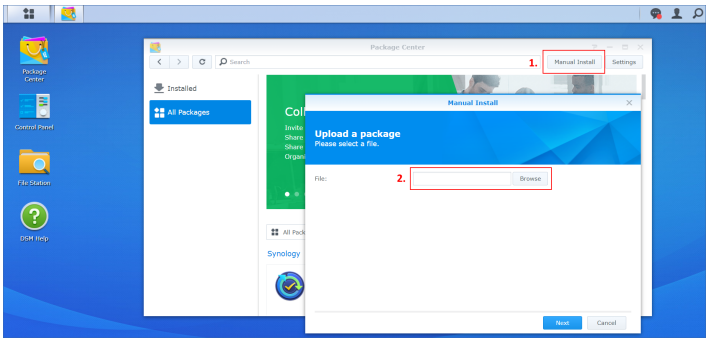
- The NAS device runs DiskStation Manager 6.2.x.

Note
Only stand alone NAS configurations are supported. Synology Highly Available (HA) configurations are not supported.

- You are a member of the **administrators** group on the NAS device.
- There are at least 200 MB of free space on the NAS volume on which you want to install the agent.

To install Agent for Synology

1. Log in to Synology DiskStation Manager.
2. Open **Package Center**.
3. Click **Manual Install**, and then click **Browse**.

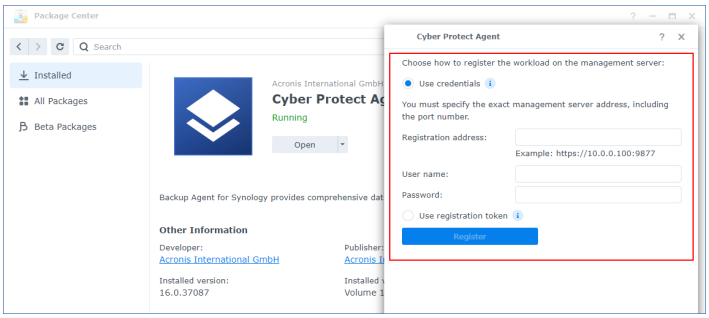


4. Select the SPK file that you downloaded from the Cyber Protect console, and then click **Next**.

   A warning that you will install a package without a digital signature is shown. This message is part of the standard installation procedure.
5. To confirm that you want to install the package, click **Yes**.
6. Select the volume on which you want to install the agent, and then click **Next**.
7. Check the settings, and then click **Apply**.

© Acronis International GmbH, 2003-2026

8. In Synology DiskStation Manager **Package Center**, open **Cyber Protect Agent for Synology**.
9. Select the registration method.



- [To register the agent by using credentials]
  - In **Registration address**, specify the management server address and port.
  - In the **User name** and **Password** fields, specify credentials for the account under which the agent will be registered. This account cannot be a partner administrator account.
- [To register the agent by using a registration token]
  - In **Registration address**, specify the management server address.
  - In the **Token** field, specify the registration token.

    For more information on how to generate a registration token, see "Generating a registration token" (p. 156).
10. Click **Register**.

When the registration completes, the Synology NAS device appears in the Cyber Protect console, on the **Devices** > **Network Attached Storage** tab.

To back up the data on the NAS device, apply a protection plan.

Updating Agent for Synology

You can update Agent for Synology 6.x to a newer version of Agent for Synology 6.x. Similarly, you can update Agent for Synology 7.x to a newer version of Agent for Synology 7.x.

To update the agent, run the newer version of the setup program in Synology DiskStation Manager. The original registration of the agent, its settings, and the plans that are applied to the protected workloads will be preserved.

Note
You cannot update the agent from the Cyber Protect console.

Upgrading Agent for Synology 6.x to Agent for Synology 7.x is supported only by uninstalling the older agent and installing the newer agent. In this case, all protection plans are revoked and you must re-apply them manually.

Agent for Synology 7.x

Prerequisites

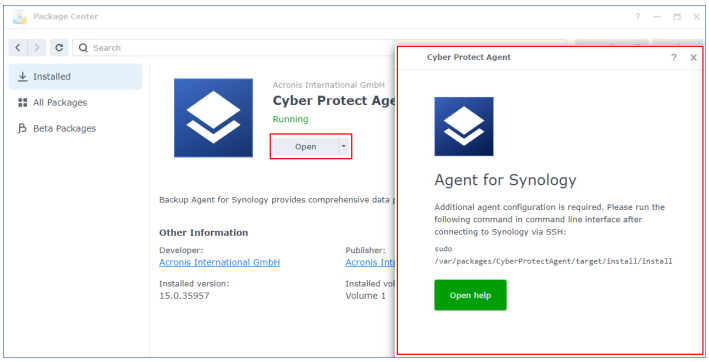
© Acronis International GmbH, 2003-2026

- You are a member of the **administrators** group on the NAS device.
- There are at least 200 MB of free space on the NAS volume on which you want to install the agent.
- An SSH client is available on your machine. This document uses Putty as an example.

To update Agent for Synology

1. In DiskStation Manager, open **Package Center**.
2. Update the agent package:
   a. Click **Manual Install**, and then click **Browse**.
   b. Select the newer SPK file for Agent for Synology 7.x that you downloaded from the Cyber Protect console, and then click **Next**.

      A warning that you will install a third-party software package is shown. This message is part of the standard installation procedure.
   c. To confirm that you want to install the package, click **Agree**.
3. Check the settings, and then click **Done**.
4. In **Package Center**, open **Cyber Protect Agent for Synology**, and then verify that you see the following screen.

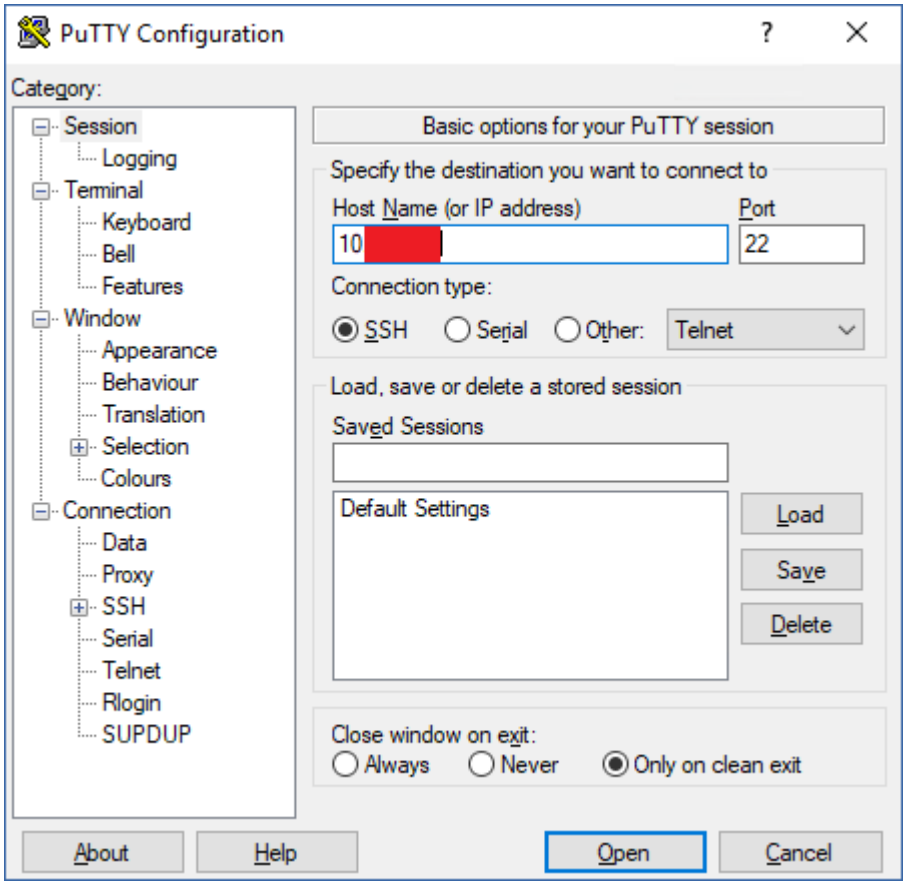


5. In Synology DiskStation Manager **Control Panel**, go to **Terminal & SNMP**, and then enable the SSH access to the NAS device.
6. Run the `install` script on the NAS device by using an SSH client (in this example, Putty).

   The script enables the root access to DSM 7.0 or later, which is required to configure the agent.

© Acronis International GmbH, 2003-2026

a. Start Putty, and then specify the IP address or host name of your Synology NAS device.



b. Click **Open**, and then log in as a Synology DSM administrator.

c. Run the following command.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

7. In Synology DiskStation Manager **Control Panel**, go to **Terminal & SNMP**, and then disable the SSH access to the NAS device. The SSH access is no longer required.

Agent for Synology 6.x

Prerequisites

- You are a member of the **administrators** group on the NAS device.
- There are at least 200 MB of free space on the NAS volume on which you want to install the agent.

To update Agent for Synology

1. In DiskStation Manager, open **Package Center**.
2. Click **Manual Install**, and then click **Browse**.
3. Select the newer SPK file for Agent for Synology 6.x that you downloaded from the Cyber Protect console, and then click **Next**.

© Acronis International GmbH, 2003-2026

A warning that you will install a package without a digital signature is shown. This message is part of the standard installation procedure.

4. To confirm that you want to install the package, click **Yes**.
5. Check the settings, and then click **Apply**.

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. 222).

To update virtual appliance version 15.24426 or later

1. Download the update package as described in https://care.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 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, see Updating agents in the cloud documentation.

SSH connections to a virtual appliance

Use a Secure Socket Shell (SSH) connection when you remotely access a virtual appliance, for maintenance purposes.

 © Acronis International GmbH, 2003-2026

Starting the Secure Shell daemon

To allow SSH connections to a virtual appliance, start the Secure Shall daemon (sshd) on the appliance.

To start the Secure Shall daemon

1. In the hypervisor software, open the console of the virtual appliance.
2. In the graphical user interface of the appliance, press CTRL+SHIFT+F2 to open the command-line interface.
3. Run the following command:

   ```
   /bin/sshd
   ```

4. [Only during the first connection to the appliance] Set the password for the `root` user.

   To learn how to set the password, see "Setting the root password on a virtual appliance" (p. 191).

Note

We recommend that you stop the Secure Shell daemon when you do not use the SSH connection.

Setting the root password on a virtual appliance

Before establishing an SSH connection to a virtual appliance for the first time, you must set the root password on the appliance.

To set the root password

1. In the hypervisor software, open the console of the virtual appliance.
2. In the graphical user interface of the appliance, press CTRL+SHIFT+F2 to open the command-line interface.
3. Run the following command:

   ```
   passwd
   ```

4. Specify a password, and then press Enter.

   The password must contain at least nine characters and must have complexity score of three or more. The complexity score is calculated automatically. To reach higher score, use a combination of special symbols, uppercase and lowercase symbols, and digits.
5. Confirm the password, and then press Enter.

Accessing a virtual appliance via an SSH client

Prerequisites

- An SSH client must be available on the remote machine. The procedure below uses the WinSCP client as an example. You can use any SSH client, by adapting the steps accordingly.

© Acronis International GmbH, 2003-2026

- The Secure Shell daemon (sshd) must be started on the virtual appliance. For more information, see "Starting the Secure Shell daemon" (p. 191).

To access a virtual appliance via WinSCP

1. On the remote machine, open WinSCP.
2. Click **Session** > **New Session**.
3. In **File protocol**, select **SCP**.
4. In **Host name**, specify the IP address of your virtual appliance.
5. In **User name** and **Password**, specify `root` and the password for the `root` user.
6. Click **Login**.

A list of all directories on the virtual appliance is shown.

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. 192)
   In this phase, you prepare the data on the original management server for migration.
2. "Operations on the target machine" (p. 194)
   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.

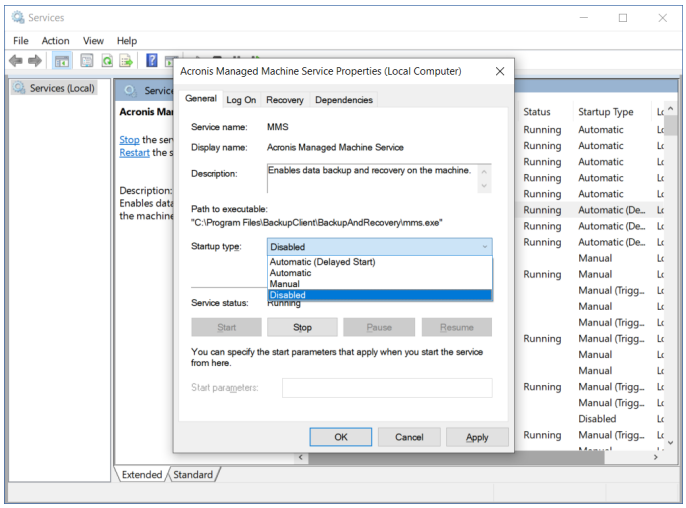
Operations on the source machine

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**.

 © Acronis International GmbH, 2003-2026



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
```


© Acronis International GmbH, 2003-2026

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. 194).

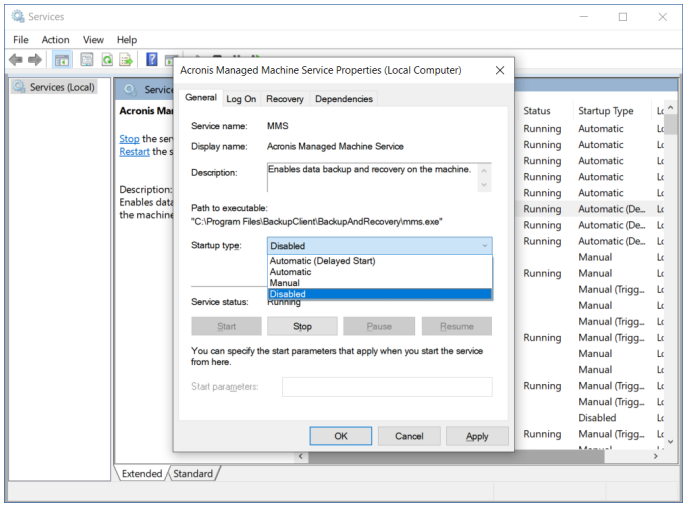
Operations on the target machine

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. 192).

To migrate the data to the new management server

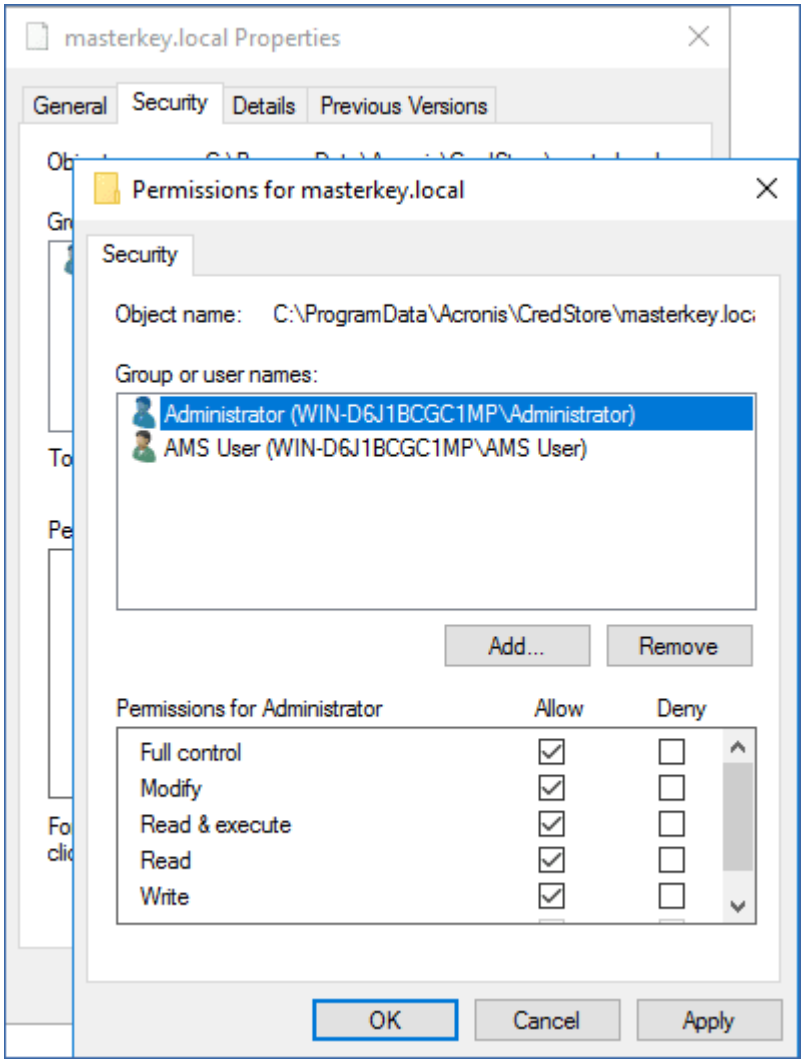
1. Set the host name of the machine on which you will install the new management server. This name must be the same as the name of the machine with the original management server.
2. Create a firewall rule to block all traffic on TCP port 9877.
3. Run the Acronis Cyber Protect setup program.
   a. Accept 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.



 © Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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. [If there is an `NGMP` folder on the server] 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
     ```

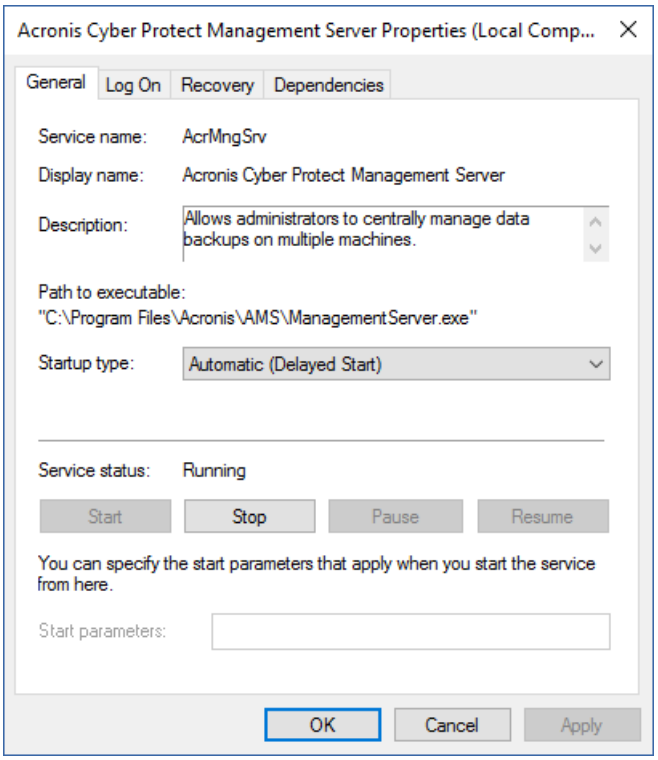
   - Create directory junction `latest` and point it to the folder named after the current NGMP version, for example:

     ```
     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\dml_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**.

© Acronis International GmbH, 2003-2026



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.

Registering a management server to the Centralized Dashboard

You can register a management server to the Centralized Dashboard by using the command-line interface. After that, you will see the data from the management server in the Centralized Dashboard.

Prerequisites

- The management server is installed and running.

To register a management server to the Centralized Dashboard

1. On the machine, on which the management server is installed, run the command-line tool as an administrator.
2. Navigate to the Account server folder (usually, `C:\Program Files\Acronis\AccountServer`).
3. Run the following command.

© Acronis International GmbH, 2003-2026

```
reg_acep_collector.exe local register -p <local_ams.param> -c <cental_ams_
address.com> -l local_ams_address.com
```

where:

`local_ams.param` is the file which contains the management server parameters.

`cental_ams_address.com` is the FQDN or the IP address of the Centralized Dashboard without the schema (http or https) or the port.

`local_ams_address.com` (optional parameter) is the FQDN or IP URI with schema and port of the local management server (for example, https://10.34.194.207:9877)

For example:

```
reg_acep_collector.exe local register -p local_ams.param -c 10.34.197.11
```

or

```
reg_acep_collector.exe local register -p C:\Users\Admin\Downloads\superset-srv1.param
-c cental_ams_address.com
```

Input example

```
c:\Program Files\Acronis\AccountServer>reg_acep_collector.exe local register /p win-
onprem2.param /c 10.34.197.11
2024/01/03 13:04:41 INFO local mode
2024/01/03 13:04:41 INFO register
2024/01/03 13:04:41 INFO collector config:
SourceUID: EE41D64C-26F5-4342-B9F2-66D2C8ACCE32
ImporterAddress: 10.34.197.11
CollectorAddress: https://win-onprem2:9877
CollectorHostName: win-onprem2
ClientID: 8e8ffc25-39b8-4182-ad40-2dd73f0be39f
ClientSecret: 2ee6j5y3l373pdzzzl3ey6wr5ebx5xlbpq35lfeb2kfxve2ppjhe
Enabled: true

2024/01/03 13:04:41 INFO Success

c:\Program Files\Acronis\AccountServer
```

Output example (Encoded output file)


```
eyJjbGllbnRfaWQiOiI4ZThmZmMyNS0zOWI4LTQxODItYWQ0MC0yZGQ3M2YwYmUzOWYiLCJjbGllbnRfc2Vj
cmV0IjoiMmVlNmo1eTNsMzczcGR6enpsM2V5NndyNWVieDV4bGJwcTM1bGZlYjJrZnh2ZTJwcGpoZSIsImFk
ZHJlc3MiOiJodHRwczovL3dpbi1vbnByZW0yOjk4NzciLCJob3N0X25hbWUiOiJ3aW4tb25wcmVtMiJ9
```


© Acronis International GmbH, 2003-2026

Note

To see information about all parameters that you can use with reg_acep_tools, run the following command:

```
reg_acep_collector.exe local -help
```

4. Copy the `local_ams.params` file to the machine, on which Centralized Dashboard is installed.
5. On the machine, on which Centralized Dashboard is installed, run the command-line tool as an administrator.
6. Navigate to the Account server folder (usually, `C:\Program Files\Acronis\AccountServer`).
7. Run the following command:

```
reg_acep_collector central register -p <local_ams.param>
```

where:

`local_ams.params` is the file which contains the management server parameters.

For example:

```
reg_acep_collector central register -p local_ams.param
```

Note

It might take several minutes for the data of the management server to become visible on the Centralized Dashboard.

8. [Optional] To check the management servers that are registered to the Centralized Dashboard, run the following command:

```
reg_acep_collector.exe central list
```

[Example]

```
reg_acep_collector.exe central list
2024/01/04 15:38:36 INFO central mode
2024/01/04 15:38:37 INFO superset db connection string:
C:/ProgramData/Acronis/CentralizedDashboard/superset.db
2024/01/04 15:38:37 INFO clients list:
2024/01/04 15:38:37 INFO win-onprem2
2024/01/04 15:38:37 INFO p16-ams1
2024/01/04 15:38:37 INFO win-onprem2
2024/01/04 15:38:37 INFO DESKTOP-GCNCFC8
2024/01/04 15:38:37 INFO win-onprem1
2024/01/04 15:38:37 INFO DESKTOP-GCNCFC8
2024/01/04 15:38:37 INFO win-onperm3
2024/01/04 15:38:37 INFO ams1
2024/01/04 15:38:37 INFO Success

c:\Program Files\Acronis\AccountServer>
```


© Acronis International GmbH, 2003-2026

Unregistering a management server from the Centralized Dashboard

You can unregister a management server from the Centralized Dashboard by using the command-line interface. After that, the data from the management server will no longer be visible in the Centralized Dashboard.

Prerequisites

- The management server is installed and running.
- The management server is connected to the Centralized Dashboard.

To unregister a management server from the Centralized Dashboard

1. On the machine on which the management server is installed, run the command-line tool as an administrator.
2. Navigate to the account server folder (usually, `C:\Program Files\Acronis\AccountServer`).
3. Run the following command.

   ```
   reg_acep_collector local unregister>
   ```

   Note
   To see information about all parameters that you can use with reg_acep_tools, run the following command:

   ```
   reg_acep_collector.exe local -help
   ```

4. On the machine on which Centralized Dashboard is installed, run the command-line tool as an administrator.
5. Navigate to the account server folder (usually, `C:\Program Files\Acronis\AccountServer`).
6. Run the following command:

   ```
   reg_acep_collector.exe central unregister -l <local_ams_name>
   ```

   Input example

   ```
   c:\Program Files\Acronis\AccountServer>reg_acep_collector.exe central unregister -l
   ams1
   2024/01/04 15:43:43 INFO central mode
   2024/01/04 15:43:44 INFO superset db connection string:
   C:/ProgramData/Acronis/CentralizedDashboard/superset.db
   2024/01/04 15:43:44 INFO unregister client
   2024/01/04 15:43:45 INFO Success

   c:\Program Files\Acronis\AccountServer>
   ```


© Acronis International GmbH, 2003-2026

Example for checking the output

```
c:\Program Files\Acronis\AccountServer>reg_acep_collector.exe central list
2024/01/04 15:48:05 INFO central mode
2024/01/04 15:48:05 INFO superset db connection string:
C:/ProgramData/Acronis/CentralizedDashboard/superset.db
2024/01/04 15:48:05 INFO clients list:
2024/01/04 15:48:05 INFO win-onprem2
2024/01/04 15:48:05 INFO p16-ams1
2024/01/04 15:48:05 INFO win-onprem2
2024/01/04 15:48:05 INFO DESKTOP-GCNCFC8
2024/01/04 15:48:05 INFO win-onprem1
2024/01/04 15:48:05 INFO DESKTOP-GCNCFC8
2024/01/04 15:48:05 INFO win-onperm3
2024/01/04 15:48:05 INFO Success

c:\Program Files\Acronis\AccountServer>
```

`ams1` is not listed in the output.

The data for the unregistered management server will be dropped automatically within 24 hours.

Device discovery

By using the device discovery functionality, you can:

- Gain complete visibility of the network devices that are available in the organization's networks.
- Use synchronization with Active Directory to reduce the efforts for provisioning resources and managing machines in a large Active Directory domain.
- Automate the installation of protection agents and the registration of machines by detecting the machines in your Active Directory domain or local network.
- Install protection agents on multiple workloads.

You can use one of the following methods to perform device discovery:

- Active Directory discovery.

  During an Active Directory discovery, the discovery agent 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.
- Local network discovery by using Device Sense ™. For more information, see "Device discovery by using Device Sense ™" (p. 208).
- Manual discovery – By using a machine IP address or host name, or by importing a list of machines from a file.

  During a manual discovery, the existing protection agents are updated and re-registered. If you perform the device discovery by using the same account under which an agent is registered, the agent will only be updated to the latest version. If you perform device discovery by using another account, the agent will be updated to the latest version and re-registered under the tenant to which the account belongs.

 © Acronis International GmbH, 2003-2026

You can also configure passive device discovery by using Device Sense ™, and view detailed information about the devices that are available in the corporate local area networks in your organization. For more information, see "Passive device discovery by using Device Sense ™" (p. 209).

Discovering multiple devices

The flow of discovering multiple devices can be summarized in the following steps:

1. Selecting the discovery method:
   - Active Directory discovery – By using a domain controller for the complete automated flow or a discovery agent for the flow with manual preconfiguration.
   - Local network discovery by using Device Sense ™.
   - Manual discovery – By using a machine IP address or host name, or by importing a list of machines from a file.
2. [For Active Directory discovery (flow with manual preconfiguration) and Manual discovery] Selecting the machines that you want to add to your tenant.
3. [For Active Directory discovery and Manual discovery] Selecting how to add these machines:
   - Install a protection agent and additional components on the machines, and register them in the Cyber Protect console.
   - Register the machines in the Cyber Protect console (if a protection agent was already installed).
   - Add the machines to the Cyber Protect console as unmanaged devices, without installing a protection agent.

   You can also apply a protection plan, monitoring plan, and a remote management plan to the machines on which you install a protection agent or which you register in the Cyber Protect console.
4. [For Active Directory discovery (flow with manual preconfiguration) and Manual discovery] Providing administrator credentials for the selected machines.
5. [For Active Directory discovery (flow with manual preconfiguration) and Manual discovery] Verifying that you can connect to the machines by using the provided credentials.

The machines that are shown in the Cyber Protect console, are divided into the following categories:

- **Discovered devices** – Machines that are discovered, but a protection agent is not installed on them.
- **Machines with agents** – Machines on which a protection agent is installed.
- **Discovered devices**/ **Devices without agent** – Machines on which a protection agent can be installed.
- **Discovered devices**/ **Local network** - Machines and network devices that were discovered by scanning local networks by using Device Sense ™.
- **Discovered devices**/ **Active Directory** - Machines that were discovered by searching the Active Directory.
- **Discovered devices**/ **Manual / From text file** - Machines that were added manually or from a text file.

 © Acronis International GmbH, 2003-2026

Device discovery requirements

Before using the device discovery functionality, ensure that the following requirements are met:

- For the **Complete automatic onboarding via Active Directory** flow, at least one domain controller with an installed protection agent must be available in your local network or Active directory domain.
- For the **Manual preconfiguration and automatic onboarding** flow, at least one machine with an installed protection agent must be available in your local network or Active directory domain. This agent will be used as a discovery agent.
- You must be assigned the Administrator role.

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.

Adding multiple devices

Before adding multiple devices, ensure that the requirements are met. For more information, see "Device discovery requirements" (p. 203).

Note
The functionality is not supported for adding domain controllers due to additional permissions required for the agent service to run.

Search Active Directory

To add multiple devices from the Active Directory

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Click **Add**.
3. In **Multiple devices**, click **Discover devices**.
   The discovery wizard opens.
4. Select the discovery agent that will perform the scan to detect machines.

   Note
   A discovery agent is a workload on which a protection agent is installed.
   The discovery agent must be a member of the Active Directory domain.
   You can select an agent that is associated with the selected unit or its child units.

5. Select **Search Active Directory**, and then click **Next**.

 © Acronis International GmbH, 2003-2026

6. In the **Search Active Directory** window, select how to search for the machines, and then click **OK**.

Option	Description
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.

7. In the list of discovered machines, select the machines that you want to add, and then click **Next**.

   The **Select onboarding option** tab opens. The following onboarding options are available.

Option	Description
Complete automatic onboarding via Active Directory	This option uses a domain controller on which a discovery agent is installed to onboard discovered devices from Active Directory. No manual preconfiguration of the devices is required.
Manual preconfiguration and automatic onboarding	This option requires manual preconfiguration of the devices and uses a discovery agent to onboard discovered devices.
Add as unmanaged machines	This option adds the discovered devices to the console as unmanaged devices, without installing a protection agent on them.

8. Depending on the onboarding option that you will select, do the following:
   - If you selected **Complete automatic onboarding via Active Directory**, complete steps 4-13 from the corresponding procedure.
   - If you selected **Manual preconfiguration and automatic onboarding**, complete steps 4-11 from the corresponding procedure.
   - If you selected **Add as unmanaged machines**, select the user account under which to register the devices, and then click **Add**.

Scan local network

To discover multiple devices by scanning the local network

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Click **Add**.
3. In **Multiple devices**, click **Discover devices**.

   The discovery wizard opens.
4. Click **Scan**.

© Acronis International GmbH, 2003-2026

The active device discovery scan starts. You are redirected to the **Discovered devices** > **Local Area Network** screen. When the scan completes, a notification is displayed. This notification shows the number of devices that were discovered during the scan and includes a link to the list of devices where you can see additional details about them.

What to do next:

- You can click the **View newly discovered devices** link in the notification, and view the devices and details about them on the **Local Area Network** tab.
- You can remotely install a protection agent on the discovered devices and register them. For more information, see "Installing agents remotely" (p. 216).
- You can exclude devices from discovery. For more information, see "Excluding devices from discovery" (p. 219).

Manually or by importing a file

To add multiple devices manually or by importing a file

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Click **Add**.
3. In **Multiple devices**, click **Discover devices**.
   The discovery wizard opens.
4. Click **Specify manually or import from file**.
5. Add machines by using one of the following options.
   - To add machines manually:
     a. In the **Add machine** field, enter the IPv4 address or hostname of the machine.
     b. Repeat the previous step for each machine that you want to add.
   - To add machines by importing a file:
     a. Click **Import machine list from file**.
     b. In the **Import machine list from file** window, drop the text file that contains the list of machines, or click **Browse**, navigate to the file, select it, and then click **Open**.
     The file must contain IP addresses or hostnames, one per line. Here is an example of the content of the file:

     ```
     156.85.34.10
     156.85.53.32
     156.85.53.12
     EN-L00000100
     EN-L00000101
     ```

   After adding machine addresses manually or importing from a file, the agent will try to ping the added machines and check their availability.
6. Click **Next**.
   The **Select onboarding option** tab opens. The following onboarding options are available.

 © Acronis International GmbH, 2003-2026

Option	Description
Complete automatic onboarding via Active Directory	This option uses a domain controller on which a discovery agent is installed to onboard discovered devices from Active Directory. No manual preconfiguration of the devices is required.
Manual preconfiguration and automatic onboarding	This option requires manual preconfiguration of the devices and uses a discovery agent to onboard discovered devices.
Add as unmanaged machines	This option adds the discovered devices to the console as unmanaged devices, without installing a protection agent on them.

7. Depending on the onboarding option that you will select, do the following:
   - If you selected **Complete automatic onboarding via Active Directory**, complete steps 4-13 from the corresponding procedure.
   - If you selected **Manual preconfiguration and automatic onboarding**, complete steps 4-11 from the corresponding procedure.
   - If you selected **Add as unmanaged machines**, select the user account under which to register the devices, and then click **Add**.

Requirements on User Account Control (UAC)

On a machine that is running Windows 7 or later and is not a member of an Active Directory domain, centralized management operations (including remote installation) require that UAC and UAC remote restrictions be disabled.

To disable UAC

Do one of the following depending on the operating system:

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

To disable UAC remote restrictions

© Acronis International GmbH, 2003-2026

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, we recommend that after finishing the management operation (for example, remote installation), you revert both settings to their original state: **EnableLUA**=**1** and **LocalAccountTokenFilterPolicy** = **0**

Agent components

When you add multiple devices that were discovered by searching in the Active Directory, you can select to install additional components.

The following table provides more information about the agent components that you can install.

Component	Description
Mandatory component	
Agent for Windows	This agent backs up disks, volumes, files and will be installed on Windows machines. It will be always installed, not selectable.
Additional components	
Antimalware and URL filtering	This component enables the Antivirus & Antimalware protection and URL filtering module in protection plans. Even if you select not to install it, it will be automatically installed later, if any of these modules is enabled in a protection plan for the machine.
Agent for Hyper-V	This agent backs up Hyper-V virtual machines. It 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. It 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. It 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. It will be installed on domain controllers. It will be installed if selected and application detected on a machine.
Agent for	This agent backs up VMware virtual machines. It will be installed on Windows machines

© Acronis International GmbH, 2003-2026

VMware (Windows)	that have network access to vCenter Server. It will be installed if selected.
Agent for Microsoft 365	This agent backs up Microsoft 365 mailboxes to a local destination. It will be installed on Windows machines. It will be installed if selected.
Agent for Oracle	This agent backs up Oracle databases. It 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. It will be installed on Windows machines. It will be installed if selected. Supported on Windows 7 Service Pack 1 and later, and Windows Server 2008 R2 Service Pack 1 and later.
Command-line tool	Supports the command-line interface with the **acrocmd** utility. **acrocmd** 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.
Bootable Media Builder	Creates bootable media. Supported on Windows and Linux.

Device discovery by using Device Sense ™

Device Sense ™ uses a sophisticated combination of techniques to scan the local networks of organizations to discover and identify devices. In addition to discovering physical and virtual machines and tablets, Device Sense ™ also discovers other network devices, such as routers, switches, printers, smartphones, and IP cameras.

By using Device Sense ™, you can achieve:

- Comprehensive network visibility - Identification of every device that is connected to a client's network.
  This helps you to maintain an accurate asset inventory and to effectively manage and support your IT infrastructure, which is essential for asset tracking and lifecycle management, and also ensures compliance with licensing agreements.
- Security and compliance - Detection of unauthorized or rogue devices that could pose security risks. Device Sense ™ helps you to ensure that each device in the network complies with security policies and regulatory requirements.
- Efficient allocation of resources - Understanding of the scope and scale of a client's network, thus allocating resources more efficiently and achieving better service planning.

Device discovery by using Device Sense ™ includes the following features:

- Automatic smart selection of discovery agents and networks to scan
- Prevention of device discovery in home or non-corporate networks

© Acronis International GmbH, 2003-2026

Note
Passive discovery by using Device Sense ™ will not scan networks that have a smaller number of agents than the number that is specified in the **Prevent device discovery in non-corporate networks** setting. At the organization level, the preconfigured value for this setting is 3, but it can be overwritten at unit level. To ensure that passive discovery scans all corporate networks, you can update the setting as suitable for your organization. For more information, see "Configuring passive device discovery" (p. 209).

- On-demand active device discovery
- Device categorization by types
- Advanced search and filtering options for browsing discovered devices
- Comprehensive details of discovered devices
- Remote installation of protection agent on discovered devices, with application of protection plans

You can use Device Sense ™ to perform passive device discovery scan or active device discovery scan. For more information, see "Passive device discovery by using Device Sense ™" (p. 209) and "Active device discovery by using Device Sense ™" (p. 210).

Note
The retention period of the information about discovered devices in the database is 3 months.

Passive device discovery by using Device Sense ™

Passive device discovery is a non-intrusive method to identify and catalog devices within a network environment without actively probing or sending requests to those devices in the organization's network.

Passive device discovery collects the following device data:

- Device name
- Device type
- OS family
- Manufacturer
- Model
- MAC address
- IP address

Configuring passive device discovery

Passive device discovery continuously scans the networks in your organization for devices. By using passive device discovery, you gain visibility of the organization's networks and the number and type of devices that are available in these networks.

To configure the passive device discovery settings

 © Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Settings** > **Management**.
2. Click the **Passive device discovery** tab.
3. Ensure that the **Enable passive device discovery** switch is enabled.
   The system automatically assigns Windows agents as discovery agents.
4. [Optional] Change the default settings.

Setting	Description
Smart auto-selection of discovery agents	Number of agents that will be automatically selected to perform passive device discovery in the local network. The default value is 1.* The maximum value is 3.
Prevent device discovery in non-corporate networks	Minimum number of agents that must be present in a network to classify it as a corporate environment and enable its scan. The default value is 3.* The maximum value is 1000.
Enhanced identification of devices in a network	Enable or disable the use of multicast signals for more precise identification of device types joining the local network. By default, the switch is disabled.*

   * The default value might differ. However, you can change the default values according to your organization's needs.
5. Click **Save**.

Active device discovery by using Device Sense ™

Active device discovery is a method used in network management in which a system actively probes or communicates with devices on a network to identify and gather information about them.

You can retrieve comprehensive and accurate data about devices in the networks, thus ensuring that all device information is clear and visible.

Active device discovery collects the following device data:

- Device name
- Device type
- OS family
- Manufacturer
- Model
- IP address
- MAC address

Running an active device discovery scan by using Device Sense ™

You can run an active scan for comprehensive data collection and identification of the devices that are connected to the local network.

To run an active scan

© Acronis International GmbH, 2003-2026

1. In the Protection console, go to **Devices** > **Discovered devices**.
2. Click the **Local network** tab.
3. Click **Run active scan**.
4. In the **Deployment agent** field, select a workload that is registered. The protection agent that is installed on this workload will be used as a deployment agent.
5. Select the network in which you want to run active scan.
6. Click **Run**.

   Active device discovery scan starts. When the scan completes, a notification is displayed. This notification shows the number of devices that were discovered during the scan and includes a link to the list of devices where you can see additional details about them.

Note
You cannot run multiple active scans simultaneously. If an active scan is in progress, you must cancel it or wait for it to complete before you can start a new scan.

Ports used by Device Sense ™

This topic lists the ports that Device Sense ™ uses.

Passive device discovery uses the following ports.

Name	Port	Comment
DHCP	udp/67	Listens for REQUEST messages
NBNS	udp/137	Listens for NAME REGISTRATION REQUEST and NAME REFRESH REQUEST packets
NBDS (Browser)	udp/138	Listens for announcement messages
SSDP	udp/1900	Listens for M-SEARCH and NOTIFY messages
WSD	udp/3702	Listens for wsd:Probe messages
MDNS	udp/5353	Listens for various service info announcements
LLMNR	udp/5355	Listens for queries
TUYA	udp/6668	Listens for discovery packets

When **Enhanced identification of devices on a network** is enabled, Device Sense ™ uses the following ports.

Name	Ports	Comment
SSDP	udp/1900	Sends M-SEARCH requests
WSD	udp/3702	Sends wsd:Probe requests

Active device discovery (on-demand scan flow) uses the following ports.

© Acronis International GmbH, 2003-2026

Name	Ports	Comment
FTP	tcp/21	Reads service banners
SSH	tcp/22	Reads service banners
TELNET	tcp/23	Reads banners
SMTP	tcp/25, tcp/587	Reads EHLO messages
RDNS	udp/53	Makes a reverse DNS request `*.in-addr.arpa`
HTTP	tcp/80, tcp/8080, and other common HTTP ports	Sends GET requests
NBNS	udp/135	Sends NBSTAT requests
SNMP	udp/161	Reads MIBs: Versions: v1, v2c; Communities: public
HTTPS	tcp/443, tcp/8443	Sends GET requests
SMB	tcp/445	Extracts data from NTLMv2 auth messages
RTSP	tcp/554	Sends OPTIONS requests
SSDP	udp/1900	Sends M-SEARCH
ARD	udp/3283	Sends Start packets
RDP	tcp/3389	Sends Connection Request and reads Connection Confirm
WSD	udp/3702	Sends wsd:Probe messages
AirPlay	tcp/5000, tcp/7000	Sends wsd:Probe messages
MDNS	udp/5353	Sends PTR messages
iRobot	udp/5678	Sends iRobot discover packets irobotmsc
VNC	udp/5900	Sends RFB ProtocolVersion and Security messages
MIIO	udp/54321	Sends Hello packets

Remote installation of agents

After the device discovery process, you can remotely install agents on discovered Windows devices.

The remote installation of agents is performed in the following way:

© Acronis International GmbH, 2003-2026

1. The discovery agent connects to the target machines by using the host name, IP address, and administrator credentials specified in the discovery wizard, and then uploads the `web_installer.exe` file to these machines.
2. The `web_installer.exe` file runs on the target machines in the unattended mode.
3. The web installer retrieves additional installation packages from the management server, and then installs them to the target machines via the `msiexec` command.
4. After the installation completes, the components are registered in the management server.

Note
Remote installation of agents is not supported for Domain Controllers, due to the additional permissions required for the agent service to run.

Preparing machines for remote installation manually

- 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, see "Requirements on User Account Control (UAC)" > To disable UAC.
- 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, see "Requirements on User Account Control (UAC)" > To disable UAC remote restrictions.
- 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**.
- Cyber Protect uses TCP port 445 for remote installation. Port 445 is automatically opened when you enable File and Printer Sharing.

Preparing machines for remote installation by using a GPO

You can configure and apply an Active Directory Group Policy object (GPO) to prepare a set of machines that are members of the Active Directory for remote installation of the Protection agents.

Prerequisites

- Your user is a member of the Domain Admins group or a domain administrator.
- **Group Policy Management Console** (GPMC) is installed on the machine on which you are logged in to create the GPO.

To prepare machines for remote installation by using a GPO

© Acronis International GmbH, 2003-2026

1. To open GPMC, press **Win** + **R**, type `gpmc.msc`, and then press **Enter**.
2. In the console tree, right-click the domain or organizational unit (OU) to which you want to apply a GPO.
3. Click **Create a GPO in this domain, and Link it here...**.
4. In the **New GPO** pop-up, enter a name for the GPO, and then click **OK**.
5. In the console tree, right-click the GPO that you created in the previous step, and then click **Edit...**.
6. Disable **Use Sharing Wizard**, by following the steps below.
   a. In the console tree, navigate to **User Configuration** > **Preferences** > **Windows Settings** > **Registry**.
   b. Right-click **Registry**, and then click **New** > **Registry Item**.
   c. In the **New Registry Properties** window, on the **General** tab, configure the registry item as follows.

Parameter	Value
Action	Update
Hive	`HKEY_CURRENT_USER`
Key Path	Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Value name	SharingWizardOn
Value type	`REG_DWORD`
Value data	0

   d. Click **Apply**, and then click **OK**.
7. [For Windows Vista and later versions] Disable User Account Control (UAC) by following the steps below.
   a. In the console tree, navigate to **Computer Configuration** > **Preferences** > **Windows Settings** > **Registry**.
   b. Right-click **Registry**, and then click **New** > **Registry Item**.
   c. In the **New Registry Properties** window, on the **General** tab, configure the registry item as follows.

Parameter	Value
Action	Update
Hive	`HKEY_LOCAL_MACHINE`
Key path	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
Value name	EnableLUA
Value type	`REG_DWORD`

© Acronis International GmbH, 2003-2026

Parameter	Value
Value Data	0

d. Click **Apply**, and then click **OK**.

8. [For Windows Vista and later versions] Disable User Account Control (UAC) Remote restrictions, by following the steps below.
   a. In the console tree, navigate to **Computer Configuration** > **Preferences** > **Windows Settings** > **Registry**.
   b. Right-click **Registry**, and then click **New** > **Registry Item**.
   c. In the **New Registry Properties** window, on the **General** tab, configure the registry item as follows.

Parameter	Value
Action	Update
Hive	`HKEY_LOCAL_MACHINE`
Key path	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Value name	LocalAccountTokenFilterPolicy
Value type	`REG_DWORD`
Value Data	1

   d. Click **Apply**, and then click **OK**.

9. Enable **File and Printer Sharing**, by following the steps below.
   a. In the console tree, navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Windows Defender Firewall with Advanced Security** > **Inbound Rules**.
   b. Right-click **Inbound Rules**, and then click **New Rule**.
   c. In **New Inbound Rule Wizard**, configure the rule as follows.
   d. On the **Rule Type** tab, select **Predefined**, select **File and Printer Sharing**, and then click **Next**.
   e. On the **Predefined Rules** tab, click **Next**.
   f. On the **Action** tab, select **Allow the connection**, and then click **Finish**.
   g. In the console tree, navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Windows Defender Firewall with Advanced Security** > **Outbound Rules**.
   h. Right-click **Outbound Rules**, and then select **New Rule**.
   i. In **New Outbound Rule Wizard**, configure the rule by performing the same actions as in steps d - f.

10. Link the GPO to the domain or OU, by following the steps below.

© Acronis International GmbH, 2003-2026

a. In the console tree, right-click the target domain or OU, and then click **Link an Existing GPO...**.
b. On the **Select GPO** screen, select the GPO that you created, and then click **OK**.

11. On the target machines that you want to prepare for a remote agent installation, force the Group Policy Update, by following the steps below.
    a. Run **Command Prompt** as an administrator.
    b. Run the following command:

    ```
    gpupdate /force
    ```

Installing agents remotely

Note

Remote installation of agents is supported for Windows devices only.

Agent installation on multiple devices is only available for devices that are in the same network and discovered by the same discovery method.

You can remotely onboard multiple discovered devices at once. The onboarding process consists of agent installation, plans application, and device registration.

Complete automatic onboarding via Active Directory

Prerequisites

At least one domain controller on which a protection agent is installed must be available in the Active Directory.

To add multiple devices by using the complete automated onbording via Active Directory

1. In the Protection console, go to **Devices** > **Discovered devices** > **Devices without agent**.
2. Select the devices that you want to protect.
3. Click **Install agent**.
4. On the **Select onboarding option** tab, click **Complete automatic onboarding via Active Directory**.
5. In the **Domain controller** field, select the domain controller.
6. In the **Domain administrator credentials** field, click **Select**.
7. On the **Credentials list** screen, select the credentials of the administrator account of the domain controller, and then click **Select credentials**.

   The domain controller scans the Active Directory for devices and displays them in a list. By default, all discovered devices are preselected, but you can clear the selection for the devices that you do not want to register and protect.
8. In the list of devices, ensure that the devices that you want to onboard are selected.
9. Click **Next**.
10. On the **Select agent components** tab, do the following:

© Acronis International GmbH, 2003-2026

a. To select the components that you want to install, click **Components to install**, and then select the components. For more information about the available components, see "Agent components" (p. 207).
b. In the **Settings** pane, configure the installation options.

Option	Description
Service logon account	The account under which the services will run. By default, **Use Service User Accounts** is selected. To change the default value, click **Change**.
Restart the device when required	Select this option if you want the device to be restarted when the installation of a component requires it.
Do not restart the device if a user is logged in	Select this option if you do not want the device to be restarted when a user is logged in to it.

c. Select the organization or unit under which you want to register the devices.
d. Click **Next**.

11. [Optional] On the **Select plans** tab, to select the protection plan that will be applied to the machines automatically, in the plan selection field, click **Change**, select the plan, and then click **Change** again.
12. Click **Next**.
13. On the **Review and register** screen, check the required licenses, and then do one of the following:
    - To select different plans, go to the **Select plans** tab, follow the procedure in step 11, and then click **Next** until you return to the **Review and register** screen.
    - To register the workloads, click **Register**.

Manual preconfiguration and automatic onboarding

Prerequisites

The devices that you want to add are configured for the remote agent installation, as described in "Preparing machines for remote installation by using a GPO" (p. 213).

To add multiple devices by using Manual preconfiguration and automatic onboarding

1. In the Protection console, go to **Devices** > **Discovered devices** > **Devices without agent**.
2. Select the devices that you want to protect.
3. Click **Install agent**.
4. On the **Select onboarding option** tab, click **Manual preconfiguration and automatic onboarding**, and then click **Next**.
5. On the **Select agent components** tab, do the following:
   a. In the **Deployment agent** field, select the workload that will be used for the remote agent installation and registration of the machines.

© Acronis International GmbH, 2003-2026

Note
A deployment agent is a workload on which a protection agent is installed.

b. To select the components that you want to install, click **Components to install**, and then select the components. For more information about the available components, see "Agent components" (p. 207).

c. In the **Settings** pane, configure the installation options.

Option	Description
Service logon account	The account under which the services will run. By default, **Use Service User Accounts** is selected. To change the default value, click **Change**.
Restart the device when required	Select this option if you want the device to be restarted when the installation of a component requires it.
Do not restart the device if a user is logged in	Select this option if you do not want the device to be restarted when a user is logged in to it.

d. Select the organization or unit under which you want to register the devices.

e. Click **Next**.

6. [Optional] On the **Select plans** tab, to select the protection plan that will be applied to the machines automatically, in the plan selection field, click **Change**, select the plan, and then click **Change** again.
7. Click **Next**.
8. On the **Credentials** tab, do the following:

a. Click **Add credentials**.

b. Select the credentials of a user with administrator rights to the selected devices, and then click **Select credentials**.

Important
Remote installation of agents only works without any preparations 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 custom administrator credentials, you must make additional manual preparations. For more information, see "Preparing machines for remote installation manually" (p. 213).

c. Click **Next**.

The system performs preliminary checks on the selected devices to ensure that they are suitable and that they have the correct setup for remote installation of the agent and the selected components.

9. On the **Connectivity** tab, do one of the following:

- If there are connectivity issues, resolve the identified connectivity issues by clicking **Change credentials for all devices**, and then click Next.

© Acronis International GmbH, 2003-2026

- If no connectivity issues are identified, click **Next**.

10. On the **Review and register** screen, check the required licenses, and then do one of the following:
    - To select different plans, go to the **Select plans** tab, follow the procedure in step 6, and then click **Next** until you return to the **Review and register** screen.
    - To register the workloads, click **Register**.

Note

A file named `RemoteInstallEntryPoint.bat` is deployed to each registered workload on the network. This file installs the components required to deploy protection agents.

On rare occasions, security scans may flag this file as suspicious or malicious. If this happens, add it to the allowlist/whitelist so the installation can complete successfully.

Excluding devices from discovery

When you exclude devices from discovery, they will not be listed in the results of discovered devices when a device discovery scan is run.

To exclude a device from discovery

1. In the Protection console, go to **Discovered devices**.
2. Click the device that you want to exclude from discovery, and then click **Exclude from discovery**.
   The device is excluded from discovery and is added to the list of devices on the **Exclusions** page.

Connecting to discovered devices remotely

You can connect remotely to discovered Windows or macOS devices and provide one-time assistance.

Prerequisites

- [For RDP connections] RDP is enabled on the Windows device.
- [For Apple Screen Sharing connections] Apple Screen Sharing is enabled on the macOS device.

To connect remotely to a discovered device

1. In the Cyber Protect console, go to **Devices** > **Discovered devices**.
2. Click the device to which you want to connect remotely.
3. Click **Remote desktop**, and then, depending on the operating system of the device, click the view mode.

Operating system	Connection protocol	View mode
Windows	RDP	**Control** - In this mode, you will be able to observe and perform operations on the remote device.

© Acronis International GmbH, 2003-2026

Operating system	Connection protocol	View mode
macOS	Apple Screen Sharing	**Control** - In this mode, you will be able to observe and perform operations on the remote device. **View-only** - In this mode, you will only be able to observe the remote device. **Curtain** - available only for macOS devices. If you connect to the remote device in curtain mode, the display of the remote device will be dimmed, and the remote user will not be able to see your actions on the device.

4. [If Connect Client is not installed on your device] In the **Connect to workload** dialog, click **Download Connect Client**, download and install the client on your device, and then click **Connect**.
5. [If a confirmation pop-up appears] Click **Open Connect Client**.
6. [For Windows devices] In the **RDP Authentication** pop-up window, enter the username, password, and domain, and then click **Connect**.
7. [For macOS devices]In the **Authentication** window, select an authentication option, provide the required credentials depending on the option that you selected, and then click **Connect**.

Authentication option	Description
With macOS credentials	You will be allowed to establish the remote connection after you provide username and password of an administrator user of the remote device.
by asking to observe	You will be allowed to establish the remote connection in observe mode after the user who is logged in on the remote device allows it.
with VNC password	You will be allowed to establish the remote connection after you provide the VNC password.

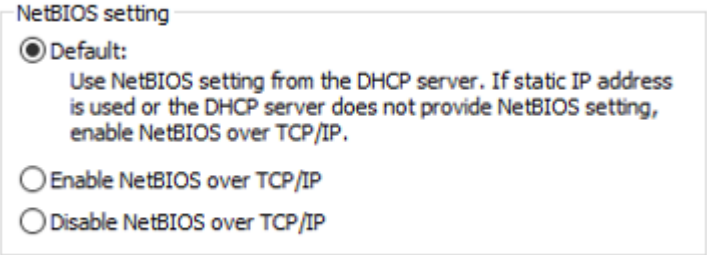
Note
The authentication options that you will see depend on the screen sharing options that are configured on the remote macOS device.

Troubleshooting device discovery

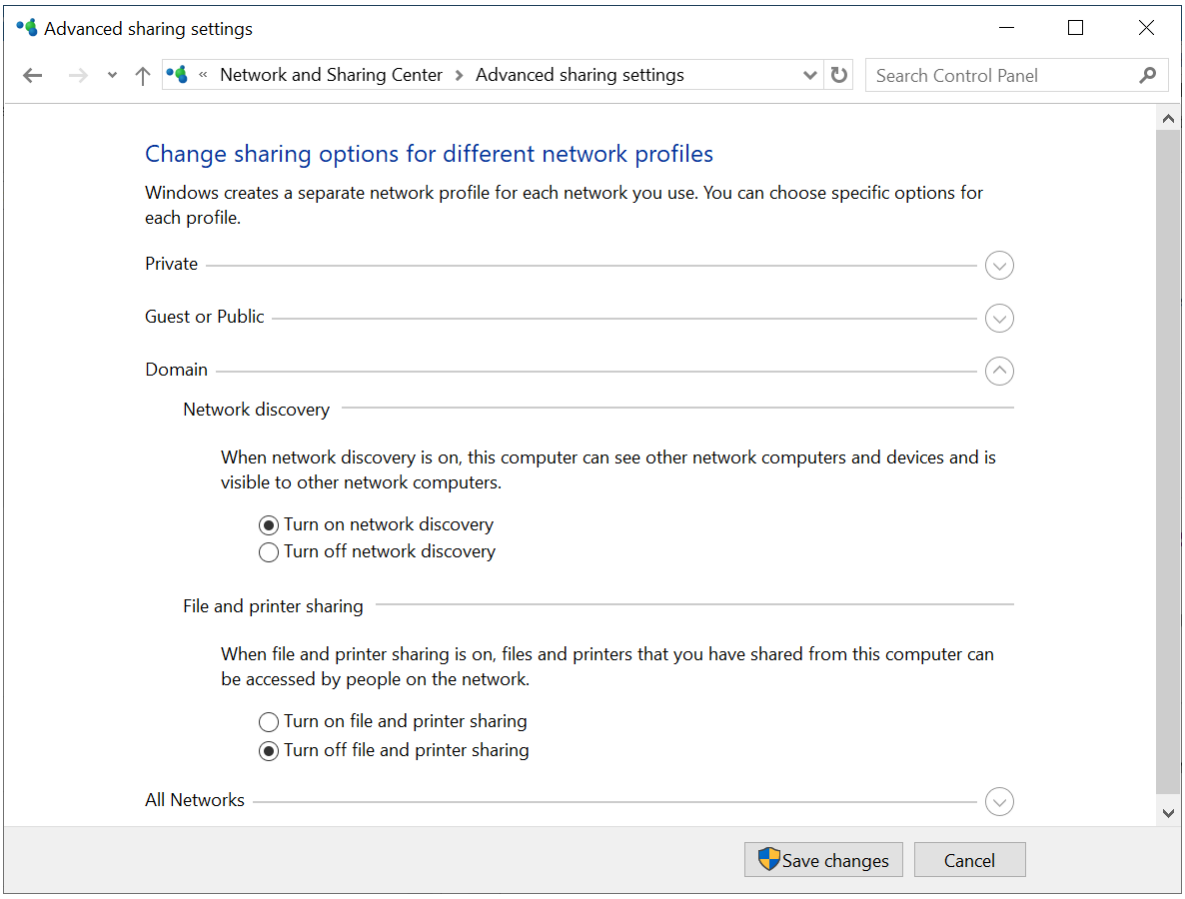
If you have any issues with the device discovery functionality, try to check the following:

© Acronis International GmbH, 2003-2026

- Check if NetBIOS over TCP/IP is enabled or set to default.



- In the "Control Panel\Network and Sharing Center\Advanced sharing settings", turn on Network discovery.



- Check if the Function Discovery Provider Host service is running on the machine that performs discovery and on the machines to be discovered.
- Check if the Function Discovery Resource Publication service is running on the machines to be discovered.

Checking for software updates

This functionality is available only to organization administrators.

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

© Acronis International GmbH, 2003-2026

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**.

Updating agents

You can update an agent from the Cyber Protect console or by downloading and running a newer version of their installation file.

Prerequisites

- On Windows machines, Cyber Protect features require Microsoft Visual C++ 2017 Redistributable. Ensure that it is already installed on your machine or install it before updating the agent. After the installation, a restart may be required. You can find the Microsoft Visual C++ Redistributable package on the Microsoft website: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.
- [For on-premises deployments] Ensure that the components for remote installation are installed with the management server. For more information, see "Components for remote installation" (p. 124).

To check the agent version

1. In the Cyber Protect console, go to **Settings** > **Agents**.
2. See the **Agent version** column.
3. [Optional] For additional information, select the machine with the agent, and then click **Details**.

To update an agent from the Cyber Protect console

1. Update the management server.
2. In the Cyber Protect console, go to **Settings** > **Agents**.

   In the **Agent version** column, the outdated agents are marked with an orange exclamation mark.
3. Select the machines on which you want to update the agents. The machines must be online.
4. Click **Update agent**.
5. Select the deployment agent.
6. Specify administrator credentials for the target machine.
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.

Update progress is shown on the **Activities** tab.

 © Acronis International GmbH, 2003-2026

Note
During the update, any backups that are in progress will fail.

To update the Cyber Protect definitions on a machine

1. In the Cyber Protect console, go to **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. In the Cyber Protect console, go to **Settings** > **Agents**.
2. Select the machine to which you want to assign the Updater role, and then click **Details**.
   For more information this role, see "Agents with the Updater role" (p. 321).
3. In the **Cyber Protect definitions** section, enable the switch **Use this agent to download and distribute patches and updates**.

To clear cached data on an agent

1. In the Cyber Protect console, go to **Settings** > **Agents**.
2. Select the machine on which you want to clear the cached data (outdated update files and patch management data), and then click **Clear cache**.

Updating protection agents on BitLocker-encrypted 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.

Affected agent versions:

- 16.0.37277

You can also check whether an update introduces changes to Startup Recovery Manager in the release notes of the protection agent.

To update the agent on a workload with BitLocker and Startup Recovery Manager enabled

1. On the workload on which you want to update the agent, suspend or disable BitLocker.
2. Update the agent.
3. Restart the workload.
4. Enable BitLocker.

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.

 © Acronis International GmbH, 2003-2026

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 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 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 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.

© Acronis International GmbH, 2003-2026

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 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 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 console, go to **Settings** > **Agents**.
2. Select the machine where the agent was installed.
3. Click **Delete**.

Ports, services, and processes used by 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).

© Acronis International GmbH, 2003-2026

Important
The outgoing ports 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.

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 International GmbH, 2003-2026

Acronis Anti-malware protection			
For more information about antivirus and antimalware features, see "Supported operating systems for antivirus and antimalware protection" (p. 681).			
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

© Acronis International GmbH, 2003-2026

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

*** 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 available for machines running Windows 10 and later.

© Acronis International GmbH, 2003-2026

Managing workloads in the Cyber Protect console

This section describes how to manage your workloads in the Cyber Protect console.

Accessing the Cyber Protect console

To access the Cyber Protect 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 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 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, see "Administrators and units".

© Acronis International GmbH, 2003-2026

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, see "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 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 console.

Configuring Edge, Opera, or Chrome

- If you access the Cyber Protect 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. 231).
- 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. 232).

Note
You can also configure the browsers by using a Group Policy in the Active Directory domain.

Configuring Firefox

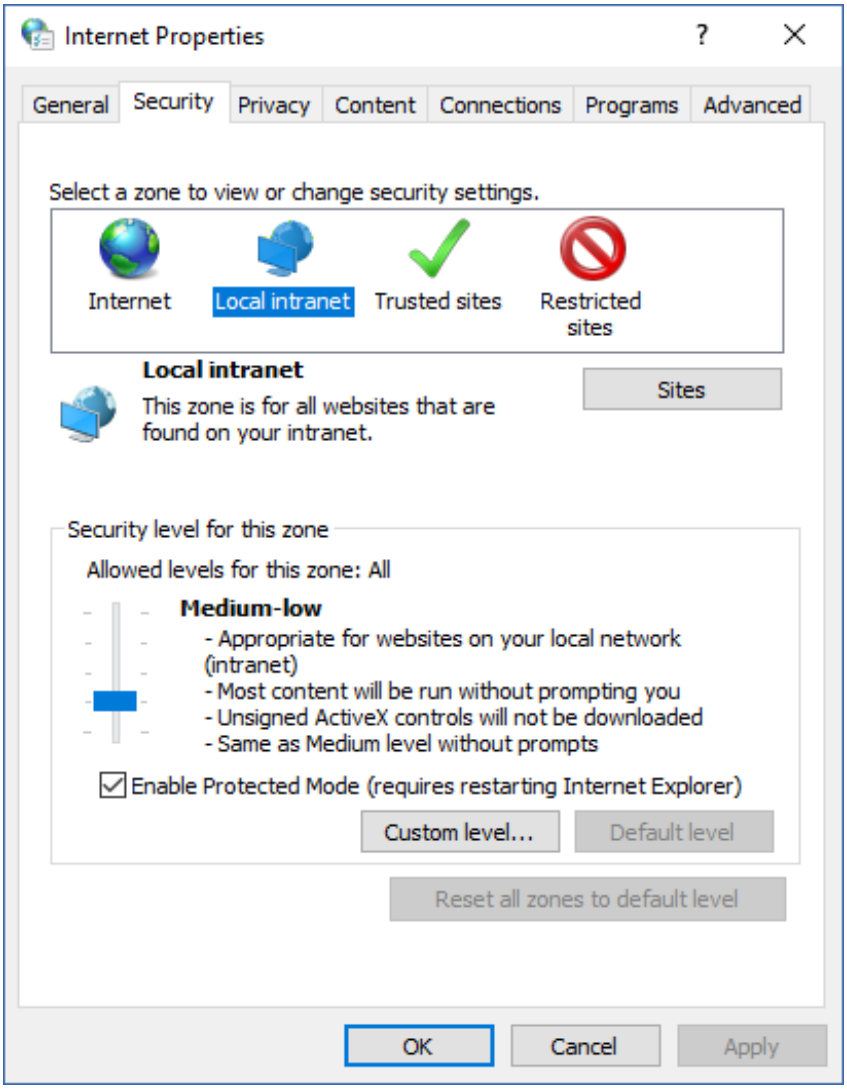
1. In the Firefox address bar, enter `about:config`, and then press Enter.
2. Click **Accept the Risk and Continue**.
3. In the search field, enter `network.negotiate-auth.trusted-uris`.
4. Double-click the `network.negotiate-auth.trusted-uris` preference, and then enter the address of the Cyber Protect web console login page.
5. In the search field, enter `network.automatic-ntlm-auth.trusted-uris`.

 © Acronis International GmbH, 2003-2026

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.

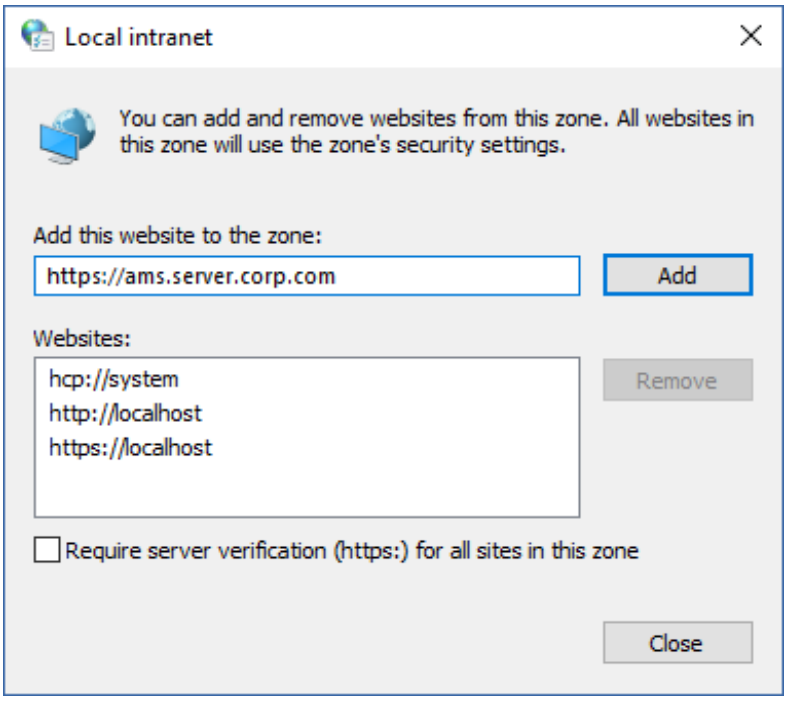
Adding the console to the list of local intranet sites

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 console login page, and then click **Add**.

© Acronis International GmbH, 2003-2026

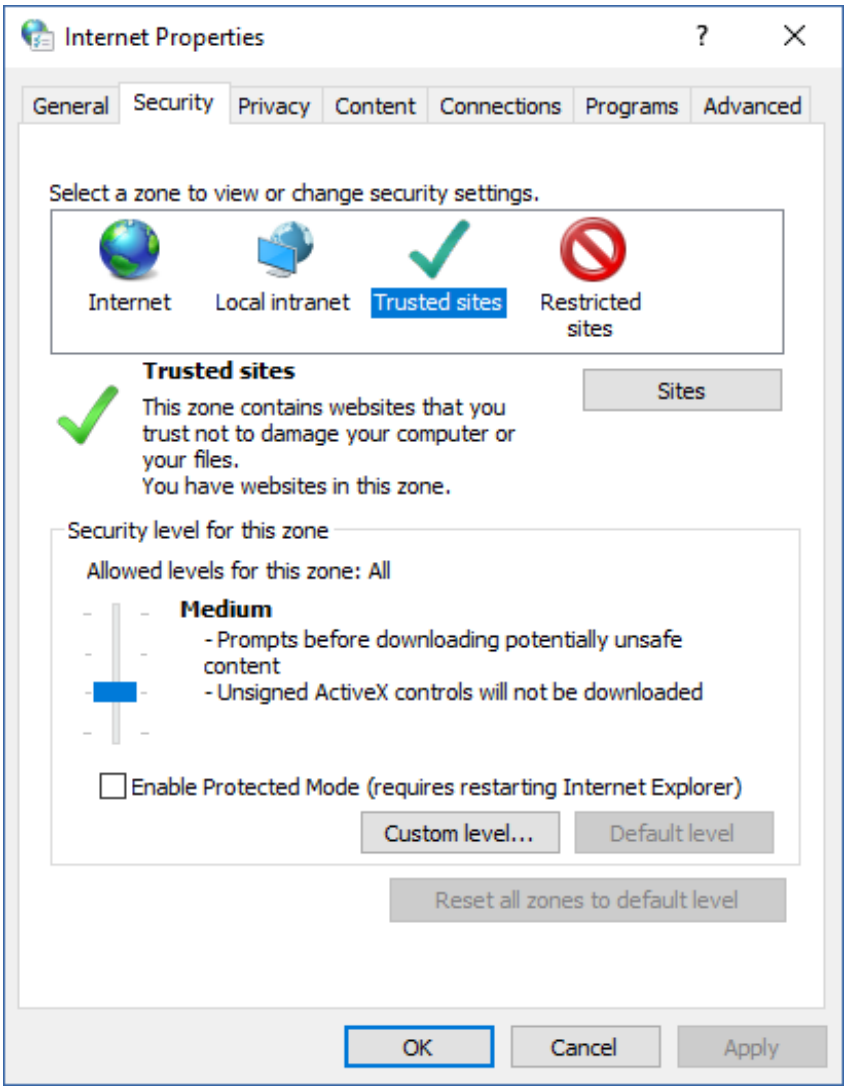


5. Click **Close**.
6. Click **OK**.

Adding the console to the list of trusted sites

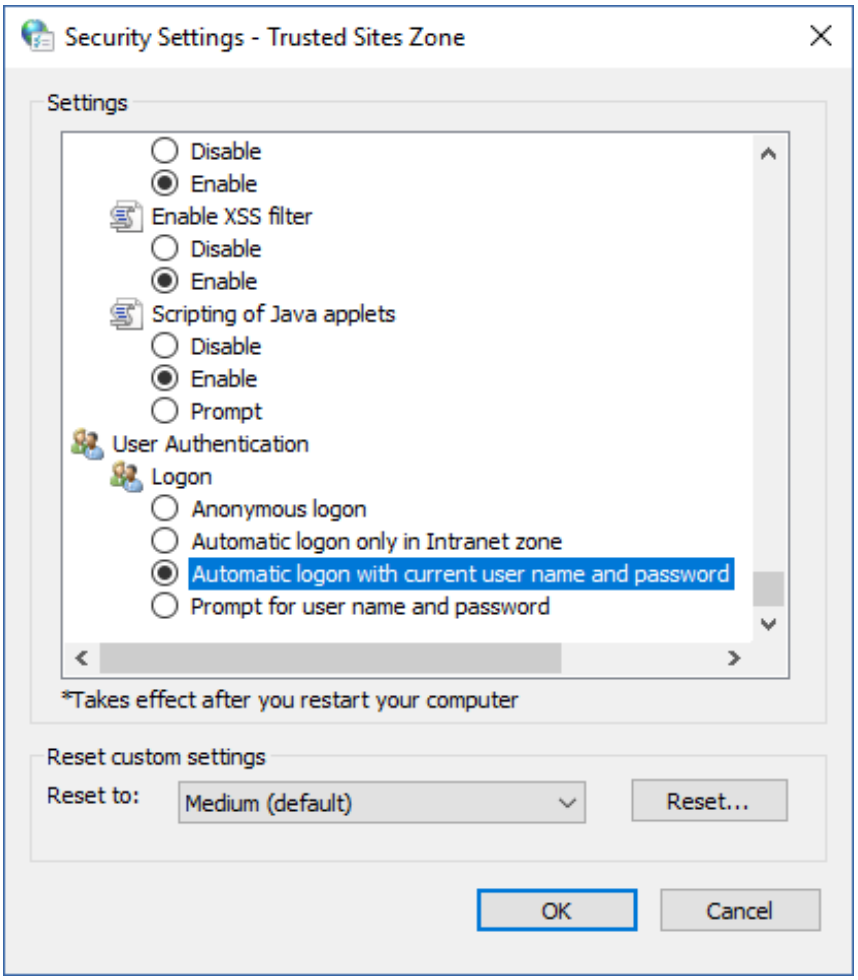
1. Go to **Control Panel** > **Internet Options**.
2. On the **Security** tab, select **Trusted sites**, and then click **Custom level**.

© Acronis International GmbH, 2003-2026



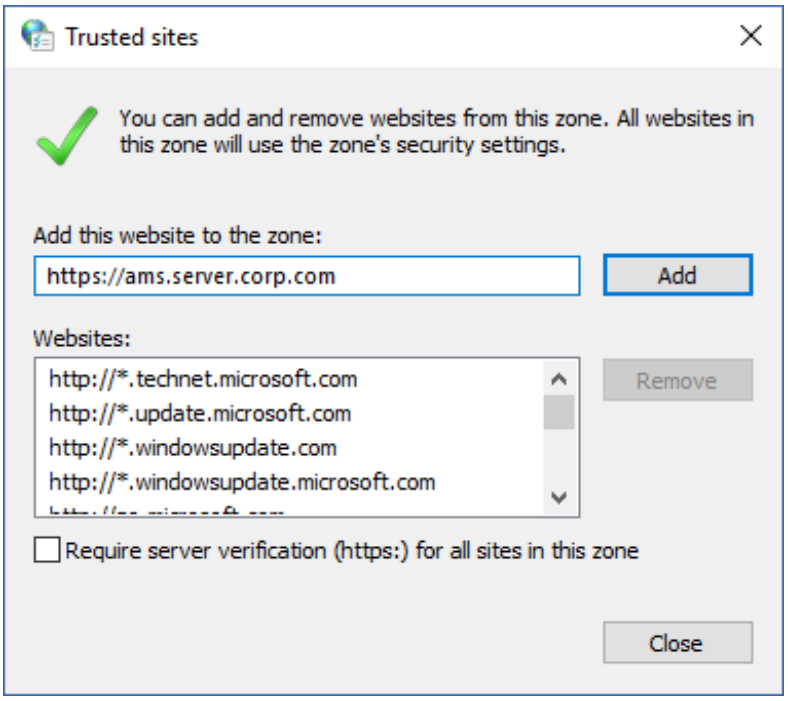
3. Under **Logon**, select **Automatic logon with current user name and password**, and then click **OK**.

© Acronis International GmbH, 2003-2026



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 console login page, and then click **Add**.

© Acronis International GmbH, 2003-2026



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

Allowing only HTTPS connections to the web console

Note
Accessing the Cyber Protect 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 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,
```


© Acronis International GmbH, 2003-2026

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

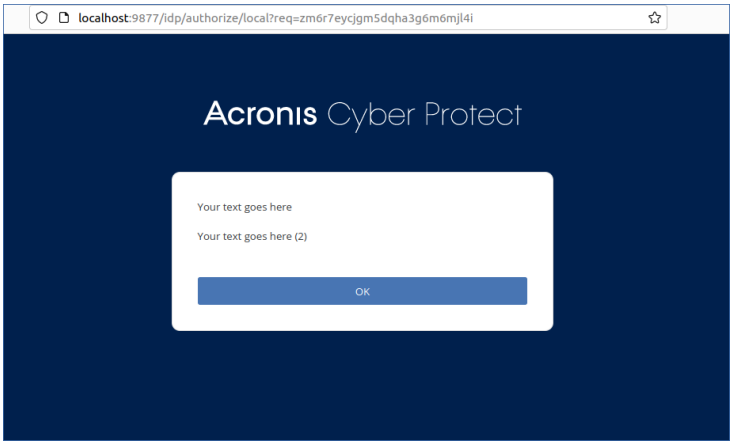
1. Open **Terminal**.
2. Run the following command in any directory:

```
sudo service acronis_asm restart
```

Adding a custom message to the web console

You can add a custom message to the Cyber Protect 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.

© Acronis International GmbH, 2003-2026

For more information on how to disable or enable the self-protection feature, see "Self-protection" (p. 688).

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 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",
```

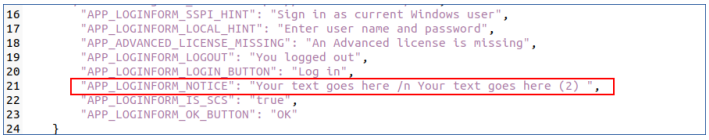
8. Under the `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"` line, add the following lines:

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

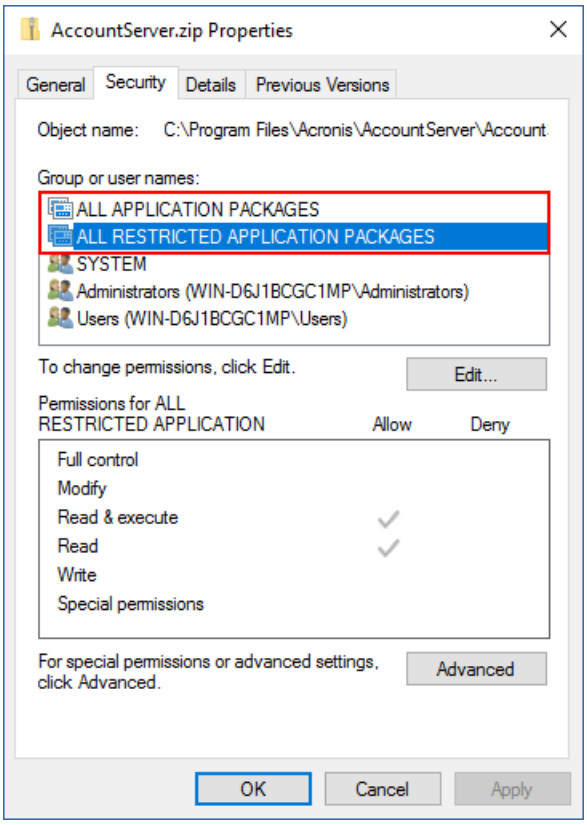
```
"APP_LOGINFORM_OK_BUTTON": "OK"
```

   For example:



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.

© Acronis International GmbH, 2003-2026



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. 242).

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 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:

© Acronis International GmbH, 2003-2026

```
"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. 242).

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 from 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 console by using the HTTPS protocol.

Optionally, you can configure the management server to prohibit accessing the Cyber Protect console via HTTP, by redirecting all users to HTTPS. For more information, see "Allowing only HTTPS connections to the web console" (p. 235).

Note
Accessing the Cyber Protect 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**.

 © Acronis International GmbH, 2003-2026

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 starts acronis_mms
```

Using a certificate issued by a trusted certificate authority

Prerequisites

- The certificate file (in the .pem format)
- The file with the private key for the certificate (usually in the .key format)
- [If the key is password-protected] The private key password

© Acronis International GmbH, 2003-2026

Important
All aliases of the management server must be included in the certificate as Subject Alternative Names (SAN).

To configure the SSL certificate settings

1. Copy the certificate and private key files to the machine on which the management server runs.
2. 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`
3. Locate the following section:

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

4. Between the quotation marks in the `"cert_file"` line, specify the full path to the certificate file.
   For example:
   - Windows (note the forward slashes):

```
"cert_file": "C:/certificate/local-domain.ams.pem"
```

   - Linux:

```
"cert_file": "/home/user/local-domain.ams.pem"
```

5. Between the quotation marks in the `"key_file"` line, specify the full path to the private key file.
   For example:
   - Windows (note the forward slashes):

```
"key_file": "C:/certificate/private.key"
```

   - Linux:

```
"key_file": "/home/user/private.key"
```

6. [If the file is password-protected] Between the quotation marks in the `"passphrase"` line, specify the password.
   For example:

```
"passphrase": "my_password"
```


© Acronis International GmbH, 2003-2026

Note

If the `"passphrase": "",` line is missing in your `api_gateway.json` configuration file, add it manually.

For example:

```
"tls": {
    "cert_file": "C:/certificate/local-domain.ams.pem",
    "key_file": "C:/certificate/private.key",
    "passphrase": "my_password",
}
```

7. Save the `api_gateway.json` file.

Important

Ensure that you do not accidentally delete any commas, brackets, or quotation marks in the configuration file.

8. 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
```

Protection plans and modules

To protect your data, you must create protection plans, and then apply them to your workloads.

A protection plan consists of different protection modules. Enable the modules that you need and configure their settings to create protection plans that meet your specific needs.

The following modules are available:

© Acronis International GmbH, 2003-2026

- **Backup**. Backs up your data sources to a local or cloud storage.
- **Disaster recovery**. Launches exact copies of your machines in the cloud site and switches the workload from corrupted original machines to the recovery servers in the cloud.
- **Antivirus and Antimalware protection**. Checks your workloads by using a built-in antimalware solution.
- [For cloud deployments] **Endpoint Detection and Response (EDR)**. Detects suspicious activity on the workload, including attacks that have gone unnoticed, and generates incidents to help you understand how an attack happened and how to prevent it from happening again.
- **URL filtering**. Protects your machines from threats originating from the Internet, by blocking access to malicious URLs and downloadable content.
- **Windows Defender Antivirus.** Manages the settings of Windows Defender Antivirus to protect your environment.
- **Microsoft Security Essentials**. Manages the settings of Microsoft Security Essentials to protect your environment.
- **Vulnerability assessment**. Checks Windows, Linux, macOS, Microsoft third-party products, and macOS third-party products installed on your machines and notifies you about vulnerabilities.
- **Patch management**. Installs patches and updates for Windows, Linux, macOS, Microsoft third-party products, and macOS third-party products on your machines, to resolve the detected vulnerabilities.
- **Data protection map**. Discovers data in order to monitor the protection status of important files.

Creating a protection plan

You can create a protection plan in the following ways:

- On the **Devices** tab. Select one or more workloads to protect, and then create a protection plan for them. Only the modules that are applicable to the selected types of workloads are shown.
- On the **Plans** > **Protection** tab. Create a protection plan, and then select one or more workloads to which to apply the plan.

You can apply a protection plan to more than one workload. You can also apply multiple protection plans to the same workload. To learn more about possible conflicts, see "Resolving plan conflicts" (p. 250).

When you create a protection plan in which the **Backup** module is enabled, you can enable backup encryption. For more information, see "Encryption" (p. 385).

To create a protection plan

Devices

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Select the workloads that you want to protect, and then click **Protect**.
3. [If there are already applied plans] Click **Add plan**.
4. Click **Create plan**.

 © Acronis International GmbH, 2003-2026

5. [Optional] To rename the protection plan, click the pencil icon, enter a new name, and then click **OK**.
6. [Optional] To enable or disable a module in the plan, toggle the switch next to the module name.
7. [Optional] To configure a module, expand it, and then change the settings.
8. Click **Create**.

Plans > Protection

1. In the Cyber Protect console, go to **Plans** > **Protection**.
2. Click **Create plan**.
3. [Optional] To rename the plan, click the pencil icon, enter a new name, and then click **OK**.
4. [Optional] To enable or disable a module in the plan, toggle the switch next to the module name.
5. [Optional] To configure a module, expand it, and then change the settings according to your needs.
6. [Optional] To add workloads to the plan, click **Add devices**, and then select the workloads.

   Note
   You can create a plan without adding any workloads. To add workloads later, edit the plan. For more information, see "Applying a protection plan to a workload" (p. 245).

7. Click **Create**.

To run a module on demand (such as **Backup**, **Antivirus and Antimalware protection**, **Vulnerability assessment**, **Patch management**, or **Data protection map**), click **Run now**.

Actions with protection plans

After creating a protection plan, you can perform the following actions with it:

- Apply a plan to a workload or a device group.
- Rename a plan.
- Edit a plan.
  You can enable and disable the modules in a plan, and change their settings.
- Enable or disable a plan.
  A disabled plan will not run on the workloads to which it is applied.
  This action is convenient for administrators who intend to protect the same workload with the same plan later. The plan is not revoked from the workload and you can quickly restore the protection by re-enabling the plan.
- Revoke a plan from a workload.
  A revoked plan is not applied to the workload anymore.
  This action is convenient for administrators who do not need rapid protection for the same workload with the same plan again. To restore the protection provided by a revoked plan, you must know the name of this plan, select it from the list of available plans, and then re-apply it to the respective workload.

 © Acronis International GmbH, 2003-2026

- Stop a plan.
  This action stops all running backup operations on all workloads to which the plan is applied. Backups will start again according to the plan schedule.

  Antimalware scanning is not affected by this action and will proceed as configured in the schedule.
- Clone a plan.
  You can create an exact copy of an existing plan. The new plan is not assigned to any workloads.
- Export and import a plan.
  You can export a plan as a JSON file, which you can import back later. Thus, you do not need to create a new plan manually and configure its settings.
- Check the details of a plan.
- Check the activities and alerts related to a plan.
- Delete a plan.

Applying a protection plan to a workload

To protect a workload, you must apply a protection plan to it.

You can apply a plan from the **Devices** tab and from the **Plans** > **Protection** tab.

Devices

1. Select one or more workloads that you want to protect.
2. Click **Protect**.
3. [If another protection plan was already applied to the selected workloads] Click **Add plan**.
   A list of available protection plans is shown.
4. Select the protection plan that you want to apply, and then click **Apply**.

Plans > Protection

1. In the Cyber Protect console, go to **Plans** > **Protection**.
2. Select the protection plan that you want to apply.
3. Click **Edit**.
4. Click **Manage devices**.
5. In the **Devices** window, click **Add**.
6. Select the workloads to which you want to apply the plan, and then click **Add**.
7. In the **Devices** window, click **Done**.
8. In the protection plan panel, click **Save**.

Editing a protection plan

When you edit a plan, you can enable and disable the modules in it, and change their settings.

You can edit a protection plan for all workloads to which it is applied or only for selected workloads.

You can edit a plan from the **Devices** tab and from the **Plans** > **Protection** tab.

© Acronis International GmbH, 2003-2026

Devices

1. Select one or more workloads to which the plan is applied.
2. Click **Protect**.
3. Select the protection plan that you want to edit.
4. Click the ellipsis icon (...) next to the plan name, and then click **Edit**.
5. Click a module that you want to edit, and then configure its settings as needed.
6. Click **Save**.
7. [If you have not selected all workloads to which the plan is applied] Select the scope of the edit:
   - To edit the plan for all workloads to which it is applied, click **Apply the changes to this protection plan (this will affect other devices)**.
   - To change the plan only for selected workloads, click **Create a new protection plan only for the selected devices**.

     As a result, the existing plan will be revoked from the selected workloads. A new protection plan with the settings that you configured will be created and applied to these workloads.

Plans > Protection

1. In the Cyber Protect console, go to **Plans** > **Protection**.
2. Select the protection plan that you want to edit.
3. Click **Edit**.
4. Click the modules that you want to edit, and then configure their settings as needed.
5. Click **Save**.

Note
Editing a plan from the **Plans** > **Protection** tab affects all workloads to which that plan is applied.

Revoking a protection plan

When you revoke a plan, you remove it from one or more workloads. The plan still protects the other workloads to which it is applied.

Note
If a backup of a workload is currently running, the plan is revoked from that workload only after the backup completes.

You can revoke a plan from the **Devices** tab and the **Plans** > **Protection** tab.

Devices

1. Select the workloads from which you want to revoke the plan.
2. Click **Protect**.
3. Select the protection plan that you want to revoke.
4. Click the ellipsis icon (...) next to the plan name, and then click **Revoke**.

Plans > Protection

© Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Plans** > **Protection**.
2. Select the protection plan that you want to revoke.
3. Click **Edit**.
4. Click **Manage devices**.
5. In the **Devices** window, select the workloads from which you want to revoke the plan.
6. Click **Remove**.
7. In the **Devices** window, click **Done**.
8. In the protection plan template, click **Save**.

Enabling or disabling a protection plan

An enabled plan is active and runs on the workloads to which it is applied. A disabled plan is inactive – it is still applied to workloads but it does not run on them.

When you enable or disable a protection plan from the **Devices** tab, your action affects only the selected workloads.

When you enable or disable a protection plan from the **Plans** > **Protection** tab, your action affects all workloads to which this plan is applied. Also, you can enable or disable multiple protection plans.

Devices

1. Select the workload whose plan you want to disable.
2. Click **Protect**.
3. Select the protection plan that you want to disable.
4. Click the ellipsis icon (...) next to the plan name, and then click **Enable** or **Disable**, respectively.

Plans > Protection

1. In the Cyber Protect console, go to **Plans** > **Protection**.
2. Select one or more protection plans that you want to enable or disable.
3. Click **Edit**.
4. Click **Enable** or **Disable**, respectively.

Note
This action does not affect protection plans that were already in the target state. For example, if your selection includes both enabled and disabled plans, and you click **Enable**, all selected plans will be enabled.

Deleting a protection plan

When you delete a plan, it is revoked from all workloads and removed from the Cyber Protect console.

Note
If a backup of a workload is currently running, the plan is deleted only after the backup completes.

© Acronis International GmbH, 2003-2026

You can delete a plan from the **Devices** tab and the **Plans** > **Protection** tab.

Devices

1. Select any workload to which the protection plan that you want to delete is applied.
2. Click **Protect**.
3. Select the protection plan that you want to delete.
4. Click the ellipsis icon (...) next to the plan name, and then click **Delete**.

Plans > Protection

1. In the Cyber Protect console, go to **Plans** > **Protection**.
2. Select the protection plan that you want to delete.
3. Click **Delete**.
4. Confirm your choice by selecting the **I confirm the deletion of plan** check box, and then click **Delete**.

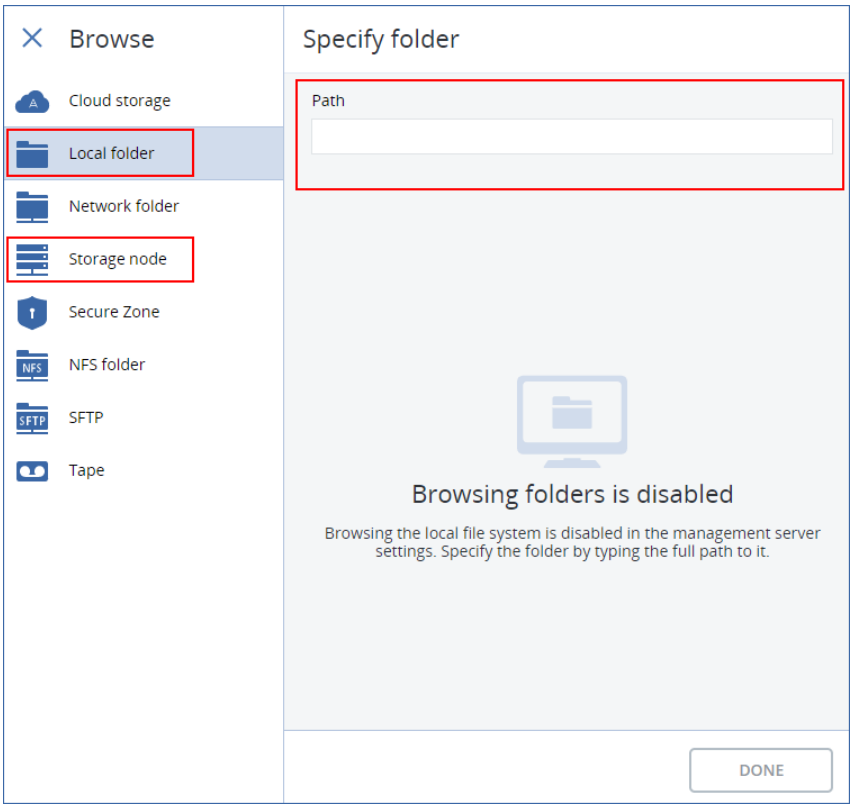
Disabling browsing of the folder tree

For security reasons, you can prevent users from browsing the folder tree in the **Local folder** and **Storage node** locations when they perform the following operations:

- Create a protection plan
- Create an off-host data protection plan (replication, validation, cleanup, conversion to VM)
- Add a location on the **Backup storage** tab of the Cyber Protect console
- Recover data
- Export a backup

Users are always able to specify the exact folder path.

© Acronis International GmbH, 2003-2026



To disable browsing of the folder tree

1. In a text editor, create a new file, and then save it as `custom_config.json`.
2. In the `custom_config.json` file, paste the following text:

```
{
"local_browsing_enabled": false
}
```

3. Save the edits.
4. Copy the `custom_config.json` file to the following folder:
   - Windows: `%ProgramData%\Acronis\WebServer`
   - Linux: `/var/lib/Acronis/WebServer`
5. Restart the Acronis Server Manager Service, as described in "To restart Acronis Service Manager Service in Windows" (p. 236).

To re-enable browsing of the folder tree

1. Open the `custom_config.json` file for editing.
   The file is located in the following folder:
   - Windows: `%ProgramData%\Acronis\WebServer`
   - Linux: `/var/lib/Acronis/WebServer`
2. Edit the text as follows:

© Acronis International GmbH, 2003-2026

```
{
"local_browsing_enabled": true
}
```

3. Save the file.
4. Restart the Acronis Server Manager Service, as described in "To restart Acronis Service Manager Service in Windows" (p. 236).

Resolving plan conflicts

You can apply multiple protection plans to the same workload. For example, you may apply one protection plan in which you enabled and configured only the **Antivirus and Antimalware** module, and another protection plan in which you enabled and configured only the **Backup** module.

You can combine protection plans in which different modules are enabled. You can also combine multiple protection plans in which only the **Backup** module is enabled. However, if any other module is enabled in more than one plan, a conflict occurs. To apply the plan, first you must resolve the conflict.

Conflict between a new and existing plan

If a new plan conflicts with an existing plan, you can resolve the conflict in one of the following ways:

- Create a new plan, apply it, and then disable the existing plan that conflicts with the new one.
- Create a new plan, and then disable it.

Conflict between an individual and group plan

If an individual protection plan conflicts with a group plan that is applied to a device group, you can resolve the conflict in one of the following ways:

- Remove the workload from the device group, and then apply the individual protection plan to it.
- Edit the existing group plan or apply a new group plan to the device group.

License issue

A protection plan module might require that a specific license is assigned to the protected workload. If the assigned license is not appropriate, you will not be able to run, update, or apply the protection plan in which the respective module is enabled.

To resolve a license issue, do one of the following:

- Disable the module that is not supported by the currently assigned license, and then continue using the protection plan.
- Change the assigned license manually in **Devices** > your workload > **Details** > **License**.

© Acronis International GmbH, 2003-2026

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

> **Note**
> 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.

Plan status

For protection and VM replication plans, for example, a clickable, color-coded status bar is available. This indicates the status of the plan on all workloads on which that plan is applied:

- OK (green)
- Warning (orange)
- Error (red)
- The plan is running (blue)
- The plan is disabled (gray)

You can click a section in the status bar to see the number of workloads that have the corresponding status.

© Acronis International GmbH, 2003-2026

Note
The plan status might not correspond to the workload status. For example, a protection plan might be successfully applied to a workload, and its status will appear as **OK** (green). At the same time, the workload could be offline, so its status on the **Devices** tab will be red.

Compatibility issues with plans

In some cases, applying a plan on a workload might cause compatibility issues.

You might observe the following issues:

- Conflicting plan – there is a conflict between the plan that you are applying and an already applied plan.
  For example, some settings in the plan might conflict with the settings in the already applied plan, the same workload might already have been protected as part of a device group, or a partner-level plan and a customer-level plan both have the same module enabled for the same workload.
- Incompatible operating system – the operating system of the workload is not supported.
- Unsupported agent – the version of the protection agent on the workload is outdated and does not support the configured functionality.
- Insufficient quota – there is not enough service quota in the tenant to assign to the selected workload.
- Incompatible workload type – the selected functionality is not available for this workload type.
- Missing advanced pack – the selected functionality is not available because a required advanced pack is not enabled for this customer.

The following table summarizes the possible compatibility issues for different plan types.

Issue/Plan type	Protection plan	Scripting plan	Monitoring plan	Remote management plan
Conflicting plan	+*	-	-	+
Incompatible operating system	+	+	+	+
Unsupported agent	+	+	+	+
Insufficient quota	+	+	+	+
Incompatible workload type	+	+	+	+
Missing advanced pack	+	-	-	-

* No conflicts are triggered if different backup settings are configured in multiple protection plans for the same workload.

© Acronis International GmbH, 2003-2026

If the plan is applied to up to 150 individually selected workloads, you will be prompted to resolve the existing conflicts before saving the plan. To resolve a conflict, remove the root cause for it or remove the affected workloads from the plan. For more information, see "Resolving compatibility issues" (p. 253). If you do not resolve the conflicts, depending on the type of compatibility issue, the whole plan or some of its modules will be disabled on the incompatible workloads, and alerts will be shown.

If the plan is applied to more than 150 workloads or to device groups, first it will be saved, and then checked for compatibility. Depending on the type of compatibility issue, the whole plan or some of its modules will be disabled on the incompatible workloads, and alerts will be shown.

Resolving compatibility issues

Depending on the cause of the compatibility issues, you can perform different actions to resolve the compatibility issues as part of the process of creating or editing a plan.

To resolve the compatibility issues

Conflicting plan

1. Click **Review issues**.
2. [To resolve the issue by removing workloads from the new plan]
   a. On the **Conflicting plan** tab, select the workloads that you want to remove.

      Note
      You cannot remove workloads that are part of a device group.

   b. Click **Remove selected workloads from the plan**.
   c. Click **Remove**, and then click **Close**.
3. [To resolve the issue by disabling the plans that are already applied to the workload]
   a. Click **Disable applied plans**.
   b. Click **Disable**, and then click **Close**.
4. [To resolve the issue by disabling the conflicting modules in the plans that are already applied to the workload]
   a. Click **Disable conflicting modules in applied plans**.
   b. Click **Disable**, and then click **Close**.

Incompatible OS

1. Click **Review issues**.
2. [To resolve the issue by removing workloads from the plan]
   a. On the **Incompatible operating system** tab, select the workloads that you want to remove.
   b. Click **Remove workloads from plan**.
   c. Click **Remove**, and then click **Close**.
3. [For monitoring plans] [To resolve the issue by disabling a monitor in the plan]

 © Acronis International GmbH, 2003-2026

   a. On the **Incompatible operating system** tab, select the monitors that you want to remove.
   b. Click **Disable monitor**.
   c. Click **Disable**, and then click **Close**.
4. [For plans different from monitoring] [To resolve the issue by disabling a module in the plan]
   a. On the **Incompatible operating system tab**, expand the conflicting module.
   b. Click **Disable module in plan**.
   c. Click **Disable**, and then click **Close**.

Unsupported agent

1. Click **Review issues**.
2. On the **Unsupported agent** tab, select the workloads that you want to remove.
3. Click **Remove workloads from plan**.
4. Click **Remove**, and then click **Close**.

Insufficient quota

1. Click **Review issues**.
2. On the **Insufficient quota** tab, select the workloads that you want to remove.
3. Click **Remove workloads from plan**.
4. Click **Remove**, and then click **Close**.

Incompatible workload type

1. Click **Review issues**.
2. On the **Insufficient quota** tab, select the workloads that you want to remove.
3. Click **Remove workloads from plan**.
4. Click **Remove**, and then click **Close**.

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.

 © Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.
   This action is not available for ESXi hosts.
3. [Optional] To create a new group, do the following:
   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`	• Host name for physical machines • Name for virtual machines • Database name • Email address for mailboxes	`name = 'en-00'`	Yes
`parameters.MacAddress`	MAC address.	`parameters.MacAddress LIKE '00-`	Yes

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation
		`22-4D-50-25-E5'`	

`comment`	Comment for a device. It can be specified automatically or manually.
	
	Default value:
	
	• For physical machines running Windows, the computer description in Windows is automatically copied as a comment. This value is synchronized every 15 minutes.
	• Empty for other devices.
	
	Note
	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.
	
	To refresh the automatically synchronized comments for your devices, restart the Managed Machine Service in **Windows Services** or run the following commands at the command prompt:
	
	`net stop mms`
	
	`net start mms`
		`comment = 'important machine'`
		
		`comment = ''` (all machines without a comment)
			Yes

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation

	To view the comment, under **Devices**, select the device, click **Details**, and then locate the **Comment** section.
	
	To add or change the comment, click **Add** or **Edit**.
	
	For devices on which a protection agent is installed, there are two separate comment fields:
	
	• Agent comment
	  ◦ For physical machines running Windows, the computer description in Windows is automatically copied as a comment. This value is synchronized every 15 minutes.
	  ◦ Empty for other devices.
	
	Note
	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.
	
	• Device comment		

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation
	◦ If the agent comment is specified automatically, it is copied as a device comment. Manually added agent comments are not copied as device comments. ◦ Device comments are not copied as agent comments. A device can have one or the both comments specified, or have them both blank. If the both comments are specified, the device comment has priority. To view an agent comment, under **Settings** > **Agents**, select the device with the agent, click **Details**, and then locate the **Comment** section. To view a device comment, under **Devices**, select the device, click **Details**, and then locate the **Comment** section. To add or change a comment manually, click **Add** or **Edit**.		
`ip`	IP address (only for physical machines).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Yes
`cpuArch`	CPU architecture.	`cpuArch = 'x64'`	Yes

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation
	Possible values: • `'x64'` • `'x86'`		
`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: • `true` • `false`	`insideVm = true`	Yes
`tzOffset`	Machine timezone offset in minutes.	`tzOffset = 120`	Yes
`parameters.Architecture`	Operating system architecture. Possible values: • `'x86'` • `'x64'`	`parameters.Architecture = 'x86'`	Yes
`osName`	Operating system name.	`osName LIKE '%Windows XP%'`	Yes
`osType`	Operating system type. Possible values: • `'windows'` • `'linux'` • `'macosx'`	`osType IN ('linux', 'macosx')`	Yes
`osProductType`	The operating system product type. Possible values: • `'dc'` Stands for Domain Controller. • `'server'` • `'workstation'`	`osProductType = 'server'`	Yes

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation
`virtualType`	Virtual machine type. Possible values: • `'vmwesx'` VMware virtual machines. • `'mshyperv'` Hyper-V virtual machines. • `'pcs'` Virtuozzo virtual machines. • `'hci'` Virtuozzo Infrastructure virtual machines. • `'scale'` Scale Computing HC3 virtual machines. • `'ovirt'` oVirt virtual machines	`virtualType = 'vmwesx'`	Yes
`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.	`osVersionMminor = 1`	Yes
`isOnline`	Machine availability. Possible values: • `true` • `false`	`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.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Yes

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation
	To get the unit ID, under **Devices**, select the device, click **Details** > **All properties**. The ID is shown in the `ownerId` field.		
`state`	Device state. Possible values: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	No
`status`	Resource status. Possible values: • `'notProtected'` • `'ok'` • `'warning'` • `'error'` • `'critical'`	`status = 'ok'`	No
`protectedByPlan`	Devices that are protected by a protection plan with a given ID.	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation
	To get the plan ID, click **Plans** > **Backup**, select the plan, click on the diagram in the **Status** column, and then click on a status. A new search with the plan ID will be created.		
`okByPlan`	Devices that are protected by a protection plan with a given ID and have an **OK** status.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`errorByPlan`	Devices that are protected by a protection plan with a given ID and have an **Error** status.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`warningByPlan`	Devices that are protected by a protection plan with a given ID and have a **Warning** status.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`runningByPlan`	Devices that are protected by a protection plan with a given ID and have a **Running** status.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`interactionByPlan`	Devices that are protected by a protection plan with a given ID and have an **Interaction Required** 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.	`id != '4B2A7A93-A44F-4155-BDE3-`	Yes

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation
	To get the device ID, under **Devices**, select the device, click **Details** > **All properties**. The ID is shown in the `id` field.	`A023C57C9431'`	

`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. The format is `'YYYY-MM-DD HH:MM'`.	`nextBackupTime >= '2022-08-11'`	No
`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 **Devices**, select the machine, click **Details** > **All properties**. Use the `"id"` value of the `agent` property.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Yes
`resourceType`	Resource type. Possible values: • `'machine'` • `'virtual_machine.vmwesx'` • `'virtual_machine.mshyperv'` • `'virtual_machine.rhev'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Yes

© Acronis International GmbH, 2003-2026

Attribute	Meaning	Search query examples	Supported for group creation
	• 'virtual_machine.kvm' • 'virtual_machine.xen'		
hasAsz	Protection agent on a physical machine with Acronis Secure Zone. Possible values: • true • false	hasAsz=true	Yes
chassis	Machine chassis type. Possible values: • unknown • laptop • desktop • server • other	chassis='laptop'	Yes

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')

© Acronis International GmbH, 2003-2026

Operator	Meaning	Examples
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'	This operator is used to test if an expression matches the wildcard pattern. The following wildcard operators can be used: • * or % The asterisk and the percent sign represent zero, one, or multiple characters • _ The underscore represents a single character	name LIKE 'en-00' name LIKE '*en-00' name LIKE '*en-00*' name LIKE 'en-00_'
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')
= or ==	*Equal to* operator.	osProductType = 'server'
!= or <>	*Not equal to* operator.	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'
<	*Less than* operator.	memorySize < 1024
>	*Greater than* operator.	diskSize > 300GB
<=	*Less than or equal to* operator.	lastBackupTime <= '2022-05-11 00:15'
>=	*Greater than or equal to* operator.	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".

© Acronis International GmbH, 2003-2026

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
Cyber protection	Not available in Cyber Backup editions	Shows overall information about the size of backups, blocked malware, blocked URLs, found vulnerabilities, and installed patches.
Protection status	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.
Patch installation status	Not available in Cyber Backup editions	Shows the number of machines grouped by patch installation status.
Missing updates by category	Not available in Cyber Backup editions	Shows the number of missing updates by category.
Disk health status	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.

© Acronis International GmbH, 2003-2026

Active alerts details	Available in all editions	Shows detailed information about the active alerts.
Existing vulnerabilities	Available in all editions	Shows the existing vulnerabilities for the operating systems and applications in your environment, and the affected machines.
Patch installation history	Not available in Cyber Backup editions	Shows detailed information about the patches that were installed.
Recently affected	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:

© Acronis International GmbH, 2003-2026

- 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%.

© Acronis International GmbH, 2003-2026

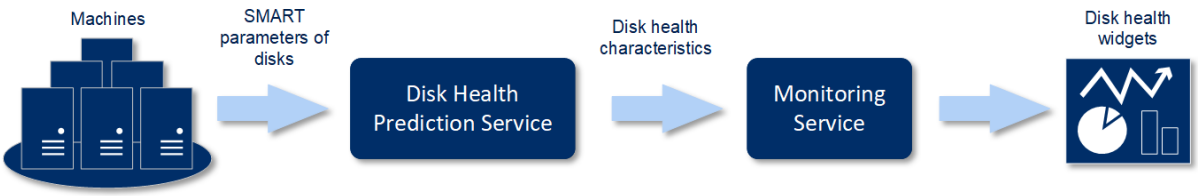
- **Warning**
  Disk health is between 30% and 70%.
- **Critical**
  Disk health is between 0% and 30%.
- **Calculating disk data**
  The current disk status and forecast are being calculated

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 console.



Disk health widgets

The results of the disk health monitoring are presented in the following widgets that are available in the Cyber Protect 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

© Acronis International GmbH, 2003-2026

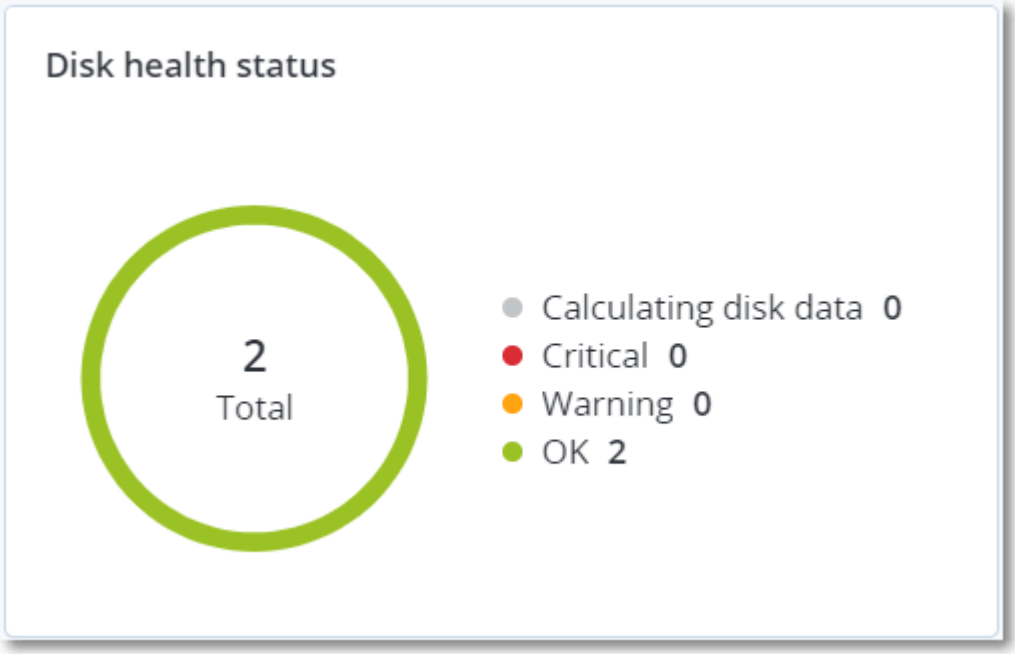
organizational unit. Only the most critical disk status is shown. The other statuses are shown in a tooltip when you hover over a particular block. The machine block size depends on the total size of all disks of the machine. The machine block color depends on the most critical disk status found.

- 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

© Acronis International GmbH, 2003-2026

- Will be improved

- **Disk health status** is a pie chart widget that shows the number of disks for each status.



© Acronis International GmbH, 2003-2026

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 widget

The data protection map allows you to obtain detailed information about the number, size, location, and protection status of all files that you consider important (based on their file extensions). The map provides a tree view, and you can drill down and up the tree.

Note
The **Data protection map** option is disabled by default in newly created protection plans.

The size of each block in the map depends on the total number and size of the files that belong to the customer, organizational unit, or machine that the block represents.

Blocks can indicate the protection status of files in the entity that they represent. The status is based on the backup plan that is currently applied on the entity (location or machine):

- **High** – all files with the extensions specified by you are backed up.
- **Medium** – 1-20% of the files are not being backed up.
- **Low** – 21-50% of the files are not being backed up.
- **Critical** – 51-100% of the files are not being backed up.

You can hover over each colored block to see more information about the number of unprotected files and their location. To protect them, click **Protect all files**.

You can also download a detailed report in CSV format.

© Acronis International GmbH, 2003-2026

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 patches on machines by the patch installation status.

Patch installation history

This widget shows the detailed information about patches on machines.

Missing updates by categories

This widget shows the number of missing updates per category. The following categories are shown:

© Acronis International GmbH, 2003-2026

- Security updates
- Critical updates
- Other

Backup scanning details

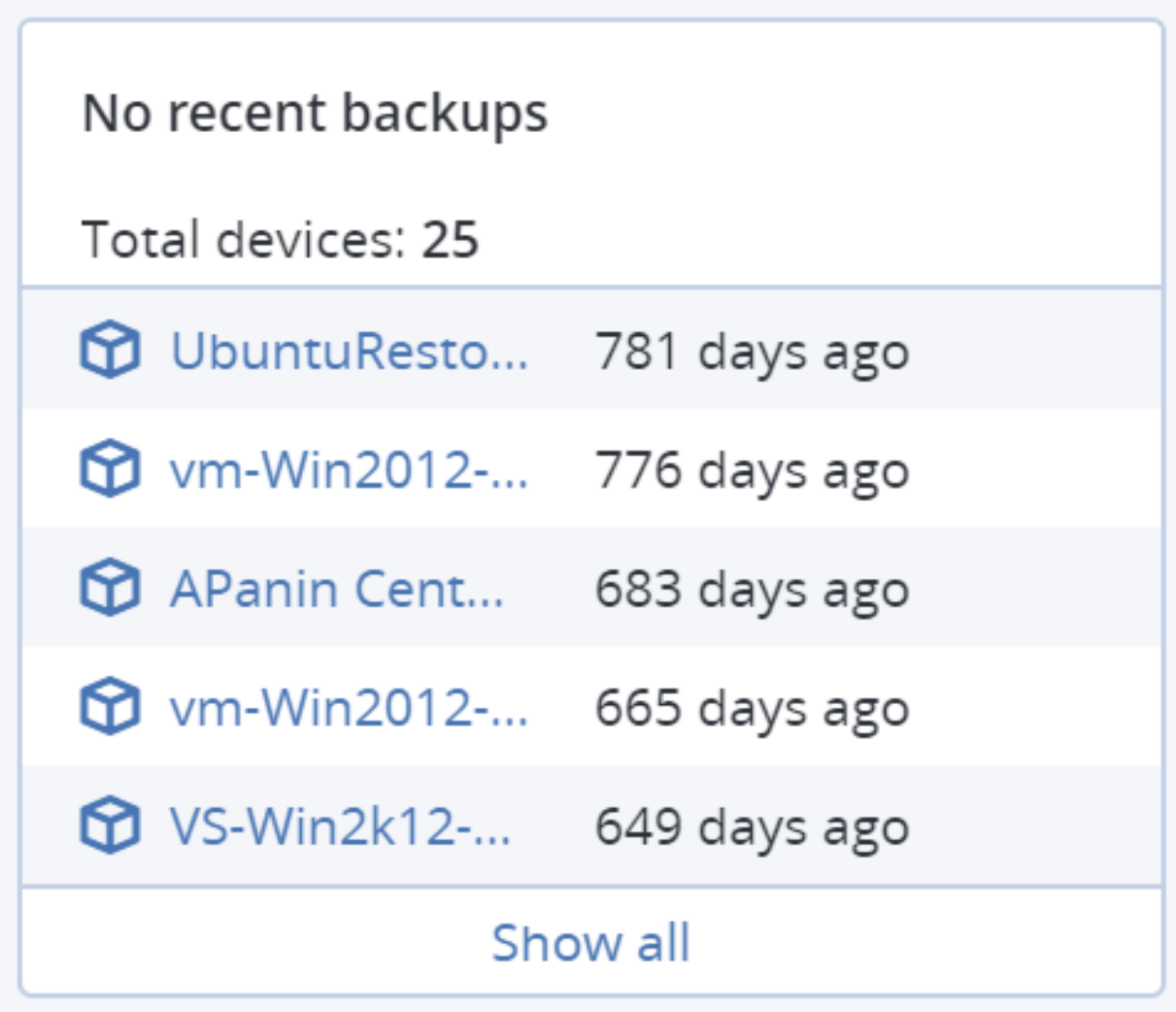
This widget is available only if Scan Service is installed on the management server. The widget shows detailed information about the threats that were detected in the backups.

Recently affected

This widget shows detailed information about workloads that were affected by threats, such as viruses, malware, and ramsomeware. You can find information about the detected threats, the time when the threats were detected, and how many files were affected.

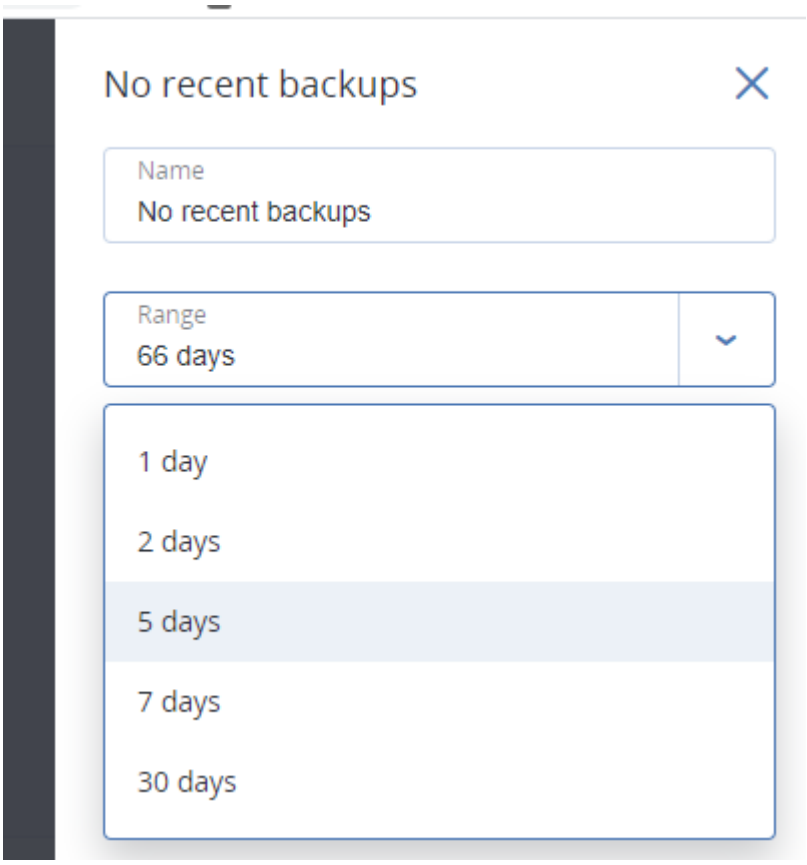
No recent backups

This widget shows workloads with applied protection plans, whose last successful backup date was earlier than the time range specified in the widget settings.



© Acronis International GmbH, 2003-2026

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.



Software inventory widgets

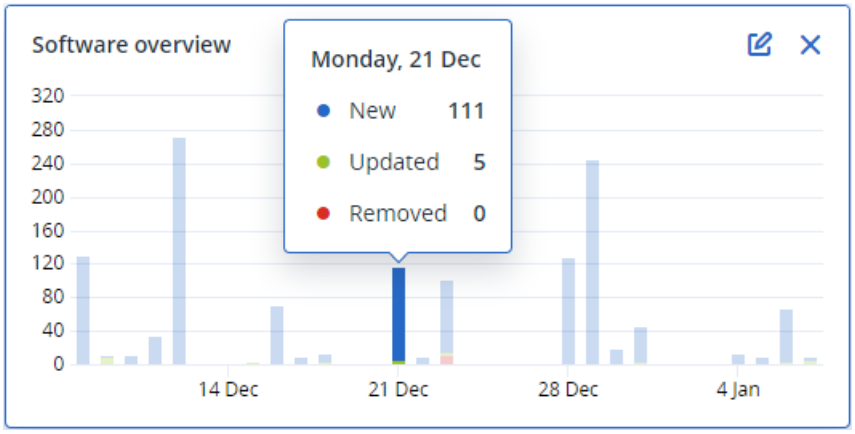
The **Software inventory** table widget shows detailed information about all the software that is installed on Windows and macOS devices in your organization.

You can filter the information in the widget by machine name, software name, vendor name, and status.

Note
In the **Machine name**, **Software name**, and **Vendor name** filters, you can select up to 20 values.

The **Software overview** widget shows the number of new, updated, and deleted applications on Windows and macOS devices in your organization for a specified time period (7 days, 30 days, or the current month).

© Acronis International GmbH, 2003-2026



When you hover over a certain bar on the chart, a tooltip with the following information shows:

New - the number of newly installed applications.

Updated - the number of updated applications.

Removed - the number of removed applications.

When you click the part of the bar for a certain status, you are redirected to the **Software Management** -> **Software Inventory** page. The information in the page is filtered for the corresponding date and status.

You can filter the information in the widget by device name.

Note
In the **Device name** filter, you can select up to 20 values.

Hardware inventory widgets

The **Hardware inventory** and **Hardware details** table widgets show information about all the hardware that is installed on physical and virtual Windows and macOS devices in your organization.

The **Hardware changes** table widget shows information about the added, removed, and changed hardware on physical and virtual Windows and macOS devices in your organization for a specified time period (7 days, 30 days, or the current month).

You can filter the results that are displayed in the hardware inventory widgets.

Note
In the **Machine name** filter, you can select up to 20 values.

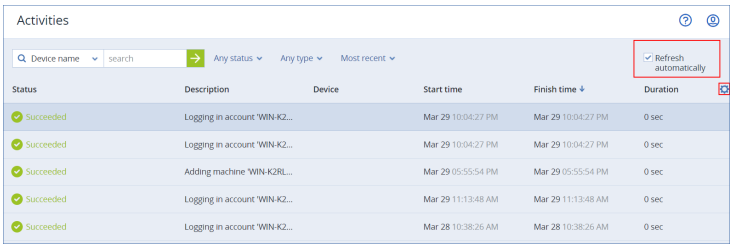
The Activities tab

The **Activities** tab provides an overview of the activities during the last 90 days.

Dates and times are shown according to the time zone settings of the machine that you use to access the Cyber Protect console.

© Acronis International GmbH, 2003-2026

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** checkbox. Frequent updates of multiple activities might degrade the performance of the management server.



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
```


© Acronis International GmbH, 2003-2026

```
    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. 242).

Cyber Protect Monitor

You can install Cyber Protect Monitor as an additional component that you select during the installation of Agent for Windows or Agent for Mac. Cyber Protect Monitor shows information about the protection status of the machine on which Agent for Windows or Agent for Mac is installed.

You can use Cyber Protect Monitor to configure the backup encryption and proxy server settings.

Cyber Protect Monitor supports the following operating systems.

- With Agent for Windows
  - Windows 10 version 1809 and later
  - Windows Server 2019 and later
- With Agent for Windows (Legacy)
  - Windows 7 and later
  - Windows Server 2008 R2 and later
- With Agent for Mac
  - All macOS versions that are supported by Agent for Mac, except macOS 10.x and macOS 11.x.

When Agent for File Sync & Share is installed on the machine, Cyber Protect Monitor provides access to the File Sync & Share service. The File Sync & Share functionality is accessible after a mandatory onboarding during which the users sign in to their own File Sync & Share account and select a personal sync folder. For more information about Agent for File Sync & Share, see the Cyber Files Cloud user guide.

Important
Cyber Protect Monitor is accessible to users who might not have administrative rights for the Cyber Protect or the File Sync & Share service.

© Acronis International GmbH, 2003-2026

The table below summarizes the operations that are available for users without administrative rights.

Installed agents	Users can	Users cannot
Agent for Windows or Agent for Mac	• Apply the default protection plan to their machines • Check the protection status of their machines • Receive Active Protection notifications • Temporarily pause the backups of their machines • Configure the proxy server settings • Change the backup encryption settings **Warning!** Changing the encryption settings in Cyber Protect Monitor overwrites the settings in the protection plan and affects all backups of the machine. This operation can cause some protection plans to fail. For more information, see "Encryption" (p. 385). There is no way to recover encrypted backups if you lose or forget the password. • Chat with a technician	• Apply custom protection plans • Manage protection plans that are already applied
Agent for Windows (Legacy)	• Apply the default protection plan to their machines • Check the protection status of their machines • Receive Active Protection notifications • Temporarily pause the backups of their machines • Configure the proxy server settings • Change the backup encryption settings	• Apply custom protection plans • Manage protection plans that are already applied

© Acronis International GmbH, 2003-2026

Installed agents	Users can	Users cannot
	Warning! Changing the encryption settings in Cyber Protect Monitor overwrites the settings in the protection plan and affects all backups of the machine. This operation can cause some protection plans to fail. For more information, see "Encryption" (p. 385). There is no way to recover encrypted backups if you lose or forget the password.	
Agent for Windows and Agent for Sync and Share Agent for Mac and Agent for Sync and Share	• Sync content between their local sync folder and their File Sync & Share account • Pause the sync operations • Change the sync folder • Check the file types that cannot be synced • Chat with a technician	• Edit the file types that cannot be synced

Configuring proxy server settings in Cyber Protect Monitor

You can configure the proxy server settings in Cyber Protect Monitor. The configuration will affect all agents that are installed on the machine.

To configure the proxy server settings

1. Open Cyber Protect Monitor, and then click the gear icon in the top right corner.
2. Click **Settings**, and then click **Proxy**.
3. Enable the **Use a proxy server** switch, and then enter the proxy server address and port.
4. [If the proxy server access is password-protected] Enable the **Password required** switch, and then enter the user name and password to access the proxy server.

   The password can include lowercase and uppercase alphanumeric characters, and the following special characters:

   ```
   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` } | { ~
   ```

5. Click **Save**.

   The proxy server settings are saved in the `http-proxy.yaml` file.

© Acronis International GmbH, 2003-2026

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	Cyber Backup	Shows all machines that were discovered in the

© Acronis International GmbH, 2003-2026

machines	Advanced Cyber Protect Advanced	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 (...).

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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`.

© Acronis International GmbH, 2003-2026

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 asm
net start asm
```

To restart the management server service in Linux

1. Open **Terminal**.
2. Run the following command in any directory:

```
sudo service acronis_asm restart
```

SIEM log forwarding

SIEM (Security Information and Event Management) platforms are cybersecurity solutions that provide centralized log management, offer real-time threat detection, facilitate incident investigations, and help organizations meet compliance requirements. They work by consolidating and analyzing security data, such as logs from firewalls, intrusion detection systems, servers, and applications. This is done in real-time, to generate prioritized alerts for any suspicious activities and potential threats. Security teams then use the consolidated data and alerts to investigate flagged cybersecurity incidents, understand their scope, and take timely action to contain and mitigate threats.

SIEM platforms provide a comprehensive view of an organization's security posture, enabling early detection of advanced threats and anomalies. They help organizations meet regulatory and industry-specific security compliance standards, by providing centralized data and reporting. They offer a centralized console for managing security events, providing better visibility into the security operations center (SOC).

© Acronis International GmbH, 2003-2026

With Acronis log forwarding plans, the SIEM Connector component on the management server writes Acronis alert and activity data to a folder on the management server, or forwards it to a remote syslog server. This data can then be ingested by the SIEM platform for processing. You can have one active log forwarding plan at a time.

Creating a SIEM log forwarding plan

Note
Only one SIEM log forwarding plan can be active at a time. The **Create** button is disabled if a plan already exists. To create a new plan, first delete the existing plan.

Important
SIEM log forwarding plans are only supported for x64 architecture.

To create a SIEM log forwarding plan

Required privileges
Administrator.

1. In the Cyber Protect console, go to **Plans** > **Log forwarding plans**.
2. Click **Create**.
3. [Optional] Change the plan default name.
   a. Click the pencil icon.
   b. Edit the name.
   c. Click the check mark to accept the changes.
4. Select the **Method** for the log forwarding plan:
   - **Files**
     This method can use either a Windows or a Linux management server.
   - **Syslog server**
     This method can use either a Windows or a Linux management server.

   For more information, see SIEM forwarding plan methods.
5. ***Files method***
   a. [Optional] Click **Specify** to change the default **File path** for the SIEM data store on the management server, and then click **Done**.

      Important
      If the specified directory is removed, SIEM forwarding stops until you either restore the removed directory or modify **File path** to a valid directory.

© Acronis International GmbH, 2003-2026

Important
On a Windows management server, the specified path must not be a reparse point, or include one in the path (for example, a OneDrive-synced folder). If you specify an invalid path, a validation error is returned. For more information, see "Files forwarding method" (p. 290).

Syslog server method

a. Enter the **Server address** of the syslog server.

Note
On a Linux management server, you can leave this field empty to use the local syslog service. On a Windows management server, you must specify a remote syslog server address; localhost is not allowed.

Important
If you are connecting to a remote syslog server, install the syslog server's TLS certificate on the management server before creating the plan. See "Installing a TLS certificate for syslog forwarding" (p. 297). When you click **Create**, the connector tests the connection and writes a test record to confirm it is working.

6. [Optional] Change the **File format**.
   - **CEF** (default)
     Vendor-neutral, standardized format, designed for security events and detailed event analysis.
   - **JSON**
     Highly flexible format that allows custom, complex data. Best for modern log management platforms.

   For more information, see "SIEM data format and examples" (p. 300).
7. [Optional] Select the Acronis data types to include in the log forwarding plan.
   By default, all available data types are included.
   a. Click on the **Data** field.
   b. Clear the checkboxes of the data types that you do not want to include.
      The available data types are:
      - **Alerts**
        Updates of critical or error messages that require a rapid response.
      - **Activities**
        All success, informational, warning, critical, and error messages (e.g., backups, DLP, URL filtering).
   c. Click **Done**.
8. Click **Create**.

© Acronis International GmbH, 2003-2026

Renaming the SIEM log forwarding plan

To rename the SIEM log forwarding plan

Required privileges
Administrator

1. In the Cyber Protect console, go to **Plans** > **Log forwarding plans**.
2. Click the plan.
   The details and actions sidebar opens.
3. Click **Rename**.
4. Edit the plan name.
5. Click **Rename**.

Editing the SIEM log forwarding plan

Note
You cannot change the **Method**. To change it, you must delete the SIEM log forwarding plan and create a new one.

To edit the SIEM log forwarding plan

Required privileges
Administrator

1. In the Cyber Protect console, go to **Plans** > **Log forwarding plans**.
2. Click the plan.
   The details and actions sidebar opens.
3. Click **Edit**.
4. Make your changes and click **Confirm**.

Deleting the SIEM log forwarding plan

Note
When you delete the SIEM log forwarding plan, data forwarding ceases, but the data which has already been forwarded is not deleted.

To delete the SIEM log forwarding plan

Required privileges
Administrator

© Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Plans** > **Log forwarding plans**.
2. Click the plan.
   The details and actions sidebar opens.
3. Click **Delete**.
4. Select the confirmation checkbox to enable the **Confirm** button.
5. Click **Confirm**.

SIEM forwarding methods

Important
SIEM forwarding plans are only supported for x64 architecture.

With Acronis SIEM forwarding, the Acronis agent writes SIEM data on an Acronis-managed writer device. It can work with one of two forwarding methods:

- **Files**
  Applicable with a Windows or a Linux writer device.
- **Syslog**
  Applicable with both Windows and Linux management servers.

Files forwarding method

This method can be implemented with either a Windows or a Linux writer device.

The SIEM data is written as files to a directory. You can specify a directory or accept the default.

Default directories

- Windows writer device: `C:\`.
- Linux writer device: `/var/log/siem`.

Important
Only administrators have access to these files.

Important
On a Windows management server, the SIEM Connector runs under the IMS user service account, which has restricted access to the file system. The specified path must not be a reparse point, or include one in the path (for example, a OneDrive-synced folder or a Desktop shortcut). If you specify an invalid path, a validation error is returned when you save the plan.

Syslog server forwarding method

A syslog server is a centralized system that receives and stores log messages using the Syslog protocol.

© Acronis International GmbH, 2003-2026

Note

Both Windows and Linux management servers support this method. The certificate and connection requirements depend on the configuration:

- ***Windows management server***

  The syslog server must be remote. Localhost is not allowed.

  A TLS certificate is required. See "Installing a TLS certificate for syslog forwarding" (p. 297).
- ***Linux management server, local syslog***

  You can leave the server address field empty to use the local syslog service via Unix socket.

  No certificate is required.
- ***Linux management server, remote syslog***

  You must specify the syslog server address.

  A TLS certificate is required. See "Installing a TLS certificate for syslog forwarding" (p. 297).

To review forwarded SIEM data

1. Execute the following command:

   Ubuntu/Debian

   `cat /var/log/syslog`

   Red Hat/Rocky Linux

   `cat /var/log/messages`

Red Hat syslog configuration example

The following is an example of a Red Hat-based (Rocky Linux) syslog configuration file.

This content is found in the `/etc/rsyslog.conf` file.

```
# rsyslog configuration file


# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# or latest version online at http://www.rsyslog.com/doc/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html


#### GLOBAL DIRECTIVES ####


# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")
```


© Acronis International GmbH, 2003-2026

```
# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")

#### MODULES ####

module(load="imuxsock"    # provides support for local system logging (e.g. via
logger command)
       SysSock.Use="off") # Turn off message reception via local log socket;
                          # local messages are retrieved through imjournal now.
module(load="imjournal"             # provides access to the systemd journal
       UsePid="system" # PID nummber is retrieved as the ID of the process the
journal entry originates from
       FileCreateMode="0644" # Set the access permissions for the state file
       StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability

# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
#module(load="imudp") # needs to be done just once
#input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
#module(load="imtcp") # needs to be done just once
#input(type="imtcp" port="514")

#### RULES ####
```


© Acronis International GmbH, 2003-2026

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog



# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log



# ### sample forwarding rule ###
#action(type="omfwd"
```


© Acronis International GmbH, 2003-2026

```
# # An on-disk queue is created for this action. If the remote host is
# # down, messages are spooled to disk and sent when it is up again.
#queue.filename="fwdRule1"       # unique name prefix for spool files
#queue.maxdiskspace="1g"         # 1gb space limit (use as much as possible)
#queue.saveonshutdown="on"       # save messages to disk on shutdown
#queue.type="LinkedList"         # run asynchronously
#action.resumeRetryCount="-1"    # infinite retries if host is down
# # Remote Logging (we use TCP for reliable delivery)
# # remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")
```

Debian syslog configuration example

The following is an example of a Debian-based (Ubuntu Linux) syslog configuration file.

This content is found in the `/etc/rsyslog.conf` file.

```
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf



#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability


# provides UDP syslog reception
```


© Acronis International GmbH, 2003-2026

```
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
```


© Acronis International GmbH, 2003-2026

```
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
```

rsyslog configuration example

This guide shows how to configure a remote syslog server to receive events from the Acronis Connector running on-premises. The connector sends events to the syslog server using TLS encryption on port 6514 by default.

Prerequisites

- A Linux machine with rsyslog installed and running
- TLS certificates: a CA certificate, server certificate, and server private key
- Network connectivity between the on-premises connector and the syslog server on port 6514 (or configured port)

Basic rsyslog configuration

Edit the rsyslog configuration file (typically /etc/rsyslog.conf or in /etc/rsyslog.d/) to enable a TLS-protected listener:

rsyslog.conf

module(load="imtcp" StreamDriver.Name="gtls" StreamDriver.Mode="1" StreamDriver.AuthMode="anon")

input(type="imtcp" port="6514")

TLS certificate configuration

Configure rsyslog to use TLS certificates for encrypted communication:

rsyslog with TLS certificates

© Acronis International GmbH, 2003-2026

global(DefaultNetstreamDriver="gtls" DefaultNetstreamDriverCAFile="/etc/rsyslog.d/ca.crt")

module(load="imtcp" StreamDriver.Name="gtls" StreamDriver.Mode="1" StreamDriver.AuthMode="x509/certvalid")

input(type="imtcp" port="6514" StreamDriver.CertFile="/etc/rsyslog.d/server.crt" StreamDriver.KeyFile="/etc/rsyslog.d/server.key")

Certificate installation

On the syslog server, place the certificates in a secure directory (e.g., /etc/rsyslog.d/):

sudo cp ca.crt /etc/rsyslog.d/ca.crt

sudo cp server.crt /etc/rsyslog.d/server.crt

sudo cp server.key /etc/rsyslog.d/server.key

sudo chown syslog:syslog /etc/rsyslog.d/server.key

sudo chmod 600 /etc/rsyslog.d/server.key

Event filtering (optional)

To route Acronis events to a specific file, add a filter rule:

:programname, isequal, "SIEM-Connector" /var/log/siem-connector.log

& stop

Restart and verify

After configuration changes, restart rsyslog and verify the listener is active:

sudo systemctl restart rsyslog

sudo ss -tlnp | grep 6514

A successful connection from the on-premises connector will produce entries in /var/log/syslog or your configured log file.

For examples of complete rsyslog.conf files for specific Linux distributions, see "Debian syslog configuration example" (p. 294) and "Red Hat syslog configuration example" (p. 291).

Installing a TLS certificate for syslog forwarding

To forward SIEM data to a remote syslog server, the syslog server must be configured to accept TLS connections. Its CA certificate must then be installed in the system trust store on the management server, so that the SIEM Connector can establish a trusted connection.

The following procedure uses `rsyslog` and `openssl` on the syslog server.

© Acronis International GmbH, 2003-2026

Note
Supported Linux distributions for the syslog server: Ubuntu (22.04 or later), Rocky Linux 9. The minimum supported version of `rsyslog` is 8.2412.0.

Note
The certificate is self-signed. The syslog server's IP address must be specified as both the Common Name (CN) and the Subject Alternative Name (SAN) in the certificate.

To configure the syslog server

Required privileges
Administrator

1. Install `rsyslog` and the required TLS packages.

   Ubuntu

   ```
   sudo apt update && sudo apt install rsyslog gnutls-bin
   ```

   Rocky Linux

   ```
   sudo dnf install rsyslog
   sudo dnf install rsyslog-gnutls
   sudo systemctl enable --now rsyslog
   ```

2. Open the port that you intend to use for TLS syslog connections (port 6514 is recommended) for incoming TCP connections.

   Ubuntu

   If `ufw` is active, run: `sudo ufw allow 6514/tcp`

   Rocky Linux

   ```
   sudo firewall-cmd --permanent --add-port=6514/tcp
   sudo firewall-cmd --reload
   ```

3. Navigate to the `rsyslog` configuration directory, where you will store the certificate files:

   ```
   cd /etc/rsyslog.d
   ```

   Note
   Placing certificates in `/etc/rsyslog.d` ensures that `rsyslog` can access them without additional system security configuration.

4. Note the IP address of the syslog server machine:

   ```
   ip a
   ```

5. Create a CA key and a self-signed CA certificate:

   ```
   sudo openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:4096 -out ca-key.pem
   sudo openssl req -x509 -new -nodes -key ca-key.pem -sha256 -days 3650 -out ca.pem -subj
   "/CN=rsyslog-ca"
   ```


© Acronis International GmbH, 2003-2026

6. Create a server key and a certificate signing request (CSR). Replace *server_IP* with the IP address of the syslog server:

   ```
   sudo openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out server-key.pem
   sudo openssl req -new -key server-key.pem -out server.csr -subj "/CN=server_IP"
   ```

7. Sign the server certificate, specifying the IP address as a Subject Alternative Name (SAN). Replace *server_IP* with the IP address of the syslog server:

   ```
   printf "subjectAltName=IP:server_IP" > san.ext
   sudo openssl x509 -req -in server.csr -CA ca.pem -CAkey ca-key.pem -CAcreateserial -out
   server-cert.pem -days 825 -sha256 -extfile san.ext
   rm san.ext
   ```

8. Set the correct ownership and permissions for the certificate files:

   Ubuntu

   ```
   sudo chown root:syslog /etc/rsyslog.d/*.pem
   sudo chmod 644 /etc/rsyslog.d/ca.pem /etc/rsyslog.d/server-cert.pem
   sudo chmod 640 /etc/rsyslog.d/server-key.pem
   ```

   Rocky Linux

   ```
   sudo chown root:root /etc/rsyslog.d/*.pem
   sudo chmod 644 /etc/rsyslog.d/ca.pem /etc/rsyslog.d/server-cert.pem
   sudo chmod 640 /etc/rsyslog.d/server-key.pem
   ```

9. Configure `rsyslog` for TLS. Add the following to `/etc/rsyslog.conf`, replacing *6514* with your chosen port number:

   ```
   global(
   DefaultNetstreamDriver="gtls"
   DefaultNetstreamDriverCAFile="/etc/rsyslog.d/ca.pem"
   DefaultNetstreamDriverCertFile="/etc/rsyslog.d/server-cert.pem"
   DefaultNetstreamDriverKeyFile="/etc/rsyslog.d/server-key.pem"
   )
   # load TCP listener
   module(
   load="imtcp"
   StreamDriver.Name="gtls"
   StreamDriver.Mode="1"
   StreamDriver.Authmode="anon"
   )
   # start up listener at port 6514
   input(
   type="imtcp"
   port="6514"
   )
   ```

   For more information, see the rsyslog TLS documentation.

10. Restart the `rsyslog` service and confirm it started without errors:

    ```
    sudo systemctl restart rsyslog
    sudo systemctl status rsyslog
    ```


© Acronis International GmbH, 2003-2026

To install the CA certificate on the management server

1. Copy `ca.pem` from `/etc/rsyslog.d/` on the syslog server to the management server.
2. Install the CA certificate in the system trust store.

   Windows (run as administrator)

   ```
   certutil -addstore -f "Root" "C:\path\to\ca.pem"
   ```

   Linux

   ```
   sudo install -m 0644 ca.pem /usr/local/share/ca-certificates/ca.crt
   sudo update-ca-certificates --fresh
   ```

   Note
   On RHEL-based systems, use `sudo update-ca-trust` instead of `update-ca-certificates`.

   ```
   sudo systemctl restart acronis_asm
   ```

Once the certificate is installed, you can create a log forwarding plan using the syslog server method. See "Creating a SIEM log forwarding plan" (p. 287).

To verify the setup

1. Generate some events, for example by logging in to the management server console.
2. Check the SIEM Connector logs for successful export records.
3. On the syslog server, check that events have been received:

   Ubuntu: `cat /var/log/syslog`

   Rocky Linux: `cat /var/log/messages`

SIEM data format and examples

The Acronis SIEM forwarding plan can send data for Acronis alerts and activities, with one of two file formats: JSON and CEF.

SIEM files include different data with distinct structures, depending on data type and the forwarding plan file format. In this section, we provide examples of data for both data types in both formats.

CEF file format

- Alert examples
- Activity examples

JSON file format

- Alert examples
- Activity examples

 © Acronis International GmbH, 2003-2026

CEF alert examples

```
Oct 15 14:45:01 WIN-R1OR1V5M79O siem_log_forwarder[8608]:
CEF:0|Acronis|DemoCustomer|1.0|BackupStatusUnknown|BackupStatusUnknown|5|cs1=
{"agentId":"c8d66ac4-0d5b-4ecb-b1b0-c3649df91231","backupLocations":
[{"type":"cloud"}],"backupSourcesType":"files","errorMessage":{"kbLink":
{"serCode":"BackupStatusUnknown"}},"planId":"a92799fc-f657-4a10-b6ed-
16975c4d0ef0","planName":"Protect Win","resourceId":"3b9187d6-0853-45ff-aab0-
0c68cd643068","resourceName":"WIN-R1OR1V5M79O"} cs1Label=alertdetails
deviceExternalId=3b9187d6-0853-45ff-aab0-0c68cd643068 dvchost=WIN-R1OR1V5M79O

Oct 15 14:42:46 WIN-R1OR1V5M79O siem_log_forwarder[8608]:
CEF:0|Acronis|DemoCustomer|1.0|BackupFailed|BackupFailed|10|cs1={"activity":
{"id":"FE0B2835-3C9D-4D5A-9D02-FD0CBE5042B8","type":"8F01AC13-F59E-4851-9204-
DE1FD77E36B4"},"activityId":"FE0B2835-3C9D-4D5A-9D02-
FD0CBE5042B8","backupLocations":
[{"name":"","type":"cloud"}],"backupSourcesType":"machines","error":
{"code":20250646,"fields":{"$module":"service_process_vsa64_41100","AgentName":"WIN-
R1OR1V5M79O","CommandID":"8F01AC13-F59E-4851-9204-DE1FD77E36B4"},"src":
{"file":"c:\\\\b\\\\1223\\\\enterprise\\\\common\\\\tol\\\\command\\\\command.cpp","
func":"Tol::`anonymous-
namespace'::MakeFailResultWithName","line":503,"tag":"0x8d165e86fb8195c5"},"suberro
r":{"code":20250646,"fields":{"$module":"gtob_backup_command_addon_vsa64_
41100","AgentName":"WIN-R1OR1V5M79O","CommandID":"8F01AC13-F59E-4851-9204-
DE1FD77E36B4"},"src":
{"file":"c:\\\\b\\\\1223\\\\enterprise\\\\common\\\\tol\\\\command\\\\command.cpp","
func":"Tol::`anonymous-
namespace'::MakeFailResultWithName","line":503,"tag":"0x8d165e86fb8195c5"},"suberro
r":{"code":10551508,"fields":{"$module":"disk_bundle_vsa64_
41100","IsReturnCode":1},"src":
{"file":"c:\\\\b\\\\1223\\\\enterprise\\\\mms\\\\managers\\\\archive\\\\impl\\\\priv
ate_
manager.cpp","func":"ArchiveManagement::PrivateArchiveManager::FindArchive","line":9
58,"tag":"0xb320396adfe3e63"},"suberror":{"code":19333376,"fields":{"$module":"disk_
bundle_vsa64_41100","Domain":"STORAGE_MANAGER","Reason":"CANotFoundErr"},"src":
{"file":"c:\\\\b\\\\1223\\\\enterprise\\\\backup\\\\online\\\\storage_manager_
client\\\\impl\\\\storage_manager_client.cpp","func":"`anonymous-
namespace'::StorageManagerImpl::GetErrorDetails","line":130,"tag":"0xb9f2653089b4a64
1"},"suberror":{"code":38207501,"fields":{"$module":"disk_bundle_vsa64_
41100","status":404,"uri":"https://eu-cloud.acronis.com:80/api/infra_
manager/v2/backup_storage"},"src":
{"file":"c:\\\\b\\\\1223\\\\enterprise\\\\backup\\\\online\\\\storage_manager_
client\\\\impl\\\\storage_manager_client.cpp","func":"`anonymous-
namespace'::StorageManagerImpl::ParseTransportResult","line":139,"tag":"0xb9f2653089
b4a64a"},"suberror":{},"text":"HTTP request failure for URL \\"https://eu-
cloud.acronis.com:80/api/infra_manager/v2/backup_storage\\".\\n Server response
code: \\"404 - Not Found: The requested resource could not be found\\".\\n Server
response message: {\\"domain\\":\\"STORAGE_
MANAGER\\",\\"code\\":\\"404\\",\\"reason\\":\\"CANotFoundErr\\",\\"debug\\":
{\\"msg\\":\\"authority id 26bc3588-4278-40bb-b980-0285c6ce519e not found in CA
table\\"},\\"message\\":\\"authority id 26bc3588-4278-40bb-b980-0285c6ce519e not
found in CA table\\"}","types":
```


© Acronis International GmbH, 2003-2026

{"$module":"A","status":"N","uri":"A"}},"text":"Storage Manager client error","types":{"$module":"A","Domain":"A","Reason":"A"}},"text":"Failed to find archive 'WIN-R1OR1V5M79O-1A57176B-90DE-494B-BB59-9325C447E513-3B9187D6-0853-45FF-AAB0-0C68CD643068A'.","types":{"$module":"A","IsReturnCode":"N"}},"text":"TOL: Failed to execute the command. Backing up","types":{"$module":"A","AgentName":"W","CommandID":"A"}},"text":"TOL: Failed to execute the command. Backing up","types":{"$module":"A","AgentName":"W","CommandID":"A"}},"errorMessage":{"code":"MemoFailedToDiscoverFesUri","context":{"Domain":"STORAGE_MANAGER","cause_str":"HTTP request failure for URL \\"https://eu-cloud.acronis.com:80/api/infra_manager/v2/backup_storage\\".\\n Server response code: \\"404 - Not Found: The requested resource could not be found\\".\\n Server response message: {\\"domain\\":\\"STORAGE_MANAGER\\",\\"code\\":\\"404\\",\\"reason\\":\\"CANotFoundErr\\",\\"debug\\":{\\"msg\\":\\"authority id 26bc3588-4278-40bb-b980-0285c6ce519e not found in CA table\\"},\\"message\\":\\"authority id 26bc3588-4278-40bb-b980-0285c6ce519e not found in CA table\\"}","effect_str":"TOL: Failed to execute the command. Backing up"},"domain":"cloud_platform","kbLink":{"build":20706,"lineTag":"0xB9F2653089B4A64A","os":"Windows","product":"cloud","serCode":"BackupFailed+0x01350016+0x01350016+0x00A100D4+0x01270100+0x0247000D","version":"15.0"},"reason":"MemoFailedToDiscoverFesUri","serCode":"0x01350016+0x01350016+0x00A100D4+0x01270100+0x0247000D"},"finishTime":1760520707,"planId":"1A57176B-90DE-494B-BB59-9325C447E513","planName":"Protect Win","resourceId":"3B9187D6-0853-45FF-AAB0-0C68CD643068","resourceName":"WIN-R1OR1V5M79O","startTime":1760520707}
cs1Label=alertdetails deviceExternalId=3B9187D6-0853-45FF-AAB0-0C68CD643068
dvchost=WIN-R1OR1V5M79O

Oct 24 15:15:00 syslog siem_log_forwarder[2622955]:
CEF:0|Acronis|DemoCustomer2|1.0|BackupCanceled|BackupCanceled|5|cs1={"activity":{"id":"4084E850-0F4A-448A-AF1A-D7B5A49567D2"},"activityId":"4084E850-0F4A-448A-AF1A-D7B5A49567D2","backupLocations":[{"name":"","type":"cloud"}],"backupSourcesType":"machines","finishTime":1761318832,"planId":"A0210313-39A8-469F-AC1D-D68B88923322","planName":"Linux","resourceId":"9386E27C-A64C-4E24-A2BC-391A0DC8F9DE","resourceName":"syslog","startTime":1761318829} cs1Label=alertdetails deviceExternalId=9386E27C-A64C-4E24-A2BC-391A0DC8F9DE dvchost=syslog

Oct 24 09:00:03 DESKTOP-VBTMUIG siem_log_forwarder[776]:
CEF:0|Acronis|DemoCustomer3|1.0|EDRIncidentDetected|EDRIncidentDetected|10|cs1={"changeId":"2","customerIncidentId":"2","customerName":"CustomerA","detectionTime":"2025-10-24T15:49:25.717247Z","edrAlertId":"c60abcd5-ffd5-4bdb-8c2c-23aa275ae0b5","incidentCategories":"MALWARE_DETECTED","incidentId":"a999c62b-9b1e-4d3a-85d9-d54743107b22","incidentTrigger":"New Text Document.txt","isMalicious":"true","isMitigated":"false","mitigationState":"NOT_MITIGATED","osType":"WINDOWS","redirectLink":"https://eu-cloud.acronis.com/ui/#/endpoint-detection/customer/101/incidents/a999c62b-9b1e-4d3a-85d9-d54743107b22/investigation","resourceId":"292ab054-61b9-41ec-9416-1f1b679a67a5","resourceName":"DESKTOP-VBTMUIG","verdict":"Malicious threat"}
cs1Label=alertdetails deviceExternalId=292ab054-61b9-41ec-9416-1f1b679a67a5
dvchost=DESKTOP-VBTMUIG

 © Acronis International GmbH, 2003-2026

CEF activity examples

```
Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|agent.add|agent.add|1|cs1=
{"IsProcessRoot":true,"Persistent":{"ID":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","Name":"WIN-
R1OR1V5M79O","OwnerID":"67"},"Specific":"Business","UserName":"WIN-
R1OR1V5M79O\\\\AMS User","isLegacy":true,"title":"Adding agent 'WIN-R1OR1V5M79O' to
the management server"} cs1Label=taskcontext cs2={"code":"ok"} cs2Label=taskresult
cs3={"uuid":"ee54f502-4a06-498c-8b00-22824ba40231","type":"A59E8BF2-39C3-42C4-B667-
CB672381A214","queue":"legacySync","priority":"normal","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"cancellable":true,"startedByUser":"WIN-
R1OR1V5M79O\\\\AMS
User","id":1634697080134496256,"idString":"1634697080134496256","state":"completed",
"issuer":{"id":"","clusterId":""},"enqueuedAt":"2025-10-
10T17:01:32.022739593Z","startedAt":"2025-10-
10T17:01:32.022739593Z","updatedAt":"2025-10-
10T17:01:32.031865547Z","completedAt":"2025-10-
10T17:01:32.022739593Z","cancelRequested":false} cs3Label=taskdetails dvchost=
suser=WIN-R1OR1V5M79O\\AMS User deviceExternalId=

Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|AddFeatures|AddFeatures|1|cs1={"_runtime":
{},"argument":{"add_components":["agentForAmp"],"remove_components":[],"AMSPort":0}}
cs1Label=activitycontext cs2={"code":"ok"} cs2Label=activityresult cs3=
{"uuid":"515980ce-3e51-4cc9-846d-
dd8d8fbd1918","type":"AddFeatures","taskId":1634696473042546688,"progress":
{"current":100,"total":100},"resource":{"id":"3B9187D6-0853-45FF-AAB0-
0C68CD643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","id":1634696841088528384,"idString":"1634696841088
528384","taskIdString":"1634696473042546688","createdAt":"2025-10-
10T17:00:32.272567181Z","startedAt":"2025-10-
10T17:00:32.272567181Z","updatedAt":"2025-10-
10T17:01:36.542446095Z","completedAt":"2025-10-10T17:01:36.542446095Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":{"id":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","clusterId":""}} cs3Label=activitydetails dvchost=WIN-R1OR1V5M79O
suser= deviceExternalId=3B9187D6-0853-45FF-AAB0-0C68CD643068

Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]:
CEF:0|Acronis|DemoCustomer2|1.0|policy.revoke|policy.revoke|1|cs1=
{"IsProcessRoot":true,"Persistent":{"PlanID":"8cc61f3c-46b0-40a6-9d60-
7d72f68555db","PlanName":"XDR plan"},"PlanName":"XDR
plan","Specific":"Business","isLegacy":true,"title":"Revoking plan 'XDR plan' with
ID '8cc61f3c-46b0-40a6-9d60-7d72f68555db' from the resource with ID '3b9187d6-0853-
45ff-aab0-0c68cd643068'"} cs1Label=activitycontext cs2={"code":"ok"}
cs2Label=activityresult cs3={"uuid":"7092f0e8-7945-4774-8453-
a28b66534d73","type":"44328016-20D7-4799-A357-
CF152C904ED0","taskId":1634699005819154432,"resource":{"id":"3b9187d6-0853-45ff-
aab0-0c68cd643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","id":1634699005819154432,"idString":"1634699005819
154432","taskIdString":"1634699005819154432","policy":{"id":"8cc61f3c-46b0-40a6-
9d60-7d72f68555db","type":"policy.protection.total","name":"XDR
```


© Acronis International GmbH, 2003-2026

plan"},"startedByUser":"DemoCustomer2","createdAt":"2025-10-10T17:09:33.40794126Z","startedAt":"2025-10-10T17:09:33.40794126Z","updatedAt":"2025-10-10T17:09:33.453071958Z","completedAt":"2025-10-10T17:09:33.40794126Z","tenant":{"id":"66","uuid":"07f6adf7-4665-4340-865d-c4a4c66f4dcd","name":"DemoCustomer2","locator":"/1/66/"},"executor":{"id":"","clusterId":""}} cs3Label=activitydetails dvchost=WIN-R1OR1V5M79O suser=DemoCustomer2 deviceExternalId=3b9187d6-0853-45ff-aab0-0c68cd643068

Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]: CEF:0|Acronis|DemoCustomer2|1.0|policy.revoke|policy.revoke|1|cs1={"IsProcessRoot":true,"Persistent":{"PlanID":"8cc61f3c-46b0-40a6-9d60-7d72f68555db","PlanName":"XDR plan"},"PlanName":"XDR plan","Specific":"Business","isLegacy":true,"title":"Revoking plan 'XDR plan' with ID '8cc61f3c-46b0-40a6-9d60-7d72f68555db' from the resource with ID '3b9187d6-0853-45ff-aab0-0c68cd643068'"} cs1Label=taskcontext cs2={"code":"ok"} cs2Label=taskresult cs3={"uuid":"7092f0e8-7945-4774-8453-a28b66534d73","type":"44328016-20D7-4799-A357-CF152C904ED0","queue":"legacySync","priority":"normal","tenant":{"id":"66","uuid":"07f6adf7-4665-4340-865d-c4a4c66f4dcd","name":"DemoCustomer2","locator":"/1/66/"},"cancellable":true,"startedByUser":"DemoCustomer2","policy":{"id":"8cc61f3c-46b0-40a6-9d60-7d72f68555db","type":"policy.protection.total","name":"XDR plan"},"resource":{"id":"3b9187d6-0853-45ff-aab0-0c68cd643068","type":"machine","name":"WIN-R1OR1V5M79O"},"id":1634699005819154432,"idString":"1634699005819154432","state":"completed","issuer":{"id":"","clusterId":""},"enqueuedAt":"2025-10-10T17:09:33.40794126Z","startedAt":"2025-10-10T17:09:33.40794126Z","updatedAt":"2025-10-10T17:09:33.453071958Z","completedAt":"2025-10-10T17:09:33.40794126Z","cancelRequested":false} cs3Label=taskdetails dvchost=WIN-R1OR1V5M79O suser=DemoCustomer2 deviceExternalId=3b9187d6-0853-45ff-aab0-0c68cd643068

Oct 10 20:14:15 WIN-R1OR1V5M79O siem_log_forwarder[8088]: CEF:0|Acronis|DemoCustomer2|1.0|AutoUpdateStandby|AutoUpdateStandby|1|cs1={"argument":{"add_components":[],"remove_components":["agentForAmp"],"AMSPort":0}} cs1Label=activitycontext cs2={"code":"ok"} cs2Label=activityresult cs3={"uuid":"5622f2e5-880e-4fae-98c4-4260373ffbd3","type":"AutoUpdateStandby","taskId":1634699287147900928,"progress":{"current":100,"total":100},"resource":{"id":"3B9187D6-0853-45FF-AAB0-0C68CD643068","type":"machine","name":"WIN-R1OR1V5M79O"},"state":"completed","id":1634699287684771840,"idString":"1634699287684771840","taskIdString":"1634699287147900928","createdAt":"2025-10-10T17:10:43.921111256Z","startedAt":"2025-10-10T17:10:43.921111256Z","updatedAt":"2025-10-10T17:10:44.319913633Z","completedAt":"2025-10-10T17:10:44.319913633Z","tenant":{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2 (DemoCustomer2)","locator":"/1/66/67/"},"executor":{"id":"c8d66ac4-0d5b-4ecb-b1b0-c3649df91231","clusterId":""}} cs3Label=activitydetails dvchost=WIN-R1OR1V5M79O suser= deviceExternalId=3B9187D6-0853-45FF-AAB0-0C68CD643068

 © Acronis International GmbH, 2003-2026

JSON alert examples


```
{"id":"A5BD4F48-6D24-4FF0-BD43-
FD7CE7367B0E","type":"EDRIncidentDetected","createdAt":"2025-10-
24T15:24:25.873371Z","severity":"warning","receivedAt":"2025-10-
24T15:24:26.63156432Z","updatedAt":"2025-10-24T15:24:26.63156432Z","tenant":
{"id":"102","uuid":"38c8ff04-99fb-446a-967d-
461a5e299814","locator":"/1/100/101/102/"},"category":"EDR","details":
{"changeId":"1","customerIncidentId":"1","customerName":"DemoCustomer","detectionTim
e":"2025-10-24T15:24:25.873371Z","edrAlertId":"637e4e23-bf95-4147-8fb8-
4b3664a7f51f","incidentCategories":"URL_BLOCKED","incidentId":"5894ce04-f94b-4cd3-
8685-f91efb3fd6a0","incidentTrigger":"no-ssl.acronis-detection-
test.com","isMalicious":"true","isMitigated":"true","mitigationState":"AUTO_
MITIGATED","osType":"WINDOWS","redirectLink":"https://eu-
cloud.acronis.com/ui/#/endpoint-detection/customer/101/incidents/5894ce04-f94b-4cd3-
8685-f91efb3fd6a0/investigation","resourceId":"292ab054-61b9-41ec-9416-
1f1b679a67a5","resourceName":"DESKTOP-VBTMUIG","verdict":"Malicious threat"}}

{"id":"33A7E16F-9FE4-08BB-0EA1-
EF91855ACAFC","type":"BackupCanceled","createdAt":"2025-10-
24T15:19:15Z","severity":"warning","receivedAt":"2025-10-
24T15:04:08.316243862Z","updatedAt":"2025-10-24T15:19:15.216375706Z","tenant":
{"id":"104","uuid":"04cc830f-cc2d-4d85-bc0c-
154d3246ed55","locator":"/1/100/103/104/"},"category":"Backup","details":
{"activity":{"id":"EA9B4383-5B06-4F5C-8008-61D329714981"},"activityId":"EA9B4383-
5B06-4F5C-8008-61D329714981","backupLocations":
[{"name":"","type":"cloud"}],"backupSourcesType":"machines","finishTime":1761319155,
"planId":"A0210313-39A8-469F-AC1D-
D68B88923322","planName":"Linux","resourceId":"9386E27C-A64C-4E24-A2BC-
391A0DC8F9DE","resourceName":"syslog","startTime":1761319142}}
```


JSON activity examples


```
{"uuid":"0b013dcd-a606-4baf-80d9-
e209d74eb0f6","type":"policy.apply","queue":"legacySync","priority":"normal","tenan
t":{"id":"66","uuid":"07f6adf7-4665-4340-865d-
c4a4c66f4dcd","name":"DemoCustomer2","locator":"/1/66/"},"cancellable":true,"started
ByUser":"DemoCustomer2","policy":{"id":"8cc61f3c-46b0-40a6-9d60-
7d72f68555db","type":"policy.protection.total","name":"XDR plan"},"resource":
{"id":"3b9187d6-0853-45ff-aab0-0c68cd643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"context":{"IsProcessRoot":true,"Persistent":{"PlanID":"8cc61f3c-46b0-
40a6-9d60-7d72f68555db","PlanName":"XDR plan"},"PlanName":"XDR
plan","Specific":"Business","isLegacy":true,"title":"Applying plan 'XDR plan' with
ID '8cc61f3c-46b0-40a6-9d60-7d72f68555db' to resource 'WIN-R1OR1V5M79O' with ID
'3b9187d6-0853-45ff-aab0-
0c68cd643068'"},"id":1634702033410387968,"idString":"1634702033410387968","state":"c
ompleted","issuer":{"id":"","clusterId":""},"enqueuedAt":"2025-10-
10T17:22:10.323642031Z","startedAt":"2025-10-
10T17:22:10.323642031Z","updatedAt":"2025-10-
10T17:22:10.350557478Z","completedAt":"2025-10-
```


© Acronis International GmbH, 2003-2026

10T17:22:10.323642031Z","cancelRequested":false,"result":{"code":"ok"}}

{"uuid":"0b013dcd-a606-4baf-80d9-
e209d74eb0f6","type":"policy.apply","taskId":1634702033410387968,"resource":
{"id":"3b9187d6-0853-45ff-aab0-0c68cd643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","context":{"IsProcessRoot":true,"Persistent":
{"PlanID":"8cc61f3c-46b0-40a6-9d60-7d72f68555db","PlanName":"XDR
plan"},"PlanName":"XDR plan","Specific":"Business","isLegacy":true,"title":"Applying
plan 'XDR plan' with ID '8cc61f3c-46b0-40a6-9d60-7d72f68555db' to resource 'WIN-
R1OR1V5M79O' with ID '3b9187d6-0853-45ff-aab0-
0c68cd643068'"},"id":1634702033410387968,"idString":"1634702033410387968","taskIdStr
ing":"1634702033410387968","policy":{"id":"8cc61f3c-46b0-40a6-9d60-
7d72f68555db","type":"policy.protection.total","name":"XDR
plan"},"startedByUser":"DemoCustomer2","createdAt":"2025-10-
10T17:22:10.323642031Z","startedAt":"2025-10-
10T17:22:10.323642031Z","updatedAt":"2025-10-
10T17:22:10.350557478Z","completedAt":"2025-10-10T17:22:10.323642031Z","tenant":
{"id":"66","uuid":"07f6adf7-4665-4340-865d-
c4a4c66f4dcd","name":"DemoCustomer2","locator":"/1/66/"},"executor":
{"id":"","clusterId":""},"result":{"code":"ok"}}

{"uuid":"fe72e679-541b-42fe-a622-
31bd5711ca1f","type":"Download","taskId":1634709492787113984,"progress":
{"current":100,"total":100},"resource":{"id":"3B9187D6-0853-45FF-AAB0-
0C68CD643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","context":{"_runtime":{},"argument":{"add_
components":[],"remove_components":
["agentForAmp"],"AMSPort":0}},"id":1634709499225370624,"idString":"16347094992253706
24","taskIdString":"1634709492787113984","createdAt":"2025-10-
10T17:53:16.811530215Z","startedAt":"2025-10-
10T17:53:16.811530215Z","updatedAt":"2025-10-
10T17:54:33.700680609Z","completedAt":"2025-10-10T17:54:33.700680609Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":{"id":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","clusterId":""},"result":{"code":"ok"}}

{"uuid":"fc557426-9e62-4550-9e8c-
b276bffa8911","type":"AutoUpdateStandby","taskId":1634702108316463104,"progress":
{"current":100,"total":100},"resource":{"id":"3B9187D6-0853-45FF-AAB0-
0C68CD643068","type":"machine","name":"WIN-
R1OR1V5M79O"},"state":"completed","context":{"argument":{"add_components":
["agentForAmp"],"remove_components":
[],"AMSPort":0}},"id":1634702109243404288,"idString":"1634702109243404288","taskIdSt
ring":"1634702108316463104","createdAt":"2025-10-
10T17:22:29.312989889Z","startedAt":"2025-10-
10T17:22:29.312989889Z","updatedAt":"2025-10-
10T17:22:29.386614232Z","completedAt":"2025-10-10T17:22:29.386614232Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":{"id":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","clusterId":""},"result":{"code":"ok"}}

{"uuid":"ae0905c8-a94c-4d18-bcd1-
d22b88dc37f6","type":"agent.add","taskId":1634710042987524096,"state":"completed","c
ontext":{"IsProcessRoot":true,"Persistent":{"ID":"c8d66ac4-0d5b-4ecb-b1b0-
c3649df91231","Name":"WIN-

 © Acronis International GmbH, 2003-2026

```
R1OR1V5M79O","OwnerID":"67"},"Specific":"Business","UserName":"WIN-R1OR1V5M79O\\AMS
User","isLegacy":true,"title":"Adding agent 'WIN-R1OR1V5M79O' to the management
server"},"id":1634710042987524096,"idString":"1634710042987524096","taskIdString":"1
634710042987524096","startedByUser":"WIN-R1OR1V5M79O\\AMS User","createdAt":"2025-
10-10T17:55:32.736020984Z","startedAt":"2025-10-
10T17:55:32.736020984Z","updatedAt":"2025-10-
10T17:55:32.745019179Z","completedAt":"2025-10-10T17:55:32.736020984Z","tenant":
{"id":"67","uuid":"ba959847-ca47-4a48-90a5-cb42789d5b34","name":"Demo Customer2
(DemoCustomer2)","locator":"/1/66/67/"},"executor":
{"id":"","clusterId":""},"result":{"code":"ok"}}

{"uuid":"6868ba4c-1859-4079-a6d2-9fcd03d5db0e","type":"F5CD89C9-3CD1-4DBC-97F3-
82BF93687B46","taskId":1639510477987147776,"state":"completed","context":
{"IsProcessRoot":true,"Persistent":{"PlanID":"9371c058-e474-4e66-b4c7-
89c1f5473276","PlanName":"EDR - XDR Protection"},"PlanName":"EDR - XDR
Protection","Specific":"Business","isLegacy":true,"title":"Editing plan 'EDR - XDR
Protection' with ID '9371c058-e474-4e66-b4c7-
89c1f5473276'"},"id":1639510477987147776,"idString":"1639510477987147776","taskIdStr
ing":"1639510477987147776","policy":{"id":"9371c058-e474-4e66-b4c7-
89c1f5473276","type":"policy.protection.total","name":"EDR - XDR
Protection"},"startedByUser":"Demo3","createdAt":"2025-10-
24T15:17:21.489728531Z","startedAt":"2025-10-
24T15:17:21.489728531Z","updatedAt":"2025-10-
24T15:17:21.494705812Z","completedAt":"2025-10-24T15:17:21.489728531Z","tenant":
{"id":"101","uuid":"d4155dae-f7cc-4063-8df5-
a0610149f074","name":"CustomerA","locator":"/1/101/"},"executor":
{"id":"","clusterId":""},"result":{"code":"ok"}}
```


SIEM troubleshooting

This section provides troubleshooting steps for common issues with SIEM. Use the sections below to find solutions for configuration problems, event export issues, plan deployment errors, and more.

Plan validation errors

A comprehensive reference of all validation error codes returned when configuring plans, including error causes, user messages, and solutions. See "SIEM validation errors" (p. 308).

Configuration issues

Problems saving plan settings, changing integration UI settings, or the component failing to start. See "Configuration troubleshooting" (p. 311).

Event export to files

Issues with events not being written to output files or files growing without bound. See "Event export (files) troubleshooting" (p. 312).

Event export to syslog

Problems connecting to remote or local syslog servers, message truncation, or no events arriving. See "Event export (syslog) troubleshooting" (p. 313).

Plan and deployment

 © Acronis International GmbH, 2003-2026

Plan validation errors, unsupported export types, or plans applied without events. See "Plan and deployment troubleshooting" (p. 315).

Logging and diagnostics

Changing log verbosity, understanding log file locations, and health checks. See "Logging and health check troubleshooting" (p. 316) and "Collecting diagnostic information" (p. 317).

SIEM validation errors

When configuring a SIEM plan, the validator checks all settings, and returns error codes for invalid fields. This page provides detailed information about each error code, its causes, and examples of the JSON responses returned by the API.

Path validation errors (invalidPath)

Path validation errors occur when the configured output path for file-based export is invalid. The error code is invalidPath with context providing specific details about what is wrong.

Scenario	User message	Details
No path provided	The path is required.	Both path_windows and path_linux are empty while export type is FILES. The UI disables the "next" and "create" buttons if paths are empty, so this should not occur in normal usage.
Relative path	The path should be absolute, not relative.	path_linux is relative (e.g., relative/path). On Windows, the on-premises writer check also rejects relative paths.
Root directory	The path resolves to a file system or drive root. This is not allowed.	Path resolves to a filesystem or drive root (e.g., C:\ on Windows or / on Linux).
Path points to a file	The path points to a file. The path should be a directory.	An existing path component is a regular file (e.g., C:\siem\events.log\sub where events.log is a file, not a directory).
Contains symlinks	The path cannot contain symlinks or junctions.	A path component is a symlink or junction (e.g., /data/link/events where /data/link is a symlink).
Cannot evaluate path	Cannot evaluate path. Try again.	Failed for a non-permission reason, such as a dangling symlink that cannot be resolved.
Cannot create directory	Cannot create the path directory. Try again.	Directory creation failed (e.g., parent directory is read-only, or insufficient permissions).

Path access denied (pathAccessDenied)

Error code: pathAccessDenied

User message: The selected path **%{path}** is not writable. Select another path.

 © Acronis International GmbH, 2003-2026

Cause: OS-level access denied when traversing the path to check for symlinks or when opening the log file (Windows).

Solution: Ensure the service account has write permissions to the configured directory.

Invalid enum value (invalidValue)

Error code: invalidValue

User message: The field has an unrecognized value.

Cause: An enum field (record_format or export_type) has an unrecognized value. This is theoretically impossible in normal usage since the UI uses radio buttons for these fields.

Example response:

{"code": "invalidValue", "message": "invalid value",

"context": {"field": "record_format", "value": "XML"}}

Invalid syslog server host (invalidSyslogServerHost)

Error code: invalidSyslogServerHost

User message: The selected syslog server host **%{host}:%{port}** is invalid. Select another host.

Causes:

- Syslog host is empty (Windows requires an explicit host)
- Host resolves to a different address than expected (DNS mismatch with TLS certificate)
- Host is localhost on Windows (127.0.0.1 or localhost are not valid remote syslog hosts)

Example responses:

{"code": "invalidSyslogServerHost", "message": "invalid Syslog server host",

"context": {"os": "windows", "host": ""}}

{"code": "invalidSyslogServerHost", "message": "invalid Syslog server host",

"context": {"host": "siem.corp.local", "resolved_host": "10.0.0.1"}}

Cannot connect to syslog server (cannotConnectToSyslogServer)

Error code: cannotConnectToSyslogServer

User message: Cannot connect to syslog server **%{address}**. Select another host.

Cause: TCP connection to a remote syslog host failed. This can be due to network connectivity issues, incorrect host/port, or firewall blocking.

Example response:

{"code": "cannotConnectToSyslogServer", "message": "cannot connect to Syslog server",

"context": {"address": "10.0.0.5:6514", "export_type": "SYSLOG", "os": "windows"}}

Invalid TLS CA certificate (invalidCACertificate)

 © Acronis International GmbH, 2003-2026

Error code: invalidCACertificate

User message: TLS certificate verification failed connecting to syslog.

Cause: TLS certificate verification failed when connecting to the syslog server. The CA certificate used to sign the syslog server certificate is not trusted by the on-premises machine.

Solution: Install the CA certificate on the on-premises machine. See "Event export (syslog) troubleshooting" (p. 313) for certificate installation steps.

Cannot connect to local syslog (cannotConnectToLocalSyslog)

Error code: cannotConnectToLocalSyslog

User message: Connection to the local syslog socket failed.

Cause: Connection to the local syslog socket failed (Linux only). This occurs when exporting to local syslog without specifying a remote host.

Solution: Ensure rsyslog (or another syslog daemon) is running and accepting connections on the local socket.

Unsupported export type (invalidSettings)

Error code: invalidSettings

User message: export_audit_log or export_events cannot be set to true.

Cause: export_audit_log or export_events is set to true (not supported on-premises). The supported export types are alerts (export_alerts) and activities (export_activities).

Solution: Disable export_audit_log and export_events in the plan settings. This should not occur in normal usage since the UI does not show these options for on-premises deployments.

Event writer test failed (failedEventWriterTest)

Error code: failedEventWriterTest

User message: The selected path **%{path}** is not writable. Select another path.

Cause: The writer was created successfully, but writing a test event failed. This typically indicates the path exists but is not writable by the service account.

Solution: Verify write permissions on the configured directory and ensure the service account can create files there.

© Acronis International GmbH, 2003-2026

Configuration troubleshooting

Note
The log file path is relative to the working directory of the service unless an absolute path is specified.

Default path to the logs directory:

- on Windows machine: **C:\ProgramData\Acronis\SIEMConnectorOnprem\Logs**
- on Linux machine: **/var/log/Acronis/SIEMConnectorOnprem**

Plan settings cannot be saved

Required information:

- URL to the partner tenant
- HAR log
- Screenshot of an error displayed in the integration UI (if applicable)
- Contents of `siem-connector.log` on the on-premises machine

Cannot change any setting in the integration UI

Required information:

- URL to the partner tenant
- HAR log
- Screenshot of an error displayed in the integration UI (if applicable)

Component fails to start

Symptoms: siem-connector exits immediately or is repeatedly restarted by the unit runner.

Check the unit restart policy in siem-connector.unit:

- max-attempts: 30, attempt-delay: 30s — the unit runner will retry up to 30 times.
- After all retries are exhausted, the integration becomes unavailable until manually restarted.

Required information:

- Contents of `siem-connector.log`
- Output of `cat /var/log/syslog | grep siem` (Linux) or the Windows Event Log entries for the service
- `siem-connector.yml` with secrets redacted

Common causes and fixes:

1. Invalid `onpremise.defaultroottenantuuid` — must be a valid UUID. The service logs `invalidDefaultRootTenantUUID`.

   Fix: set a correct UUID in `siem-connector.yml`:

   onpremise:

© Acronis International GmbH, 2003-2026

defaultroottenantuuid: "<valid-uuid>"

2. `addon.url` is not set — the service logs `addon.url` is not specified.

   Fix: provide the full URL of the SIEM Connector HTTP endpoint in `siem-connector.yml`:

   addon:

   url: "http://127.0.0.1:<port>"

3. Database file is locked or corrupted — SQLite database `siem-connector.db` cannot be opened.

   Fix: stop the service, remove or rename the database file, and restart the service. The service will recreate the database and re-apply migrations on startup.

Event export (files) troubleshooting

Note

The log file path is relative to the working directory of the service unless an absolute path is specified.

Default path to the logs directory:

- on Windows machine: **C:\ProgramData\Acronis\SIEMConnectorOnprem\Logs**
- on Linux machine: **/var/log/Acronis/SIEMConnectorOnprem**

Events are not written to the output file

Symptoms: the output file (`siem_data.log` / `siem_data.jsonl`) is not created, or no new records appear after events are generated.

Required information:

- Contents of `siem-connector.log`
- Plan settings screenshot (export type, output path, record format)
- Output of `ls -la <configured_path>` (Linux) or `dir <configured_path>` (Windows)

Common causes and fixes:

1. Path not configured — both `path_windows` and `path_linux` are empty when export type is FILES. The validator logs `invalidPath`.

   Fix: set at least one path in the plan settings that matches the OS of the on-premises machine.

2. `path_linux` is not an absolute path — the validator rejects relative paths.

   Fix: use an absolute path, e.g. `/var/log/siem`.

3. Permission denied — the service account does not have write access to the output directory. The service logs `pathAccessDenied`.

   Fix: grant write permissions to the service account on the configured directory.

4. Disk full — the configured directory has no free space.

   Fix: free disk space or point the path to a volume with sufficient capacity.

   Default rotation settings: `maxsize`: 50 MB, `maxbackups`: 100, `maxage`: 14 days. Adjust in `siem-connector.yml` under `writer:` if needed.

Output file grows without bound / old files are not deleted

© Acronis International GmbH, 2003-2026

Default rotation is controlled by the `writer` section in `siem-connector.yml`:

writer:

filename: siem_data # base name — extension added automatically (.log or .jsonl)

maxsize: 50 # MB per file before rotation

maxbackups: 100 # number of rotated files to keep

maxage: 14 # days to keep old files (0 = keep forever)

compress: false # gzip rotated files

localtime: true # use local time in rotated file names

Required information to diagnose retention issues:

- Current `writer` block from `siem-connector.yml`
- Output of `ls -lh <configured_path>`

Event export (syslog) troubleshooting

Note
The log file path is relative to the working directory of the service unless an absolute path is specified.

Default path to the logs directory:

- on Windows machine: **C:\ProgramData\Acronis\SIEMConnectorOnprem\Logs**
- on Linux machine: **/var/log/Acronis/SIEMConnectorOnprem**

Cannot connect to the remote syslog server

Symptoms: plan validation fails or the connection test reports `cannotConnectToSyslogServer`.

Required information:

- `syslog_host` and `syslog_port` values from the plan settings
- Error message from `siem-connector.log`
- Output of `openssl s_client -connect <host>:<port>` from the on-premises machine

Common causes and fixes:

1. TLS certificate verification failure — logged as `invalidCACertificate`. The CA certificate used to sign the syslog server certificate is not trusted by the on-premises machine.
   Fix (Windows, run as Administrator):
   certutil -addstore -f "Root" "C:\path\to\ca.pem"
   Fix (Linux):
   sudo cp ca.pem /usr/local/share/ca-certificates/siem-rsyslog-ca.crt
   sudo update-ca-certificates

© Acronis International GmbH, 2003-2026

2. Wrong host or port — the syslog server is unreachable because the host or port is incorrect. Default port is 6514.

   Fix: verify the `syslog_host` and `syslog_port` values in the plan settings. Check network connectivity: `nc -zv <host> <port>`.
3. Localhost / loopback address on Windows — on Windows, `127.0.0.1` or `localhost` is not a valid remote syslog host. The service logs `invalidSyslogServerHost` with `is_localhost: true`.

   Fix: use an actual remote IP address.
4. Hostname resolves to a different address — if the DNS name of the syslog server resolves to a different IP than the one registered in the server TLS certificate, validation will fail. The service logs `invalidSyslogServerHost` with both `host` and `resolved_host` fields.

   Fix: use the IP address directly as `syslog_host` and ensure it matches the certificate SAN.

For detailed information about configuring a remote syslog server to receive Acronis events, see "rsyslog configuration example" (p. 296).

Cannot connect to local syslog (Linux)

Symptoms: export type is SYSLOG with no `syslog_host`, but events are not forwarded to the local syslog. Error logged: `cannotConnectToLocalSyslog`.

Required information:

- Output of `systemctl status rsyslog`
- Contents of `/var/log/syslog`

Fix: ensure rsyslog (or another syslog daemon) is running and accepting connections on the local socket.

Syslog server receives no messages after a successful connection test

Required information:

- Contents of `siem-connector.log` filtered for the plan ID
- Contents of `/var/log/syslog` on the rsyslog machine

Common causes:

1. Events are not being generated — see "Plan and deployment troubleshooting" (p. 315).
2. The agent poller has not yet received events from the cloud (polling interval: 500 ms by default; backoff on errors up to 1 h).

Exported events are truncated

Events longer than the maximum record size are automatically truncated. The service logs a WARN message: `Truncating exported event record, length X, maximum is Y` with the first 200 characters of the original record.

Required information:

- The warning log entry with `event_record`, `event_format`, `customer_tenant_uuid`, and `location` fields
- Plan `record_format` setting (CEF or JSON)

 © Acronis International GmbH, 2003-2026

Plan and deployment troubleshooting

Plan validation issues

The validator returns a `SIEMConnector` domain error for each invalid setting field. Look for these error codes in the UI or in `siem-connector.log`:

Code	Meaning
`invalidPath`	`path_windows` / `path_linux` is empty or not absolute
`pathAccessDenied`	service cannot write to the configured path
`invalidSyslogSettings`	syslog settings sent to a non-on-premises deployment
`invalidSyslogServerHost`	syslog host is empty (Windows), is localhost (Windows), or resolves incorrectly
`invalidCACertificate`	TLS CA certificate is not trusted
`cannotConnectToSyslogServer`	TCP TLS connection to the syslog server failed
`cannotConnectToLocalSyslog`	local syslog socket is unavailable (Linux)
`invalidSettings`	`export_audit_log` or `export_events` is true (not supported on-premises)
`invalidPolicyName`	plan name is empty
`failedEventWriterTest`	the writer test write failed after validation passed

For additional details about each error code, see "SIEM validation errors" (p. 308).

Required information for any plan validation issue:

- URL to the partner tenant
- HAR log captured while saving or enabling the plan
- Plan settings screenshot

export_audit_log or export_events is rejected

On-premises deployments do not support audit log or generic event export (`export_audit_log: true` / `export_events: true`). The supported export types are alerts (`export_alerts`) and activities (`export_activities`).

Fix: disable `export_audit_log` and `export_events` in the plan settings.

Plan is applied but no events arrive

Required information:

- URL to the partner / customer tenant
- Contents of `siem-connector.log` for the relevant time window
- Confirmation that events were generated (e.g. a user login was performed)

Checklist:

 © Acronis International GmbH, 2003-2026

1. Verify the plan is enabled and applied to the device.
2. Check `siem-connector.log` for a line like `Starting initial setup of the Event Manager poller` — this means the agent started successfully.
3. The agent polls the cloud every 500 ms by default (`agent.poller.polling.pollinterval`). On errors it backs off up to 1 h (`maxerrorbackoffinterval`). Check for repeated error log lines.
4. Generate a test event (e.g. log in to the Cyber Protection Console) and wait up to 1–2 minutes.
5. Confirm the output file or syslog destination is being written to.

Logging and health check troubleshooting

Note

The log file path is relative to the working directory of the service unless an absolute path is specified.

Default path to the logs directory:

- on Windows machine: **C:\ProgramData\Acronis\SIEMConnectorOnprem\Logs**
- on Linux machine: **/var/log/Acronis/SIEMConnectorOnprem**

Increasing log verbosity

Edit **siem-connector.yml** and set the log level to **debug**:

log:

level: debug

Restart the service after changing the configuration.

Log file location and rotation

Default log configuration in siem-connector.yml:

log:

format: json

level: info

output: file

file:

path: siem-connector.log

rotation:

compress: true

maxbackups: 10

maxsize: 25M

Health check

© Acronis International GmbH, 2003-2026

The service exposes a health check endpoint used by the unit runner:

- Endpoint: **GET /healthz**
- Timeout: 5 s
- Check interval: 30 s
- Max consecutive failures before restart: 3

To check manually from the on-premises machine:

curl -s http://127.0.0.1:<port>/healthz

A 200 OK response means the service is healthy.

Collecting diagnostic information

Note
The log file path is relative to the working directory of the service unless an absolute path is specified.

Default path to the logs directory:

- on Windows machine: **C:\ProgramData\Acronis\SIEMConnectorOnprem\Logs**
- on Linux machine: **/var/log/Acronis/SIEMConnectorOnprem**

When filing a support request for an on-premises issue, always include the following information:

- URL to the partner tenant.
- `siem-connector.log` (or the relevant portion, filtered by time).
- `siem-connector.yml`, with passwords and secrets redacted.
- OS and version of the on-premises machine (Windows / Linux distribution).
- Screenshot or JSON of the plan settings.
- Steps to reproduce the problem, including what events were generated, and when.

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. 282).

 © Acronis International GmbH, 2003-2026

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:

 © Acronis International GmbH, 2003-2026

- **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 displays the time until expiration of the password for user's access to Acronis Cyber Protect Management Server. This is the local or domain password with which the user logs on to the

© Acronis International GmbH, 2003-2026

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 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 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 console, go to **Settings** > **Protection**.

For more information about specific settings and procedures, see 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:

- Vulnerability assessment
- Patch management

© Acronis International GmbH, 2003-2026

Note

Antimalware definitions are updated separately and are not affected by the Updater role. Each agent downloads antimalware updates from the selected source. For the available sources, see Source of the latest protection definitions.

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.

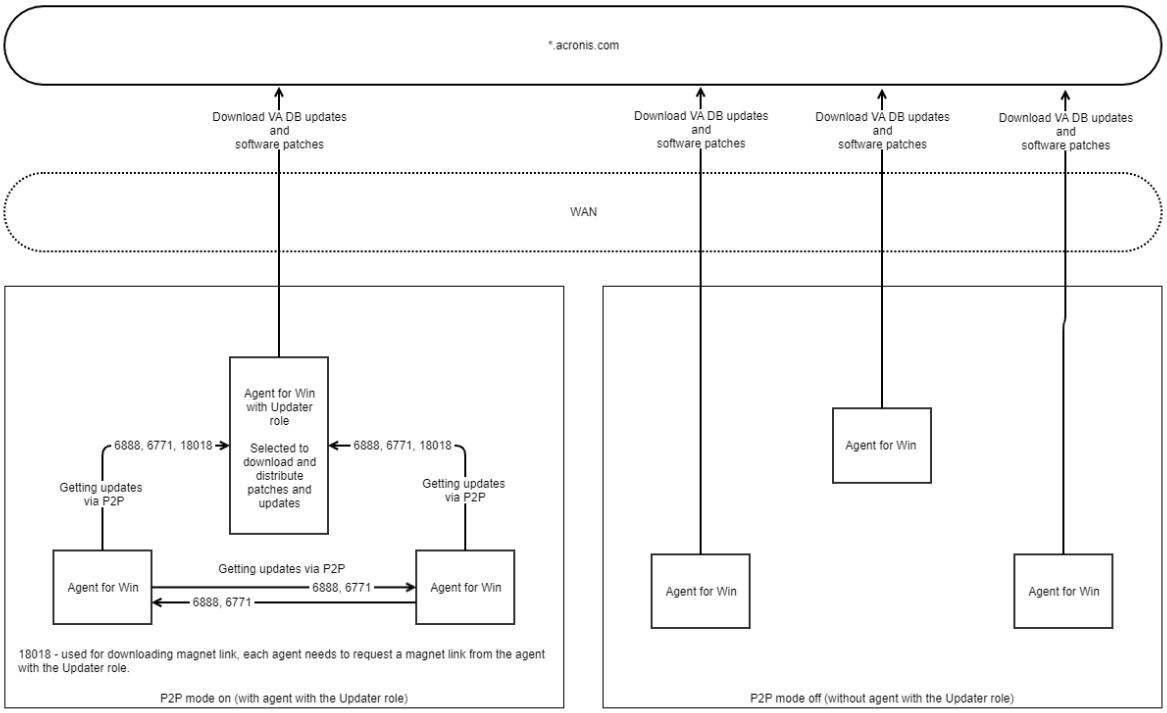
The agents without the Updater role will connect to the Internet if there is no dedicated updater agent in the environment, or if the connection to a dedicated updater agent cannot be established for about five minutes.

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.

© Acronis International GmbH, 2003-2026



To prepare a machine for the Updater role

1. 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).
2. Restart the Acronis Agent Core Service.
3. 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

1. In the Cyber Protect console, go to **Settings** > **Agents**.
2. Select the machine with the agent to which you want to assign the Updater role.
3. 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

© Acronis International GmbH, 2003-2026

1. In the Cyber Protect 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:

© Acronis International GmbH, 2003-2026

```
{
        "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, see "Updating the protection definitions" (p. 320).
- **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, see "Updating the protection definitions in an air-gapped environment" (p. 325). 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 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.

 © Acronis International GmbH, 2003-2026

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 console, under **Cyber Protection Desktop** in the right-hand menu.

Updating the protection definitions in an air-gapped environment

You can update the protection definitions in air-gapped environments by using an auxiliary management server that has connection to the internet.

To update the protection definitions in an air-gapped environment

1. Outside your air-gapped environment, install an Acronis Management Server that can access the Internet. For the purpose of this procedure, we will call this server the online management server.

   For more information on how to do that, see "Installing the management server" (p. 102).
2. Download the protection definitions to the online management server and copy them to a removable storage device.

   For more information on this step, see "Downloading the protection definitions to an online management server" (p. 325).
3. Transfer the definitions to an HTTP server in the air-gapped environment.

   For more information on this step, see "Transferring protection definitions to an HTTP server" (p. 329).
4. Configure the management server in the air-gapped environment to use the HTTP server as the source for updated protection definitions.

   For more information on this step, see "Configuring the source of protection definitions on an air-gapped management server" (p. 330).

Downloading the protection definitions to an online management server

After installing a management server that can access the Internet, download the latest protection definitions to it, and then copy them to a removable drive, such as a USB flash memory stick or an external hard drive.

To download and copy the protection definitions

 © Acronis International GmbH, 2003-2026

1. On the machine with the online management server, copy the `AtpDatabaseMirror` folder to a location of your choice. For example, the desktop or the `Temp` folder.

   You can find the `AtpDatabaseMirror` folder in the following location:

   - Windows: `%ProgramFiles%\Acronis\`
   - Linux: `/usr/lib/Acronis/`
2. In the copied `AtpDatabaseMirror` folder, edit the `atp_database_mirror.json` file as follows:
   a. Change the value of `enable_appdata_as_root` to `false`.
   b. Change the value of `is_on_premise` to `false`.
   c. Change the values of all entries of `local_path` to the absolute path of the location where you want to save the protection definitions.

   Note
   Use only forward slashes, both for Windows and Linux file paths.

   For example:

Original value	Edited value (Windows)	Edited value (Linux)

`"name": "WWW_VERSIONDIR",`
`"desc": "Document root for the versioned updates",`
`"local_path": "scanner"`
	`"name": "WWW_VERSIONDIR",`
	`"desc": "Document root for the versioned updates",`
	`"local_path": "C:/Users/JohnDoe/Desktop/definitions/scanner"`
		`"name": "WWW_VERSIONDIR",`
		`"desc": "Document root for the versioned updates",`
		`"local_path": "/home/JohnDoe/Desktop/scanner"`

`"name": "WWW_DIR",`
`"desc": "x86 32-bit anti-malware database",`
`"download_url": "av32bit"`
`"local_path": "scanner/av32bit"`
	`"name": "WWW_DIR",`
	`"desc": "x86 32-bit anti-malware database",`
	`"download_url": "av32bit"`
	`"local_path": "C:/Users/JohnDoe/Desktop/definitions/scanner/av32bit"`
		`"name": "WWW_DIR",`
		`"desc": "x86 32-bit anti-malware database",`
		`"download_url": "av32bit"`
		`"local_path": "/home/JohnDoe/Desktop/scanner/av32bit"`

© Acronis International GmbH, 2003-2026

Original value	Edited value (Windows)	Edited value (Linux)
"name": "WWW_DIR64", "desc": "x86-64 64-bit anti-malware database", "download_url": "av64bit" **"local_path": "scanner/av64bit"**	name": "WWW_DIR64", "desc": "x86-64 64-bit anti-malware database", "download_url": "av64bit" **"local_path": "C:/Users/JohnDoe/Desktop/definitions/scanner/av64bit"**	name": "WWW_DIR64", "desc": "x86-64 64-bit anti-malware database", "download_url": "av64bit" **"local_path": "/home/JohnDoe/Desktop/scanner/av64bit"**
"name": "ngmp", "download_url": "https://dl.acronis.com/u/am/ngmp/update-index.json", **"local_path": "ngmp"**	"name": "ngmp", "download_url": "https://dl.acronis.com/u/am/ngmp/update-index.json", **"local_path": "C:/Users/JohnDoe/Desktop/definitions/ngmp"**	"name": "ngmp", "download_url": "https://dl.acronis.com/u/am/ngmp/update-index.json", **"local_path": "/home/JohnDoe/Desktop/ngmp"**
"name": "vapm", "download_url": "https://dl.acronis.com/u/vapm/v2/update-index.json", **"local_path": "vapm"**	"name": "vapm", "download_url": "https://dl.acronis.com/u/vapm/v2/update-index.json", **"local_path": "C:/Users/JohnDoe/Desktop/definitions/vapm"**	"name": "vapm", "download_url": "https://dl.acronis.com/u/vapm/v2/update-index.json", **"local_path": "/home/JohnDoe/Desktop/vapm"**

3. Save the edited `atp_database_mirror.json` file.
4. Stop the **Acronis Management Server** service by using the following command:
   - Windows (Command Prompt):

```
sc stop AcrMngSrv
```


© Acronis International GmbH, 2003-2026

- Linux (Terminal):

```
sudo systemctl stop acronis_ams.service
```

5. Use Command Prompt or Terminal to navigate to the copied `AtpDatabaseMirror` folder and start the `AtpDatabaseMirror` tool by using the following command:
   - Windows (Command Prompt)

     ```
     atp_database_mirror.exe -config atp_database_mirror.json
     ```

     For example, if you copied the folder to the desktop:

     ```
     cd C:\Users\JohnDoe\Desktop\ AtpDatabaseMirror
     ```

     ```
     atp_database_mirror.exe -config atp_database_mirror.json
     ```

   - Linux (Terminal)

     Navigate to the copied folder by using the `cd` command and then run

     ```
     sudo ./atp_database_mirror -config atp_database_mirror.json
     ```

   When all updates are downloaded to the folders that you specified in `local_path`, the following line will appear in the Command Prompt or the Terminal window:

   ```
   standing by for 1m0s
   ```

6. Stop the `AtpDatabaseMirror` tool by pressing CTRL+C.

   At this point, the definitions are downloaded to the folders that you specified as `local_path` in the `atp_database_mirror.json` file. Per the example above, the definitions will be located as follows:

Folder	Contents
`C:\Users\JohnDoe\Desktop\definitions\ngmp`	Advanced detection definitions
`C:\Users\JohnDoe\Desktop\definitions\scanner`	Antivirus and Antimalware definitions
`C:\Users\JohnDoe\Desktop\definitions\vapm`	Vulnerability assessment and patch management definitions

7. Zip the folder that contains the definitions to a removable drive.

   In this example, zip the `definitions` folder.

Next, you must copy the definitions from the removable drive to an HTTP server in your air-gapped environment. You can use the air-gapped management server as an HTTP server. For more information, see "Transferring protection definitions to an HTTP server" (p. 329).

 © Acronis International GmbH, 2003-2026

Transferring protection definitions to an HTTP server

To distribute protection definitions in your air-gapped environment, you need a dedicated HTTP server. You can either use an existing HTTP server within your environment or start one on the Acronis Management Server (AMS) machine using the Python instance included with the management server installation.

To configure an HTTP server on the air-gapped management server machine

1. On the air-gapped AMS machine, navigate to `C:\Program Files\Acronis\PyShell` and place an empty `index.html` file in this folder.
   This is required to prevent directory listing.
2. Copy the definition folders from the removable drive to folder `C:\Program Files\Acronis\PyShell\defvirus`.
3. To prevent directory listing on the HTTP server, place the empty `index.html` file in the definitions subfolders:
   - `ngmp`
   - `scanner`
   - `vapm`
4. Use Command Prompt to start the HTTP server from folder `C:\Program Files\Acronis\PyShell`.

```
cd C:\Program Files\Acronis\PyShell
```

```
Python.exe -m http.server 8080
```

Enter the URL of the HTTP server in the configuration files

1. In the folders where you copied the protection definitions, open the following files for editing:
   - `./ngmp/update-index.json`
   - `./vapm/update-index.json`
2. In both `update-index.json` files, edit all URL handles for all OS versions to add a prefix with the IP address and port number of the HTTP server.
   For example, assuming that the IP address of the HTTP host is `10.0.0.52`, and the port is `8080`, the string for `Windows x86 "url": "ngmp/win86/ngmp_<version>.zip"` should be modified as follows:

```
"url": "http://10.0.0.52:8080/ngmp/win86/ngmp_1_0_4560_3881.zip",
```

   where `10.0.0.52:8080` is the IP address and port number of the server, and `_0_4560_3881` is the factory version number of the corresponding definitions file.
3. Save your edits in both `update-index.json` files.

Next, you must configure the source of the protection definitions on the air-gapped management server. For more information, see "Configuring the source of protection definitions on an air-gapped management server" (p. 330).

 © Acronis International GmbH, 2003-2026

Configuring the source of protection definitions on an air-gapped management server

After configuring the HTTP server, you must configure the air-gapped management server to use it as the source of protection definitions.

To configure the source of protection definitions on the air-gapped management server

1. In the Cyber Protect console of the air-gapped management server, go to **Settings** > **Protection** > **Protection definitions update** > **Definitions**.
2. Select **Custom**, and then specify the following paths, where `<IP>` is the address of your HTTP server:
   - For **Antivirus and Antimalware definitions**:
     `http://<IP>:8080/scanner`
   - For **Advanced detections definitions**:
     `http://<IP>:8080/ngmp/update-index.json`
   - For **Vulnerability assessment and patch management definitions**:
     `http://<IP>:8080/vapm/update-index.json`

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

The functionality that is described in this section is available only to organization administrators.

Units and administrative accounts

To manage units and administrative accounts, in the Cyber Protect 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. In 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, see "Creating units" (p. 338).

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.

 © Acronis International GmbH, 2003-2026

Administrative accounts

Any account that is able to sign in to the Cyber Protect console is an administrative account.

In the Cyber Protect 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, has 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, see 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`.
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. 242).

© Acronis International GmbH, 2003-2026

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, see "Adding administrative accounts" (p. 334).

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 console. It only allows the gathering of diagnostic data, such as system reports. The read-only role does not allow the browsing of backups or the browsing of the content of backed-up mailboxes.
- **Auditor**
  This role provides read-only access to the **Activities** tab in the Cyber Protect console. For more information about this tab, see "The Activities tab" (p. 277). 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 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.

 © Acronis International GmbH, 2003-2026

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 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 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

© Acronis International GmbH, 2003-2026

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.
   The following options are available.

Role	Service
Company administrator	Account-wide role. This role includes the administrator role in Management Portal and in the Protection service.
Administrator Read-only administrator	Management Portal
Administrator Backup administrator Backup operator* Read-only administrator Restore operator* Security administrator User*	Protection

   * Not an administrator role.
8. Repeat steps 4-6 for all users or groups that you want to add.

© Acronis International GmbH, 2003-2026

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 that are running on Linux machines.

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.

Backup administrator role

The Backup administrator role is designed for organizations that need a dedicated user profile focused solely on backup operations. This role provides full access to backup-related features while restricting access to other areas of the Acronis Cyber Protect Cloud system, such as security management.

This role is ideal for IT personnel who manage backup tasks but should not have access to broader system features. This role bridges the gap between full administrators and read-only users. It can be assigned on users under customer and unit tenants.

The Backup administrator role is available in all editions of Acronis Cyber Protect Cloud, including both on-premises and cloud installations.

A Backup administrator can perform the following tasks:

- Add devices.
- Assign existing protection plans to devices.
- Start and stop protection plans.
- Recover data from backups.
- View backup storage locations.
- Create, edit, delete, and disable backup protection plans.
- Create and delete backup storage locations.
- Enable or disable immutable storage.
- Delete archives and backups.

A Backup administrator cannot perform the following tasks:

- View or operate on non-backup features (for example, security management).
- Apply, revoke, or edit protection plans that include non-backup features.

© Acronis International GmbH, 2003-2026

Backup operator role

The Backup operator role is designed for users who need access to core backup operations without broader administrative privileges.

This role is ideal for organizations that want to delegate backup tasks, such as device management and recovery, while restricting access to security settings and system configurations. It is intended to users responsible for executing backup workflows, such as adding devices, assigning protection plans, and performing recovery tasks, and provides balance between operational flexibility and security restrictions. It can be assigned on users under customer and unit tenants.

This role inherits basic viewing permissions from the read-only role to enable access to the Cyber Protect Cloud console.

The Backup operator role is available in all editions of Acronis Cyber Protect, including both on-premises and cloud installations.

A Backup operator can perform the following tasks:

- Add devices and applications.
- Assign or revoke existing protection plans from devices.
- Start and stop protection plans.
- Recover data from backups (files, volumes, devices, applications).
- Run replicate, validate, and convert-to-VM operations.
- View backup storage locations (read-only).
- View activity monitor and reports.
- Change their own passwords.

A Backup operator cannot perform the following tasks:

- Create, edit, import, clone, or delete protection plans.
- Disable encryption.
- Create, delete, or modify backup storage locations.
- Modify immutable storage settings.
- Delete archives or backup slices.
- Disable protection plans.
- Create, delete, or modify users.
- Change user roles.
- Access or operate on non-backup features (for example, security management).

Security Administrator role

The Security Administrator role provides Acronis Cyber Protect customers in on-premises deployments with dedicated access to manage security-related features in the Acronis Cyber Protect Cloud console. This role is designed to isolate security operations from broader administrative functions, ensuring focused control over protection plans and security policies.

© Acronis International GmbH, 2003-2026

This role is intended for customer tenant users who require access to security alerts and protection plan management, without full administrative privileges. It grants permissions that are required to perform security operations and inherits read-only permissions from the Administrator role.

Security Administrators can perform the following tasks:

- Protection Plans (Security Policies Only)
  - Create, edit, apply, revoke, import, export, clone, delete, enable, and disable protection plans that contain only security policies.
  - Assign security-only protection plans to devices.
  - View disabled security policies and re-enable them.
  - View settings of all protection plans (including non-security policies) in read-only mode.
- Security Features
  - Manage Antivirus & Antimalware, URL filtering, Microsoft Defender Antivirus, Microsoft Security Essentials, Vulnerability Assessment, Patch Management, and Data Protection Map.
  - Configure and manage backup scanning plans.

    Note
    To this, the role has access to encryption passwords for backups.

  - Manage allowlist settings:
    - Enable/disable automatic generation.
    - Adjust heuristic protection levels.
    - Manually add files.
    - View whitelist details.
  - Manage quarantine:
    - Delete and restore entries.
- Remote connection
  - Establish remote connections through the NEAR protocol.
  - Send Command Prompt commands remotely.
- Monitoring and Reporting
  - View activity monitor, reports, widgets, and alerts.
  - Clear alerts.
  - Device Management
  - Add devices and applications.

Security Administrators cannot perform the following tasks:

- Modify or assign protection plans containing non-security policies.
- Start or stop backups.
- Modify encryption or immutable storage settings.
- Create, delete, or modify users or their roles.
- Perform recovery operations.

© Acronis International GmbH, 2003-2026

- Browse or recover from backup storage locations.
- Download or export reports.
- Change widget positions.

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**.

Viewing the last logged-in user

If you enable the **Show last logged-in** setting in the remote management plan that is applied to a workload, the system will record information about the users who log in to the device. You can view this information in the Dashboard or in the workload's details.

For more information about the **Show last logged-in** setting, see Remote management plans.

To view the user who last logged in to a device

1. Click **Devices**.

   The **All devices** screen opens. In the **Last login** column, you can see the name of the user who logged in last on each device. In the **Last login time** column, check the time when the user logged in last on each device.
2. Click a device for which you want to check the details.
3. Click the **Details** icon.
4. In the **Last users logged in** section, check the name of the user who logged in to the device last and the date and time of the last login.

   Note
   The system lists up to 5 different users who logged in to the device last.

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

applied. You can adjust the settings as needed and apply this plan or create a new one.

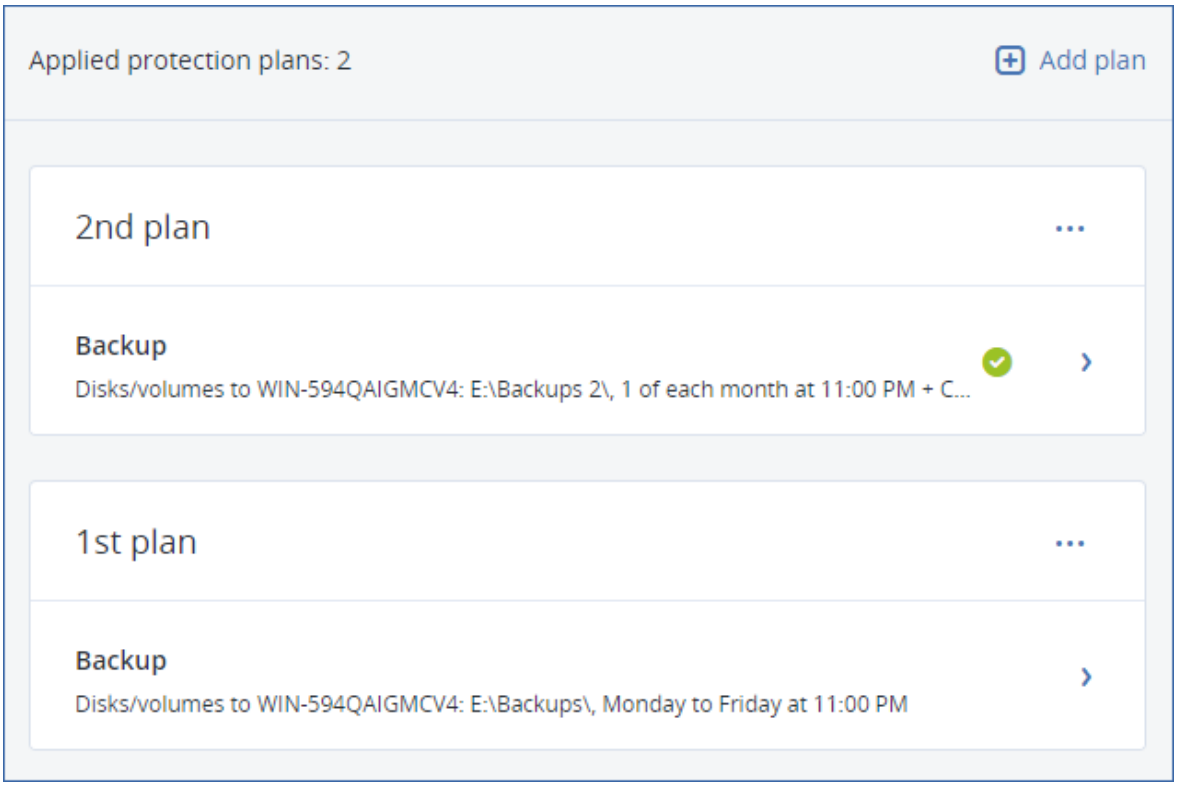
3. To create a new plan, click **Create plan**. Enable the **Backup** module and unroll the settings.
4. [Optional] To modify the protection plan name, click the default name.
5. [Optional] To modify the Backup module parameters, click the corresponding section of the protection plan panel.
6. [Optional] To modify the backup options, click **Change** next to **Backup options**.
7. Click **Create**.

© Acronis International GmbH, 2003-2026

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	HOW LONG TO KEEP
Disks/volumes (physical	Direct selection	Cloud Local folder	Always incremental	By number of backups

© Acronis International GmbH, 2003-2026

machines)	Policy rules File filters	Network folder SFTP server* NFS* Secure Zone* Managed location* Tape device*	(single-file)* Always full Weekly full, Daily incremental Monthly full, Weekly differential, Daily incremental (GFS) Custom (Full, differential, incremental)	By backup age (single rule/per backup set) 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 (Full, differential, incremental)	
ESXi configuration	Direct selection	Local folder Network folder SFTP server NFS*		
SQL databases	Direct selection	Cloud Local folder Network folder Managed location*	Always full Weekly full, daily incremental Custom (Full, incremental)	

© Acronis International GmbH, 2003-2026

<table>
<tr><td></td><td></td><td rowspan="2">Tape device</td><td rowspan="2"></td><td rowspan="4"></td></tr>
<tr><td>Exchange databases</td><td>Direct selection</td></tr>
<tr><td>Exchange mailboxes</td><td>Direct selection</td><td rowspan="3">Cloud
Local folder
Network folder
Managed location*</td><td rowspan="3">Always incremental (single-file)</td></tr>
<tr><td>Microsoft 365 mailboxes</td><td>Direct selection</td><td>By number of backups
By backup age (single rule/per backup set)
Keep indefinitely</td></tr>
</table>

* See the limitations below.

Note
Backups to public cloud require a **Local backup** storage quota.

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.

© Acronis International GmbH, 2003-2026

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.

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, see "Selecting disks/volumes" (p. 344).

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.

Backup and recovery of disks that contain GPT protective partitions are supported.

AppleRAID configurations are not supported.

 © Acronis International GmbH, 2003-2026

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 iSCSI, 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.

© Acronis International GmbH, 2003-2026

- `[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-l-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

 © Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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 network folder must be accessible from the selected machine.
   c. Select the files and folders that you want back up.
      You can select a combination of up to 1,000 files and folders.
      Alternatively, you can specify the path to a file or folder, and then click the arrow button.
   d. [For shared folders] Specify the user name and password for the shared folder.
      Backing up folders with anonymous access is not supported.
   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:

© Acronis International GmbH, 2003-2026

- `[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 directory where all user profiles are located by default.

    Note
    This selection rule does not support custom paths for user profiles. If the user profile is not in the **/home** directory, its content will not be backed up.

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.

    Note
    This selection rule does not support custom paths for user profiles. If the user profile is not in the **/Users** folder, its content will not be backed up.

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**.

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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, see Acronis Cyber Protect Editions Comparison including Cloud deployment.

How it works

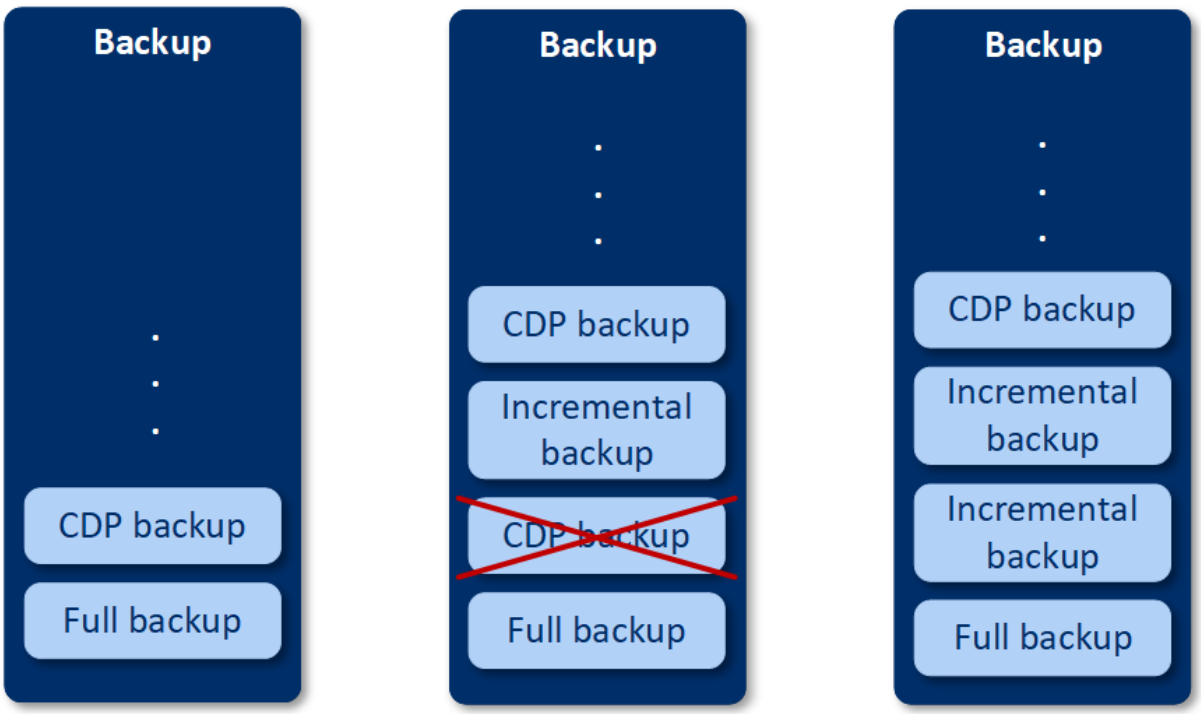
Let's call the backup that is created on continuous basis the CDP backup. For the CDP backup to be created, a full backup or incremental backup has to be created preliminarily.

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.

© Acronis International GmbH, 2003-2026



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.

Note
Continuous data protection is enabled by default for protection plans that you create from the **Devices** tab, if you use an Advanced license and you are not using other advanced backup features for the selected machines. If you already have a plan with Continuous data protection for a selected machine, Continuous data protection will not be enabled by default for that machine in newly created plans.
Continuous data protection is not enabled by default for plans created for device groups.

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:

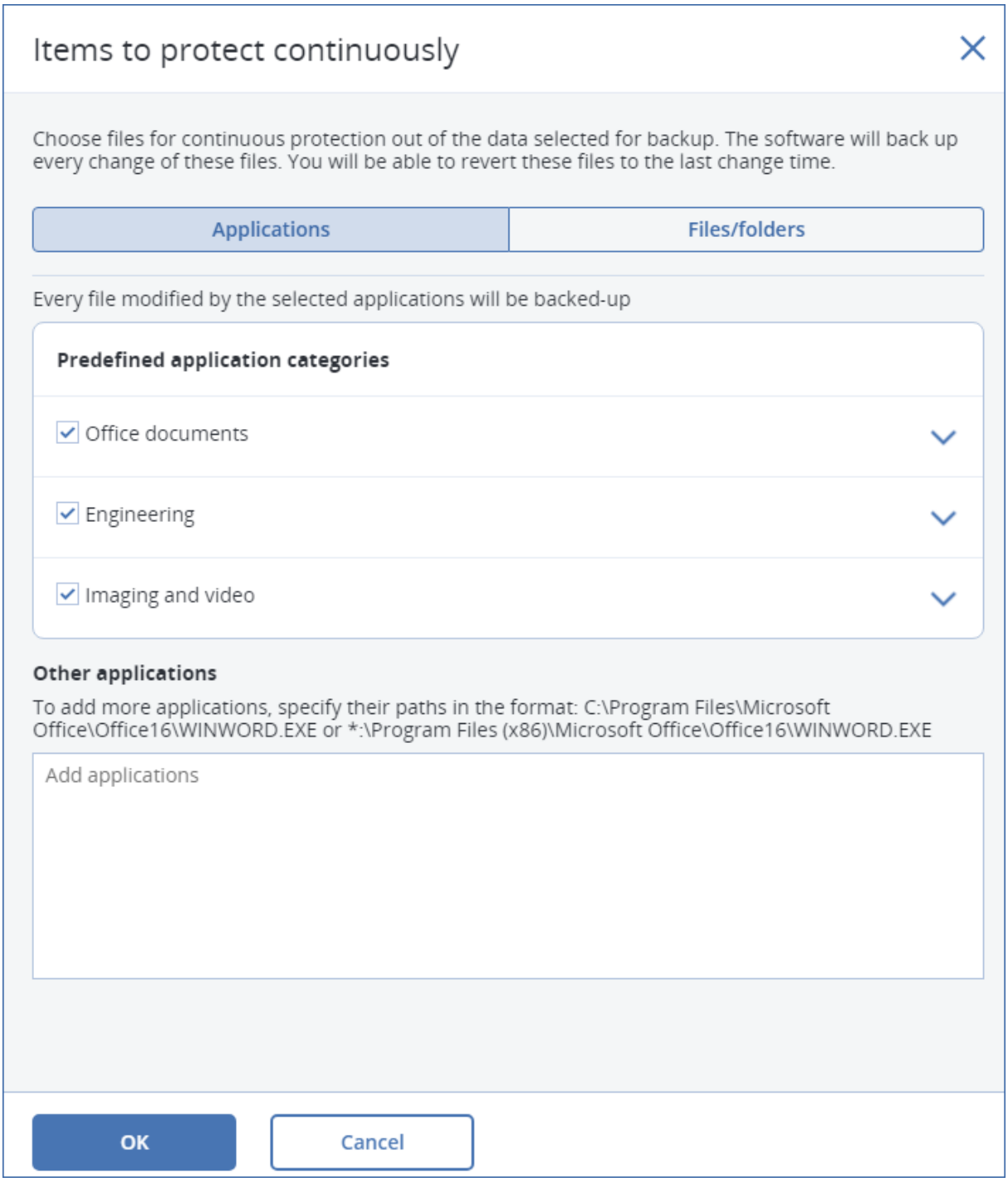
© Acronis International GmbH, 2003-2026

- 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 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.

© Acronis International GmbH, 2003-2026



- 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:

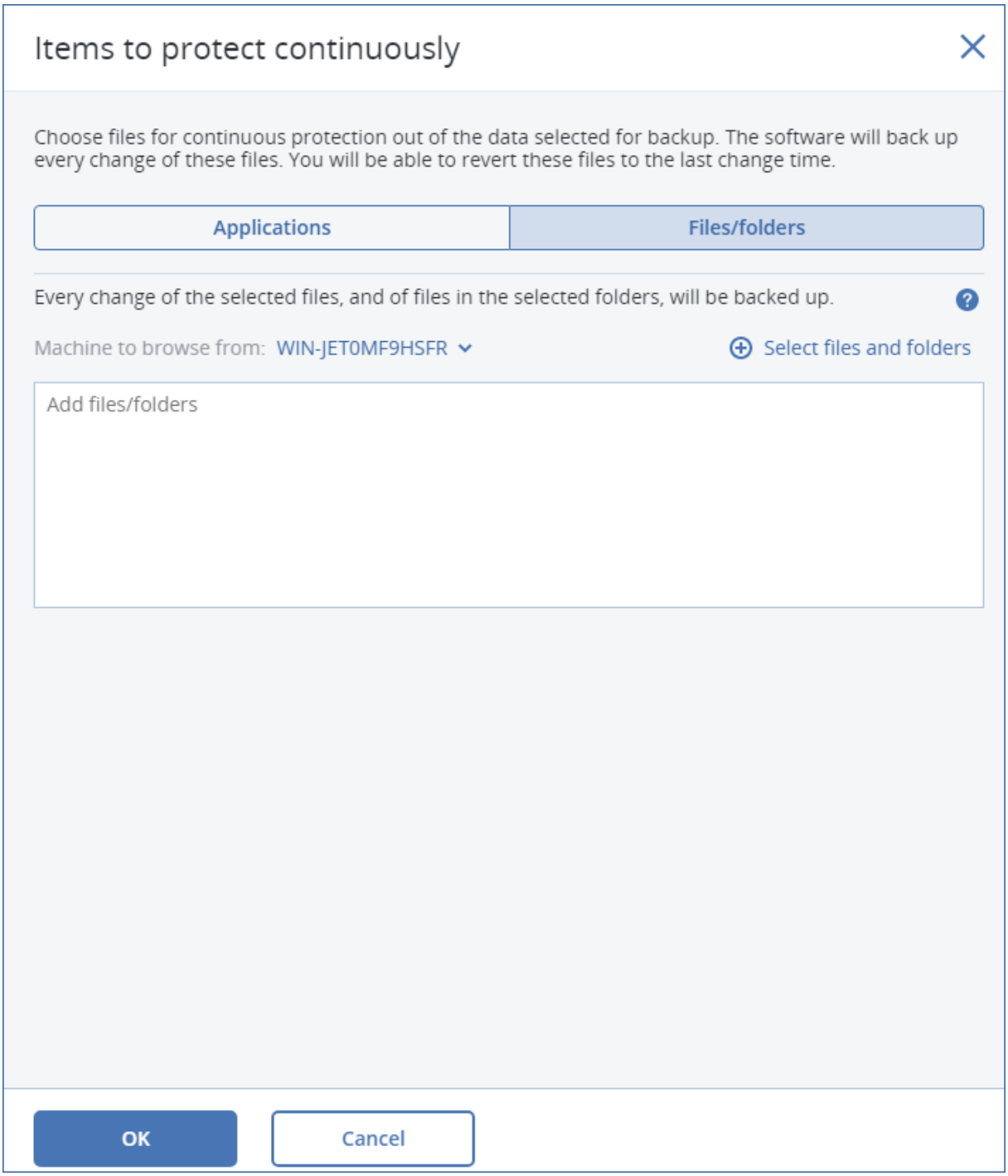
  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  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.

© Acronis International GmbH, 2003-2026



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.

   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\

© Acronis International GmbH, 2003-2026

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, see "Selecting files/folders". When ready, click **Done**.

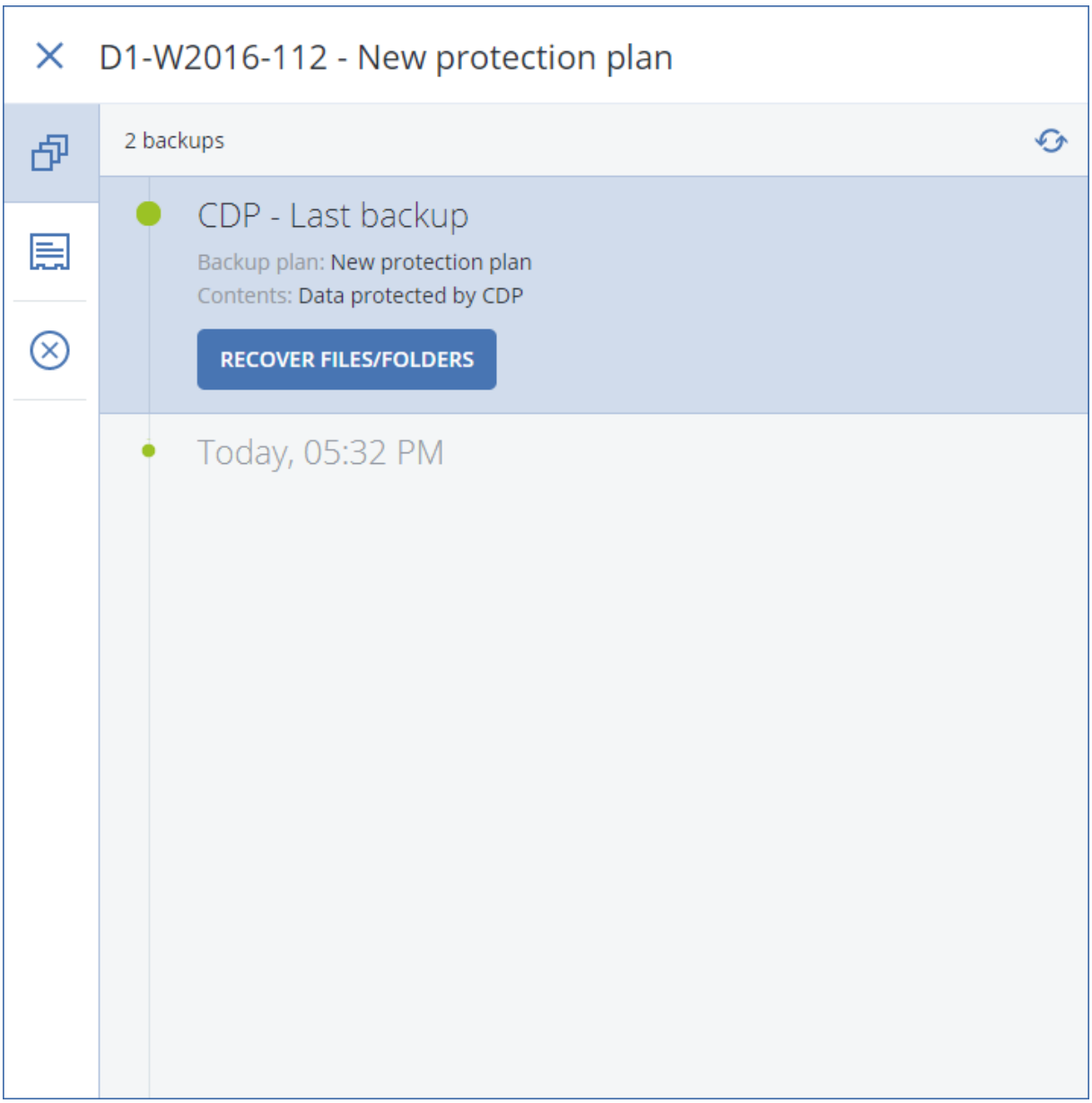
2. Click **Create**.

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.



© Acronis International GmbH, 2003-2026

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.

Note
Backups to public cloud require a **Local backup** storage quota.

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 International GmbH, 2003-2026

- **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, see "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, see "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

© Acronis International GmbH, 2003-2026

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 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, see "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**

© Acronis International GmbH, 2003-2026

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, see "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

© Acronis International GmbH, 2003-2026

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.

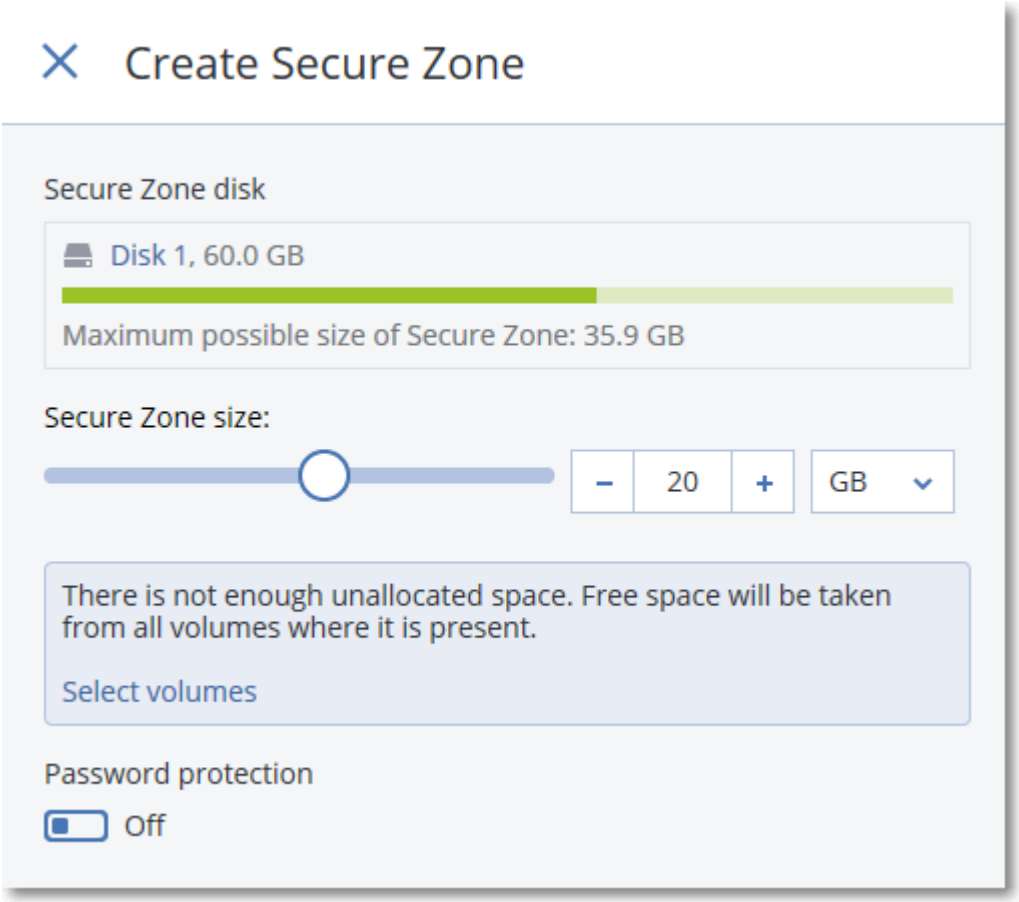
How to create Secure Zone

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.

© Acronis International GmbH, 2003-2026



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

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

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

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

© Acronis International GmbH, 2003-2026

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

About Acronis Cyber Infrastructure

Acronis Cyber Protect 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.

© Acronis International GmbH, 2003-2026

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 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.

Backup schedule

You can configure a backup to run automatically at a specific time, at specific intervals, or on a specific event.

Scheduled backups for non-cloud-to-cloud resources run according to the time zone settings of the workload on which the protection agent is installed. For example, if you apply the same protection plan to workloads with different time zones settings, the backups will start according to the local time zone of each workload.

Scheduling a backup includes the following actions:

- Selecting a backup scheme
- Configuring the time or selecting the event that triggers the backup
- Configuring optional setting and start conditions

Backup schemes

A backup scheme is a part of the protection plan schedule that defines which type of backup (full, differential, or incremental) is created and when. You can select one of the predefined backup schemes or create a custom scheme.

The available backup schemes and types depend on the backup location and source. For example, a differential backup is not available when you back up SQL data, Exchange data, or system state.

Note

- The **Always incremental (single-file)** scheme is not supported for tape devices.
- Tape devices are supported only in on-premises deployments.

© Acronis International GmbH, 2003-2026

Backup scheme	Description	Configurable elements
Always incremental (single-file)	The first backup is full and might be time-consuming. Subsequent backups are incremental and significantly faster. The backups use the single-file backup format[1]*. By default, backups are performed on a daily basis, Monday to Friday. We recommend that you use this scheme when you store your backups in the cloud storage, because incremental backups are fast and involve less network traffic.	• Schedule type: monthly, weekly, daily, hourly • Backup trigger: time or event • Start time • Start conditions • Additional options
Always full	All backups in the backup set are full. By default, backups are performed on a daily basis, Monday to Friday.	• Schedule type: monthly, weekly, daily, hourly • Backup trigger: time or event • Start time • Start conditions • Additional options
Weekly full, Daily incremental	A full backup is created once a week and other backups are incremental. The first backup is full and the other backups during the week are incremental, then the cycle repeats. To select the day on which the weekly full backup is created, in the protection plan, click the gear icon, and then go to **Backup options** > **Weekly backup**. By default, backups are performed on a daily basis, Monday to Friday.	• Backup trigger: time or event • Start time • Start conditions • Additional options
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.	• Change the existing schedule per backup type: ◦ Schedule type: monthly, weekly,

[1]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.

© Acronis International GmbH, 2003-2026

Backup scheme	Description	Configurable elements
	Note This is a predefined custom scheme. In the protection plan, it is shown as **Custom**.	daily, hourly ◦ Backup trigger: time or event ◦ Start time ◦ Start conditions ◦ Additional options • Add new schedules per backup type
Custom	You must select the backup types (full, differential, and incremental), and configure a separate schedule for each of them*.	• Change the existing schedule per backup type: ◦ Schedule type: monthly, weekly, daily, hourly ◦ Backup trigger: time or event ◦ Start time ◦ Start conditions ◦ Additional options • Add new schedules per backup type

* After you create a protection plan, you cannot switch between **Always incremental (single-file)** and the other backup schemes, and vice versa. **Always incremental (single-file)** is a single-file format scheme, and the other schemes are multi-file format. If you want to switch between formats, create a new protection plan.

Backup types

The following backup types are available:

- Full—a full backup contains all source data. This backup is self-sufficient. To recover data, you do not need access to any other backups.

  Note
  The first backup created by any protection plan is a full backup.

- Incremental—an incremental backup stores changes to the data since the latest backup, regardless of whether the latest backup is full, differential, or incremental. To recover data, you need the whole chain of backups on which the incremental backup depends, back to the initial full backup.
- Differential—a differential backup stores changes to the data since the latest full backup. To

© Acronis International GmbH, 2003-2026

recover data, you need both the differential backup and the corresponding full backup on which the differential backup depends.

Running a backup on a schedule

To run a backup automatically at a specific time or on a specific event, enable a schedule in the protection plan.

To enable a schedule

1. In the protection plan, expand the **Backup** module.
2. Click **Schedule**.
3. Enable the schedule switch.
4. Select the backup scheme.
5. Configure the schedule as required, and then click **Done**.
   For more information about the available scheduling options, see "Schedule by time" (p. 367) and "Schedule by events" (p. 369).
6. [Optional] Configure start conditions or additional scheduling options.
7. Save the protection plan.

As a result, a backup operation starts every time when the schedule conditions are met.

To disable a schedule

1. In the protection plan, expand the **Backup** module.
2. Click **Schedule**.
3. Disable the schedule switch.
4. Save the protection plan.

As a result, the backup runs only if you start it manually.

Note
If the schedule is disabled, the retention rules are not applied automatically. To apply them, run the backup manually.

Schedule by time

The following table summarizes the scheduling options that are based on time. The availability of these options depends on the backup scheme. For more information, see "Backup schemes" (p. 364).

Option	Description	Examples
Monthly	Select the months, days of the month or days of the week, and then select the backup start time.	Run a backup on January 1, and February 3, at 12:00 AM. Run a backup on the first day of each month, at 10:00 AM.

 © Acronis International GmbH, 2003-2026

Option	Description	Examples
		Run a backup on March 1, March 5, April 1, and April 5, at 09:00 AM. Run a backup on the second and third Friday of each month, at 11:00 AM. Run a backup on the last Wednesday of the month, at 10:30 PM.
Weekly	Select the days of the week, and then select the backup start time.	Run a backup Monday to Friday, at 10:00 AM. Run a backup on Monday, at 11:00 PM. Run a backup on Tuesday and Saturday, at 08:00 AM.
Daily	Select the days (everyday or weekdays only), and then select the backup start time.	Run a backup every day, at 11:45 AM. Run a backup Monday to Friday, at 09:30 PM.
Hourly	Select the days of the week, and then select a time interval between two consecutive backups and the time range within which the backups run. When you configure the interval in minutes, you can select a suggested interval between 10 and 60 minutes, or specify a custom one, for example, 45 or 75 minutes.	Run a backup every hour between 08:00 AM and 06:00 PM, Monday to Friday. Run a backup every 3 hours between 01:00 AM and 06:00 PM, on Saturday and Sunday.

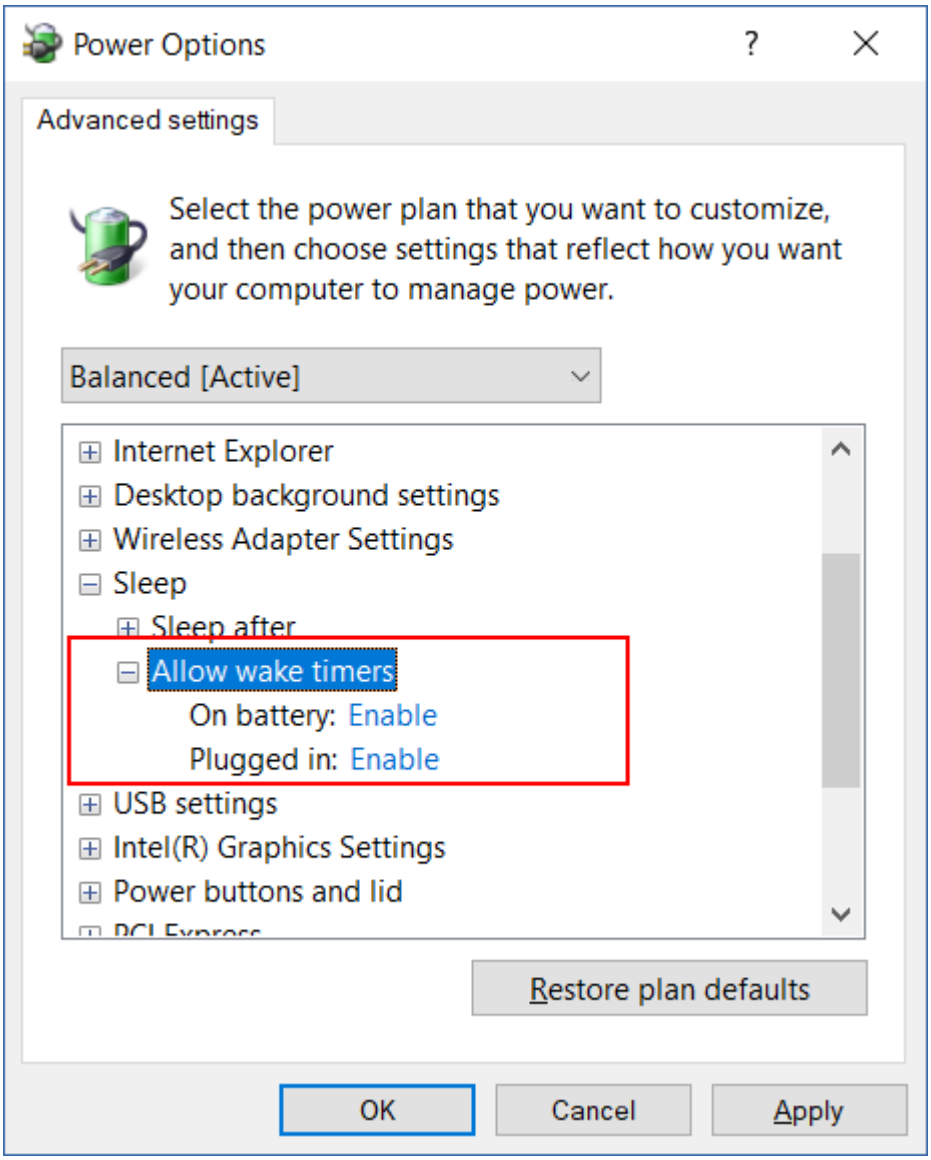
Additional options

When you schedule a backup by time, the following additional scheduling options are available.

To access them, in the **Schedule** pane, click **Show more**.

- **If the machine is turned off, run missed tasks at the machine startup**
  Default setting: Disabled.
- **Prevent the sleep or hibernate mode during backup**
  This option is applicable only to machines running Windows.
  Default setting: Enabled.
- **Wake up from the sleep or hibernate mode to start a scheduled backup**
  This option is applicable only to machines running Windows, in the power plans for which the **Allow wake timers** option is enabled.

© Acronis International GmbH, 2003-2026



This option does not use the Wake-on-LAN functionality and is not applicable to powered-off machines.

Default setting: Disabled.

Schedule by events

To configure a backup that runs upon a specific event, select one of the following options.

Option	Description	Examples
Upon time since last backup	A backup starts after a specified period following the last successful backup.	Run a backup one day after the last successful backup. Run a backup four hours after the last successful backup.

© Acronis International GmbH, 2003-2026

Option	Description	Examples
	Note This option depends on how the previous backup completed. If a backup fails, the next backup will not start automatically. In this case, you must run the backup manually and ensure that it completes successfully, in order to reset the schedule.	
When a user logs on to the system	A backup starts when a user logs in to the machine. You can configure this option for any login or for a login of a specific user. **Note** Logging in with a temporary user profile will not start a backup.	Run a backup when user John Doe logs in.
When a user logs off the system	A backup starts when a user logs off the machine. You can configure this option for any logoff or for the logoff of a specific user. **Note** Logging off from a temporary user profile will not start a backup. Shutting down a machine will not start a backup.	Run a backup when every user logs off.
On the system startup	A backup runs when the protected machine starts up.	Run a backup when a user starts the machine.
On the system shutdown	A backup runs when the protected machine shuts down.	Run a backup when a user shuts down the machine.
On Windows Event Log event	A backup runs upon a Windows event that you specify.	Run a backup when event 7 of type error and source disk is recorded in the Windows System log.

The availability of these options depends on the backup source and the operating system of the protected workloads. The table below summarizes the available options for Windows, Linux, and macOS.

© Acronis International GmbH, 2003-2026

Event	Backup source (What to back up)					
	Entire machine, Disks/volumes, or Files/folders (physical machines)	**Entire machines or Disk/volumes (virtual machines)**	**ESXi configuration**	**Microsoft 365 mailboxes**	**Exchange databases and mailboxes**	**SQL databases**
Upon time since last backup	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
When a user logs on to the system	Windows	N/A	N/A	N/A	N/A	N/A
When a user logs off the system	Windows	N/A	N/A	N/A	N/A	N/A
On the system startup	Windows, Linux, macOS	N/A	N/A	N/A	N/A	N/A
On the system shutdown	Windows	N/A	N/A	N/A	N/A	N/A
On Windows Event Log event	Windows	N/A	N/A	Windows	Windows	Windows

On Windows Event Log event

You can automatically run a backup when a specific event is recorded in a Windows Event log, such as the Application log, Security log, or System log.

Note

You can browse the events and view their properties in **Computer Management** > **Event Viewer** in Windows. To open the Security log, you need administrator rights.

© Acronis International GmbH, 2003-2026

Event parameters

The following table summarizes the parameters that you must specify when configuring the **On Windows Event Log event** option.

Parameter	Description
Log name	The name of the log. Select the name of a standard log (Application, Security, System) or specify another log name. For example, Microsoft Office Sessions.
Event source	The event source indicates the program or the system component that caused the event. For example, disk. Any event source that contains the specified text string will trigger the scheduled backup. This option is not case-sensitive. For example, if you specify `service`, both Service Control Manager and Time-Service event sources will trigger a backup.
Event type	Type of the event: Error, Warning, Information, Audit success, or Audit failure.
Event ID	The event ID identifies a particular kind of event within an event source. For example, an Error event with event source disk and event ID 7 occurs when Windows discovers a bad block on a disk, while an Error event with event source disk and event ID 15 occurs when a disk is not ready for access.

Example: Emergency backup in case of bad blocks on the hard disk

One or more bad blocks on a hard disk drive might indicate an imminent fail. That is why you might want to create a backup when a bad block is detected.

When Windows detects a bad block on the disk, an error event with the event source disk and event number 7 is recorded to the system log. In the protection plan, configure the following schedule:

- Schedule: On Windows Event log event
- Log name: System
- Event source: disk
- Event type: Error
- Event ID: 7

Important
To ensure that the backup completes despite the bad blocks, in **Backup options**, go to **Error handling**, and then select the **Ignore bad sectors** check box.

© Acronis International GmbH, 2003-2026

Start conditions

To make a backup run only if specific conditions are met, configure one or more start conditions. If you configure multiple conditions, all of them must be met simultaneously for the backup to start. You can specify a period after which the backups will run, regardless of whether the conditions are met. For more information about this backup option, see "Task start conditions" (p. 447).

Start conditions are not applicable when you start a backup manually.

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

Start condition	Backup source (What to back up)					
	Entire machine, Disks/volumes, or Files/folders (physical machines)	**Entire machines or Disk/volumes (virtual machines)**	**ESXi configuration**	**Microsoft 365 mailboxes**	**Exchange databases and mailboxes**	**SQL databases**
User is idle	Windows	N/A	N/A	N/A	N/A	N/A
The backup location's host is available	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Users logged off	Windows	N/A	N/A	N/A	N/A	N/A
Fits the time interval	Windows, Linux, macOS	Windows, Linux	N/A	N/A	N/A	N/A
Save battery power	Windows	N/A	N/A	N/A	N/A	N/A
Do not start when on metered connection	Windows	N/A	N/A	N/A	N/A	N/A
Do not start when connected to the following Wi-Fi	Windows	N/A	N/A	N/A	N/A	N/A

© Acronis International GmbH, 2003-2026

Start condition	Backup source (What to back up)					
	Entire machine, Disks/volumes, or Files/folders (physical machines)	Entire machines or Disk/volumes (virtual machines)	ESXi configuration	Microsoft 365 mailboxes	Exchange databases and mailboxes	SQL databases
networks						
Check device IP address	Windows	N/A	N/A	N/A	N/A	N/A

User is idle

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

Example

Run a backup every day at 09:00 PM, preferably when the user is idle. If the user is still active by 11:00 PM, run the backup anyway.

- Schedule: **Daily**, **Run every day**. Start at: **09:00 PM**.
- Condition: **User is idle**.
- Backup start conditions: **Wait until the conditions are met**, **Start the task anyway after 2** hours.

As a result:

- If the user is idle before 09:00 PM, the backup starts at 09:00 PM.
- If the user becomes idle between 09:00 PM and 11:00 PM, the backup starts immediately.
- If the user is still active at 11:00 PM, the backup starts at 11:00 PM.

The backup location's host is available

"The backup location's host is available" means that the machine that hosts the backup location is available over the network.

This condition is applicable to 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.

© Acronis International GmbH, 2003-2026

Example

You run backups to a network folder every workday at 09:00 PM. If the machine that hosts the folder is not available at that moment (for example, due to maintenance), you want to skip the backup and wait for the scheduled start on the next workday.

- Schedule: **Daily**, **Run Monday to Friday**. Start at: **09:00 PM**.
- Condition: **The backup location's host is available**.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

- If the host is available at 09:00 PM, the backup starts immediately.
- If the host is not available at 09:00 PM, the backup starts the next workday (if the host is available at 09:00 PM on this day).
- If the host is never available on workdays at 09:00 PM, the backup never starts.

Users logged off

Use this start condition to postpone a backup until all users log off from a Windows machine.

Example

You run a backup every Friday at 08:00 PM, preferably when all users are logged off. If one of the users is still logged in at 11:00 PM, run the backup anyway.

- Schedule: **Weekly**, on Fridays. Start at: **08:00 PM**.
- Condition: **Users logged off**.
- Backup start conditions: **Wait until the conditions are met**, **Start the backup anyway after 3** hours.

As a result:

- If all users are logged off at 08:00 PM, the backup starts at 08:00 PM.
- If the last user logs off between 08:00 PM and 11:00 PM, the backup starts immediately.
- If there are still logged-in users at 11:00 PM, the backup starts at 11:00 PM.

Fits the time interval

Use this start condition to restrict a backup start to a specified interval.

Example

A company backs up user data and servers to different locations on the same network-attached storage.

The workday starts at 08:00 AM and ends at 05:00 PM. User data should be backed up as soon as the users log off, but not earlier than 04:30 PM.

© Acronis International GmbH, 2003-2026

The company's servers are backed up every day at 11:00 PM. User data should preferably be backed up before 11:00 PM, in order to free network bandwidth for the server backups.

Backing up user data takes no more than one hour, so the latest backup start time is 10:00 PM. If a user is still logged in within the specified time interval, or logs off at any other time, the backup of the user data should be skipped.

- Event: **When a user logs off the system**. Specify the user account: **Any user**.
- Condition: **Fits the time interval** from **04:30 PM** to **10:00 PM**.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

- If the user logs off between 04:30 PM and 10:00 PM, the backup starts immediately.
- If the user logs off at any other time, the backup is skipped.

Save battery power

Use this start condition to prevent a backup if a machine (for example, a laptop or a tablet) is not connected to a power source. Depending on the value of the Backup start conditions option, the skipped backup will or will not start after the machine is connected to a power source.

The following options are available:

- **Do not start when on battery**
  A backup will start only if the machine is connected to a power source.
- **Start when on battery if the battery level is higher than**
  A backup will start if the machine is connected to a power source or if the battery level is higher than a specified value.

Example

You back up your data every workday at 09:00 PM. If your machine is not connected to a power source, you want to skip the backup to save the battery power and wait until you connect the machine to a power source.

- Schedule: **Daily**, **Run Monday to Friday**. Start at: **09:00 PM**.
- Condition: **Save battery power**, **Do not start when on battery**.
- Backup start conditions: **Wait until the conditions are met**.

As a result:

- If the machine is connected to a power source at 09:00 PM, the backup starts immediately.
- If the machine is running on battery power at 09:00 PM, the backup starts when you connect the machine to a power source.

Do not start when on metered connection

Use this start condition to prevent a backup (including a backup to a local disk) if the machine is connected to the Internet through a connection that is set as metered in Windows. For more

 © Acronis International GmbH, 2003-2026

information about metered connections in Windows, refer to https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

The additional start condition **Do not start when connected to the following Wi-Fi networks** is automatically enabled when you enable the **Do not start when on metered connection** condition. This is an additional measure to prevent backups over mobile hotspots. The following network names are specified by default: android, phone, mobile, and modem.

To remove these names from the list, click the X sign. To add a new name, type it in the empty field.

Example

You back up your data every workday at 09:00 PM. If the machine is connected to the Internet by using a metered connection, 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: **09:00 PM**.
- Condition: **Do not start when on metered connection**.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

- At 09:00 PM, if the machine is not connected to the Internet through a metered connection, the backup starts immediately.
- At 09:00 PM, if the machine is connected to the Internet through a metered connection, the backup starts on the next workday.
- If the machine is always connected to the Internet through a metered connection on workdays at 09:00 PM, the backup never starts.

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

Use this start condition to prevent a backup (including a backup to a local disk) if the machine is connected to any of the specified wireless networks (for example, if you want to restrict backups through a mobile phone hotspot).

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, not case-sensitive. For example, if you specify `phone` as the network name, the backup will not start when the machine is connected to any of the following networks: `John's iPhone`, `phone_wifi`, or `my_PHONE_wifi`.

The start condition **Do not start when connected to the following Wi-Fi** is automatically enabled 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.

To remove these names from the list, click the X sign. To add a new name, type it in the empty field.

Example

You back up your data every workday at 09:00 PM. If the machine is connected to the Internet through a mobile hotspot, you want to skip the backup and wait for the scheduled start on the next

 © Acronis International GmbH, 2003-2026

workday.

- Schedule: **Daily**, **Run Monday to Friday**. Start at: **09:00 PM**.
- 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:

- If the machine is not connected to the specified network at 09:00 PM, the backup starts immediately.
- If the machine is connected to the specified network at 09:00 PM, the backup starts the next workday.
- If the machine is always connected to the specified network on workdays at 09:00 PM, the backup never starts.

Check device IP address

Use this start condition to prevent a backup (including a backup to a local disk) if any of the machine IP addresses are within or outside of the specified IP address range. Thus, for example, you can avoid large data transit charges when backing up machines of users who are overseas, or you can prevent backups over a Virtual Private Network (VPN) connection.

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.

Example

You back up your data every workday at 09:00 PM. If the machine is connected to the corporate network by using a VPN tunnel, you want to skip the backup.

- Schedule: **Daily**, **Run Monday to Friday**. Start at **09:00 PM**.
- 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:

- If the machine IP address is not in the specified range at 09:00 PM, the backup starts immediately.
- If the machine IP address is in the specified range at 09:00 PM, the backup starts when the machine obtains a non-VPN IP address.
- If the machine IP address is always in the specified range on workdays at 09:00 PM, the backup never starts.

© Acronis International GmbH, 2003-2026

Additional scheduling options

You can configure the backups to run only if specific conditions are met, to run only during a specified period, or to run with a delay compared to the schedule.

To configure start conditions

1. In the protection plan, expand the **Backup** module.
2. Click **Schedule**.
3. On the **Schedule** pane, click **Show more**.
4. Select the check boxes next to the start conditions that you want to include, and then click **Done**.
   For more information about the available start conditions and how to configure them, see "Start conditions" (p. 373).
5. Save the protection plan.

To configure a time range

1. In the protection plan, expand the **Backup** module.
2. Click **Schedule**.
3. Select the **Run the plan within a date range** check box.
4. Specify the period according to your needs, and then click **Done**.
5. Save the protection plan.

As a result, the backups will run only during the specified period.

To configure a delay

To avoid excessive network load when you back up multiple workloads to a network location, you can configure a small random delay as a backup option. In cloud deployments, this option is enabled by default, and the maximum delay is set to 30 minutes.

1. In the protection plan, expand the **Backup** module.
2. Click **Backup options**, and then select **Scheduling**.
   The delay value for each workload is selected randomly between zero and the maximum value you specify. By default, the maximum value is 30 minutes.
   For more information about this backup option, see "Scheduling" (p. 441).
   The delay value for each workload is calculated when you apply the protection plan to that workload, and remains the same until you edit the maximum delay value.
3. Specify the period according to your needs, and then click **Done**.
4. Save the protection plan.

Running a backup manually

You can manually run scheduled and unscheduled backups.

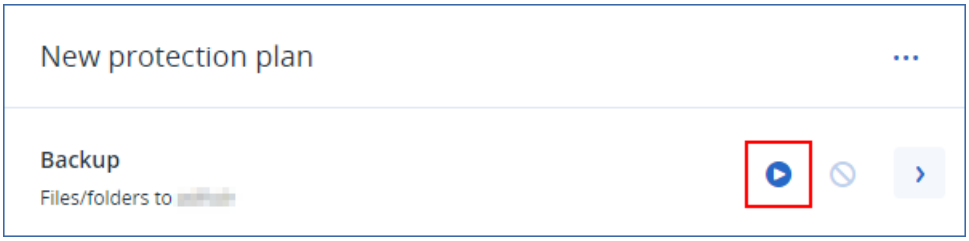
To run a backup manually

 © Acronis International GmbH, 2003-2026

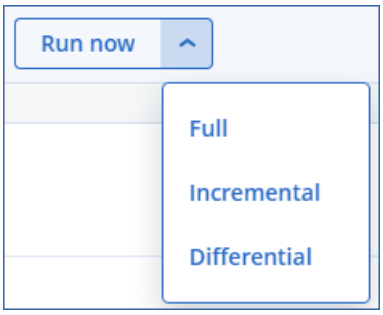
1. In the Cyber Protect console, go to **Devices**.
2. Select the workload for which you want to run a backup, and then click **Protect**.
3. Select the protection plan that you want to create the backup.

   If no protection plan is applied to the workload, apply an existing plan or create a new one.

   For more information about how to create a protection plan, see "Creating a protection plan" (p. 243).
4. [To create the default type of backup] In the protection plan, click the **Run now** icon.

   Alternatively, in the protection plan, expand the **Backup** module, and then click the **Run now** button.
5. [To create a specific type of backup] In the protection plan, expand the **Backup** module, click the arrow next to the **Run now** button, and then select the backup type.

   Note
   Selecting the type is not available for backup schemes that use only one backup method, for example, **Always incremental (single-file)** or **Always full**.

As a result, the backup operation starts. You can check its progress and its result on the **Devices** tab, in the **Status** column.

Retention rules

To delete older backups automatically, configure the backup retention rules in the protection plan.

You can base the retention rules on any of the following backup properties:

- Number
- Age
- Size

© Acronis International GmbH, 2003-2026

The available retention rules and their options depend on the backup scheme. The rules are also relevant to agents, workloads, and cloud to cloud backups. For more information, see "Retention rules according to the backup scheme" (p. 382).

Depending on the configuration of the protection plan, retention rules are applied to an archive before or after a backup.

You can disable the automatic cleanup of older backups, by selecting the **Keeping backups infinitely** option while configuring the retention rules. This might result in increased storage usage, and you have to delete the unnecessary old backups manually.

Important tips

- Retention rules are part of the protection plan. If you revoke or delete a plan, the retention rules in that plan will no longer be applied. For more information about how to delete the backups that you no longer need, see "Deleting backups" (p. 456).
- You can configure a retention rule to run either before or after the backup operation, which results in a different number or size of the retained backups.

  For example, in **How many to keep** > **By number of backups**, you select 2. The following table compares the results of applying the retention rules before or after the backup.

Before backup	After backup
◦ A cleanup operation runs. Two backups are kept. ◦ A backup operation runs. A new backup is created. Result: Three backups are available.	◦ A backup operation runs. A new backup is created. ◦ A cleanup operation runs. Two backups are kept. Result: Two backups are available.

- If, according to the backup scheme and backup format, each backup is stored as a separate file, you cannot delete a backup on which other incremental or differential backups depend. This backup will be deleted according to the retention rules applied to the dependent backups. This configuration may result in increased storage usage because the deletion of some backups is postponed. Also, the backup age, number, or size of backups may exceed the values that you specified. For more information about how to change this behavior, see "Backup consolidation" (p. 403).
- Backups that are stored on a tape are deleted only when the tape is overwritten.
- By default, the newest backup that a protection plan creates is never deleted. However, if you configure a retention rule to clean up the backups before starting a new backup operation, and set the number of backups to keep to zero, the newest backup will also be deleted.

  Warning!
  If you apply this retention rule to a backup set with a single backup, and the backup operation fails, you will not be able to recover your data, because the existing backup will be deleted before a new one is created.

© Acronis International GmbH, 2003-2026

Retention rules according to the backup scheme

The available retention rules and their settings depend on the backup scheme that you use in the protection plan. For more information about the backup schemes, see "Backup schemes" (p. 364).

The following table summarizes the available retention rules and their settings.

Backup scheme	Schedule	Available retention rules and settings
Always incremental (single-file)	Monthly Weekly Daily Hourly Event-triggered backups	By number of backups By backup age (separate settings for monthly, weekly, daily, and hourly backups) Keep backups indefinitely
Always full	Monthly Weekly Daily Hourly Event-triggered backups	By number of backups By backup age (separate settings for monthly, weekly, daily, and hourly backups) By total size of backups Keep backups indefinitely
Weekly full, Daily incremental	Daily Event-triggered backups	By number of backups By backup age (separate settings for weekly and daily backups) By total size of backups Keep backups indefinitely
Monthly full, Weekly differential, daily incremental	Monthly Weekly Daily Hourly Event-triggered backups	By number of backups By backup age (separate settings for full, differential, and incremental backups) By total size of backups Keep backups indefinitely
Custom	Monthly Weekly Daily Hourly Event-triggered backups	By number of backups By backup age (separate settings for full, differential, and incremental backups) By total size of backups Keep backups indefinitely

© Acronis International GmbH, 2003-2026

Why are there monthly backups with an hourly scheme?

Depending on the backup scheme, you can configure the **By backup age** option for one the following backups:

- Monthly, weekly, daily, and hourly backups.

  These setting are available with all non-custom backup schemes, and are based on time. All these backups (monthly, weekly, daily, and hourly) are available, even if you configure your backups to run hourly. See the example below.

Backup	Description
Monthly	A monthly backup is the first backup each month.
Weekly	A weekly backup is the first backup on the day of the week that you specify in the Weekly backup option. This day is considered as the beginning of the week in terms of retention rules. If a weekly backup is also the first backup of the month, it is considered a monthly backup. In this case, a weekly backup is created on the selected day the following week.
Daily	A daily backup is the first backup of the day, unless this backup falls within the definition of a monthly or weekly backup. In this case, a daily backup is created the following day.
Hourly	An hourly backup is the first backup of the hour, unless this backup falls within the definition of a monthly, weekly, or daily backup. In this case, an hourly backup is created the next hour.

- Full, differential, and incremental backups.

  These setting are available for the **Custom** backup scheme, and are based on the backup method. The **Monthly full, Weekly differential, Daily incremental** is a pre-configured custom scheme.

Example

You use the **Always incremental (single-file)** backup scheme with the default setting for hourly backups:

- Scheduled by time.
- Backups run hourly: Monday to Friday, every 1 hour, from 08:00 AM to 06:00 PM.
- The **Weekly backup** option is set to Monday.

In the **How long to keep** section of the protection plan, you can apply retention rules to monthly, weekly, daily, and hourly backups.

The following table summarizes the backup types that are created during an 8-day period.

© Acronis International GmbH, 2003-2026

Date	Day of week	Description
July 1	Monday	The first backup each month is monthly, so the first backup today is a monthly backup. The other backups during the day are hourly. This week, the first backup is considered a monthly backup. That is why there is no weekly backup. The first backup next week will be a weekly backup.
July 2	Tuesday	The first backup is daily, the other backups during the day are hourly.
July 3	Wednesday	The first backup is daily, the other backups during the day are hourly.
July 4	Thursday	The first backup is daily, the other backups during the day are hourly.
July 5	Friday	The first backup is daily, the other backups during the day are hourly.
July 6	Saturday	The first backup is daily, the other backups during the day are hourly.
July 7	Sunday	The first backup is daily, the other backups during the day are hourly.
July 8	Monday	The first backup is weekly, the other backups during the day are hourly.

Configuring retention rules

The retention rules are part of the protection plan, and their availability and options depend on the backup scheme. For more information, see "Retention rules according to the backup scheme" (p. 382).

To configure the retention rules

1. In the protection plan, expand the **Backup** module.
2. Click **How many to keep**.
3. Select one of the following options:
   - **By number of backups**
   - **By backup age**

     Separate settings for monthly, weekly, daily, and hourly backups are available. The maximum value for all types is 9999.

     You can also use a single setting for all backups.
   - **By total size of backups**

 © Acronis International GmbH, 2003-2026

This setting is not available with the **Always incremental (single-file)** backup scheme.

- **Keep backups indefinitely**

4. [If you did not select **Keep backups indefinitely**] Configure the values for the selected option.
5. [If you did not select **Keep backups indefinitely**] Select when the retention rules are applied:
   - After backup
   - Before backup

     This option is not available when backing up Microsoft SQL Server clusters or Microsoft Exchange Server clusters.
6. Click **Done**.
7. Save the protection plan.

Encryption

Cyber Protect uses two levels of security to protect backed-up data from unauthorized access.

Backed-up data is encrypted with a 256-bit key, which is in turn encrypted by using the SHA-2 (256-bit) hash of a user-provided encryption password as a key, as follows:

1. When creating a protection plan with encryption enabled, the user specifies an encryption password.

   Warning!
   Cyber Protect does not store this password. Recovering a lost password is not possible.

2. Password-Based Key Derivation Function 2 (PBKDF2) is applied to the user-provided encryption password 1,048,576 times (2 to the power of 20). As a result, a SHA-2 (256-bit) hash is created. This is the first key, which is used to encrypt the second key.
3. A random 256-bit key is created by using OpenSSL. This is the second key, which is used to encrypt the backed-up data.
4. The second key is encrypted by using Advanced Encryption Standard (AES-256), and the hash that is derived from the user-provided encryption password.
5. The encrypted second key is added to the backup archive.
6. Backed-up data is encrypted by using Advanced Encryption Standard with the Galois/Counter Mode (AES-256 GCM) and the second key.
7. When recovering data, the user must provide the encryption password. The hash of that password is the first encryption key. This key is used to decrypt the second key. With the second key, the backup archive can be decrypted and recovered.

Note
Using the AES-256 algorithm with a strong password provides quantum-resistant encryption. It is safe against cryptanalytic attacks that rely on quantum computing.

We recommend that you encrypt all backups that are stored in the cloud storage, especially if your company is subject to regulatory compliance.

© Acronis International GmbH, 2003-2026

You can configure encryption in the following ways:

- In the protection plan
- As a machine property, by using the Cyber Protect Monitor or the command-line interface

Configuring encryption in the protection plan

In a protection plan, encryption is enabled by default.

To configure encryption in a plan

1. In a protection plan, expand the **Backup** module.
2. In the **Encryption** row, click **Specify password**.
3. Specify and confirm the encryption password.
4. Click **OK**.

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

You cannot change the encryption settings after you apply the protection plan. To use different encryption settings, create a new plan.

Configuring encryption as a machine property

You can configure backup encryption as a machine property. In this case, backup encryption is not configured in the protection plan, but on the protected workload. Encryption as a machine property uses the AES algorithm with a 256-bit key (AES-256).

Note
Using the AES-256 algorithm with a strong password provides quantum-resistant encryption. It is safe against cryptanalytic attacks that rely on quantum computing.

Configuring encryption as a machine property 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 the machine will override the encryption settings in the protection plan. Any backup will be encrypted, even if encryption is disabled in the Backup module settings.

If you have more than one Agent for VMware connected to the same vCenter Server, and you configure encryption as a machine property, you must use the same encryption password on all machines with Agent for VMware, because of the load balancing between the agents.

You can configure encryption as a machine property in the following ways:

- On the command line
- In Cyber Protect Monitor (Available for Windows and macOS)

© Acronis International GmbH, 2003-2026

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

To configure encryption as a machine property

On the command line

1. Log in as an administrator in Windows or the root user in Linux.
2. Navigate to the **acropsh** tool, as follows:
   - For Windows:

     ```
     <installation_path>\PyShell\bin\
     ```

     where `<installation_path>` is `%ProgramFiles%\Acronis` for the on-premises deployment and `%ProgramFiles%\BackupClient` for the cloud deployment.
   - For Linux:

     ```
     /usr/sbin/
     ```

   - For a virtual appliance:

     ```
      /./sbin/
     ```

3. Run the following command:
   - For Windows

     ```
     acropsh.exe -m manage_creds --set-password <password>
     ```

   - For Linux and virtual appliance

     ```
     acropsh -m manage_creds --set-password <password>
     ```

   where `<password>` is your encryption password.

In Cyber Protect Monitor

1. Log in as an administrator.
2. Click the Cyber Protect Monitor icon in the notification area (in Windows) or the menu bar (in macOS).
3. Click the gear icon, and then click **Settings** > **Encryption**.
4. Select **Set a password for this machine**. Specify and confirm the encryption password.
5. Click **Save**.

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

To reset the encryption settings

© Acronis International GmbH, 2003-2026

1. Log in as an administrator in Windows or root user in Linux.
2. Navigate to the **acropsh** tool, as follows:
   - For Windows:

     ```
     <installation_path>\PyShell\bin\
     ```

     Where `<installation_path>` is `%ProgramFiles%\Acronis` for the on-premises deployment and `%ProgramFiles%\BackupClient` for the cloud deployment.
   - For Linux:

     ```
     /usr/sbin/
     ```

   - For a virtual appliance:

     ```
     /./sbin/
     ```

3. Run the following command:
   - For Windows

     ```
     acropsh.exe -m manage_creds --reset
     ```

   - For Linux and virtual appliance

     ```
     acropsh -m manage_creds --reset
     ```

   Important
   If you reset the encryption as a machine property or change the encryption password after a protection plan creates a backup, the next backup operation will fail. To continue backing up the workload, create a new protection plan.

Conversion to a virtual machine

Note
This feature is available with an Advanced license.

You can create a virtual machine from a disk-level backup that includes an operating system. Thus, you can quickly start a pre-created standby machine or perform cross-platform recovery. For example, you can recover a backup of a physical or virtual machine to a different hypervisor.

A protection agent that has access to the backup archive performs the conversion. For more information about the available options, see "Types of conversion to virtual machine" (p. 390).

Conversion plans

You can schedule conversions and incrementally apply backed-up changes to the resulting virtual machine.

 © Acronis International GmbH, 2003-2026

- "Conversion to a virtual machine with a separate conversion plan" (p. 394) – you specify a conversion schedule independently of the backup schedule.
- "Conversion to a virtual machine with the protection plan" (p. 391) – the conversion is performed automatically after each backup or replication.

Alternative options

The following options do not support scheduling or incremental updates.

- "Recovering a physical machine as a virtual machine" (p. 511) – a one-time conversion in which you select disks and adjust the settings for each virtual disk.

  Use this method when you want to perform the conversion once or occasionally, for example, for cross-platform recovery.
- "Running a virtual machine from a backup (Instant Restore)" (p. 468) – starts a temporary virtual machine directly from a backup without a full conversion.

  Unlike a converted machine, the resulting virtual machine uses resources only while it is running, and datastore space is required only for storing changes to the virtual disks. The host does not access the virtual disks directly – instead, it communicates with the agent, which reads data from the backup. As a result, performance is lower than that of a converted machine. For more information, see "Running a virtual machine from a backup (Instant Restore)" (p. 468).

Limitations

- 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.
- Backups that are stored on NFS or on an SFTP server cannot be converted in a separate conversion plan.
- Backups that are stored in Secure Zone can be converted only by the agent that is running on the same machine.
- Backups can be converted to a Scale Computing HC3 virtual machine only in a separate conversion plan.
- If the backup contains Linux logical volumes (LVM), you must create it by using Agent for VMware, Agent for Hyper-V, Agent for Scale Computing HC3, or Agent for Proxmox. Converted machines must match the platform of the original machine (VMware ESXi, Hyper-V, Scale Computing HC3, or Proxmox VE). 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 it is started on a host with a different CPU type, the guest system displays a driver error. Update this driver manually.
- With Proxmox, conversion to a virtual machine is also supported on storages that do not provide snapshot capabilities. In such cases, incremental updates of the resulting virtual machine are not

 © Acronis International GmbH, 2003-2026

possible. For more details about the storage types that are supported by Proxmox, see https://pve.proxmox.com/pve-docs/chapter-pvesm.html.

Types of conversion to virtual machine

When you convert a backup to a virtual machine, you can choose one of the following conversion types:

- Save the resulting virtual machine as a set of files

  With this option, the conversion process creates one or more virtual disk files without requiring access to a hypervisor. You can save the files to a local or network folder and, later, manually use them on a hypervisor.

  The resulting files depend on the selected type, as follows:

  - **VMware Workstation** creates VMDK files
  - **VHDX files** creates VHDX and VMX files

  The following table shows which agents you can use to create a virtual machine as a set of files.

Conversion to a virtual machine (as a set of files)	Agent that performs conversion			
	Agent for VMware	Agent for Hyper-V	Agent for Windows	Agent for Linux
VMware Workstation	+	+	+	+
VHDX files	+	+	+	+

  With this conversion type, each conversion recreates the virtual machine from scratch.

  Note
  Even though Locally Attached Storage (LAS) connected to Agent for VMware (Virtual Appliance) might appear as a target for VM files (.vhdx/.vmdk), this scenario is not supported.

  Cyber Protect temporarily renames the existing machine, and then creates a new virtual machine with the original name. If conversion is successful, the old machine is deleted. If conversion fails, the old machine is restored. Additional temporary storage is required, because both an old and a new machines exist during processing.

- Create the resulting virtual machine directly on a virtualization server

  With this option, the conversion process creates a virtual machine directly on the selected virtualization server. Unlike conversion as a set of files, this method supports incremental updates.

  During the first conversion, Cyber Protect creates a new virtual machine.

  For subsequent conversions:

  - If no full backup has occurred since the last conversion, an incremental update is performed, and only changed data are transferred to the virtual machine. Incremental updates are faster and reduce network and CPU usage on the host that is used for this conversion.

© Acronis International GmbH, 2003-2026

- If a full backup has occurred, or if an incremental update is not possible (for example, due to missing intermediate snapshots), the virtual machine is created from scratch.

This approach avoids temporary duplication of full virtual machines, and minimizes processing overhead when incremental updates are available.

The following table shows which agents you can use to create a virtual machine on a specific type of virtualization server.

Conversion to a virtual machine	Agent that performs conversion			
	Agent for VMware	Agent for Hyper-V	Agent for Scale Computing HC3	Agent for Proxmox
VMware ESXi	+	–	–	–
Microsoft Hyper-V	–	+	–	–
Scale Computing HC3	–	–	+	–
Proxmox	–	–	–	+

Intermediate snapshots

To enable incremental updates of the resulting virtual machine, Cyber Protect stores an intermediate snapshot named **Replica**. This snapshot captures the state of the virtual machine after the most recent successful conversion. You can revert the virtual machine to this snapshot if you want to discard any subsequent changes, and return to the last converted state.

For conversions to Scale Computing HC3 virtual machines, an additional snapshot named **Utility Snapshot** is created. This snapshot is used only by Cyber Protect and must remain intact to ensure proper operation.

Conversion to a virtual machine with the protection plan

You can add conversion to a virtual machine as part of a protection plan. In this case, the conversion is performed automatically after each backup (if configured for the primary location) or after each replication (if configured for the second and further locations).

For information about the available conversion types and limitations, see "Types of conversion to virtual machine" (p. 390).

To configure conversion to a virtual machine with the protection plan

VMware ESXi

1. Create or edit a protection plan that has a backup module.
2. In the protection plan, find the backup destination from which you want to convert backups.
3. Under this destination, click **Convert to VM**.
4. Enable the **Conversion** switch.
5. In **Convert to**, select **VMware ESXi**.

 © Acronis International GmbH, 2003-2026

6. In **Host**, select the target host, specify the virtual machine name, and then click **OK**.
7. [Optional] In **Agent**, select the agent that will perform the conversion.
   By default, the conversion is performed by the agent that creates the backup. If you select a different agent, ensure that it can access the backup location (for example, a network folder).
8. In **Datastore**, select the storage for the virtual machine.
9. In **Provisioning mode**, select the disk provisioning mode.
10. In **VM settings**, change the memory size, the number of processors, or the network connections of the virtual machine, and then click **OK**.
11. Click **Done**.

Microsoft Hyper-V

1. Create or edit a protection plan that has a backup module.
2. In the protection plan, find the backup destination from which you want to convert backups.
3. Under this destination, click **Convert to VM**.
4. Enable the **Conversion** switch.
5. In **Convert to**, select **Microsoft Hyper-V**.
6. In **Host**, select the target host, specify the virtual machine name, and then click **OK**.
7. [Optional] In **Agent**, select the agent that will perform the conversion.
   By default, the conversion is performed by the agent that creates the backup. If you select a different agent, ensure that it can access the backup location (for example, a network folder).
8. In **Path**, select the storage for the virtual machine.
9. In **Provisioning mode**, select the disk provisioning mode.
10. In **VM settings**, change the memory size, the number of processors, or the network connections of the virtual machine, and then click **OK**.
11. Click **Done**.

Scale Computing HC3

1. Create or edit a protection plan that has a backup module.
2. In the protection plan, find the backup destination from which you want to convert backups.
3. Under this destination, click **Convert to VM**.
4. Enable the **Conversion** switch.
5. In **Convert to**, select **Scale Computing HC3**.
6. In **Host**, select the target host, specify the virtual machine name, and then click **OK**.
7. [Optional] In **Agent**, select the agent that will perform the conversion.
   By default, the conversion is performed by the agent that creates the backup. If you select a different agent, ensure that it can access the backup location (for example, a network folder).
8. In **VM settings**, change the memory size, the number of processors, or the network connections of the virtual machine, and then click **OK**.
9. Click **Done**.

Proxmox VE

© Acronis International GmbH, 2003-2026

1. Create or edit a protection plan that has a backup module.
2. In the protection plan, find the backup destination from which you want to convert backups.
3. Under this destination, click **Convert to VM**.
4. Enable the **Conversion** switch.
5. In **Convert to**, select **Proxmox VE**.
6. In **Host**, select the target host, specify the virtual machine name, and then click **OK**.
7. [Optional] In **Agent**, select the agent that will perform the conversion.

   By default, the conversion is performed by the agent that creates the backup. If you select a different agent, ensure that it can access the backup location (for example, a network folder).
8. In **Datastore**, select the storage for the virtual machine.
9. In **Provisioning mode**, select the disk provisioning mode.
10. In **VM settings**, change the memory size, the number of processors, or the network connections of the virtual machine, and then click **OK**.
11. Click **Done**.

VMware Workstation

1. Create or edit a protection plan that has a backup module.
2. In the protection plan, find the backup destination from which you want to convert backups.
3. Under this destination, click **Convert to VM**.
4. Enable the **Conversion** switch.
5. In **Convert to**, select **VMware Workstation**.
6. In **Path**, specify where to save the virtual machine files and the file name, and then click **Done**.

   Note
   Each conversion overwrites the VMDK files in the target location.

7. [Optional] In **Agent**, select the agent that will perform the conversion.

   By default, the conversion is performed by the agent that creates the backup. If you select a different agent, ensure that it can access the backup location (for example, a network folder).
8. Click **Done**.

VHDX files

1. Create or edit a protection plan that has a backup module.
2. In the protection plan, find the backup destination from which you want to convert backups.
3. Under this destination, click **Convert to VM**.
4. Enable the **Conversion** switch.
5. In **Convert to**, select **VHDX files**.
6. In **Path**, specify where to save the virtual machine files and the file name, and then click **Done**.

   Note
   Each conversion overwrites the VHDX and VMX files in the target location.

© Acronis International GmbH, 2003-2026

7. [Optional] In **Agent**, select the agent that will perform the conversion.
   By default, the conversion is performed by the agent that creates the backup. If you select a different agent, ensure that it can access the backup location (for example, a network folder).
8. Click **Done**.

Conversion to a virtual machine with a separate conversion plan

To convert a disk-level backup to a virtual machine, you must create a conversion plan.

You can use this plan to migrate a virtual machine to a non-original hypervisor. For example, you can convert a backup of a VMware virtual machine to a Proxmox virtual machine.

Also, with a conversion plan, you can update the resulting virtual machine after each incremental or differential backup.

Note
Incremental updates are not available for virtual machines that are created by **VMware Workstation** and **VHDX files** options. For more information, see "Types of conversion to virtual machine" (p. 390).

To create a conversion plan

VMware ESXi

1. In the Cyber Protect console, go to **Management** > **Conversion to VM**.
2. Click **Create plan**.
3. [Optional] To rename the plan, click the pencil icon, enter a new name, and then click **OK**.
4. In **Convert to**, select **VMware ESXi**.
5. In **Host**, select the target host, specify the virtual machine name, and then click **OK**.
6. In **Agent**, select the agent that will perform the conversion.
7. In **Items to convert**, select one or more backups to convert, and then click **Done**.
   To switch between selecting individual backups and backup locations, click **Locations** / **Backups**.
   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. [If prompted] Specify the credentials to access the backup location, and then click **OK**.
9. In **Datastore**, select the storage for the virtual machine.
10. In **Provisioning mode**, select the disk provisioning mode.
11. In **VM settings**, change the memory size, the number of processors, or the network connections of the virtual machine, and then click **OK**.
12. [Optional] In **Schedule**, change the plan schedule, and then click **OK**.
13. [If the selected backups are encrypted] Turn on the **Backup password** switch, provide the encryption password, and then click **OK**.
14. [Optional] To change error handling, performance, pre-post commands or task failure handling,

 © Acronis International GmbH, 2003-2026

click the gear icon, update the settings, and then click **Done**.

15. Click **Create**.

Microsoft Hyper-V

1. In the Cyber Protect console, go to **Management** > **Conversion to VM**.
2. Click **Create plan**.
3. [Optional] To rename the plan, click the pencil icon, enter a new name, and then click **OK**.
4. In **Convert to**, select **Microsoft Hyper-V**.
5. In **Host**, select the target host, specify the virtual machine name, and then click **OK**.
6. In **Agent**, select the agent that will perform the conversion.
7. In **Items to convert**, select one or more backups to convert, and then click **Done**.

   To switch between selecting individual backups and backup locations, click **Locations** / **Backups**.

   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. In **Path**, select the storage for the virtual machine.
9. In **Provisioning mode**, select the disk provisioning mode.
10. [Optional] In **VM settings**, change the memory size, the number of processors, or the network connections of the virtual machine, and then click **OK**.
11. [Optional] In **Schedule**, change the plan schedule, and then click **OK**.
12. [If the selected backups are encrypted] Turn on the **Backup password** switch, provide the encryption password, and then click **OK**.
13. [Optional] To change error handling, performance, pre-post commands or task failure handling, click the gear icon, update the settings, and then click **Done**.
14. Click **Create**.

Scale Computing HC3

Note
Virtual machines that are replicated via the native Scale Computing VM replication functionality cannot be backed up.

1. In the Cyber Protect console, go to **Management** > **Conversion to VM**.
2. Click **Create plan**.
3. [Optional] To rename the plan, click the pencil icon, enter a new name, and then click **OK**.
4. In **Convert to**, select **Scale Computing HC3**.
5. In **Host**, select the target host, specify the virtual machine name, and then click **OK**.
6. In **Agent**, select the agent that will perform the conversion.
7. In **Items to convert**, select one or more backups to convert, and then click **Done**.

   To switch between selecting individual backups and backup locations, click **Locations** / **Backups**.

   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.

© Acronis International GmbH, 2003-2026

8. [Optional] In **VM settings**, change the memory size, the number of processors, or the network connections of the virtual machine, and then click **OK**.
9. [Optional] In **Schedule**, change the plan schedule, and then click **OK**.
10. [If the selected backups are encrypted] Turn on the **Backup password** switch, provide the encryption password, and then click **OK**.
11. [Optional] To change error handling, performance, pre-post commands or task failure handling, click the gear icon, update the settings, and then click **Done**.
12. Click **Create**.

Proxmox VE

1. In the Cyber Protect console, go to **Management** > **Conversion to VM**.
2. Click **Create plan**.
3. [Optional] To rename the plan, click the pencil icon, enter a new name, and then click **OK**.
4. In **Convert to**, select **Proxmox VE**.
5. In **Host**, select the target host, specify the virtual machine name, and then click **OK**.
6. In **Agent**, select the agent that will perform the conversion.
7. In **Items to convert**, select one or more backups to convert, and then click **Done**.

   To switch between selecting individual backups and backup locations, click **Locations** / **Backups**.

   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. [If prompted] Specify the credentials to access the backup location, and then click **OK**.
9. In **Datastore**, select the storage for the virtual machine.

   Note
   Conversion to a virtual machine is also supported on storages that do not provide snapshot capabilities. In such cases, incremental updates of the resulting virtual machine are not possible. For more details about the storage types that are supported by Proxmox, see https://pve.proxmox.com/pve-docs/chapter-pvesm.html.

10. In **Provisioning mode**, select the disk provisioning mode.
11. [Optional] In **VM settings**, change the memory size, the number of processors, or the network connections of the virtual machine, and then click **OK**.
12. [Optional] In **Schedule**, change the plan schedule, and then click **OK**.
13. [If the selected backups are encrypted] Turn on the **Backup password** switch, provide the encryption password, and then click **OK**.
14. [Optional] To change error handling, performance, pre-post commands or task failure handling, click the gear icon, update the settings, and then click **Done**.
15. Click **Create**.

VMware Workstation

1. In the Cyber Protect console, go to **Management** > **Conversion to VM**.
2. Click **Create plan**.

© Acronis International GmbH, 2003-2026

3. [Optional] To rename the plan, click the pencil icon, enter a new name, and then click **OK**.
4. In **Convert to**, select **VMware Workstation**.
5. In **Agent**, select the agent that will perform the conversion.
6. In **Items to convert**, select one or more backups to convert, and then click **Done**.

   To switch between selecting individual backups and backup locations, click **Locations** / **Backups**.

   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.
7. [If prompted] Specify the credentials to access the backup location, and then click **OK**.
8. In **Path**, select a location for virtual machine files, and then click **Done**.

   Note
   Each conversion overwrites the VMDK files in the target location.

9. [Optional] In **Schedule**, change the plan schedule, and then click **OK**.
10. [If the selected backups are encrypted] Turn on the **Backup password** switch, provide the encryption password, and then click **OK**.
11. [Optional] To change error handling, performance, pre-post commands or task failure handling, click the gear icon, update the settings, and then click **Done**.
12. Click **Create**.

VHDX files

1. In the Cyber Protect console, go to **Management** > **Conversion to VM**.
2. Click **Create plan**.
3. [Optional] To rename the plan, click the pencil icon, enter a new name, and then click **OK**.
4. In **Convert to**, select **VHDX files**.
5. In **Agent**, select the agent that will perform the conversion.
6. In **Items to convert**, select one or more backups to convert, and then click **Done**.

   To switch between selecting individual backups and backup locations, click **Locations** / **Backups**.

   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.
7. [If prompted] Specify the credentials to access the backup location, and then click **OK**.
8. In **Path**, select a location for virtual machine files, and then click **Done**.

   Note
   Each conversion overwrites the VHDX and VMX files in the target location.

9. [Optional] In **Schedule**, change the plan schedule, and then click **OK**.
10. [If the selected backups are encrypted] Turn on the **Backup password** switch, provide the encryption password, and then click **OK**.
11. [Optional] To change error handling, performance, pre-post commands or task failure handling, click the gear icon, update the settings, and then click **Done**.
12. Click **Create**.

© Acronis International GmbH, 2003-2026

Replication

With replication, each new backup is automatically copied to a replication location. The backups in the replication location do not depend on the backups in the source location, and vice versa.

Only the last backup in the source location is replicated. However, if earlier backups are not replicated (for example, due to a network connection problem), the replication operation will include all backups that are created after the last successful replication.

If a replication operation is interrupted, the processed data will be used by the next replication operation.

Note
This topic describes replication as a part of a protection plan. You can also create a separate backup replication plan. For more information, see "Backup replication" (p. 464).

Usage examples

- Ensuring reliable recovery
  Store your backups both on-site (for immediate recovery) and off-site (to guarantee that the backups stay safe even in case of storage failure or a natural disaster that affects the primary location).
- 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
  Configure retention rules to delete the older backups from a fast storage, in order to save on storage costs.

Supported locations

Location	As source location	As replication location
Local folder	+	+
Network folder	+	+
Cloud storage	-*	+
Secure Zone	+	+
SFTP server	+	+
Locations managed by a storage node	+	+
Tape device	-	+

To enable replication

 © Acronis International GmbH, 2003-2026

1. In a protection plan, expand the **Backup** module, and then click **Add location**.

   Note
   The **Add location** option is not available when you select the cloud storage or a tape device in **Where to back up**.

2. From the list of available locations, select the replication location.

   The location appears in the protection plan as **2nd location**, **3rd location**, **4th location**, or **5th location**, depending on the number of locations you added for replication.
3. [Optional] Click the gear icon to configure the options for the replication location.
   - **Performance and backup window** – set the backup window for the selected location, as described in "Performance and backup window" (p. 432). These settings define the replication performance.
   - **Remove location** – delete the currently selected replication location.
4. [Optional] In the **How many to keep** row under the replication location, configure the retention rules for that location, as described in "Retention rules" (p. 380).
5. [Optional] Repeat steps 1 – 4 to add more replication locations.

   You can configure up to four replication locations (**2nd location**, **3rd location**, **4th location**, and **5th location**). If you select **Cloud storage**, you cannot add more replication locations.

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 the this dependency, use a separate plan for backup replication. For more information about this specific plan, see "Backup replication" (p. 464).

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, see "Off-host data protection plans" (p. 462).

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.

© Acronis International GmbH, 2003-2026

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.

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**

© Acronis International GmbH, 2003-2026

	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	-	-	-	-	-	-	+	+	+	-

© Acronis International GmbH, 2003-2026

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	+	+	+	+	+	+	+	+	+	+
Pre/Post commands	+	+	+	+	+	+	+	+	+	+
Pre/Post data capture commands	+	+	+	+	+	+	+	-	-	+
Scheduling										
Distribute start times within a time window	+	+	+	+	+	+	+	+	+	+
Limit the number of simultaneously running backups	-	-	-	-	-	-	+	+	+	-

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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
Version 11 backup format	One TIB file and one XML metadata file	Multiple TIB files and one XML metadata file (traditional format)
Version 12 backup format	One TIBX file per backup chain (a full or differential backup, and all incremental backups that depend on it)	

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

© Acronis International GmbH, 2003-2026

Default backup file name

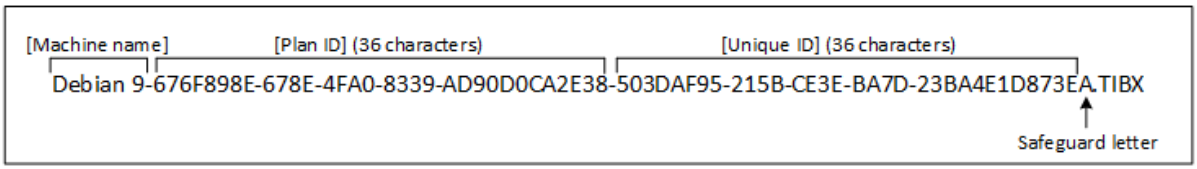
The default backup file name is `[Machine Name]-[Plan ID]-[Unique ID]A`.

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

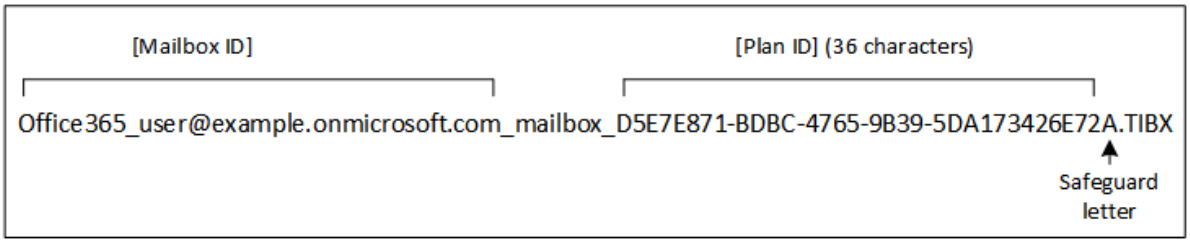
The name consists of the following variables:

- `[Machine Name]` This variable is replaced with the name of the machine (the same name that is shown in the Cyber Protect 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:

© Acronis International GmbH, 2003-2026

```
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

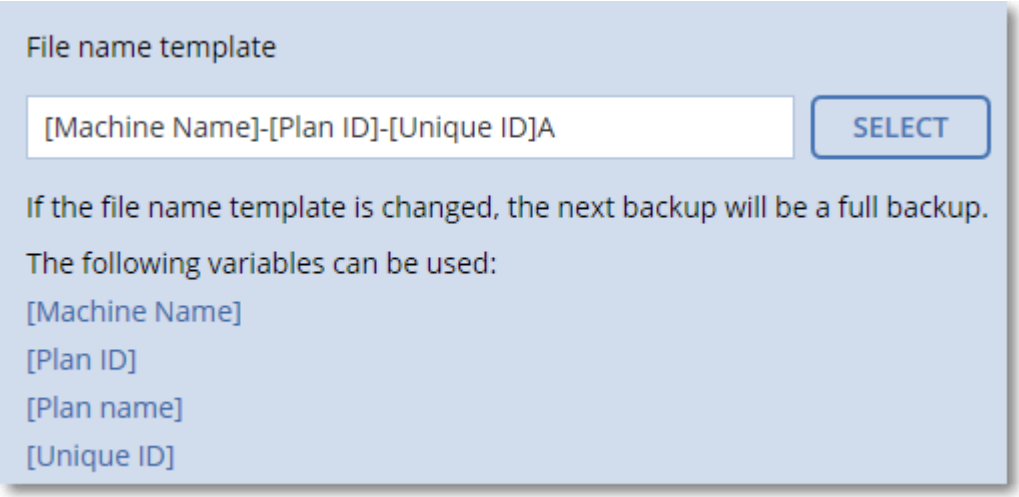
- **View user-friendly file names**

  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 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.

© Acronis International GmbH, 2003-2026



- **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.

 © Acronis International GmbH, 2003-2026

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**
Version 11 backup format	One TIB file and one XML metadata file	Multiple TIB files and one XML metadata file (traditional format)
Version 12 backup format	One TIBX file per backup chain (a full or differential backup, and all incremental backups that depend on it)	

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:

© Acronis International GmbH, 2003-2026

- 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.

© Acronis International GmbH, 2003-2026

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, see "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, see "Protecting Database Availability Groups (DAG)".

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

 © Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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:

© Acronis International GmbH, 2003-2026

- With the default values, the backup will fail after (300 seconds + 30 seconds) * (300 + 1) = 99330 seconds, or ~27.6 hours.
- If you set **Number of attempts** to 1 and **Interval between attempt**s to 1 second, the backup will fail after (300 seconds + 1 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.

 © Acronis International GmbH, 2003-2026

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 available with the XFS, JFS, exFAT, ReFS, and ReiserFS4 file systems. For more information, see "Supported file systems" (p. 72).

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).

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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, see 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.

© Acronis International GmbH, 2003-2026

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 and later
- Windows Server 2012 R2 and later

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 console, go to **Devices** > **All devices**. Alternatively, the protection plan can be created from the **Plans** tab.
2. Select the device and click **Protect**.

© Acronis International GmbH, 2003-2026

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 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

© Acronis International GmbH, 2003-2026

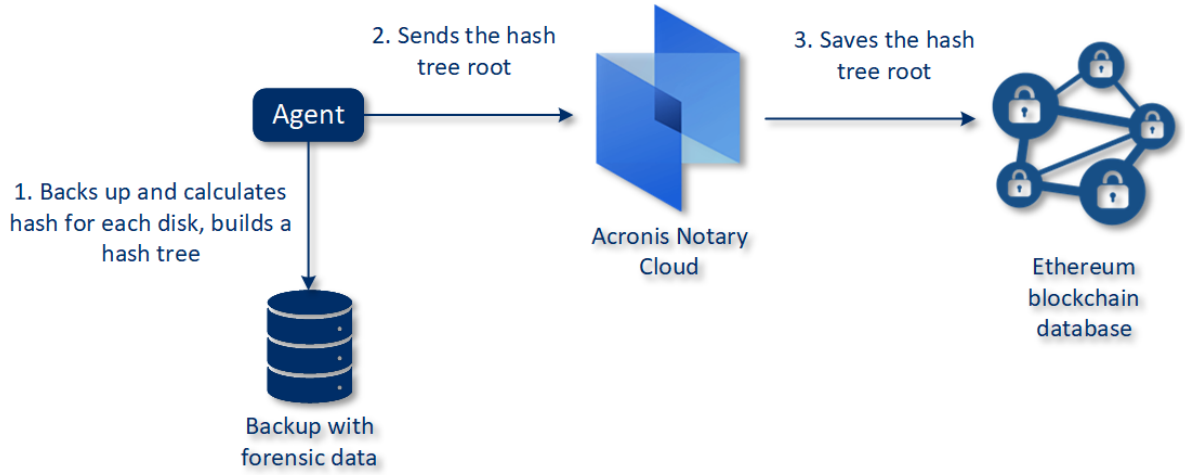
service saves the hash tree root in the Ethereum blockchain database to ensure that this value does not change.

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.

Notarization of 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.

© Acronis International GmbH, 2003-2026

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. You can use this tool 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\Defa
  ult\<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`

© Acronis International GmbH, 2003-2026

- `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

© Acronis International GmbH, 2003-2026

```
--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
```


© Acronis International GmbH, 2003-2026

`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`	A backup location URI. The possible formats of the "--loc" option are:
	• Local path name (Windows)
	`c:/upload/backups`
	• Local path name (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Cloud storage
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`

© Acronis International GmbH, 2003-2026

	`<IP_address>` – you can find it in the registry key in Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri `<path_to_certificate>` – a path to the certificate file to access Cyber Protect Cloud. For example, in Windows this certificate is located in `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt` where `<username>` – is your account name to access Cyber Protect Cloud.
`--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.
	Output example without `--raw`:
	`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`
	Output with `--raw`:
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

`--utc`	Shows dates in UTC

`--progress`	Shows progress of the operation.
	For example:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

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**.

© Acronis International GmbH, 2003-2026

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**.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

One-click recovery

Note
This feature is available with the following licenses:

- Acronis Cyber Protect Advanced
- Acronis Cyber Protect Backup Advanced

With One-click recovery, you can automatically recover a disk backup of your Windows or Linux machine. The backup can be of the entire machine, or of specific disks or volumes on the machine. Machines with Secure Boot and BitLocker encryption are supported.

One-click recovery supports the following operations:

- Automatic recovery from the latest backup
- Recovery from a specific backup (also known as a recovery point) within the backup archive

One-click recovery supports the following backup storages:

- Secure Zone
- Network folder
- Cloud storage

Note
One-click recovery is not supported for backups in locations that are managed by a storage node.

Important
Suspend the BitLocker encryption until the next restart of your machine when you perform any of the following operations:

- Creating, modifying, or deleting Secure Zone.
- Enabling or disabling Startup Recovery Manager.
- [Only if Startup Recovery Manager was not already enabled] Running the first backup after enabling One-click recovery in the protection plan. This operation enables Startup Recovery Manager automatically.
- Updating Startup Recovery Manager, for example by updating the protection.

If the BitLocker encryption was not suspended during these operations, you will need to specify your BitLocker PIN after restarting the machine.

Enabling One-click recovery

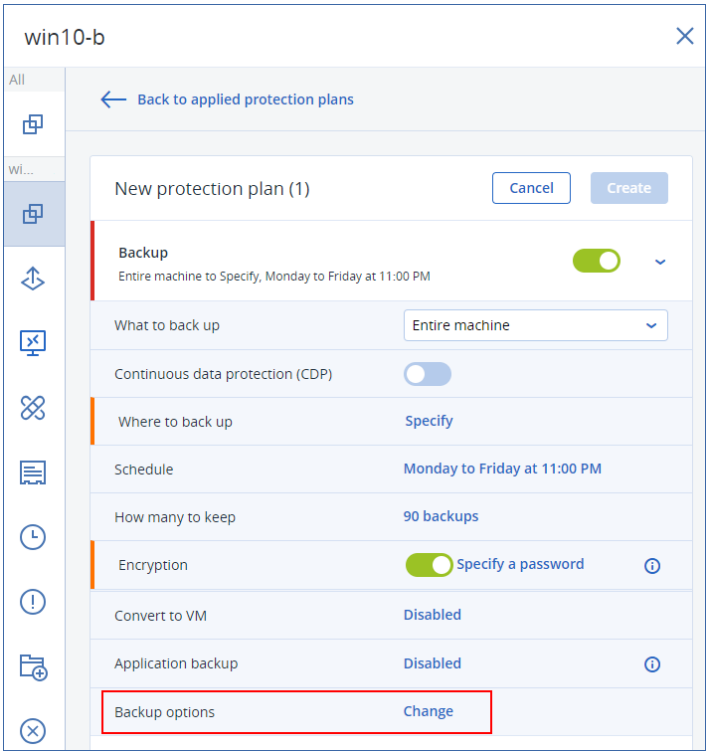
One-click recovery is a backup option in the protection plan. For more information on how to create a plan, see "Creating a protection plan" (p. 243).

 © Acronis International GmbH, 2003-2026

Note
Enabling One-click recovery also enables Startup Recovery Manager on the target machine. If Startup Recovery Manager cannot be enabled, the backup operation that creates One-click recovery backups will fail. For more information about Startup Recovery Manager, see "Startup Recovery Manager" (p. 635).

To enable One-click recovery

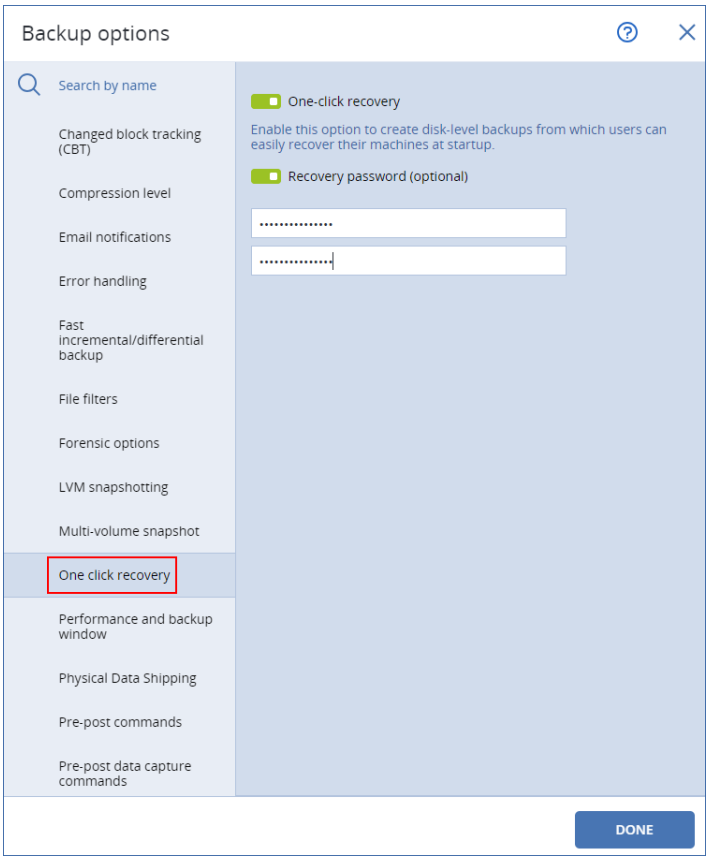
1. In the protection plan, expand the **Backup** module.
2. In **What to back up**, select **Entire machine** or **Disk/volumes**.
3. [If you selected **Disk/volumes**]. In **Items to back up**, specify the disk or volumes to back up.
4. In **Backup options**, click **Change**, and then select **One-click recovery**.



5. Enable the **One-click recovery** switch.
6. [Optional] Enable the **Recovery password** switch, and then specify a password.

Important
We strongly recommend that you specify a recovery password. Ensure that the user who performs One-click recovery on the target machine knows this password.

© Acronis International GmbH, 2003-2026



7. Click **Done**.
8. Configure the other elements of the protection plan according to your needs, and then save the plan.

As a result, after the protection plan runs and creates a backup, One-click recovery becomes accessible to the users of the protected machine.

Disabling One-click recovery

You can disable One-click recovery for a specific workload in the following ways:

- Disable the **One-click recovery** option in the protection plan that is applied to the workload.
- Revoke the protection plan in which the **One-click recovery** option is enabled.
- Delete the protection plan in which the **One-click recovery** option is enabled.

Recovering a machine with One-click recovery

Prerequisites

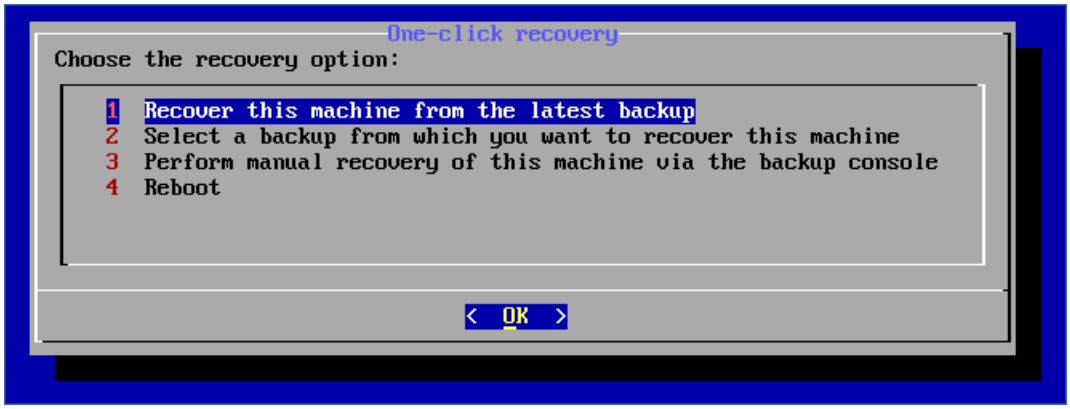
- A protection plan with enabled **One-click recovery** backup option is applied to the machine.
- There is at least one disk backup of the machine.

To recover a machine

© Acronis International GmbH, 2003-2026

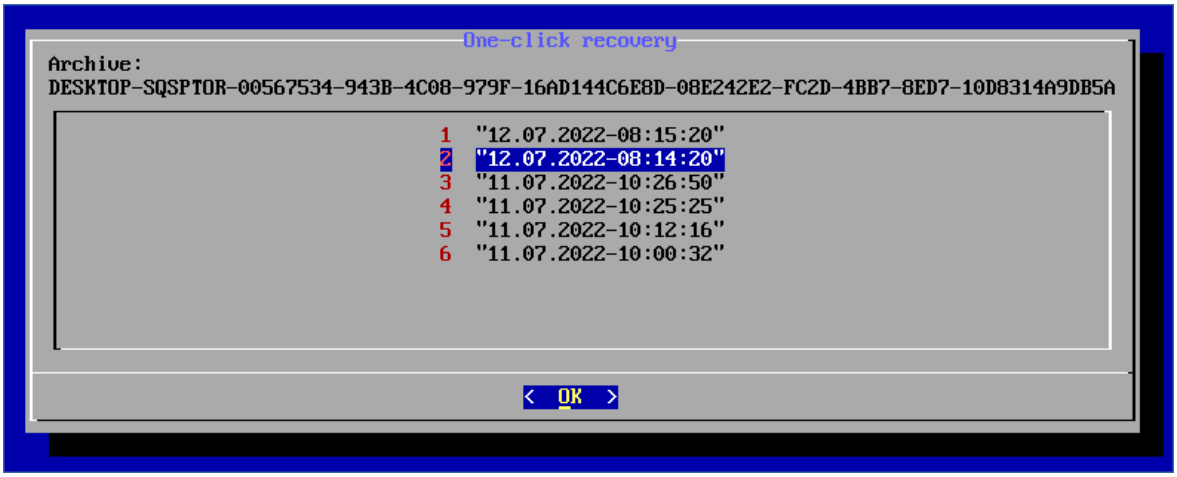
1. Reboot the machine that you want to recover.
2. During the reboot, press F11 to enter Startup Recovery Manager.

   The rescue media window opens.
3. Select **Acronis Cyber Protect**.
4. [If a recovery password was specified in the protection plan] Enter the recovery password, and then click **OK**.
5. Select a One-click recovery option.
   - To recover the latest backup automatically, select the first option, and then click **OK**.
   - To recover another backup within the backup archive, select the second option, and then click **OK**.



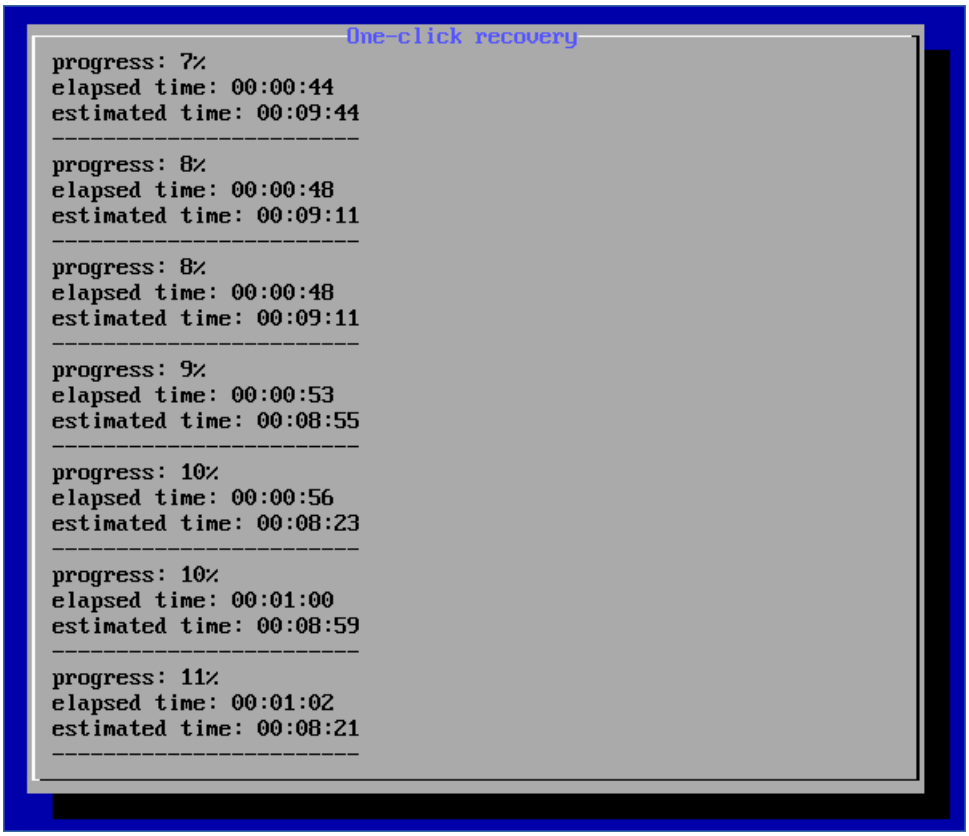
6. Confirm your choice by clicking **Yes**.

   The rescue media window opens, and then disappears. The recovery procedure continues without it.
7. [If you chose to recover a specific backup] Select the backup that you want to recover, and then click **OK**.



After a while, the recovery starts and its progress is shown. When the recovery completes, your machine reboots.

© Acronis International GmbH, 2003-2026



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.

This option is effective only for the backup and backup replication processes. Post-backup commands and other operations included in a protection plan (for example, validation) 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, it 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

 © Acronis International GmbH, 2003-2026

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

Note
You can configure performance and backup window for every replication location individually. To access the settings of the replication location, in the protection plan, click the gear icon next to the location name, and then click **Performance and backup window**.

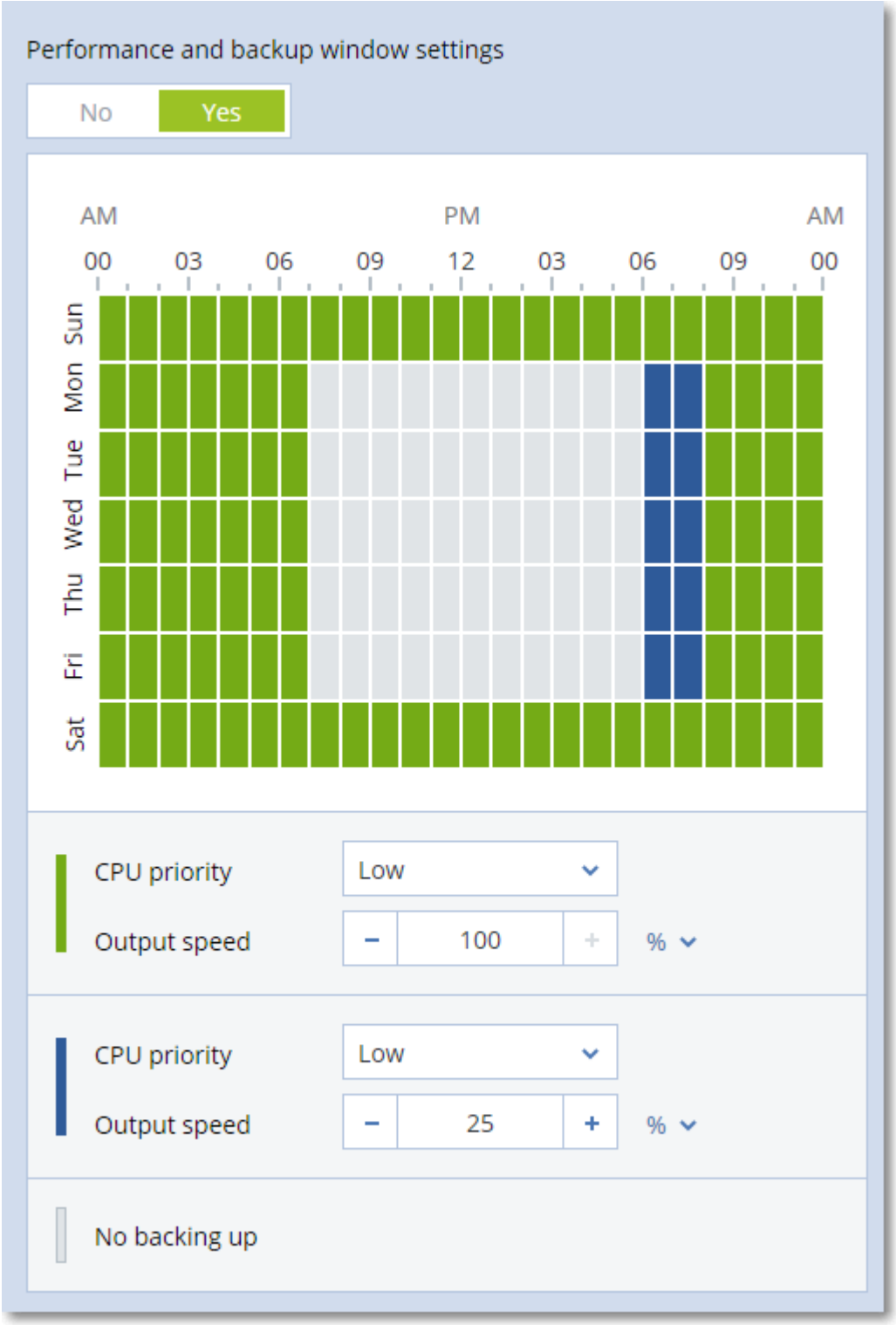
Backup window

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.

© Acronis International GmbH, 2003-2026



CPU priority

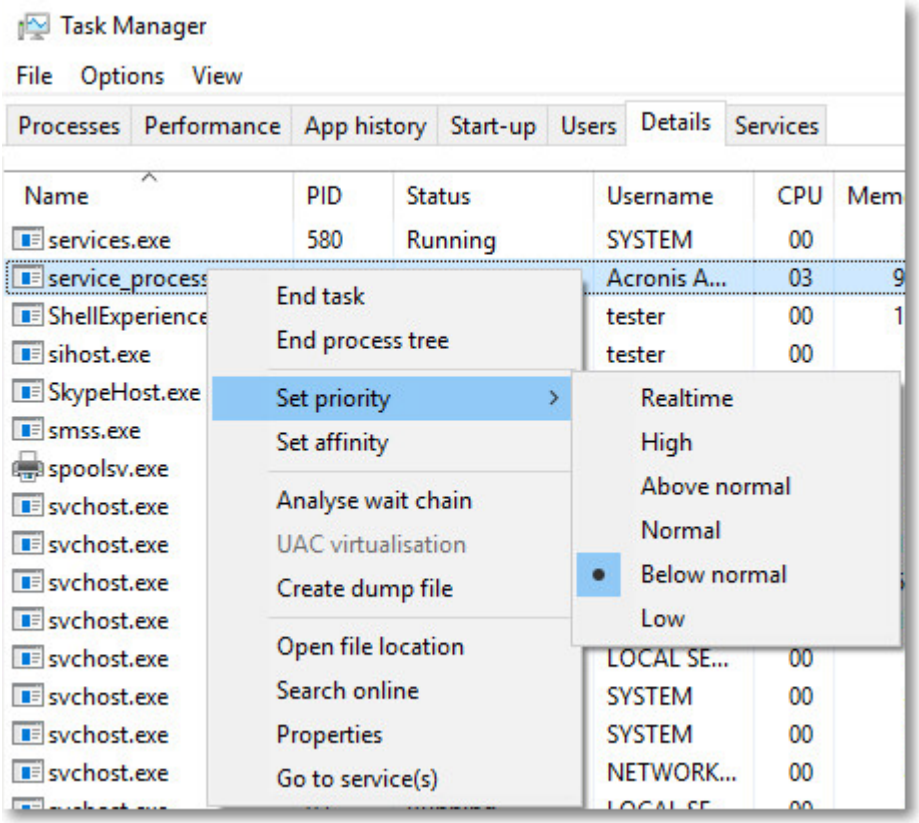
This parameter defines the priority of the backup process in the operating system.

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

© Acronis International GmbH, 2003-2026

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 macOS.



The table below summarizes the mapping for this setting in Windows, Linux, and macOS.

Cyber Protect priority	Windows priority	Linux and macOS niceness
Low	Below normal	10
Normal	Normal	0
High	High	-10

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

© Acronis International GmbH, 2003-2026

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 available if the backup or replication 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.

Use this option to ship the first full backup created by a protection plan to the cloud storage on a hard disk drive by using the Physical Data Shipping service. The subsequent incremental backups are performed over the network.

For local backups that are replicated to cloud, incremental backups continue and are saved locally until the initial backup is uploaded in the cloud storage. Then all incremental changes are replicated to the cloud and the replication continues per the backup schedule.

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. [To ship backups that have cloud storage as the primary backup location]
   a. Create a new protection plan with backup to cloud.
   b. In the **Backup options** row, click **Change**.
   c. In the list of available options, click **Physical Data Shipping**.

   You can back up directly to a removable drive or back up to a local or a network folder, and then copy/move the backup(s) to the drive.

© Acronis International GmbH, 2003-2026

2. [To ship local backups that are replicated to cloud]
   a. Create a new protection plan with backup to a local or network storage.
   b. Click **Add location** and select **Cloud storage**.
   c. In the **Cloud storage** location row, click the gear wheel and select **Physical Data Shipping**.
3. Under **Use Physical Data Shipping**, click **Yes** and **Done**.
   The Encryption option is enabled automatically in the protection plan because all backups that are shipped must are encrypted.
4. In the **Encryption** row, click **Specify a password** and enter a password for encryption.
5. In the **Physical Data Shipping** row, select the removable drive where the initial backup will be saved.
6. Click **Create** to save the protection plan.
7. 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 the web interface:
   - [For on-premises deployment] Log in to your Acronis account, and then click **Go to Tracking Console** under **Physical Data Shipping**.
   - [For cloud deployment] Log in to Management Portal, click **Overview** > **Usage**, and then click **Manage service** under **Physical Data Shipping**.

   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.

8. 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.

9. 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.

Pre-backup command	Backup	Post-backup command

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

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

* 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.

	<---------- **Backup** ---------->				
Pre-backup command	Pre-data capture command	Data capture	Post-data capture command		Post-backup command

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

© Acronis International GmbH, 2003-2026

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

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

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

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".)

© Acronis International GmbH, 2003-2026

3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command's execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

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

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

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 "Backup schedule" (p. 364).

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:

© Acronis International GmbH, 2003-2026

- **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. 498).

  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**.

 © Acronis International GmbH, 2003-2026

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.

 © Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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 you 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.**

© Acronis International GmbH, 2003-2026

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`

© Acronis International GmbH, 2003-2026

`[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" (p. 373).

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

 © Acronis International GmbH, 2003-2026

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 applicable only to Windows operating systems.

It defines whether a backup can succeed if one or more Volume Shadow Copy Service (VSS) writers fail and which provider has to notify the VSS-aware applications that the backup will start.

Using the Volume Shadow Copy Service 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.

You may also 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 then specify post-data capture commands that will resume the database operations after the snapshot is taken.

Note
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.

Ignore failed VSS writers

You can select one of the following:

© Acronis International GmbH, 2003-2026

- **Ignore failed VSS writers**

  With this option, you can achieve successful backups even when one or more VSS writers fail.

  Important

  Application-aware backups will always fail if the application-specific writer fails. For example, if you are making application-aware backup of SQL Server data, and **SqlServerWriter** fails, the backup operation will also fail.

  When this option is enabled, up to three consecutive attempts for a VSS snapshot will be made. In the first attempt, all VSS writers are required. If this attempt fails, it will be repeated. If the second attempt also fails, the failed VSS writers will be excluded from the scope of the backup operation, and then a third attempt will be made. If the third attempt is successful, the backup will complete with a warning about the failed VSS writers. If the third attempt is not successful, the backup will fail.

- **Require successful processing for all VSS writers**

  If any of the VSS writers fails, the backup operation will also fail.

Select the snapshot provider

You can select one of the following:

- **Automatically select snapshot provider**

  Automatically select the hardware snapshot provider, a software snapshot provider, or the Microsoft Software Shadow Copy provider.

  Note

  We recommend that you use automatic selection of a snapshot provider whenever possible.

- **Use Microsoft Software Shadow Copy provider**

  We recommend that you force the use of the Microsoft Software Shadow Copy provider if you have other third-party VSS providers that you do not want to use, and when the protected workload does not contain Cluster Shared volumes.

  Warning!

  Force the use of Microsoft Software Shadow Copy provider only if you need to use it explicitly, because it may cause backups to fail in environments with Cluster Shared volumes and other volumes not supported by the Microsoft Software Shadow Copy provider.

Enable VSS full backup

If this option is enabled, the 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**.

© Acronis International GmbH, 2003-2026

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.

Important
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 controls the creation of quiesced snapshots for protected virtual machines.

The preset is: **Enabled**.

When this option is enabled, the transactions of all VSS-aware applications running in the virtual machine are completed before taking a quiesced snapshot.

If a quiesced snapshot cannot be taken for some reason, the outcome of the backup operation depends on the application backup settings as follows.

- If application backup is set to **Enabled** and a quiesced snapshot cannot be taken after the number of re-attempts specified in the Error handling option, the backup fails.
- If application backup is set to **Disabled** and a quiesced snapshot cannot be taken after the number of re-attempts specified in the Error handling option, a crash-consistent backup is created.
  To make the backup fail instead of creating a crash-consistent backup, select the **Fail backup if taking a quiesced snapshot is not possible** check box.

When this option is disabled, a non-quiesced snapshot is taken. The virtual machine will be backed up in a crash-consistent state.

The following table summarizes the available settings and their results.

Settings	Quiesced snapshot was taken successfully		Quiesced snapshot was not taken	
	Application backup enabled	Application backup disabled	Application backup enabled	Application backup disabled
Volume Shadow Copy Service (VSS) for virtual	Quiesced snapshot is taken.	Quiesced snapshot is taken.	Backup fails.	Non-quiesced snapshot is taken. Crash-consistent

 © Acronis International GmbH, 2003-2026

Settings	Quiesced snapshot was taken successfully		Quiesced snapshot was not taken	
	Application backup enabled	**Application backup disabled**	**Application backup enabled**	**Application backup disabled**
machines enabled **Fail backup if taking a quiesced snapshot is not possible** not selected	Application-consistent backup is created.	Application-consistent backup is created.		backup is created.
Volume Shadow Copy Service (VSS) for virtual machines enabled **Fail backup if taking a quiesced snapshot is not possible** selected	Quiesced snapshot is taken. Application-consistent backup is created.	Quiesced snapshot is taken. Application-consistent backup is created.	Backup fails.	Backup fails.
Volume Shadow Copy Service (VSS) for virtual machines disabled	Non-quiesced snapshot is taken. Crash-consistent backup is created.	Non-quiesced snapshot is taken. Crash-consistent backup is created.	Non-quiesced snapshot is taken. Crash-consistent backup is created.	Non-quiesced snapshot is taken. Crash-consistent backup is created.

Enabling **Volume Shadow Copy Service (VSS) for virtual machines** also triggers the pre-freeze and post-thaw scripts that you might have on the backed-up virtual machine. For more information on these scripts, see "Running pre-freeze and post-thaw scripts automatically" (p. 486).

To take a quiesced snapshot, the backup software applies VSS inside a virtual machine by using VMware Tools, Hyper-V Integration Services, Virtuozzo Guest Tools, Red Hat Virtualization Guest Tools, or QEMU Guest Tools, respectively.

Note

For Red Hat Virtualization (oVirt) virtual machines, we recommend that you install QEMU Guest Tools instead of Red Hat Virtualization Guest Tools. Some versions of Red Hat Virtualization Guest Tools do not support application-consistent snapshots.

This option does not affect Scale Computing HC3 virtual machines. For them, quiescing depends on whether Scale Tools are installed on the virtual machine.

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**.

© Acronis International GmbH, 2003-2026

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**.

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.

© Acronis International GmbH, 2003-2026

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.

After unmounting a volume mounted from a backup in the read/write mode, a new recovery point is added, even if the mounted volume was not modified. The cause is that Windows automatically discovers newly appeared volumes and applies metadata changes to them, which forces Acronis Cyber Protect to preserve these changes in a new recovery point during unmounting.

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.

© Acronis International GmbH, 2003-2026

- **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.

© Acronis International GmbH, 2003-2026

Validating backups

Validation is an operation that checks the possibility of data recovery from a backup. For more information about this operation, see "Validation" (p. 465).

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, see "The Backup storage tab" (p. 452).
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

Note
Exporting backups from tapes is not supported.

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.

 © Acronis International GmbH, 2003-2026

- 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

A backup archive contains one or more backups. You can delete specific backups (recovery points) in an archive or the whole archive.

Deleting the backup archive deletes all backups in it. Deleting all backups of a workload deletes the backup archives that contain these backups.

Note
Continuous data protection prevents the deletion of backup archives. If you want to manually delete a backup that is created with CDP enabled, you need to revoke or delete the corresponding protection plan first.

You can delete backups by using the Cyber Protect console – on the **Devices** tab and on the **Backup storage** tab. Also, you can delete backups from the cloud storage by using the Web Restore console.

Warning!
If immutable storage is disabled, backed-up data is permanently deleted and cannot be recovered.

To delete backups or backup archives

On the Devices tab

This procedure applies only to online workloads.

© Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Select the workload backups of which you want to delete.
3. Click **Recovery**.
4. [If more than one backup location is available] Select the backup location.
5. [To delete all backups of the workload] Click **Delete all**.
   Deleting all backups also deletes the backup archives that contain these backups.
6. [To delete a specific backup] Select the backup (recovery point) that you want to delete, and then click **Actions** > **Delete**.
7. [When deleting all backups] Select the check box, and then click **Delete** to confirm your decision.
8. [When deleting a specific backup] Click **Delete** to confirm your decision.

On the Backup storage tab

This procedure applies to online and offline workloads.

1. In the Cyber Protect console, go to **Backup storage**.
2. Select the location from which you want to delete backups.
3. Select the backup archive from which you want to delete backups.
   The archive name uses the following template:
   <workload name> - <protection plan name>
4. [To delete the whole backup archive] Click **Delete**.
   Deleting a backup archive deletes all backups in that archive.
5. [To delete a specific backup in the backup archive] Click **Show backups**.
   a. Select the backup (recovery point) that you want to delete.
   b. Click **Actions** > **Delete**.
6. [When deleting a backup archive] Select the check box, and then click **Delete** to confirm your decision.
7. [When deleting a specific backup] Click **Delete** to confirm your decision.

In the Web Restore console

This procedure applies only to backup archives in the cloud storage.

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Select the workload backups of which you want to delete, 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**.
   You are redirected to the Web Restore console.
5. In the Web Restore console, under **Machines**, click the workload name.
6. Under **Last version**, click the date, and then click **Delete**.
   This action is only available on the backup archive level. You cannot drill down the archive and delete specific backups from it.
7. Click **Delete** to confirm your decision.

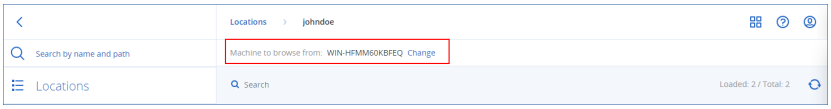
© Acronis International GmbH, 2003-2026

Deleting backups outside the Cyber Protect console

We recommend that you delete backups by using the Cyber Protect console. If you delete backups from the cloud storage by using the Web Restore console or delete local backups by using a file manager, you must refresh the backup location to sync the changes to the Cyber Protect console.

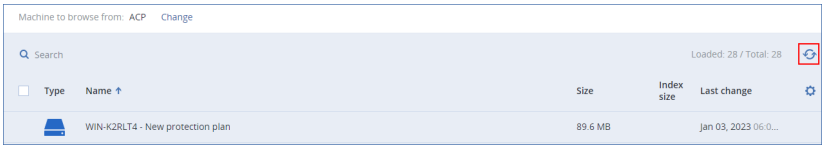
Prerequisite

- An online agent that can access the backup location must be selected as **Machine to browse from** in the Cyber Protect console.



To refresh a backup location

1. In the Cyber Protect console, go to **Backup storage**.
2. Select the backup location in which the deleted backups were stored.
3. Click the **Refresh** icon.



Understanding the detection of bottlenecks

The bottleneck detection feature helps you understand where you can improve performance by highlighting which component in your system was the slowest during a backup or recovery process.

As bottlenecks *always* occur in any transmission event, it does not necessarily mean they need to be resolved. Your backups may be already fast enough and meet your backup windows perfectly, as well as meet your SLAs, so there is typically nothing you need to actually resolve.

You can easily view and track bottlenecks in the **Activity details** tab. To do this, in the Cyber Protect console, go to **Monitoring > Activities**, and then click the relevant activity. For more information about viewing bottlenecks, see "Viewing bottleneck details" (p. 460) and "On what workloads, agents, and backup locations are bottlenecks shown?" (p. 462).

What is a bottleneck?

Bottlenecks are typically caused due to a slow component in the processing chain, in other words, a component that the other components wait for.

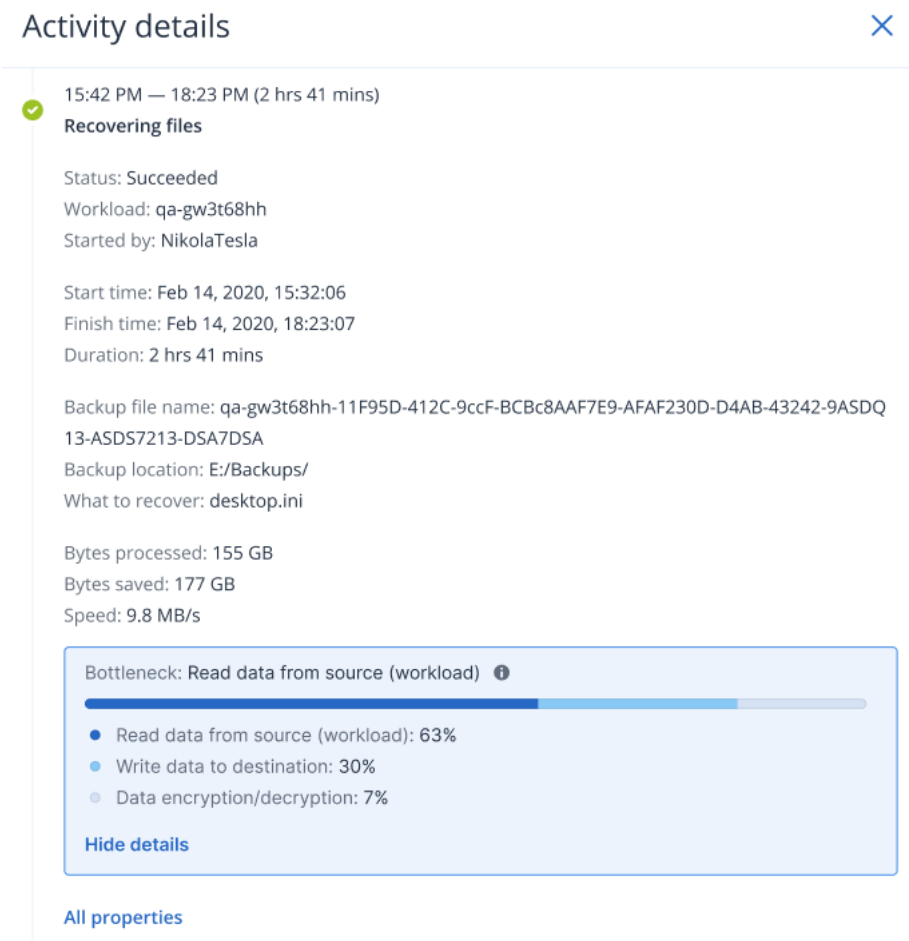
The bottleneck detection feature enables you to track these slow components during the backup and recovery process, helping you understand which of the following component types is the slowest:

© Acronis International GmbH, 2003-2026

- **Source**: At a glance, you can determine if the reading speed from the backup/recovery source is causing a bottleneck.
- **Destination**: Understand if the writing speed to the backup/recovery destination is affecting performance.
- **Agent**: Understand if the agent is processing the data fast enough.

The bottleneck type, whether from the source, destination, or agent, can change at different times during the backup/recovery activity. The percentages shown in the **Bottleneck** section of the **Activity details** tab below (for example, **Read data from source (workload): 63%**), represent the percentage of time when this type of bottleneck was encountered. In this case, for 63% of the recovery activity time, the bottleneck type was reading data, in other words, the slow speed in reading data from the backup archive by the agent.

Similarly, for 30% of the time, the bottleneck was due to the slow speed in writing data to the recovery destination (**Write data to destination: 30%**).



Note

It is normal behavior to see bottleneck statistics in the **Activity details** tab. These statistics are only available for tasks more than one minute long.

© Acronis International GmbH, 2003-2026

How to reduce bottlenecks

As mentioned above, the bottleneck detection feature highlights the *read* and *write* data flow between backup components. The *read* statistics refer to the data flow from the data source to the agent which performs the backup/recovery operation, and the *write* statistics refer to the data flow between the agent and the backup archive (the destination).

To reduce bottlenecks and improve the read/write data flow performance, you should analyze the channel between the agent and the data source/backup archive. For example, you can try benchmarking your hard disks if the agent is backing up some local files.

Viewing bottleneck details

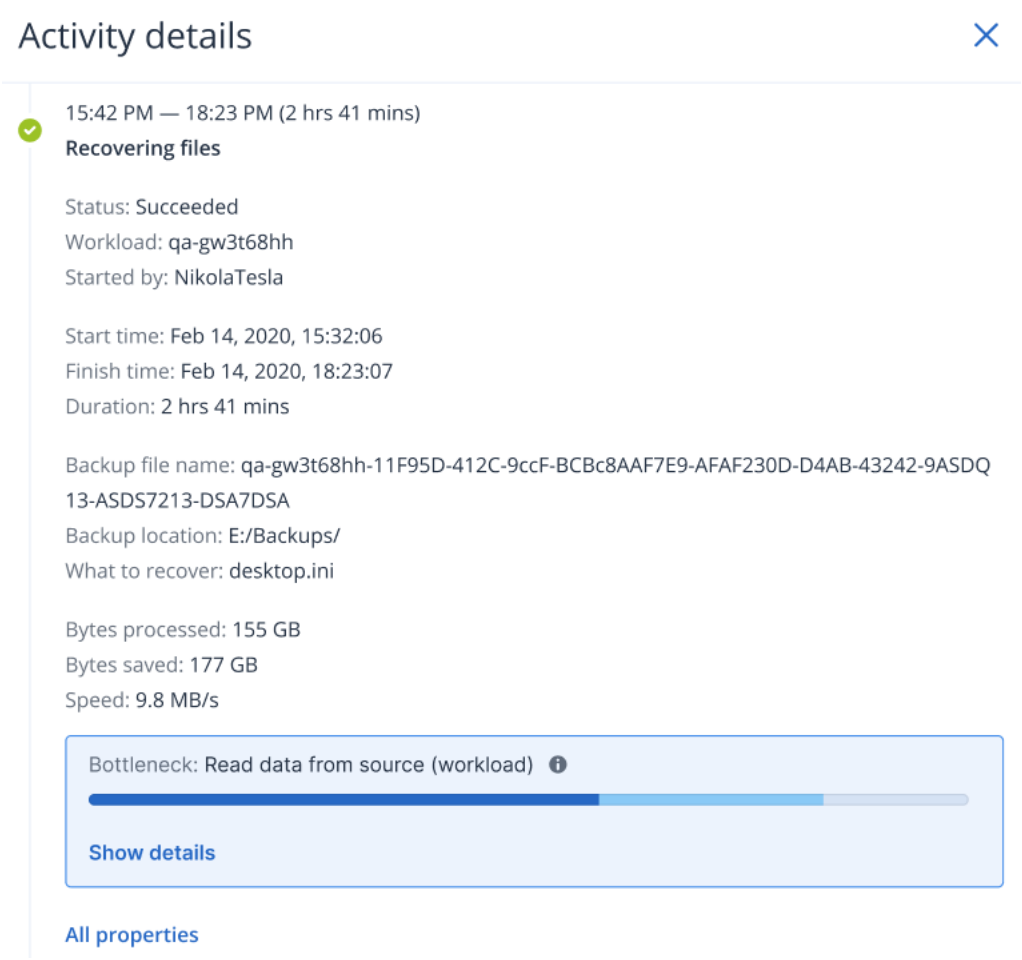
You can view detected bottlenecks for any type of backup, backup replication, or recovery process (to any type of destination folder or location), including virtual machine backups, machine backups, and file/folder backups. You can also view bottlenecks for virtual machine replication and failback activities.

For more information on the definition and core concepts of bottleneck types, see "Understanding the detection of bottlenecks" (p. 458).

To view bottleneck details

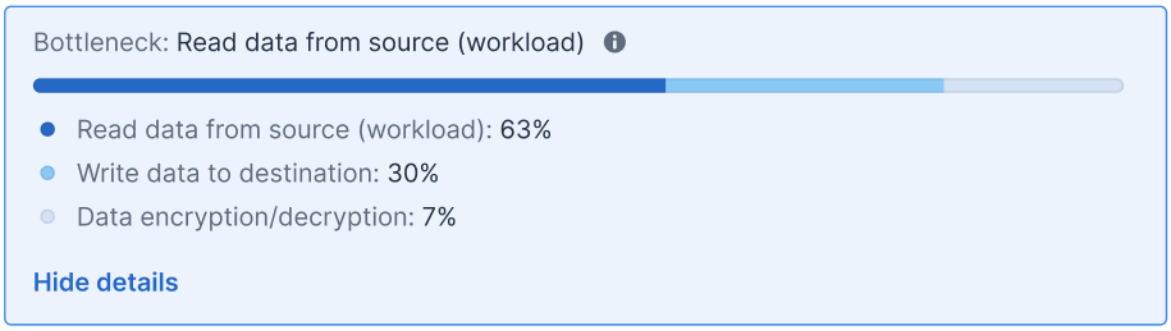
1. In the Cyber Protect console, go to **Monitoring > Activities**.
2. Click on the relevant activity.
   In the **Activity details** tab, the **Bottleneck** section is shown in blue.

© Acronis International GmbH, 2003-2026



3. Click **Show details** to view the most frequently encountered bottleneck during the backup/recovery operation.

   The **Bottleneck** section expands to show a summary of the relevant bottleneck types.



   In the example above, the bottleneck that accounted for 63% of the entire operation's time was caused by the *Read* operation (performed by the agent).

Note

The bottleneck values update dynamically every minute while the corresponding activity is running.

© Acronis International GmbH, 2003-2026

On what workloads, agents, and backup locations are bottlenecks shown?

The detection of bottlenecks is available for the following types of workloads, agents, and backup locations:

- Disk/image-level backups performed by:
  - Agent for Windows
  - Agent for Linux
  - Agent for Mac
  - Agent for VMware (both Virtual Appliance and Windows, including VM replication and failback from replica (restore from replica) activities)
  - Agent for Hyper-V
  - Agent for Scale Computing HC3
  - Agent for oVirt (KVM)
  - Agent for Virtuozzo
- File-level backups
  - Agent for Windows
  - Agent for Linux
  - Agent for Mac
- Application-level backups
  - Agent for SQL
  - Agent for Exchange
  - Agent for Oracle
  - Agent for SAP HANA
- Backup locations
  - Acronis Cloud storage (including partner-hosted storage)
  - Network shares (SMB + NFS)
  - Local folders
  - Locations defined by script
  - Acronis Secure Zone

Off-host data protection plans

Note
This feature is available with an Advanced license.

Replication, validation, and cleanup are usually performed by the protection agent that performs the backup. This puts additional load on the machine on which the agent is running, even after the backup process is complete. To offload the machine, you can create off-host data protection plans – that is, separate plans for replication, validation, cleanup, and conversion to a virtual machine.

With the off-host data protection plans, you can do the following:

© Acronis International GmbH, 2003-2026

- Choose different agents for the backup and off-host data protection operations
- Schedule the off-host data processing operations during off-peak hours to minimize the network bandwidth consumption
- Schedule the off-host data processing operations during non-business hours, if you do not want to install a dedicated agent for off-host data processing

If you are using a storage node, we recommended that you install a dedicated agent the machine with the node.

Note
The off-host data processing plans run according to the time settings of the management server. On the contrary, the protection plans and VM replication plans run according to the time settings of the machine on which the protection agent is installed.

Backup scanning plans

Note
Backup scanning for Microsoft 365 is available only in cloud deployments. You cannot configure a backup scanning plan for Microsoft 365 in an on-premises deployment.

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. 110).

Backup scanning plans are supported for **Entire machine** and **Disks/volumes** 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 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**.

 © Acronis International GmbH, 2003-2026

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. 399).

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.

 © Acronis International GmbH, 2003-2026

9. In **Retention rules**, specify the retention rules for the target location.

   The following options are available:

   - **By number of backups**
   - **By backup age** (separate settings for monthly, weekly, daily, and hourly backups)
   - **By total size of backups**
   - **Keep backups indefinitely**

   Note
   Selecting this option will result in increased storage usage. You must delete the unnecessary backups manually.

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, see "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.

© Acronis International GmbH, 2003-2026

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**.

© Acronis International GmbH, 2003-2026

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. In **Retention rules**, specify the retention rules.

© Acronis International GmbH, 2003-2026

The following options are available:

- **By number of backups**
- **By backup age** (separate settings for monthly, weekly, daily, and hourly backups)
- **By total size of backups**

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**.

Special operations with virtual machines

Running a virtual machine from a backup (Instant Restore)

By using **Run as VM**, you can start a virtual machine from a disk-level backup that contains an operating system. This operation, also known as Instant Restore, quickly brings a virtual machine online.

While this virtual machine is running, its disks are emulated directly from the backup, and storage space is only required for recording the on-going changes.

The virtual machine that is created by using **Run as VM** is designed for short-term use. Typical use cases include:

- Disaster recovery: Instantly bring online a copy of a failed machine.
- Backup verification: Run a machine directly from its backup to confirm that the guest operating system and applications function correctly.
- Accessing application data: Use the application's native management tools on the running machine to access or extract required data.

We recommend that you keep the temporary machine for up to three days, and then remove it or convert it to a regular virtual machine, by finalizing it.

While the temporary virtual machine exists, retention rules cannot be applied to the backup on which it relies. However, backups of the original machine can continue to run normally.

Prerequisites

- At least one agent (depending on the hypervisor, Agent for VMware, Agent for Hyper-V, or Agent for Proxmox) must be registered in the Cyber Protect console.
- The backup from which you run the temporary virtual machine can be located in a network folder or in a local folder. If you select a network folder, the protection agent must be able to access it. You can also run the virtual machine from a backup that is stored in cloud storage. However, performance will be slower because this operation requires intensive random-access reads from the backup.

© Acronis International GmbH, 2003-2026

- **Run as VM** requires either a backup of the entire machine or a backup of all volumes that are needed for the operating system to start.
- To run a virtual machine from a backup, you can use backups of both physical and virtual machines. You cannot use backups of containers.
- If the backup contains Linux logical volumes (LVM), you must create it by using Agent for VMware, Agent for Hyper-V, or Agent for Proxmox. The temporary virtual machine must match the platform of the original machine (VMware ESXi, Hyper-V, or Proxmox).

Finalization

Running a virtual machine directly from a backup requires an uninterrupted connection to both the backup location and the protection agent. If this connection is lost, the machine can become inaccessible or even corrupted.

Finalization is the process of converting this temporary virtual machine into an independent, permanent virtual machine that is stored on production-ready storage. During finalization, the Cyber Protect recovers the machine's virtual disks and applies all changes that were made while the machine was running. The virtual machine remains powered on throughout the entire process.

Before starting finalization, ensure that the selected storage has enough free space, supports appropriate sharing capabilities, and provides the performance that is required for production workloads.

Note
Finalization is not supported for Hyper-V machines that run on Windows Server 2008/2008 R2 and Microsoft Hyper-V Server 2008/2008 R2 because these operating systems do not provide a required API.

Finalization vs backup recovery

The finalization process is slower than a backup recovery for two main reasons:

- During finalization, the protection agent must perform random reads across various parts of the backup. During backup recovery, it reads the backup sequentially, which is significantly faster.
- If the virtual machine is running during finalization, the agent must read data from the backup to support both the running virtual machine and the finalization process. In backup recovery, the virtual machine is stopped, which makes data access more efficient.

Finalization of machines running from cloud backups

Finalization requires intensive access to the backed-up data, and its speed depends heavily on the bandwidth between the backup location and the agent. As a result, finalization is typically slower for backups that are stored in the cloud than for backups that are stored locally. If the Internet connection is very slow or unstable, finalizing a machine running from a cloud backup might even fail.

© Acronis International GmbH, 2003-2026

We recommend that you run virtual machines from local backups whenever possible if you plan to perform finalization.

Note
For VMware workloads, finalization speed depends on whether the protection agent is connected to a VMware ESXi host or to vCenter. Due to the way VMware APIs operate, connecting to vCenter can slow down the finalization process. To improve performance, use a dedicated Agent for VMware to perform the **Run as VM** operation and finalization. Connect this agent to the ESXi host instead of vCenter.

Running a virtual machine from a backup

You can run a virtual machine from a disk-level backup that includes an operating system.

Note
The **Run as VM** operation (Instant Restore) is not supported for backups that are stored on S3-compatible object storages.

To run a virtual machine form a backup (Instant Restore)

VMware ESXi

1. In the Cyber Protect console, select a backup (recovery point) that you want to run as a virtual machine.
2. Click **Run as VM**.
3. [Optional] In **Power state**, choose whether the new virtual machine will start automatically after creation.
4. In **Target machine**, select **VMware ESXi** as a hypervisor, select a location and name for the resulting virtual machine, and then click **OK**.
5. In **Datastore**, select storage for the virtual machine.
   While the virtual machine is running, changes to its virtual disks are written to storage. Ensure that the selected storage has enough free space. If you plan to make the virtual machine permanent, select storage that is appropriate for production workloads.
6. [Optional] In **VM settings**, edit the memory size or network connections of the virtual machine, and then click **OK**.
7. Click **Run now**.

Microsoft Hyper-V

1. In the Cyber Protect console, select a backup (recovery point) that you want to run as a virtual machine.
2. Click **Run as VM**.
3. [Optional] In **Power state**, choose whether the new virtual machine will start automatically after creation.

 © Acronis International GmbH, 2003-2026

4. In **Target machine**, select **Hyper-V** as a hypervisor, select a location and name for the resulting virtual machine, and then click **OK**.
5. In **Path**, select a location for the virtual machine.

   While the virtual machine is running, changes to its virtual disks are written to storage. Ensure that the selected storage has enough free space. If you plan to make the virtual machine permanent, select storage that is appropriate for production workloads.
6. [Optional] In **VM settings**, edit the memory size or network connections of the virtual machine, and then click **OK**.
7. Click **Run now**.

Proxmox VE

1. In the Cyber Protect console, select a backup (recovery point) that you want to run as a virtual machine.
2. Click **Run as VM**.
3. [Optional] In **Power state**, choose whether the new virtual machine will start automatically after creation.
4. In **Target machine**, select **Proxmox VE** as a hypervisor, select a location and name for the resulting virtual machine, and then click **OK**.
5. In **Storage**, select storage for the virtual machine.

   While the virtual machine is running, changes to its virtual disks are written to storage. Ensure that the selected storage has enough free space. If you plan to make the virtual machine permanent, select storage that is appropriate for production workloads.
6. [Optional] In **VM settings**, edit the memory size or network connections of the virtual machine, and then click **OK**.
7. Click **Run now**.

As a result, the virtual machine that is run from a backup appears in the Cyber Protect console with one of the following icons:

for VMware ESxi, for Hyper-V, and for Proxmox VE. You cannot back up these machines.

Deleting a virtual machine running from a backup

You can delete a virtual machine that is running from a backup in the Cyber Protect console.

We recommend that you do not delete such machines directly in vSphere, Hyper-V, or Proxmox VE consoles. The backup on which these machines depend might be temporarily locked and it might not be deleted by a scheduled retention rule.

To delete a virtual machine that is running from a backup

1. In the Cyber Protect console, select a machine that is running from a backup.
2. In **Actions**, click **Delete**.

© Acronis International GmbH, 2003-2026

3. To confirm your choice, click **Delete**.

As a result, the machine is removed from the Cyber Protect console, the hypervizor inventory, and the virtual machine storage. All changes that were made to the data while the machine was running, are discarded.

Finalizing a virtual machine running from a backup

You can make a virtual machine that is running from a backup permanent, by finalizing it.

To finalize a virtual machine that is running from a backup (Instant Restore)

VMware ESXi

1. In the Cyber Protect console, select a machine that is running from a backup.
2. In **Actions**, click **Finalize**.
3. Specify a name for the permanent virtual machine.
4. Select the disk provisioning mode.
5. Click **Finalize**.

Microsoft Hyper-V

1. In the Cyber Protect console, select a machine that is running from a backup.
2. In **Actions**, click **Finalize**.
3. Specify a name for the permanent virtual machine.
4. Click **Finalize**.

Proxmox VE

1. In the Cyber Protect console, select a machine that is running from a backup.
2. In **Actions**, click **Finalize**.
3. Specify a name for the permanent virtual machine.
4. Click **Finalize**.

Working in VMware vSphere

This section describes operations that are specific for VMware vSphere environments.

Backup and recovery in vSphere Client

If Acronis Management Server is running on a Windows machine, you can deploy the Acronis vCenter plugin.

With this plugin, you can back up and recover virtual machines in vSphere Client, without using the Cyber Protect console for routine tasks.

The plugin is supported on the HTML-5 client for vSphere 7.0.1 and newer.

Deploying the vCenter plugin

To back up and recover virtual machines in vSphere Client, you must deploy the vCenter plugin.

 © Acronis International GmbH, 2003-2026

Note
The vCenter plugin is only available if Acronis Management Server is running on a Windows machine.

Prerequisites

- Agent for VMware (Virtual Appliance) or Agent for VMware (Windows) is configured in your environment.

To deploy the vCenter plugin

1. Log in to the Cyber Protect console as an administrator.
2. Go to **Settings** > **Agents**, select the agent for VMware, and then click **Details**.
   If you have multiple agents for VMware in the same environment, select an agent of your choice.
3. In the **Assigned virtual machines** section, under **vCenter/ESXi**, enable the switch.
4. Specify the credentials for an account with the **Administrator** role in vCenter, and then click **OK**.

As a result, the vCenter plugin is deployed and enabled on the selected vCenter. Users whose roles include the **Cyber Protection management (backup/recovery plugin)** privilege will be able to back up and recover virtual machines by using vSphere Client.

Removing the vCenter plugin

You can remove the vCenter plugin in the Cyber Protect console.

Prerequisites

- Agent for VMware (Virtual Appliance) or Agent for VMware (Windows) is configured in your environment.

To remove the vCenter plugin

1. Log in to the Cyber Protect console as an administrator.
2. Go to **Settings** > **Agents**, select the agent for VMware, and then click **Details**.
   If you have multiple agents for VMware in the same environment, select an agent of your choice.
3. In the **Assigned virtual machines** section, under **vCenter/ESXi**, disable the switch.
4. Click **OK** to confirm your choice.

As a result, the vCenter plugin is removed from vCenter. The **Cyber Protection management (backup/recovery plugin)** privilege is removed from the vCenter user roles, and deleted. Backup and recovery functionality in vSphere Client becomes unavailable.

Creating a backup

In vSphere Client, you can run protection plans that have been applied in the Cyber Protect console.

Prerequisites

© Acronis International GmbH, 2003-2026

- The plugin for vCenter is deployed.
- Your vCenter user role includes the **Cyber Protection management (backup/recovery plugin)** privilege.
- A protection plan is applied to the virtual machine in the Cyber Protect console.

To create a backup

From the Configure tab

1. Log in to vSphere Client.
2. Go to **Inventory**, and then select the virtual machine that you want to back up.
3. On the **Configure** tab, under **Cyber Protection**, select **Cyber Protection**.
4. In the **Backups** section, select a plan, and then click **Run now**.

   If no protection plans are available, go to the Cyber Protect console and apply a plan to the virtual machine.

From the right-click menu

1. Log in to vSphere Client.
2. Go to **Inventory**, and then right-click the virtual machine that you want to back up.
3. From the menu, select **Cyber Protection** > **Quick backup**.

As a result, the most recently run protection plan runs again.

Recovering a virtual machine

In vSphere Client, you can recover an entire virtual machine.

Prerequisites

- The plugin for vCenter is deployed.
- Your vCenter user role includes the **Cyber Protection management (backup/recovery plugin)** privilege.
- At least one backup of the machine is available.

To recover a virtual machine

1. Log in to vSphere Client.
2. Go to **Inventory**, and then select the virtual machine that you want to recover.
3. On the **Configure tab**, under **Cyber Protection**, select **Cyber Protection**.
4. In the **Recovery** section, select a backup (recovery point), and then click **Confirm**.
5. [If prompted] Specify the credentials for the backup location, and then click **OK**.
6. Click **Recover**.

As a result, the selected backup will overwrite all data on the virtual machine. Any data that is not included in the backup will be lost.

© Acronis International GmbH, 2003-2026

Viewing the backup status in vSphere Client

You can view the backup status and last backup time for an individual virtual machine or for all machines on a specific level, such as host, data center, folder, resource pool, or vCenter.

To view the backup status and last backup

Individual virtual machine

1. Log in to vSphere Client.
2. Go to **Inventory**, and then select a virtual machine.
3. On the **Summary** tab, check the **Custom attributes** section.

All virtual machines

1. Log in to vSphere Client.
2. Go to **Inventory**, and then select a host, data center, folder, resource pool, or vCenter.
3. On the **VMs** tab, check the **Last backup** and **Backup status** columns.

Note
These columns are available if the user account that Agent for VMware uses has the **Manage custom attributes** and **Set custom attribute** privileges. For more information, see "Enabling the Last backup and Backup status columns in vSphere Client" (p. 475).

Enabling the **Last backup** and **Backup status** columns in vSphere Client

You can enable the **Last backup** and **Backup status** columns on the **VMs** tab for the whole host, data center, folder, resource pool, or vCenter.

To enable the Last backup and Backup status columns

1. In vSphere Client, go to **Administration** > **Access control**.
2. Click **Roles**, and then select the role that Agent for VMware uses.
   For more information about that role, see "Required privileges for Agent for VMware" (p. 488).
3. Click **Edit**, and then add the following privileges:
   - **Global** > **Manage custom attributes**
   - **Global** > **Set custom attribute**
4. Click **Save**.

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.

 © Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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**.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.

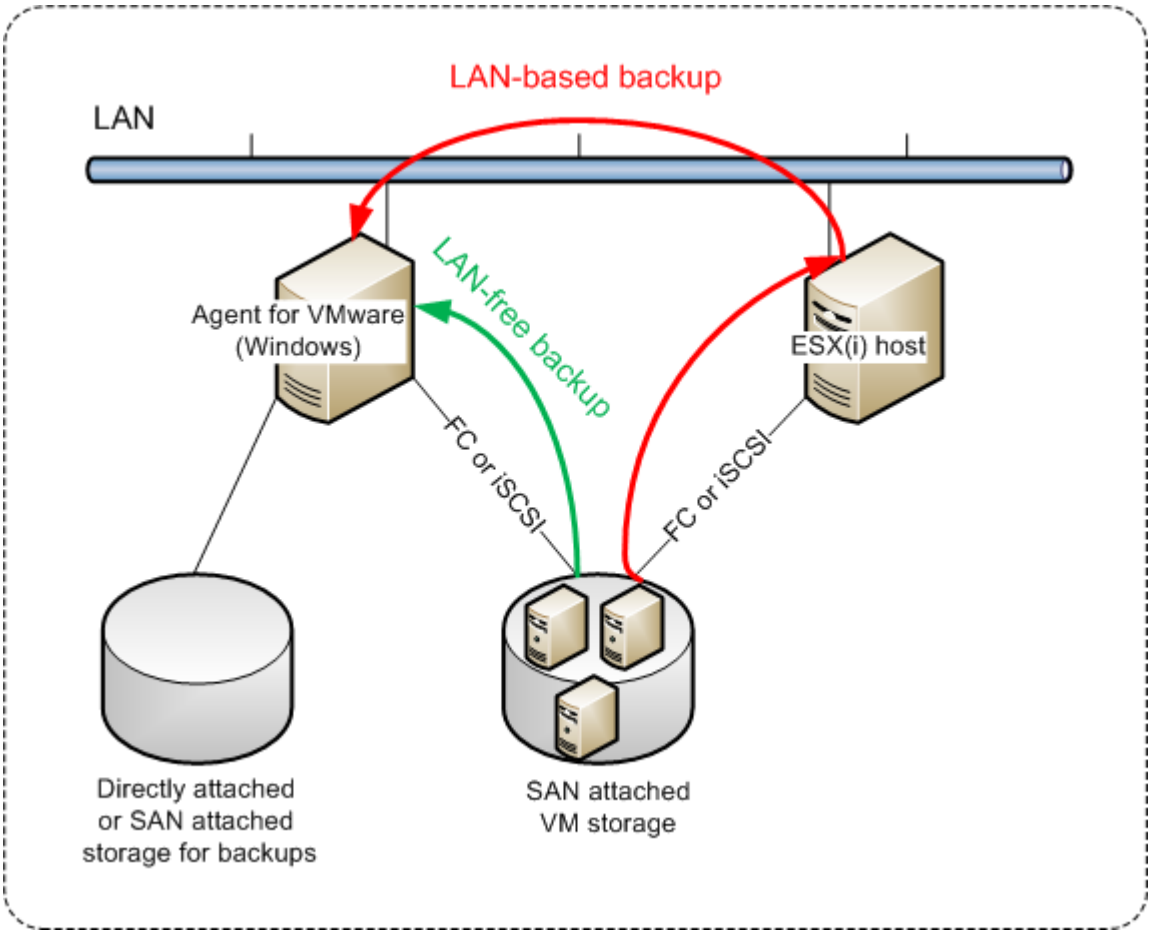
LAN-free backup

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.

© Acronis International GmbH, 2003-2026



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

 © Acronis International GmbH, 2003-2026

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

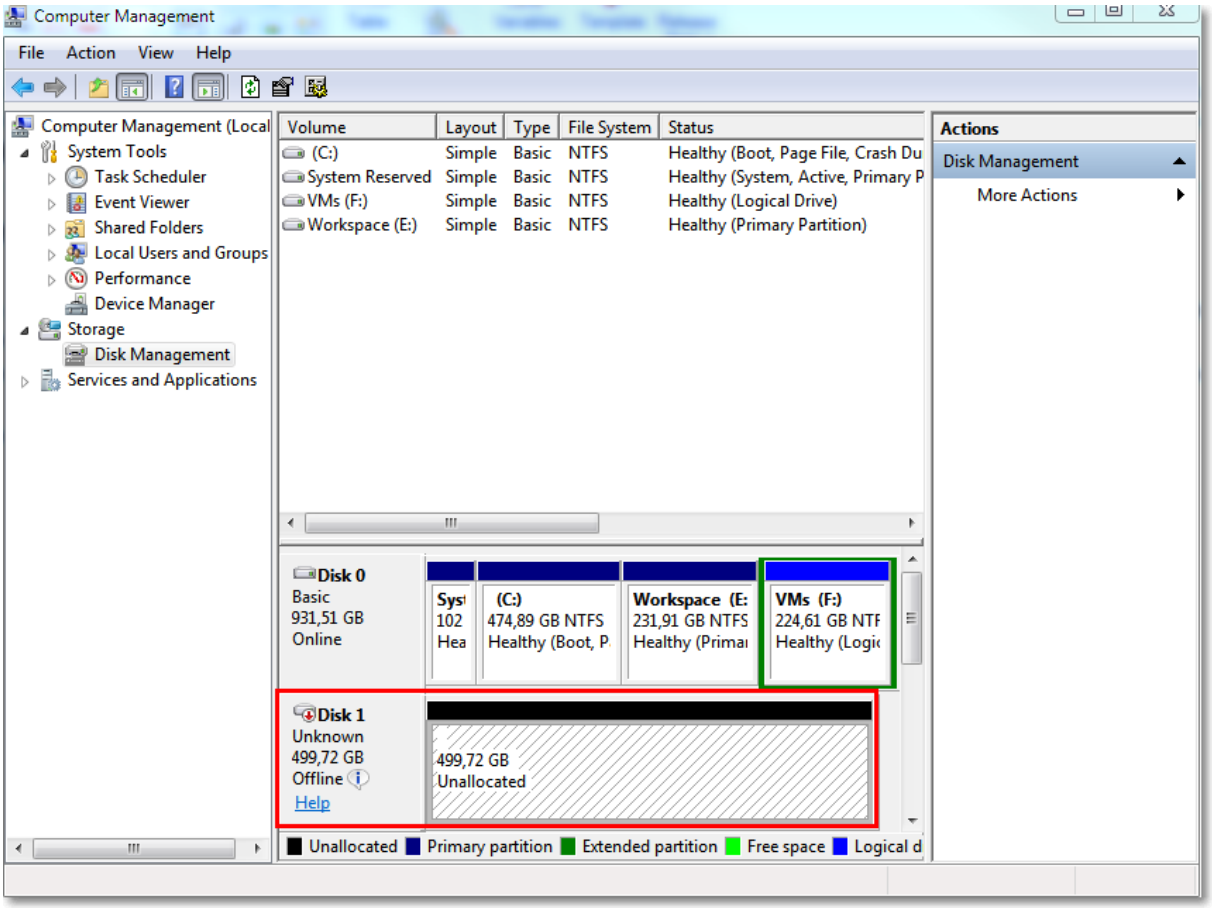
1. Go to **Control Panel** > **Administrative Tools** > **iSCSI Initiator**.

   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.

© Acronis International GmbH, 2003-2026



Virtual machine binding

This topic describes 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.

© Acronis International GmbH, 2003-2026

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**.

© Acronis International GmbH, 2003-2026

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.
- It is necessary to bind VMs to an agent if the agent uses 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.

Running pre-freeze and post-thaw scripts automatically

With VMware Tools, you can automatically run custom pre-freeze and post-thaw scripts on virtual machines that you back up in the agentless mode. Thus, for example, you can run custom quiescing scripts and create application-consistent backups for virtual machines running applications that are not VSS-aware.

Prerequisites

The pre-freeze and post-thaw scripts must be located in a specific folder on the virtual machine.

© Acronis International GmbH, 2003-2026

- For Windows virtual machines, the location of this folder depends on the ESXi version of the host.

  For example, for virtual machines running on an ESXi 6.5 host, this folder is `C:\Program Files\VMware\VMware Tools\backupScripts.d\`. You must create the `backupScritps.d` folder manually. Do not store other types of files in this folder because this may cause VMware Tools to become unstable.

  For more information about the location of the pre-freeze and post-thaw scripts for other ESXi versions, refer to the VMware documentation.
- For Linux virtual machines, copy your scripts to the `/usr/sbin/pre-freeze-script` and `/usr/sbin/post-thaw-script` directories, respectively. The scripts in `/usr/sbin/pre-freeze-script` are run when you create a snapshot and those in `/usr/sbin/post-thaw-script` are run when the snapshot is finalized. The scripts must be executable by the VMware Tools user.

To run pre-freeze and post-thaw scripts automatically

1. Ensure that VMware Tools are installed on the virtual machine.
2. On the virtual machine, put your custom scripts in the required folder.
3. In the protection plan for this machine, enable the **Volume Shadow Copy Service (VSS) for virtual machines** option.

   This creates a VMware snapshot with the **Quiesce guest file system** option enabled, which in turn triggers the pre-freeze and post-thaw scripts inside the virtual machine.

You do not need to run custom quiescing scripts on virtual machines running VSS-aware applications, such as Microsoft SQL Server or Microsoft Exchange. To create an application-consistent backup for such machines, enable the **Volume Shadow Copy Service (VSS) for virtual machines** option in the protection plan.

Support for virtual machine migration

This section contains information about migration of virtual machines within a vSphere environment, including migration between ESXi hosts that are part of a vSphere cluster.

vMotion allows moving the state and configuration of a virtual machine to another host, while the machine's disks remain in the same location on a shared storage. Storage vMotion allows moving the disks of a virtual machine from one datastore to another.

- Migration with vMotion, including Storage vMotion, is not supported for a virtual machine that runs Agent for VMware (Virtual Appliance), and is disabled automatically. This virtual machine is added to the **VM overrides** list in the vSphere cluster configuration.
- When a backup of a virtual machine starts, migration with vMotion, including Storage vMotion, is automatically disabled. This virtual machine is temporarily added to the **VM overrides** list in the vSphere cluster configuration. After the backup finishes, the **VM overrides** settings are automatically reverted to their previous state.
- A backup cannot start for a virtual machine while its migration with vMotion, including Storage vMotion, is in progress. The backup for this machine will start when its migration finishes.

© Acronis International GmbH, 2003-2026

Protection of virtualization environments

In the Cyber Protect console, you can view the vSphere, Hyper-V, and Virtuozzo environments in their native presentation. After you install and register the corresponding agent, the **VMware**, **Hyper-V**, or **Virtuozzo** tab appears under **Devices**.

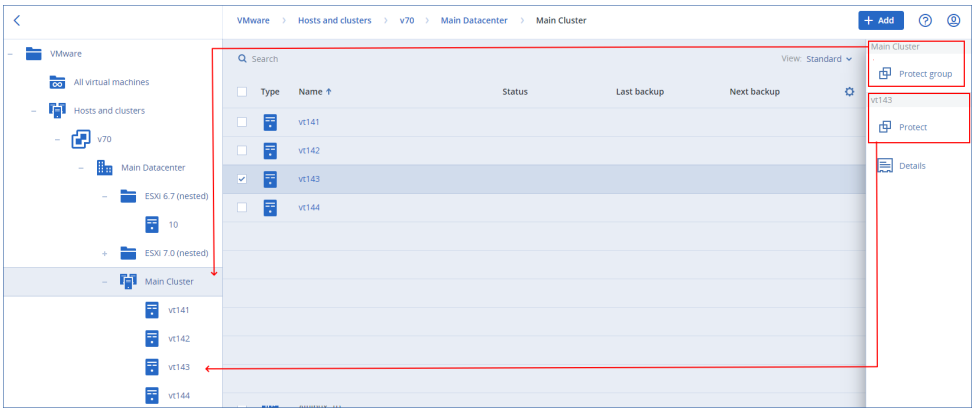
For example, on the **VMware** tab, you can back up the following vSphere infrastructure objects:

- vCenter
- Datacenter
- Folder
- Cluster
- ESXi host
- Resource pool
- Virtual machine

To apply a plan to a selected infrastructure object, click **Protect**. All child objects will be backed up.

To apply a plan to the parent object of the selected infrastructure object, click **Protect group**. All child objects of the parent object will be backed up.

For example, if you apply a plan to an ESXi host, all virtual machines on the host will be backed up. If you apply a plan to the parent cluster, all virtual machines on all hosts in this cluster will be backed up.



Required privileges for Agent for VMware

Note
To enable backups of virtual machines, install vStorage APIs on the ESXi host. For more information, see this knowledge base article.

Agent for VMware authenticates to vCenter or the ESXi host by a user account that is specified during the agent deployment. The user account must have a role that includes the privileges listed in the table below. We recommend that you use a dedicated account and role, instead of using an existing account that has the Administrator role.

© Acronis International GmbH, 2003-2026

The user account must be granted permission to access all levels of the vSphere infrastructure, such as vCenter, datacenters, clusters, ESXi hosts, resource pools, and virtual machines. To learn how to add a permission on the vCenter level and propagate it to the other levels, see "Granting access permission to the user account" (p. 494).

You can change the user account that is used by Agent for VMware without redeploying the agent. To learn how to change the account, see "Changing the user account for Agent for VMware" (p. 495).

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						
	Disable methods	+	+	+		
	Enable methods	+	+	+		
	Licenses	+	+	+	+	
	Manage custom	+	+	+		

© Acronis International GmbH, 2003-2026

Object	Privilege	Operation				
		Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup	VA deployment
	attributes					
	Set custom attribute	+	+	+		
Host > **Configuration**						
	Virtual machine autostart configuration					+
	Storage partition configuration				+	
Host > **Inventory**						
	Modify cluster					+
Host > **Local operations**						
	Create virtual machine				+	+
	Delete virtual machine				+	+
	Reconfigure virtual machine				+	+
Network						
	Assign network		+	+	+	+
Resource						

© Acronis International GmbH, 2003-2026

Object	Privilege	Operation				
		Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup	VA deployment
	Assign virtual machine to resource pool		+	+	+	+
	Import					+
Virtual machine > Change Configuration						
	Acquire disk lease	+		+		
	Add existing disk	+	+		+	
	Add new disk		+	+	+	+
	Add or remove device		+		+	+
	Advanced configuration	+	+	+		+
	Change CPU count		+			
	Change Memory		+			
	Change Settings		+	+	+	
	Change resource	+	+			
	Modify device settings	+	+			
	Remove disk	+	+	+	+	

© Acronis International GmbH, 2003-2026

Object	Privilege	Operation				
		Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup	VA deployment
	Rename		+			
	Set annotation				+	
	Toggle disk change tracking	+		+		
Virtual machine > **Guest operations**						
	Guest operation modifications	+**				
	Guest Operation program execution	+**				+
	Guest operation queries	+**				+
Virtual machine > **Interaction**						
	Acquire guest control ticket (in vSphere 4.1 and 5.0)				+	+
	Configure CD media		+	+		
	Console interaction					+
	Guest				+	+

© Acronis International GmbH, 2003-2026

Object	Privilege	Operation				
		Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup	VA deployment
	operating system management by VIX API (in vSphere 5.1 and later)					
	Power off			+	+	+
	Power on		+	+	+	+
Virtual machine > **Inventory**						
	Create from existing		+	+	+	
	Create new		+	+	+	+
	Move					+
	Register				+	
	Remove		+	+	+	+
	Unregister				+	
Virtual machine > **Provisioning**						
	Allow disk access		+	+	+	
	Allow read-only disk access	+		+		
	Allow virtual machine download	+	+	+	+	
Virtual						

© Acronis International GmbH, 2003-2026

Object	Privilege	Operation				
		Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup	VA deployment
machine > **State** **Virtual machine** > **Snapshot management** (vSphere 6.5 and later)						
	Create snapshot	+		+	+	+
	Remove snapshot	+		+	+	+
vApp						
	Add virtual machine				+	

* This privilege is required only for backing up encrypted machines.

** This privilege is required only for application-aware backups.

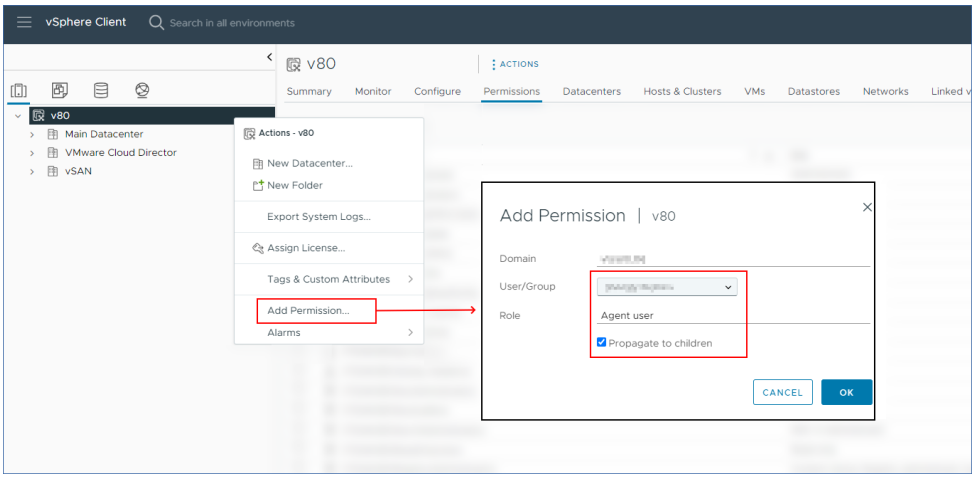
Granting access permission to the user account

The user account that is used by Agent for VMware must have access to all levels of the vSphere infrastructure, such as vCenter, datacenters, clusters, ESXi hosts, resource pools, and virtual machines.

To grant access permission to the user account

1. In vSphere Client, go to **Inventory**.
2. Right-click the **vCenter** object for which you want to grant permission, and then click **Add Permission**.
3. In the **Add Permission** dialog, select a user account and a role.
   The role must include the privileges that are listed in "Required privileges for Agent for VMware" (p. 488).
4. Select the **Propagate to children** check box.
5. Click **OK**.

 © Acronis International GmbH, 2003-2026



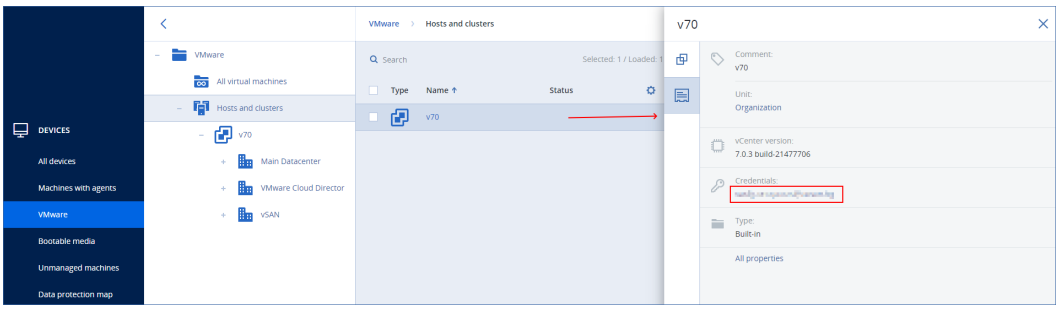
Changing the user account for Agent for VMware

In the Cyber Protect console, you can change the user account for an individual agent, or for all agents, on vCenter or an ESXi host.

To change the user account for Agent for VMware

For all agents

1. In the Cyber Protect console, go to **Devices** > **VMware**.
2. Click **Hosts and clusters**.
3. In the main panel, click the empty space next to the name of vCenter or the stand-alone ESXi host.
4. On the right panel, click **Details**.
5. Under **Credentials**, click the user account.



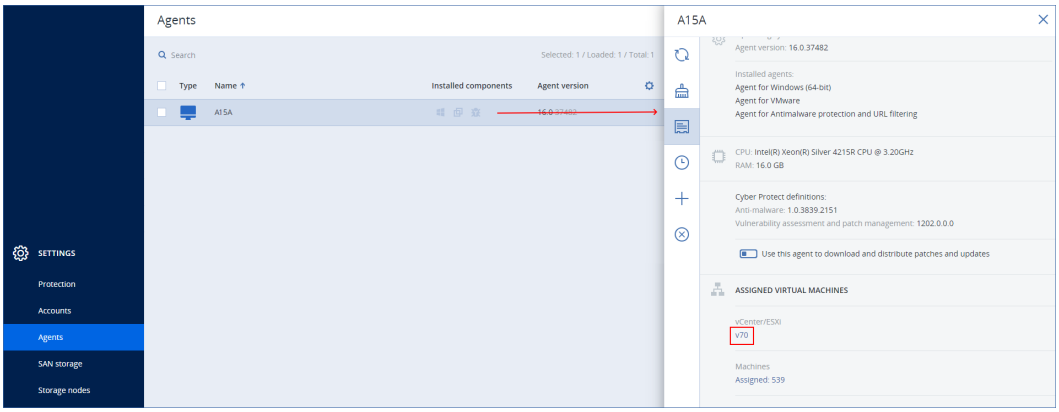
6. Specify the new user account and the password for that account.
7. Click **OK**.

As a result, all agents on this vCenter or ESXi host will use the new user account.

For an individual agent

1. In the Cyber Protect console, go to **Settings** > **Agents**.
2. Select the agent.
3. On the right panel, click **Details**.
4. Under **Assigned virtual machines**, click the vCenter/ESXi name.

© Acronis International GmbH, 2003-2026



5. In the **Add VMware vCenter or ESXi host** screen, specify the new user account and the password for that account.
6. Click **Configure**.

Required ports for backup and replication of VMware virtual machines

Ensure that the following TCP ports are open on the VMware/ESXi host.

- 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 **2029**

  Agent for VMware (Virtual Appliance) listens on this port for incoming requests to the NFS server, which is hosted on the agent. Connections via this port are required for running a virtual machine from a backup (Instant Restore).
- 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" (p. 480)). 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.

© Acronis International GmbH, 2003-2026

Using locally attached storage

With Agent for VMware (Virtual Appliance) or Agent for Scale Computing HC3, you can use locally attached storage to eliminate the network traffic between the protection agent and the backup location.

Important
Locally attached storage (LAS) is designed for small environments with a single protection agent (virtual appliance). Using multiple protection agents with locally attached storage in the same environment might result in duplicated backups, because the virtual machines are randomly distributed among the agents, and each agent uses its own locally attached storage.

In VMware environments, you can use multiple virtual appliances if you manually bind each virtual appliance to all virtual machines that this appliance will back up. For more information, see "Virtual machine binding" (p. 484).

Note
The recommended disk size for locally attached storage is up to 5 TB. Larger disks might also work but such configurations are not tested. You can attach larger disks at your own risk.

If you need to back up more than 5 TB of data, we recommend that you use a different storage type. For example, you can attach a virtual disk to a virtual machine in the environment, and then create a network share on this disk. Then, you can use the network share as a backup destination, instead of using locally attached storage.

You can configure locally attached storage when you deploy a virtual appliance, or you can configure the storage later.

For more information about configuring local storage while deploying a virtual appliance, see "Configuring the virtual appliance" (p. 161) (for VMware) and "Configuring the virtual appliance" (p. 165) (for Scale Computing).

To configure local storage after deploying a virtual appliance

1. In your virtual machine environment, select the virtual appliance, and then open its settings for editing.
2. Add a new hard disk to the virtual appliance.

   The disk size must be at least 10 GB.

   Warning!
   If you use a disk that contains data, the data will be deleted.

3. In your virtual machine environment, open the console of the virtual appliance.
4. Under **Local storages**, click **Refresh**.

   The **Create storage** button becomes active.
5. Click **Create storage**, and then select the disk that you added to the virtual appliance.

 © Acronis International GmbH, 2003-2026

- Select a drive letter.
- [Optional] Specify a disk label.

  The label length is limited to 16 characters, due to file system restrictions.

6. Click **OK**.
7. Click **Yes**.

To select locally attached storage as a backup destination

- When you create a protection plan, in **Where to back up**, select **Local folders**, and then specify the drive letter of locally attached storage. For example, **D:**.

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. This might affect the backup performance and overload the host and the virtual machine storage. You can avoid such issues by configuring a limitation on the agent level.

To limit the number of simultaneous backups on the agent level

Agent for VMware (Windows)

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

This procedure applies to virtual appliances, such as Agent for VMware (Virtual Appliance), Agent for Scale Computing, Agent for oVirt, and Agent for Nutanix.

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="Tdword">"10"</value>
</key>
```

4. Replace `10` with the maximum number of simultaneous backups that you want to set.
5. Save the file.
6. Restart the agent by running the `reboot` command.

Agents bundled with Agent for Linux

This procedure applies to agent that are bundeled with Agent for Linux, such as Agent for Proxmox and Agent for Virtuozzo.

1. 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 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="Tdword">"10"</value>
</key>
```

4. Replace `10` with the maximum number of parallel backups that you want to set.
5. Save the file.
6. Run the following command to restart the agent:

```
sudo service acronis_mms restart
```

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

 © Acronis International GmbH, 2003-2026

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 "Recovery of physical machines" (p. 510). When you configure 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, see the following articles:

  Amazon EC2: 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.

© Acronis International GmbH, 2003-2026

Recovery

Recovery cheat sheet

The following table summarizes the available recovery methods.

What to recover	Recovery method
Physical machine (Windows or Linux)	Using the Cyber Protect console Using bootable media
Physical machine (Mac)	Using bootable media
Virtual machine (Such as VMware, Hyper-V, Red Hat Virtualization (oVirt), Scale Computing HC3, or Proxmox)	Using the Cyber Protect console Using bootable media
Virtual machine (Virtuozzo Server, Virtuozzo Infrastructure)	Using the Cyber Protect console
Container (Virtuozzo Server, Proxmox)	Using the Cyber Protect console
ESXi configuration	Using bootable media
Files/Folders	Using the Cyber Protect console Downloading files from the cloud storage Using bootable media Extracting files from local backups
SQL databases	Using the Cyber Protect console
Exchange databases	Using the Cyber Protect console
Exchange mailboxes	Using the Cyber Protect console
Microsoft 365 mailboxes	Using the Cyber Protect console
Oracle databases	Using Oracle Explorer tool

© Acronis International GmbH, 2003-2026

Limitations

- You cannot recover files and folders from disk-level backups of NTFS volumes on which data deduplication is enabled.
- 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.

Cross-platform recovery

You can recover a disk-level backup to a physical machine or to a virtual machine. For example, a disk-level backup is an **Entire machine** backup or a **Disk/volumes** backup that contains the system disk and the boot disk.

Cross-platform recovery (machine migration) is performed in the following cases:

- When you recover a backup of a physical machine to a virtual machine.
- When you recover a backup of a virtual machine to a physical machine.
- When you recover a backup of a virtual machine to a virtual machine on a different type of hypervisor.

Note
If a virtual machine is backed up by a protection agent installed inside the guest operating system, the backup is treated as a physical machine backup.

The following tables summarize the available options for cross-platform recovery according to the backed-up workload.

Physical machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes

© Acronis International GmbH, 2003-2026

Target workload	Supported
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Broadcom (VMware) ESXi virtual machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Microsoft Hyper-V virtual machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes

© Acronis International GmbH, 2003-2026

Target workload	Supported
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Virtuozzo Server virtual machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Virtuozzo Server container

Target workload	Supported
Physical machine	No
Broadcom (VMware) ESXi virtual machine	No

© Acronis International GmbH, 2003-2026

Target workload	Supported
Microsoft Hyper-V virtual machine	No
Virtuozzo Server virtual machine	No
Virtuozzo Server container	Yes
Cyber Frame virtual machine	No
Scale Computing HyperCore virtual machine	No
RHV/oVirt virtual machine	No
Nutanix virtual machine	No
Proxmox virtual machine	No
Proxmox container	No

Cyber Frame virtual machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Scale Computing HyperCore virtual machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes

© Acronis International GmbH, 2003-2026

Target workload	Supported
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Red Hat Virtualization/oVirt virtual machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Nutanix virtual machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes

© Acronis International GmbH, 2003-2026

Target workload	Supported
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Proxmox virtual machine

Target workload	Supported
Physical machine	Yes
Broadcom (VMware) ESXi virtual machine	Yes
Microsoft Hyper-V virtual machine	Yes*
Virtuozzo Server virtual machine	Yes
Virtuozzo Server container	No
Cyber Frame virtual machine	Yes
Scale Computing HyperCore virtual machine	Yes
RHV/oVirt virtual machine	Yes
Nutanix virtual machine	Yes
Proxmox virtual machine	Yes
Proxmox container	No

Proxmox container

Target workload	Supported
Physical machine	No
Broadcom (VMware) ESXi virtual machine	No

© Acronis International GmbH, 2003-2026

Target workload	Supported
Microsoft Hyper-V virtual machine	No
Virtuozzo Server virtual machine	No
Virtuozzo Server container	No
Cyber Frame virtual machine	No
Scale Computing HyperCore virtual machine	No
RHV/oVirt virtual machine	No
Nutanix virtual machine	No
Proxmox virtual machine	No
Proxmox container	Yes

Note
The Secure Boot setting is not backed up. If Secure Boot is enabled on the original machine, the virtual machine recovered as a new machine will not boot. To start the recovered machine, disable Secure Boot in the VM console after recovery.

Note
- * EFI-based machines are recovered as Generation 2 virtual machines.
- * You cannot recover macOS virtual machines to Hyper-V hosts because Hyper-V does not support macOS. You can recover macOS virtual machines to VMware hosts that are installed on Mac hardware.

Cross-platform recovery via bootable media

You can perform a cross-platform recovery by using bootable media.

We recommend that you use bootable media instead of the Cyber Protect console in the following cases:

- Performing a migration that is not natively supported.
  For example, use bootable media to recover a physical machine or a non-Virtuozzo Server virtual machine as a Virtuozzo Server virtual machine on a Virtuozzo host.
- Performing migration of a Linux machine that contains logical volumes (LVM).
  Use Agent for Linux or bootable media to create the backup, and then use bootable media to recover the backup.
- Providing drivers for specific hardware that is critical for the system bootability.
  Build bootable media that can use the required drivers. For more information, see "Bootable Media Builder" (p. 605).

 © Acronis International GmbH, 2003-2026

Recovery of physical machines

You can recover a disk-level backup of a physical machine to another physical machine or to a virtual machine. For example, a disk-level backup is an **Entire machine** backup or a **Disk/volumes** backup that contains the system disk and boot disk.

Limitations

- In the Cyber Protect console, you cannot recover backups of macOS physical machines to another physical machine.
- You cannot recover backups of macOS physical machines to a virtual machine.
- During a recovery to a virtual machine, Cyber Protect stops the target virtual machine without a prompt. After the recovery, you must restart this machine manually. You can change the default behavior in **Recovery options** > **VM power management**.

If you want to recover one of the following, use bootable media instead of the Cyber Protect console:

- A physical machine running macOS.

  Note
  You cannot recover disk-level backups of Intel-based Macs to Macs that use Apple silicon processors, and vice-versa. You can recover files and folders.

- Any operating system to a bare metal machine or to an offline machine.
- The structure of logical volumes. For example, volumes created by Logical Volume Manager in Linux). With the bootable media, you can automatically recreate the logical volume structure.

For more information about recovering machines by bootable media, see "Recovering workloads by using bootable media" (p. 533)

Recovering a physical machine as a physical machine

You can recover a disk-level backup of a physical machine to the original machine or to a new machine.

This procedure describes recovery from the Cyber Protect console. Alternatively, you can use bootable media to recover a backup (including a backup of an offline machine) to a physical machine. For more information, see "Recovering workloads by using bootable media" (p. 533).

To recover a physical machine as a physical machine

1. In the Cyber Protect console, do one of the following:
   - [For online machines] On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).

 © Acronis International GmbH, 2003-2026

Note
The recovery points are filtered by backup storage.

- [For online and offline machines] On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
- [For offline machines] [If the backup location is the cloud storage or a shared storage that other agents can access]
  - On the **Devices** tab, select a backed-up machine, and then click **Recovery**.
  - Click **Select machine**, select a target machine that is online, and then click **OK**.
  - Select a backup (recovery point).

2. Click **Recover** > **Entire machine**.
   A target machine is automatically selected.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. Select an online machine, and then click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. [Optional] Configure the disk mapping between the backed-up machine and the target machine.
   a. [To configure the mapping on a disk level]
      i. Click **Disk mapping**.
      ii. Configure the disk mapping between the backed-up machine and the target machine.
      iii. Click **Done**.
   b. [To configure the mapping on a volume level]
      i. Click **Disk mapping**, and then, in the upper-right corner, click **Switch to volume mapping**.
      ii. Configure the volume mapping between the backed-up machine and the target machine.
      iii. Click **Done**.
7. [Optional] [Only available for Windows machines] To ensure that the recovered data is malware-free, enable the **Safe recovery** switch. For more information, see "Safe recovery" (p. 546).
8. Click **Start recovery**.
9. [Optional] If you prefer to restart the machine manually after the recovery, clear the **Automatically restart the machine, if required** checkbox. For more information, see "Recovery with restart" (p. 540).
10. To confirm that you want to overwrite the disks of the target machine, click **Start recovery**.

You can check the recovery progress in the Cyber Protect console, on the **Activities** tab.

Recovering a physical machine as a virtual machine

You can recover a disk-level backup of a physical machine to a virtual machine. This operation is called cross-platform recovery (machine migration). For more information, see "Cross-platform

 © Acronis International GmbH, 2003-2026

recovery" (p. 503).

Prerequisites

- An agent for the relevant hypervisor is installed in your environment. For example, recovery to a VMware ESXi virtual machine requires Agent for VMware that is installed and registered in the Cyber Protect console.

To recover a physical machine as a virtual machine

The procedures are listed according to the type of the target virtual machine.

VMware ESXi

1. In the Cyber Protect console, do one of the following:
   - [For online machines] On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).

     Note
     The recovery points are filtered by backup storage.

   - [For online and offline machines] On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
   - [For offline machines] [If the backup location is the cloud storage or a shared storage that other agents can access]
     - On the **Devices** tab, select a backed-up machine, and then click **Recovery**.
     - Click **Select machine**, select a target machine that is online, and then click **OK**.
     - Select a recovery point.

     Note
     You can also recover an offline machine by using bootable media. See "Recovering workloads by using bootable media" (p. 533).

2. Click **Recover** > **Entire machine**.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. In **Recover to**, select **Virtual machine**.
5. Select a target machine.
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Broadcom (VMware) ESXi**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]

© Acronis International GmbH, 2003-2026

    i. Select **Existing machine**.
    ii. Select the target machine.
    iii. Click **OK**.
6. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
7. [Optional] [When recovering to a new machine] Configure additional options:
   a. To change the storage for the virtual machine, click **Datastore**, and then select a datastore.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   c. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
      i. Configure the settings.
      ii. Click **OK**.
8. Click **Start recovery**
9. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Hyper-V

1. In the Cyber Protect console, do one of the following:
   - [For online machines] On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).

     Note
     The recovery points are filtered by backup storage.

   - [For online and offline machines] On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
   - [For offline machines] [If the backup location is the cloud storage or a shared storage that other agents can access]
     - On the **Devices** tab, select a backed-up machine, and then click **Recovery**.
     - Click **Select machine**, select a target machine that is online, and then click **OK**.
     - Select a recovery point.

     Note
     You can also recover an offline machine by using bootable media. See "Recovering workloads by using bootable media" (p. 533).

2. Click **Recover** > **Entire machine**.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. In **Recover to**, select **Virtual machine**.
5. Select a target machine.

 © Acronis International GmbH, 2003-2026

a. Click **Target machine**.
b. [If multiple hypervisors are available] Select **Microsoft Hyper-V**.
c. [To perform recovery to a new machine]
   i. Select **New machine**.
   ii. Select a host.
   iii. In **Machine name**, specify a name for the new machine.
   iv. Click **OK**.
d. [To perform recovery to an existing machine]
   i. Select **Existing machine**.
   ii. Select the target machine.
   iii. Click **OK**.

6. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
7. [Optional] [When recovering to a new machine] Configure additional options:
   a. To change the storage for the virtual machine, click **Path**, and then select a storage.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   c. To change the storage, interface, or provisioning mode for each virtual disk, click **Disk mapping**.
      i. In the target disk section, click **Change**.
      ii. Click the gear icon.
      iii. Configure the settings.
      iv. Click **Done**.
   d. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
      i. Configure the settings.
      ii. Click **OK**.
8. Click **Start recovery**
9. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Cyber Frame

1. In the Cyber Protect console, do one of the following:
   - [For online machines] On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).

     Note
     The recovery points are filtered by backup storage.

© Acronis International GmbH, 2003-2026

- [For online and offline machines] On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
- [For offline machines] [If the backup location is the cloud storage or a shared storage that other agents can access]
  - On the **Devices** tab, select a backed-up machine, and then click **Recovery**.
  - Click **Select machine**, select a target machine that is online, and then click **OK**.
  - Select a recovery point.

Note
You can also recover an offline machine by using bootable media. See "Recovering workloads by using bootable media" (p. 533).

2. Click **Recover** > **Entire machine**.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. In **Recover to**, select **Virtual machine**.
5. Select a target machine.
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Cyber Frame**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
6. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
7. [Optional] [When recovering to a new machine] Configure additional options.
   a. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   b. To change the storage policy for the target disk, click **Disk mapping**.
      i. In the target disk section, click **Change**.
      ii. Click the gear icon.
      iii. Select the storage policy for the disk.
      iv. Click **Done**.
   c. To change the network adapters, click **VM settings**.

 © Acronis International GmbH, 2003-2026

i. Configure the settings.
ii. Click **OK**.

8. Click **Start recovery**
9. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Scale Computing HC3

1. In the Cyber Protect console, do one of the following:
   - [For online machines] On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).

     Note
     The recovery points are filtered by backup storage.

   - [For online and offline machines] On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
   - [For offline machines] [If the backup location is the cloud storage or a shared storage that other agents can access]
     - On the **Devices** tab, select a backed-up machine, and then click **Recovery**.
     - Click **Select machine**, select a target machine that is online, and then click **OK**.
     - Select a recovery point.

     Note
     You can also recover an offline machine by using bootable media. See "Recovering workloads by using bootable media" (p. 533).

2. Click **Recover** > **Entire machine**.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. In **Recover to**, select **Virtual machine**.
5. Select a target machine.
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Scale Computing HC3**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
6. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.

 © Acronis International GmbH, 2003-2026

7. [Optional] [When recovering to a new machine] Configure additional options.
   a. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   b. To change the storage container, interface, or provisioning mode for each virtual disk, click **Disk mapping**.
      i. In the target disk section, click **Change**.
      ii. Click the gear icon.
      iii. Configure the settings.
      iv. Click **Done**.
8. Click **Start recovery**
9. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

oVirt

1. In the Cyber Protect console, do one of the following:
   - [For online machines] On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).

     Note
     The recovery points are filtered by backup storage.

   - [For online and offline machines] On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
   - [For offline machines] [If the backup location is the cloud storage or a shared storage that other agents can access]
     - On the **Devices** tab, select a backed-up machine, and then click **Recovery**.
     - Click **Select machine**, select a target machine that is online, and then click **OK**.
     - Select a recovery point.

     Note
     You can also recover an offline machine by using bootable media. See "Recovering workloads by using bootable media" (p. 533).

2. Click **Recover** > **Entire machine**.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. In **Recover to**, select **Virtual machine**.
5. Select a target machine.
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **oVirt**.
   c. [To perform recovery to a new machine]

 © Acronis International GmbH, 2003-2026

i. Select **New machine**.
ii. Select a host.
iii. In **Machine name**, specify a name for the new machine.
iv. Click **OK**.

d. [To perform recovery to an existing machine]
i. Select **Existing machine**.
ii. Select the target machine.
iii. Click **OK**.

6. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
7. [Optional] [When recovering to a new machine] Configure additional options:
   a. To change the storage for the virtual machine, click **Storage domain**, and then select a storage.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
8. Click **Start recovery**
9. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Nutanix

1. In the Cyber Protect console, do one of the following:
   - [For online machines] On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).

     Note
     The recovery points are filtered by backup storage.

   - [For online and offline machines] On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
   - [For offline machines] [If the backup location is the cloud storage or a shared storage that other agents can access]
     - On the **Devices** tab, select a backed-up machine, and then click **Recovery**.
     - Click **Select machine**, select a target machine that is online, and then click **OK**.
     - Select a recovery point.

     Note
     You can also recover an offline machine by using bootable media. See "Recovering workloads by using bootable media" (p. 533).

2. Click **Recover** > **Entire machine**.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.

 © Acronis International GmbH, 2003-2026

4. In **Recover to**, select **Virtual machine**.
5. Select a target machine.
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Nutanix**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
6. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
7. [Optional] [When recovering to a new machine] Configure additional options.
   a. To change the storage for the virtual machine, click **Storage container**, and then select a storage.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   c. To change the storage containerod or interface, click **Disk mapping**.
      i. In the target disk section, click **Change**.
      ii. Click the gear icon.
      iii. Configure the settings.
      iv. Click **Done**.
   d. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
      i. Configure the settings.
      ii. Click **OK**.
8. Click **Start recovery**
9. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Proxmox

1. In the Cyber Protect console, do one of the following:
   - [For online machines] On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).

© Acronis International GmbH, 2003-2026

Note
The recovery points are filtered by backup storage.

- [For online and offline machines] On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
- [For offline machines] [If the backup location is the cloud storage or a shared storage that other agents can access]
  - On the **Devices** tab, select a backed-up machine, and then click **Recovery**.
  - Click **Select machine**, select a target machine that is online, and then click **OK**.
  - Select a recovery point.

Note
You can also recover an offline machine by using bootable media. See "Recovering workloads by using bootable media" (p. 533).

2. Click **Recover** > **Entire machine**.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. In **Recover to**, select **Virtual machine**.
5. Select a target machine.
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Proxmox**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
6. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
7. [Optional] [When recovering to a new machine] Configure additional options:
   a. To change the storage for the virtual machine, click **Storage**, and then select a storage.
   b. To change the disk mapping, disk controller type, disk provisioning mode, or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.

 © Acronis International GmbH, 2003-2026

Note

- To recover a disk as VirtIO type disk, in the recovery options, select NVME.
- During a recovery to a new machine, VDMK disks are recovered as QCOW2 disks or RAW disks (if you change the provisioning type to thick).

c. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
   i. Configure the settings.
   ii. Click **OK**.

8. Click **Start recovery**
9. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

You can check the recovery progress in the Cyber Protect console, on the **Activities** tab.

Recovery of virtual machines

You can recover a disk-level backup of a virtual machine to a physical machine or another virtual machine. For example, a disk-level backup is an **Entire machine** backup or a **Disk/volumes** backup that contains the system disk and boot disk.

Limitations

- During a recovery to a virtual machine, Cyber Protect stops the target virtual machine without a prompt. After the recovery, you must restart this machine manually. You can change the default behavior in **Recovery options** > **VM power management**.
- You can recover a backup of a virtual machine to a physical machine if the disk configuration of the target machine exactly matches the disk configuration in the backup. Alternatively, you can perform a virtual-to-physical migration by using bootable media. See "Recovering workloads by using bootable media" (p. 533).
- 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.

Recovering a virtual machine as a physical machine

You can recover a disk-level backup of a virtual machine to a physical machine. This operation is called cross-platform recovery (machine migration). For more information, see "Cross-platform recovery" (p. 503).

The following procedure describes recovery from the Cyber Protect console. Alternatively, you can use bootable media to recover a backup of a virtual machine to a physical machine. For more information, see "Recovering workloads by using bootable media" (p. 533).

To recover a virtual machine as a physical machine

 © Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. In **Recover to**, select **Physical machine**.

   A target machine is automatically selected.
5. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. Select an online machine, and then click **OK**.
6. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
7. [Optional] Configure the disk mapping between the backed-up machine and the target machine.
   a. [To configure the mapping on a disk level]
      i. Click **Disk mapping**.
      ii. Configure the disk mapping between the backed-up machine and the target machine.
      iii. Click **Done**.
   b. [To configure the mapping on a volume level]
      i. Click **Disk mapping**, and then, in the upper-right corner, click **Switch to volume mapping**.
      ii. Configure the volume mapping between the backed-up machine and the target machine.
      iii. Click **Done**.

   Note
   You can select individual disks or volumes for recovery. Ensure that the disk or volume configuration of the backed-up machine matches exactly the disk or volume configuration of the target machine.

8. [Optional] [Only available for Windows machines] To ensure that the recovered data is malware-free, enable the **Safe recovery** switch. For more information, see "Safe recovery" (p. 546).
9. Click **Start recovery**
10. [Optional] If you prefer to restart the machine manually after the recovery, clear the **Automatically restart the machine, if required** checkbox. For more information, see "Recovery with restart" (p. 540).
11. To confirm that you want to overwrite the disks of the target machine, click **Start recovery**.

You can check the recovery progress in the Cyber Protect console, on the **Activities** tab.

© Acronis International GmbH, 2003-2026

Recovering a virtual machine as a virtual machine

You can recover a backup of a virtual machine to the original hypervisor or to a different type of hypervisor. Recovery to a different type of hypervisor is called cross-platform recovery (machine migration). For more information, see "Cross-platform recovery" (p. 503).

Recovering to a virtual machine on which a protection agent is not installed is done on the hypervisor level. This is an agentless recovery.

Recovery to a virtual machine on which a protection agent is installed is an agent-based recovery. This type of recovery is the same as a recovery to a physical machine.

Prerequisites

- An agent for the relevant hypervisor is installed in your environment. For example, recovery to a VMware ESXi virtual machine requires Agent for VMware that is installed and registered in the Cyber Protect console.

To recover a virtual machine as a virtual machine

The procedures are listed according to the type of the target virtual machine.

VMware ESXi

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.

   The original virtual machine is selected as a target machine.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **VMware ESXi**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.

 © Acronis International GmbH, 2003-2026

6. [Optional] [When recovering to a new machine] Configure additional options:
   a. To change the storage for the virtual machine, click **Datastore**, and then select a datastore.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   c. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
      i. Configure the settings.
      ii. Click **OK**.
7. Click **Start recovery**
8. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Hyper-V

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original virtual machine is selected as a target machine.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Microsoft Hyper-V**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. [Optional] [When recovering to a new machine] Configure additional options:
   a. To change the storage for the virtual machine, click **Path**, and then select a storage.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.

© Acronis International GmbH, 2003-2026

    i. Configure the disk mapping or select the disks that you want to recover.
    ii. Click **Done**.
  c. To change the storage, interface, or provisioning mode for each virtual disk, click **Disk mapping**.
    i. In the target disk section, click **Change**.
    ii. Click the gear icon.
    iii. Configure the settings.
    iv. Click **Done**.
  d. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
    i. Configure the settings.
    ii. Click **OK**.
7. Click **Start recovery**
8. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Virtuozzo

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original virtual machine is selected as a target machine.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
  a. Click **Target machine**.
  b. [If multiple hypervisors are available] Select **Virtuzzo**.
  c. [To perform recovery to a new machine]
    i. Select **New machine**.
    ii. Select a host.
    iii. In **Machine name**, specify a name for the new machine.
    iv. Click **OK**.
  d. [To perform recovery to an existing machine]
    i. Select **Existing machine**.
    ii. Select the target machine.
    iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. [Optional] [When recovering to a new machine] Configure additional options:

© Acronis International GmbH, 2003-2026

a. To change the storage for the virtual machine, click **Path**, and then select a storage.
b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
   i. Configure the disk mapping or select the disks that you want to recover.
   ii. Click **Done**.
c. To change the storage, interface, or provisioning mode for each virtual disk, click **Disk mapping**.
   i. In the target disk section, click **Change**.
   ii. Click the gear icon.
   iii. Configure the settings.
   iv. Click **Done**.
d. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
   i. Configure the settings.
   ii. Click **OK**.

7. Click **Start recovery**
8. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Cyber Frame

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original virtual machine is selected as a target machine.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Cyber Frame**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.

© Acronis International GmbH, 2003-2026

5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. [Optional] [When recovering to a new machine] Configure additional options.
   a. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   b. To change the storage policy for the target disk, click **Disk mapping**.
      i. In the target disk section, click **Change**.
      ii. Click the gear icon.
      iii. Select the storage policy for the disk.
      iv. Click **Done**.
   c. To change the network adapters, click **VM settings**.
      i. Configure the settings.
      ii. Click **OK**.
7. Click **Start recovery**
8. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Scale Computing HC3

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original virtual machine is selected as a target machine.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Scale Computing HC3**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.

© Acronis International GmbH, 2003-2026

6. [Optional] [When recovering to a new machine] Configure additional options.
   a. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   b. To change the storage container, interface, or provisioning mode for each virtual disk, click **Disk mapping**.
      i. In the target disk section, click **Change**.
      ii. Click the gear icon.
      iii. Configure the settings.
      iv. Click **Done**.
7. Click **Start recovery**
8. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

oVirt

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original virtual machine is selected as a target machine.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **oVirt**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. [Optional] [When recovering to a new machine] Configure additional options:
   a. To change the storage for the virtual machine, click **Storage domain**, and then select a storage.

© Acronis International GmbH, 2003-2026

b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
   i. Configure the disk mapping or select the disks that you want to recover.
   ii. Click **Done**.
7. Click **Start recovery**
8. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Nutanix

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original virtual machine is selected as a target machine.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Nutanix**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. [Optional] [When recovering to a new machine] Configure additional options.
   a. To change the storage for the virtual machine, click **Storage container**, and then select a storage.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   c. To change the storage containerod or interface, click **Disk mapping**.
      i. In the target disk section, click **Change**.
      ii. Click the gear icon.

© Acronis International GmbH, 2003-2026

iii. Configure the settings.
iv. Click **Done**.

d. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
   i. Configure the settings.
   ii. Click **OK**.

7. Click **Start recovery**
8. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

Proxmox

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up machine, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original virtual machine is selected as a target machine.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target machine:
   a. Click **Target machine**.
   b. [If multiple hypervisors are available] Select **Proxmox**.
   c. [To perform recovery to a new machine]
      i. Select **New machine**.
      ii. Select a host.
      iii. In **Machine name**, specify a name for the new machine.
      iv. Click **OK**.
   d. [To perform recovery to an existing machine]
      i. Select **Existing machine**.
      ii. Select the target machine.
      iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. [Optional] [When recovering to a new machine] Configure additional options:
   a. To change the storage for the virtual machine, click **Storage**, and then select a storage.
   b. To change the disk mapping, disk controller type, disk provisioning mode, or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.

© Acronis International GmbH, 2003-2026

Note

- To recover a disk as VirtIO type disk, in the recovery options, select NVME.
- During a recovery to a new machine, VDMK disks are recovered as QCOW2 disks or RAW disks (if you change the provisioning type to thick).

c. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **VM settings**.
   i. Configure the settings.
   ii. Click **OK**.

7. Click **Start recovery**
8. [When recovering to an existing machine] To confirm that you want to overwrite the target machine, click **Start recovery**.

You can check the recovery progress in the Cyber Protect console, on the **Activities** tab.

Recovering containers

You can recover a backed-up container to the original container or to a new container on the same hypervisor.

Cross-platform recovery is not supported for containers.

To recover a container

Virtuozzo container

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up container, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original container is selected as a target container.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target container:
   a. Click **Target container**.
   b. [If multiple hypervisors are available] Select **Virtuozzo**.
   c. [To perform recovery to a new container]
      i. Select **New container**.
      ii. Select a host.
      iii. In **Container name**, specify a name for the new container.
      iv. Click **OK**.
   d. [To perform recovery to an existing container]

© Acronis International GmbH, 2003-2026

    i. Select **Existing container**.
    ii. Select the target container.
    iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. [Optional] [When recovering to a new container] Configure additional options:
   a. To change the storage for the virtual machine, click **Storage**, and then select a storage.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   c. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **Container settings**.
      i. Configure the settings.
      ii. Click **OK**.
7. Click **Start recovery**
8. [When recovering to an existing container] To confirm that you want to overwrite the target container, click **Start recovery**.

Proxmox container

1. In the Cyber Protect console, do one of the following:
   - On the **Devices** tab, select a backed-up container, click **Recovery**, and then select a backup (recovery point).
   - On the **Backup storage** tab, select a backup archive, and then select a backup (recovery point).
2. Click **Recover** > **Entire machine**.
   The original container is selected as a target container.
3. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
4. [Optional] To change the target container:
   a. Click **Target container**.
   b. [If multiple hypervisors are available] Select **Proxmox**.
   c. [To perform recovery to a new container]
      i. Select **New container**.
      ii. Select a host.
      iii. In **Container name**, specify a name for the new container.
      iv. Click **OK**.
   d. [To perform recovery to an existing container]
      i. Select **Existing container**.
      ii. Select the target container.
      iii. Click **OK**.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.

© Acronis International GmbH, 2003-2026

6. [Optional] [When recovering to a new container] Configure additional options:
   a. To change the storage for the virtual machine, click **Storage**, and then select a storage.
   b. To change the disk mapping or exclude some of the backed-up disks from the recovery, click **Disk mapping**.
      i. Configure the disk mapping or select the disks that you want to recover.
      ii. Click **Done**.
   c. To change the memory size, the number of virtual processors, or the network connections of the target machine, click **Container settings**.
      i. Configure the settings.
      ii. Click **OK**.
7. Click **Start recovery**
8. [When recovering to an existing container] To confirm that you want to overwrite the target container, click **Start recovery**.

You can check the recovery progress in the Cyber Protect console, on the **Activities** tab.

Recovering workloads by using bootable media

You can recover a workload by using bootable media in the following ways:

- Locally, on the recovered workload.
  For more information, see "Recovering backups by using bootable media locally" (p. 571).
- Remotely, with bootable media that is registered in the Cyber Protect console.
  For more information, see "Recovering backups by using bootable media remotely" (p. 602).

You can use ready-made bootable media or create your own bootable media. For more information, see "Creating bootable media" (p. 533).

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:

 © Acronis International GmbH, 2003-2026

- 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 files

Recovering files by using the Cyber Protect console

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, see "File filters"

   Note
   Search is not available for disk-level backups that are stored in the cloud storage.

© Acronis International GmbH, 2003-2026

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.

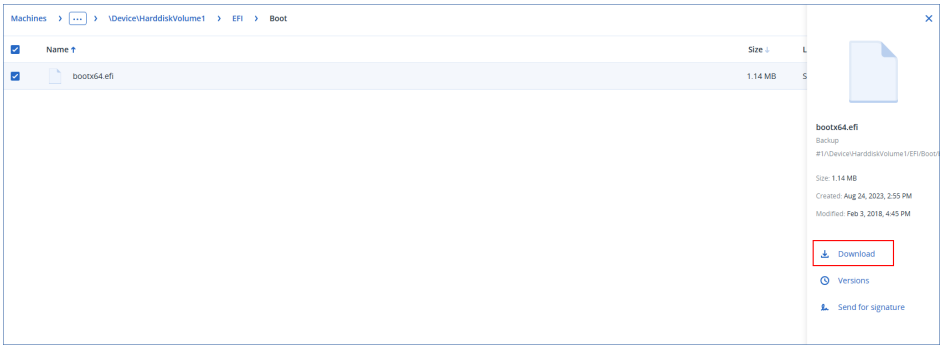
© Acronis International GmbH, 2003-2026

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**.



Downloading large files

Errors might occur when downloading large files from backups.

If the error `0x1c0000b: Cannot download because it is not a file.` occurs, increase the `write_timeout` value in the `api_gateway.json` file, and then try downloading the file again.

To increase the `write_timeout` value

1. On the machine running the management server, open the following configuration file with a text editor:
   - In Windows: `%ProgramData%\Acronis\ApigGateway\api_gateway.json`
   - In Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
2. Locate the `write_timeout` line, and then add a zero (0) at the end of the value.

Note
This value specifies the timeout in nanoseconds.

3. Save the `api_gateway.json` file.
4. Restart Acronis Service Manager Service as described in "Allowing only HTTPS connections to the web console" (p. 235).

Note
Use the procedure that corresponds to the operating system where the management server runs.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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, see "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.

© Acronis International GmbH, 2003-2026

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 ESXi configuration

To recover an ESXi configuration, you need Linux-based bootable media. For information about how to create bootable media, see "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**.

© Acronis International GmbH, 2003-2026

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 with restart

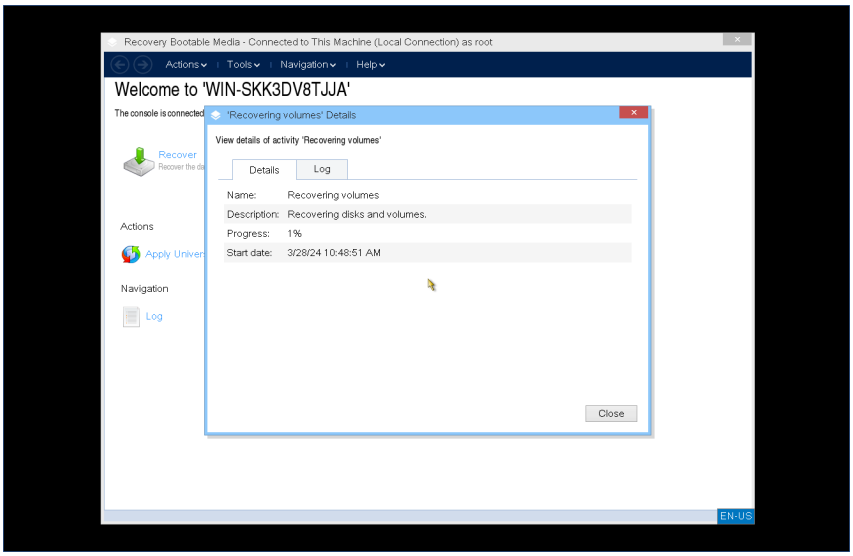
A restart is required when you recover the following:

- An operating system
  For example, when you recover an entire machine or the system volume of a machine.
- Encrypted volumes
  For example, when you recover BitLocker-encrypted or CheckPoint-encrypted volumes.

Important
Backed-up encrypted volumes are recovered as non-encrypted.

A recovery environment is automatically prepared on the recovered machine. When the environment is ready, the machine restarts, and then the recovery environment opens. When the recovery completes, the operating system starts.

© Acronis International GmbH, 2003-2026



Note

Preparing the WinRE recovery environment might take up to three minutes.

For more information about the available recovery environments, see "Recovery environments" (p. 541).

Recovery environments

You can use WinRE or Linux recovery environment.

The table below summarizes the available options.

Recovered machine	Recovery environment	
	WinRE	Linux
Windows	Yes	Yes (Default)
Linux	N/A	Yes

Disk space requirements

The recovery environment requires disk space for temporary files. The requirements vary depending on the recovered machine.

The table below summarizes the available options.

Recovery environment	Boot mode	Machine with non-encrypted system volume	Machine with encrypted system volume
WinRE	BIOS	1 GB in the `Windows\Temp` folder	1 GB in the `Windows\Temp` folder
	UEFI	1 GB in the `Windows\Temp` folder	1 GB in the `Windows\Temp` folder

© Acronis International GmbH, 2003-2026

Recovery environment	Boot mode	Machine with non-encrypted system volume	Machine with encrypted system volume
Linux*	BIOS	200 MB on the system volume	400 MB on an unencrypted volume
	UEFI	200 MB on the EFI system partition (ESP)	One of the following: • 400 MB on the EFI system partition (ESP) • 200 MB on the EFI system partition (ESP) and 200 MB on an unencrypted partition that is accessible during the boot process

* Recovery of a machine with encrypted system volume requires at least one non-encrypted volume on the same machine.

Limitations

- Before recovery, you must lock all encrypted non-system volumes. You can lock a volume by opening a file that resides on it. If the volume is not locked, the recovery will continue without restart, and the volume might not be recognized by the operating system.

  You do not need to lock an encrypted system volume.

Troubleshooting

If a recovery fails and the error `Cannot get file from partition` is shown after restart, disable Secure Boot. For more information, see Disabling Secure Boot in the Microsoft documentation.

Changing the recovery environment

You can change the default recovery environment on Windows workloads.

On Linux workloads, only the Linux recovery environment is available.

To set WinRE

1. In Windows, open **Regedit**.
2. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Create a new string value, and then name it **RebootEnvironmentType**.
4. Open the string value for editing.
5. In **Value data**, specify `Windows`.
6. Click **OK**.

To set Linux

© Acronis International GmbH, 2003-2026

1. In Windows, open **Regedit**.
2. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Create a new string value, and then name it **RebootEnvironmentType**.
4. Open the string value for editing.
5. In **Value data**, specify `Linux`.
6. Click **OK**.

To reset the default settings

1. In Windows, open **Regedit**.
2. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
3. Delete the **RebootEnvironmentType** string value.
4. To confirm your choice, click **Yes**.

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

 © Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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:

© Acronis International GmbH, 2003-2026

- 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.

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 Continous 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.

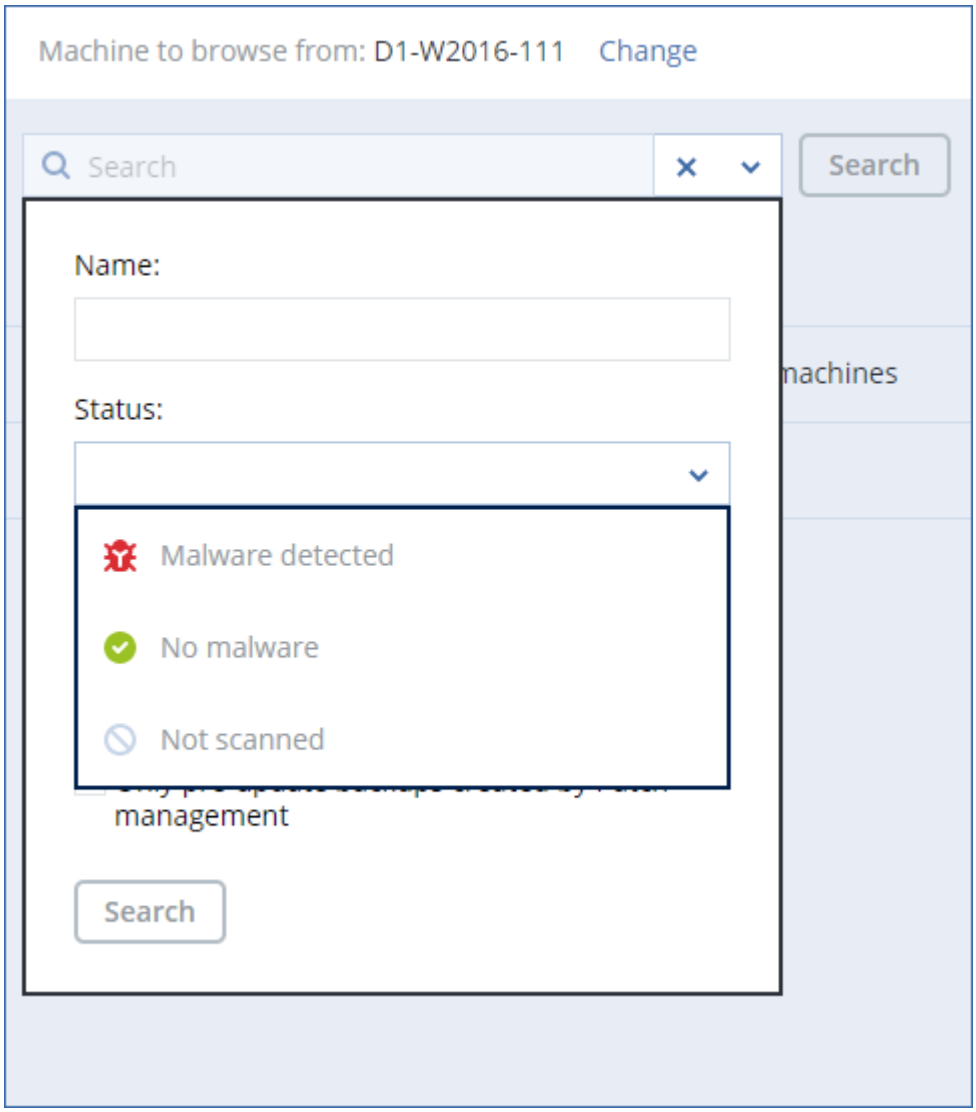
How it works

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.

© Acronis International GmbH, 2003-2026



Automatic domain rejoin

You can automatically join a recovered Windows workload to an Active Directory domain.

Limitations

- Automatic domain rejoin is supported for physical and virtual machines on which a protection agent is installed. Virtual machines that are recovered from agentless backups cannot automatically rejoin a domain.
- Automatic domain rejoin is not available on the machine where the management server is installed, even if a protection agent is also installed on the same machine.
- Automatic domain rejoin is supported by the following agents:
  - Agent for Windows version 16 Update 4 or later.
  - WinRE-based bootable media that is registered on the management server and is used in the Cyber Protect console. The bootable media must be created with Acronis Cyber Protect 16 Update 4 or later.

© Acronis International GmbH, 2003-2026

- The version of the agents that perform the following operations must be 16 Update 4 or later:
  - The agent that creates the backup.

    This agent creates a backup that supports automatic domain rejoin.
  - The agent that recovers the backup.

    This agent verifies the specified domain credentials, so that the recovered workload could rejoin the Active Directory domain.
  - The agent on the recovered workload.

    This agent joins the workload to the Active Directory domain after the recovery completes.

  These operations might be performed by a single agent. For example, the protection agent that is installed on the backed-up workload recovers the workload, and then joins it to an Active Directory domain. In other scenarios, these operations might be performed by different agents. For example, a bootable media recovers a workload, and then the agent on the recovered workload joins it to an Active Directory domain.

For more information about configuring the automatic domain rejoin, see:

- When recovering a workload with a protection agent: "Recovery of physical machines" (p. 510).
- When recovering a workload with bootable media: "Recovering backups by using bootable media remotely" (p. 602).

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

 © Acronis International GmbH, 2003-2026

Backup validation	+	+	+	+	+	+	+	+	+
Boot mode	+	-	-	-	-	-	-	+	-
Date and time for files	-	-	-	+	+	+	+	-	-
Error handling	+	+	+	+	+	+	+	+	+
File exclusions	-	-	-	+	+	+	+	-	-
File-level security	+	+	-	+	+	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
Full path recovery	-	-	-	+	+	+	+	-	-
Mount points	-	-	-	+	-	-	-	-	-
Performance	+	+	-	+	+	+	-	+	+
Pre/post commands	+	+	-	+	+	+	-	+	+
SID changing	+	-	-	-	-	-	-	-	-
VM power management	-	-	-	-	-	-	-	+	-
"Tape management" (p. 556) > Use a disk cache to	-	-	-	+	+	+	-	-	-

© Acronis International GmbH, 2003-2026

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:

 © Acronis International GmbH, 2003-2026

- **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.

© Acronis International GmbH, 2003-2026

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 applicable when recovering files from disk-level and file-level backups of volumes formatted with file systems that support permissions. Examples include NTFS and ReFS on

 © Acronis International GmbH, 2003-2026

Windows, and ext4, XFS, JFS, ReiserFS, and F2FS on Linux.

This option defines whether to recover file permissions for the recovered files.

The preset is: **Enabled**.

If this option is enabled, the original file permissions (such as NTFS ACLs on Windows or POSIX permissions on Linux) are recovered. If this option is disabled, the files inherit the permissions from the folder to which they are recovered.

File systems that do not support permissions, such as FAT16, FAT32, and exFAT, are not supported by this option.

Important
File permissions cannot be recovered when the backup is stored on an SMB network share and the files are recovered to a different location. This is because SMB shares do not fully support the file permission attributes that are required for this option.

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.

 © Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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

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

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

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

© Acronis International GmbH, 2003-2026

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**.

© Acronis International GmbH, 2003-2026

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 psee 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.

© Acronis International GmbH, 2003-2026

Disaster recovery

This feature is available only in cloud deployments of Acronis Cyber Protect. For a detailed description of this functionality, please see https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html.

© Acronis International GmbH, 2003-2026

Bootable media

Important
Some of the features described in this section are only available for on-premises deployments.

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, Windows Preinstallation Environment (WinPE), or Windows Recovery Environment (WinRE), 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 a bare metal machine
- Create basic or dynamic volumes on a bare metal machine
- 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 Windows-based) for Windows, Linux or macOS computers. For a fully-featured bootable media, you must 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.

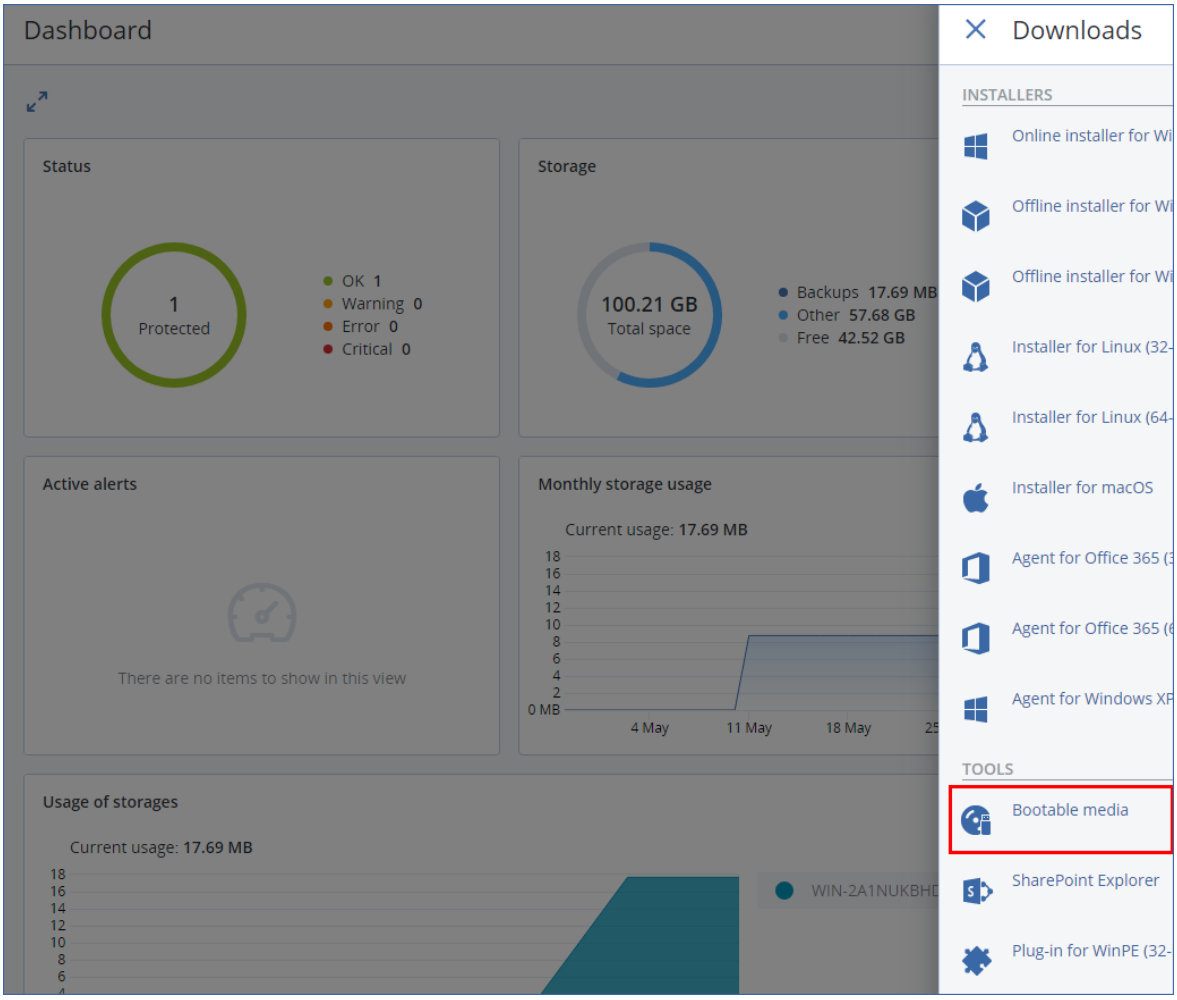
© Acronis International GmbH, 2003-2026

Note

The ready-made bootable media does not support storage node, tape locations, or SFTP locations. If you want to use these storage locations in your on-premises deployment, you must create your own bootable media by using the Bootable Media Builder. See this knowledge base article.

To download a ready-made bootable media

1. In the Cyber Protect 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 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**.

© Acronis International GmbH, 2003-2026

3. On the page that opens, locate **Additional downloads**, and then click **Bootable Media ISO (for Windows and Linux)**.

Linux-based or Windows-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 console.

A list of the hardware supported by Linux-based media is available in this knowledge base article.

Windows-based

Windows-based bootable media contains either a Windows Recovery Environment (WinRE) or Windows Preinstallation Environment (WinPE) and Acronis Plugin for WinPE, which is a modification of the protection agent that can run in the preinstallation environment.

Windows-based media proved to be the most convenient bootable solution in large environments with heterogeneous hardware.

Advantages:

- Windows-based bootable media provides more functionality than the Linux-based bootable media. For example, 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.

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:

- 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

© Acronis International GmbH, 2003-2026

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.

- The bootable media with Linux-like volume representation shows local disks and volumes as unmounted (sda1, sda2...).
- 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.
- 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**.
- Tasks cannot be scheduled. If you need to repeat an operation, configure it from scratch.
- The log lifetime is limited to the current session. You can save the entire log or the filtered log entries to a file.
- 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.

Creating backups by using bootable media locally

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 creating a bootable media, see Linux-based bootable media or Windows-based bootable media, respectively.

Running the bootable media requires 1.5 GB of RAM.

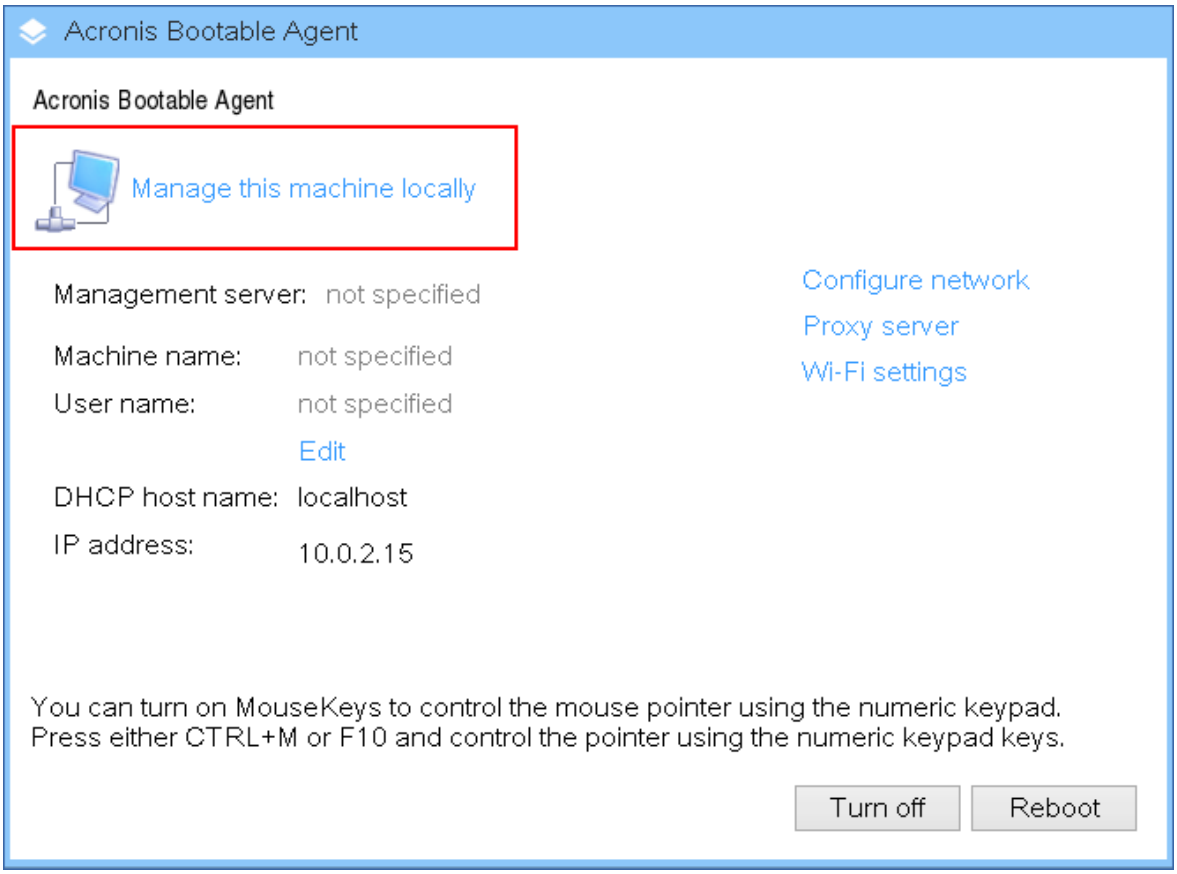
To back up data with bootable media

© Acronis International GmbH, 2003-2026

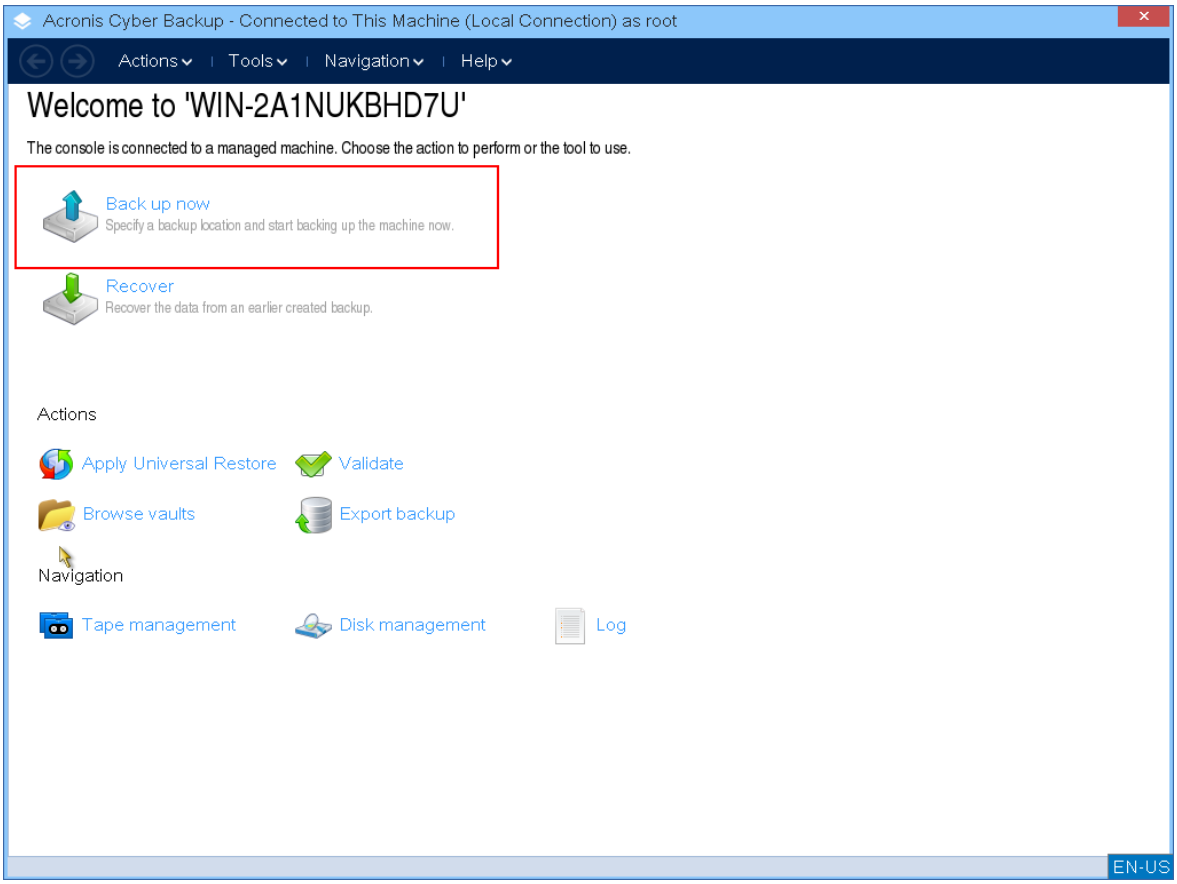
1. Boot from Acronis bootable rescue media.

2. To back up the local machine, click **Manage this machine locally**. For remote connections, see "Registering bootable media on the management server" (p. 601).

© Acronis International GmbH, 2003-2026



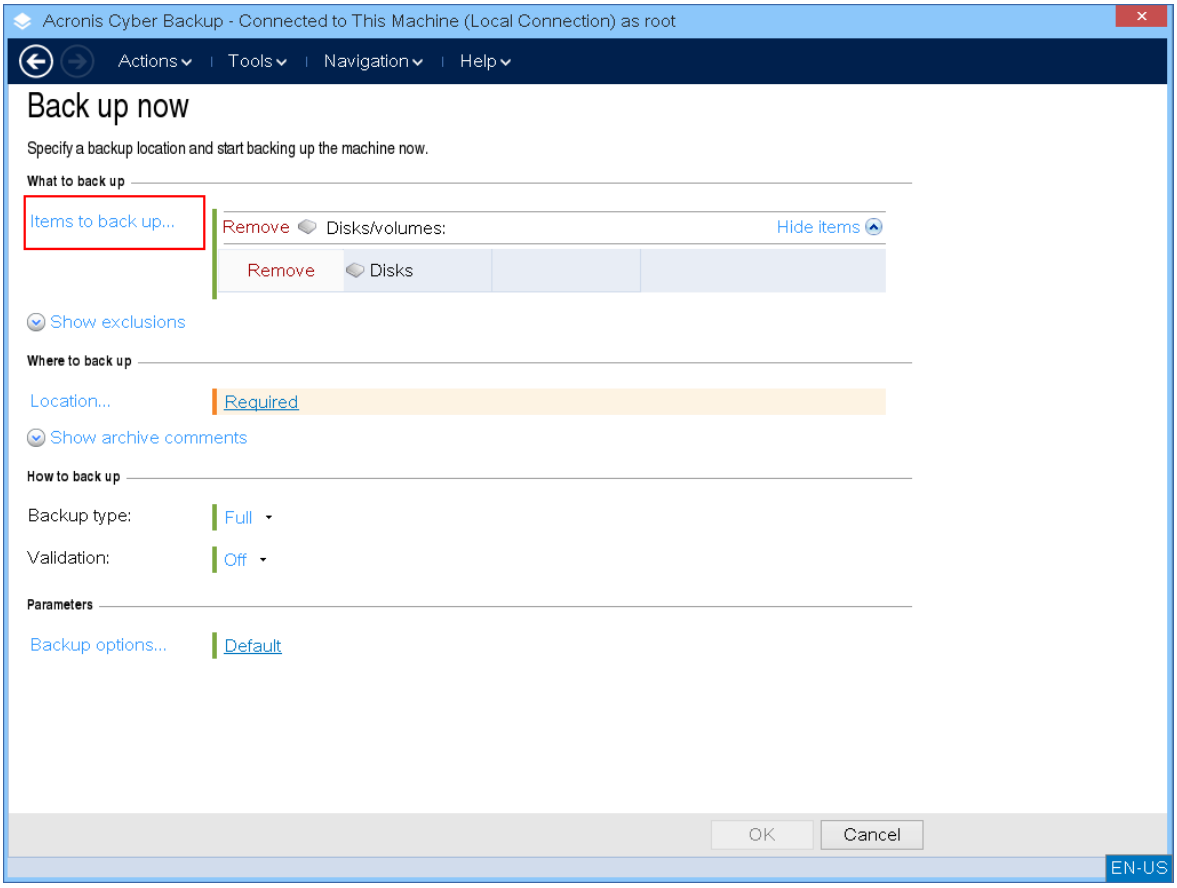
3. Click **Back up now**.



© Acronis International GmbH, 2003-2026

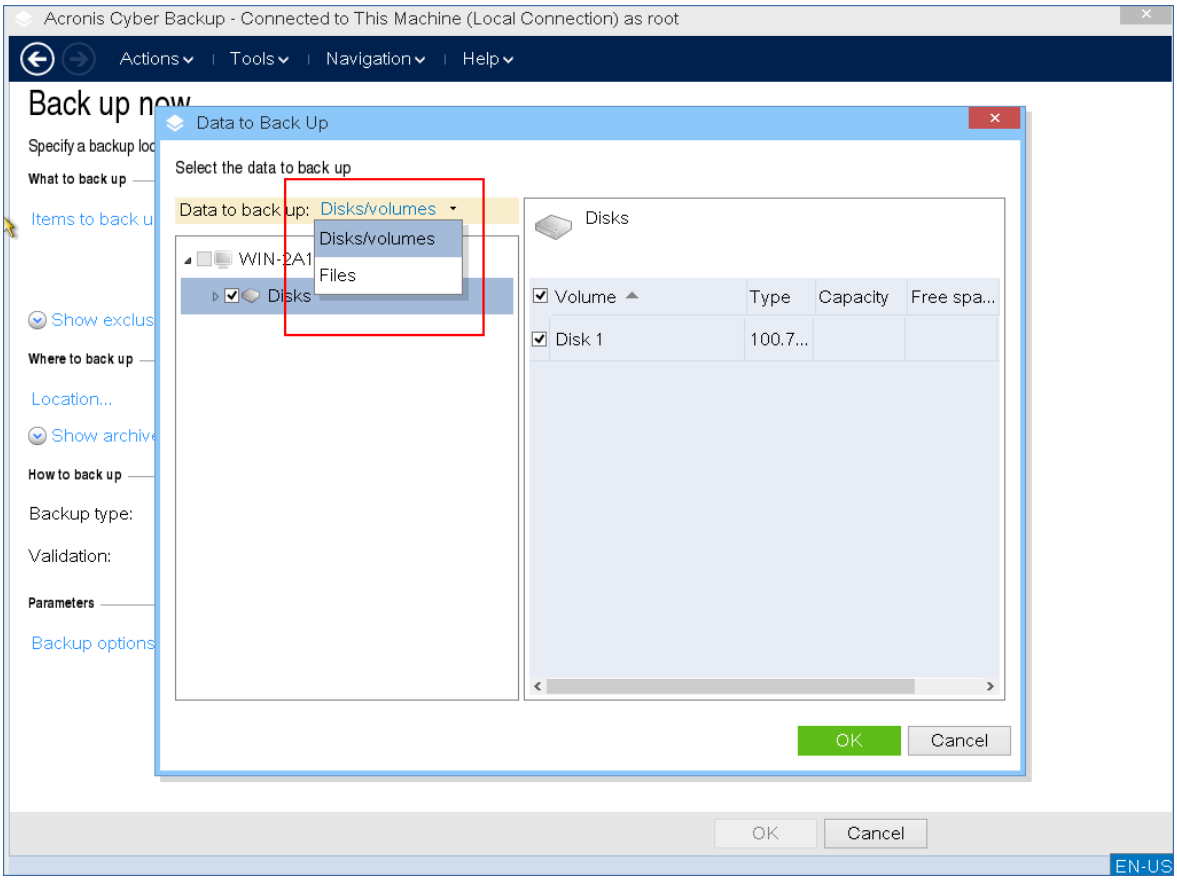
4. All non-removable disks of the machine are automatically selected for backup. To change the data that will be backed up, click **Items to backup**, and then select the desired disks or volumes. When selecting data to back up, you may see the following message: "*This machine cannot be selected directly. 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.



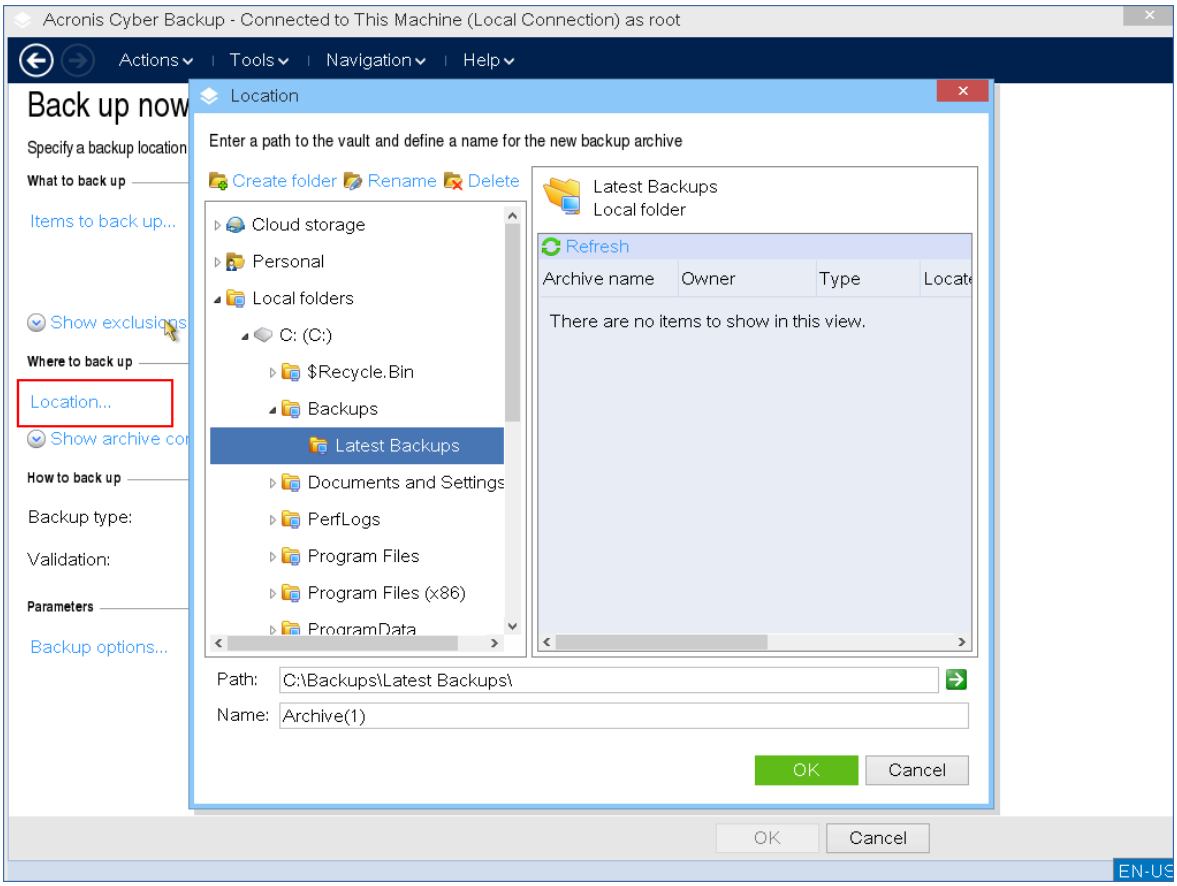
5. If you need to back up files or folders instead of disks, switch to **Files** in **Data to back up**. Only disk/partition and file/folder backup are available under bootable media. Other types of backups, such as database backup, are only available under the running operating system.

© Acronis International GmbH, 2003-2026



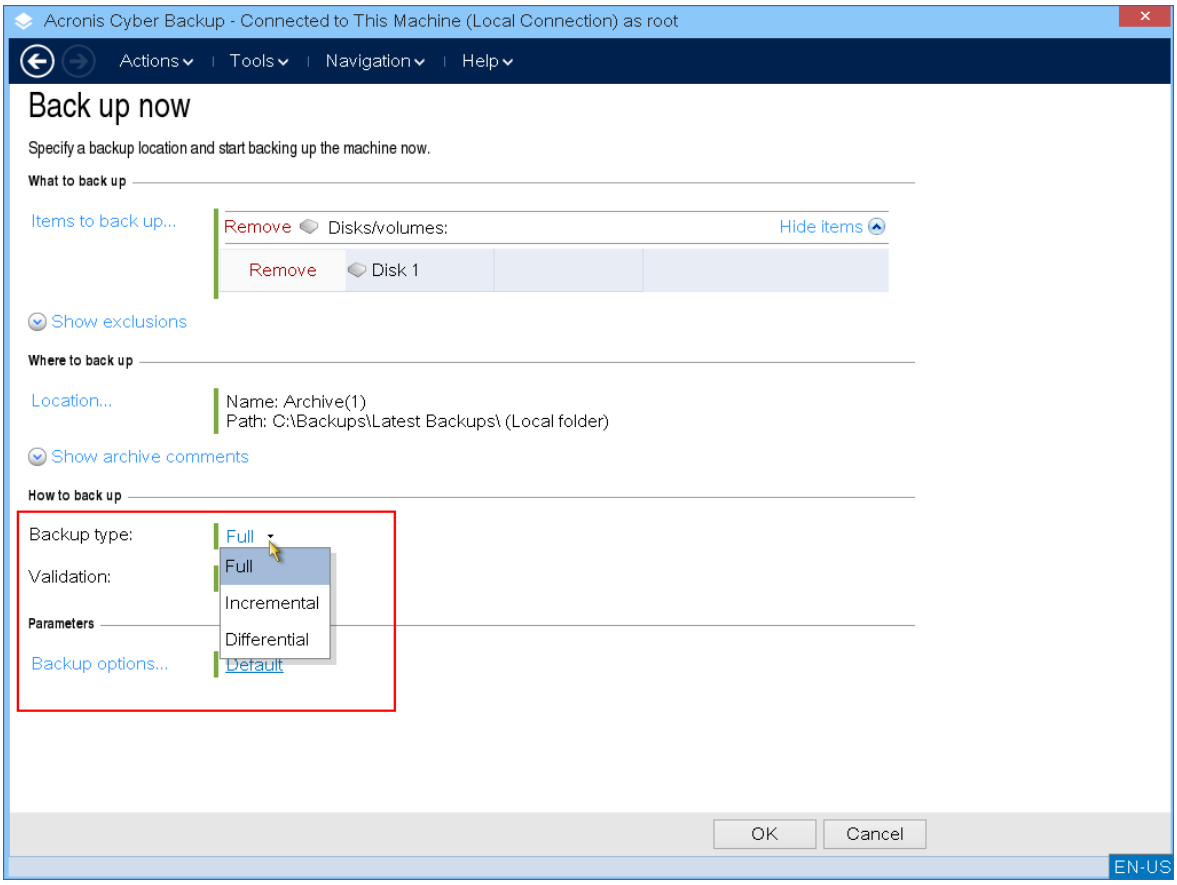
6. Click **Location** to select where the backup will be saved.

© Acronis International GmbH, 2003-2026



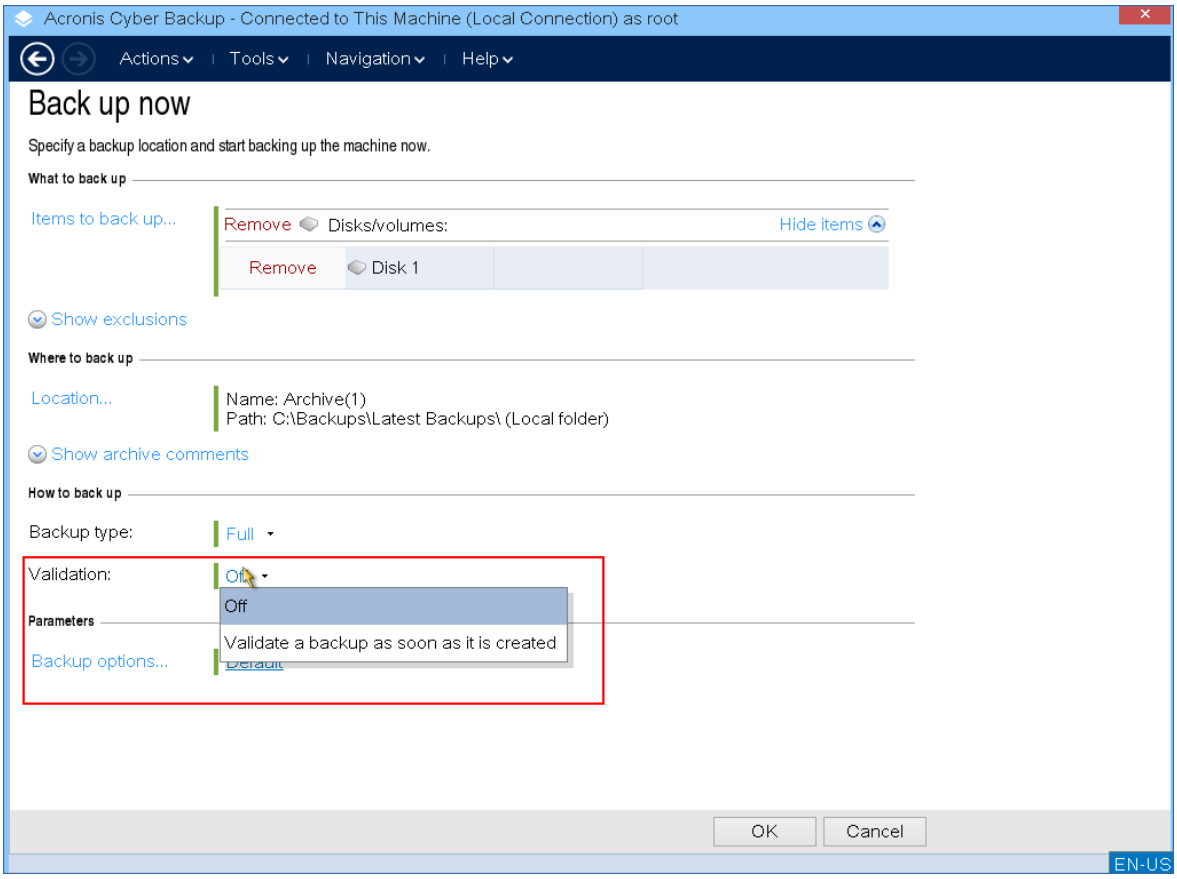
7. Specify the location and name for your backup.
8. Specify the backup type. If this is the first backup in this location, a full backup will be created. If you continue a chain of backups, you can select **Incremental** or **Differential**, to save space. For more information about the backup types, see this knowledge base article.

© Acronis International GmbH, 2003-2026



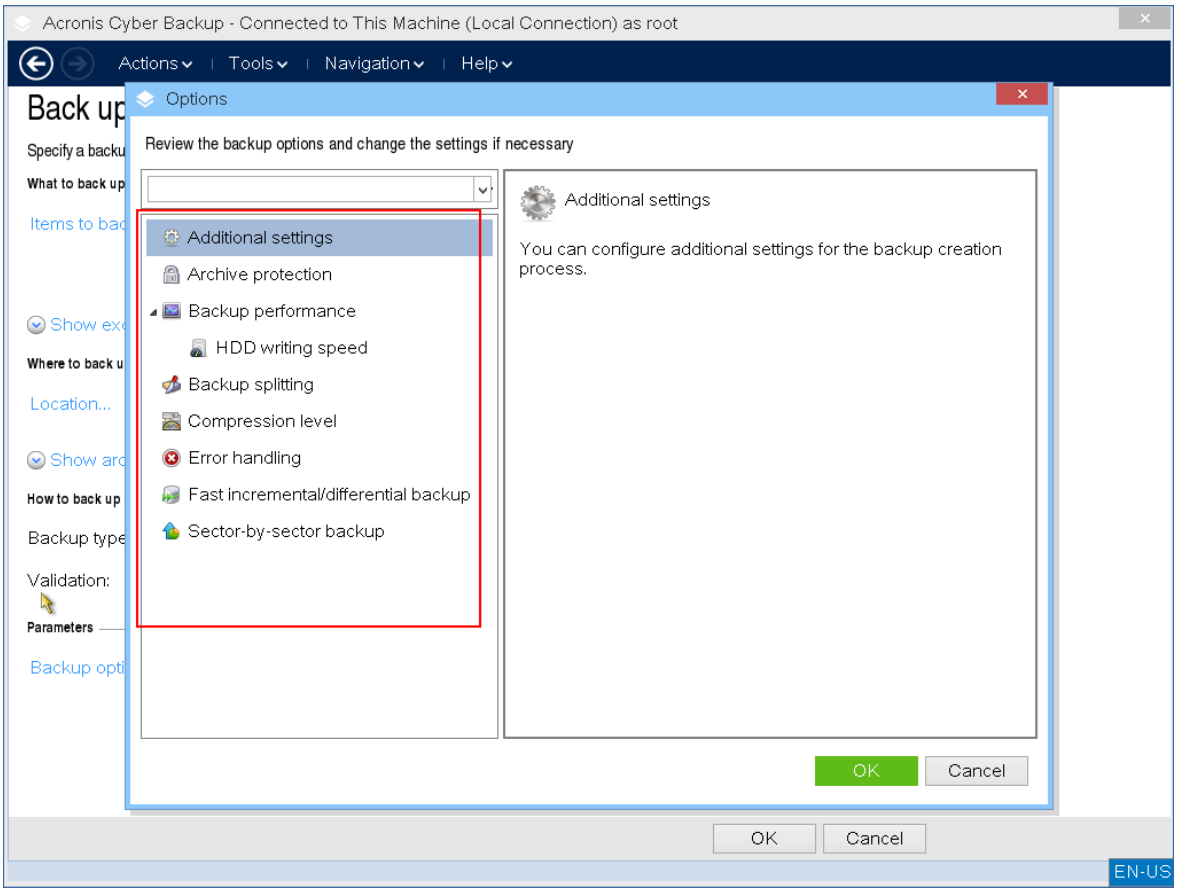
9. [Optional] If you want to validate the backup file, select **Validate a backup as soon as it is created**.

© Acronis International GmbH, 2003-2026



10. [Optional] Specify the backup options that you might need – such as password for the backup file, backup splitting, or error handling.

© Acronis International GmbH, 2003-2026

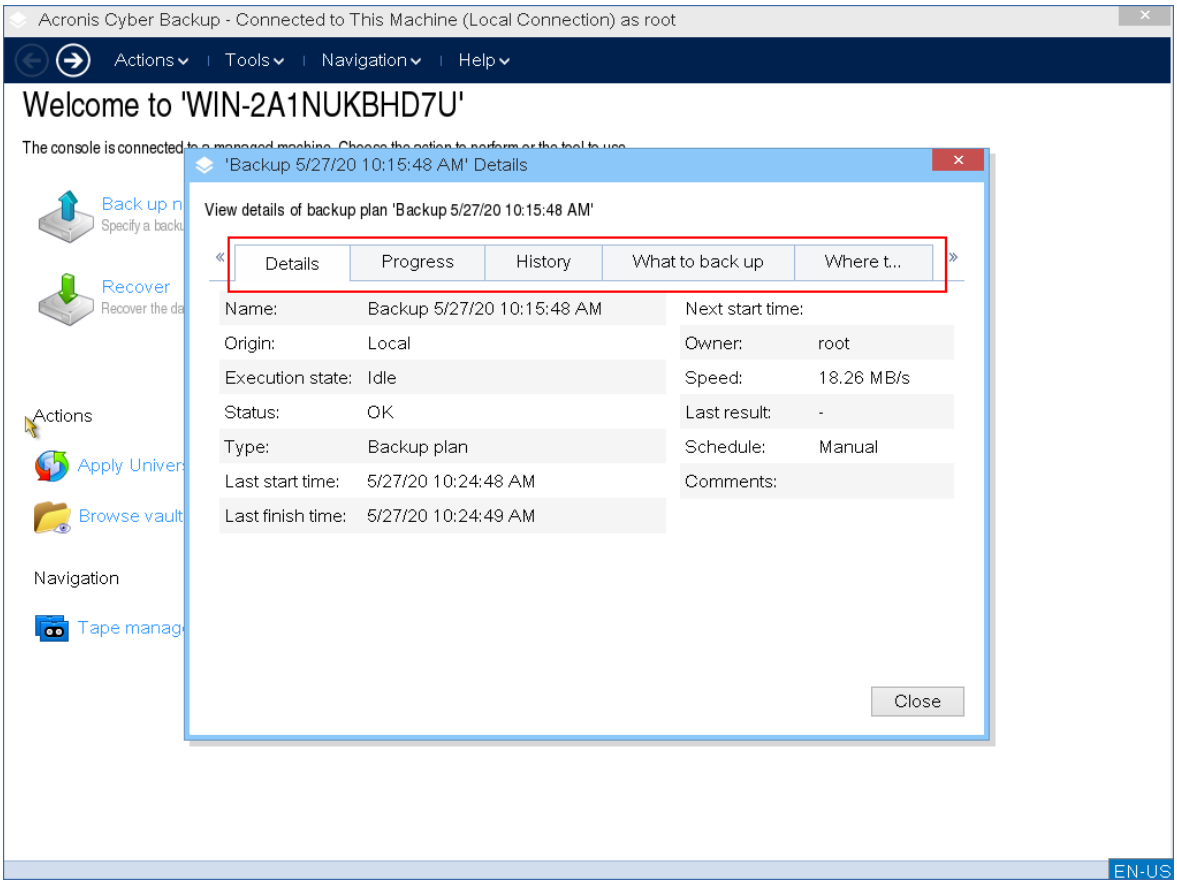


11. Click **OK** to start the backup.

    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.

© Acronis International GmbH, 2003-2026



Recovering backups by using bootable media locally

This procedure applies to Linux-based and Windows-based bootable media that are used locally, on the recovered workload.

For more information about using registered bootable media in the Cyber Protect console, see "Recovering backups by using bootable media remotely" (p. 602).

Running the bootable media requires 1.5 GB of RAM.

Prerequisites and limitations

- When recovering APFS-formatted volumes to a non-original machine or to bare metal, manually recreate the original disk configuration, by using Apple's **Disk Utility**. For more information, see https://support.apple.com/guide/disk-utility/welcome.

  Note
  Starting with macOS 11 Big Sur, **System volume** cannot be backed up and recovered. To recover a bootable macOS system, you must recover **Data volume**, and then install macOS on it.

- You cannot access the backup locations on Acronis Cyber Infrastructure with bootable media that is run locally. To browse these backup locations, register the bootable media on the management server, and then, in the Cyber Protect console, go to **Backup storage**. When performing recovery, select the bootable media in **Machine to browse from**.

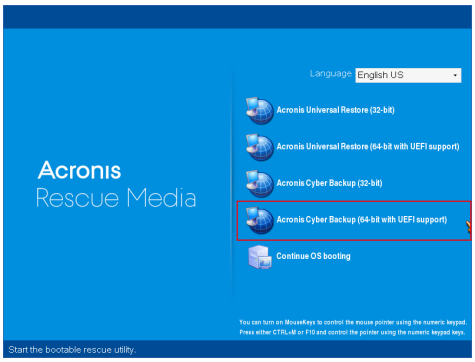
© Acronis International GmbH, 2003-2026

- Acronis Universal Restore is required when you recover data to dissimilar hardware.
  Acronis Universal Restore is not available when the backup is located in Acronis Secure Zone.

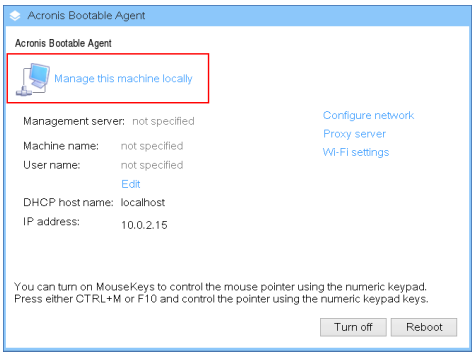
To recover backups by using bootable media locally

Linux-based bootable media

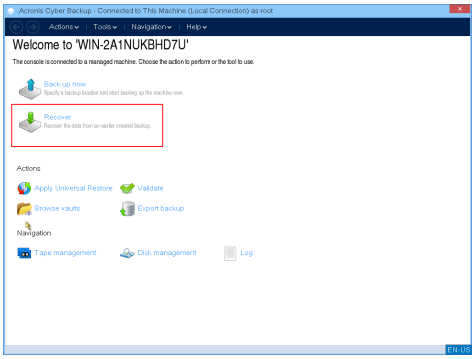
1. Boot the workload that you want to recover with bootable media.
   Depending on the type of the bootable media, it might be called rescue media.



2. Click **Manage this machine locally**.

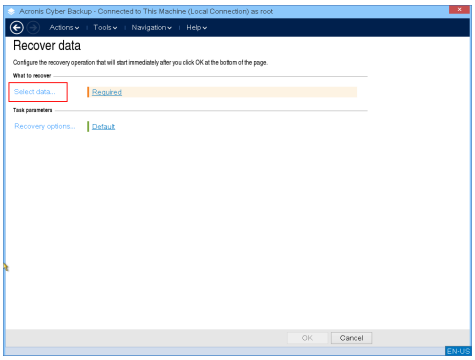


3. Click **Recover**.

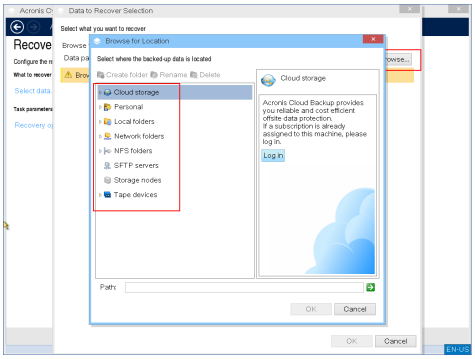


4. In **What to recover**, click **Select data**.

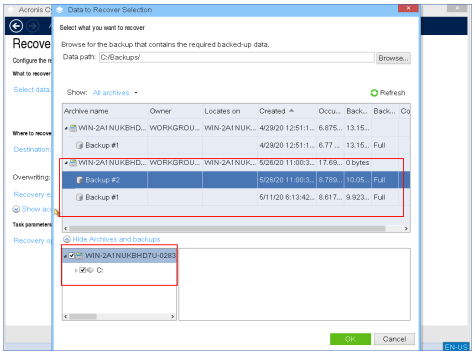
© Acronis International GmbH, 2003-2026



5. Click **Browse**, and then select the backup location.
6. [If the backup is in the cloud storage] Log in to the account to which the backed-up machine is assigned.



7. Click **OK**.
8. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
9. Select a backup archive and a backup (recovery point) from which you want to recover data.



10. [If prompted] Specify the backup encryption password.
11. [If you recover a disk-level backup] Select the recovery scope.

    Disk-level backups contain volumes, disks, and files. File-level backups contain only files.

    Important

    If the backed-up machine has dynamic disks or logical volumes (LVM), select **Volumes**.

12. Select the items that you want to recover, and then click **OK**.
13. [Optional] [When recovering disks or volumes] To change that automatic mapping between the backed-up disks or volumes and target disks or volumes, click the link under **Recover to**, map

© Acronis International GmbH, 2003-2026

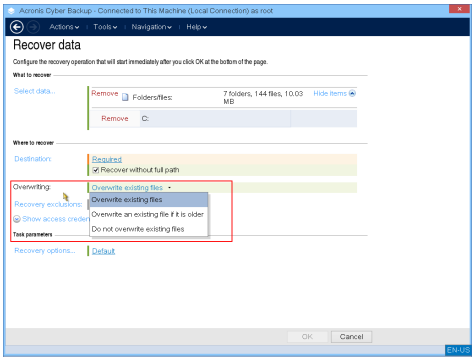
the disks or volumes manually, and then click **OK**.

Note
Changing disk layout may affect the operating system bootability. We strongly recommend that you use the disk layout of the original machine.

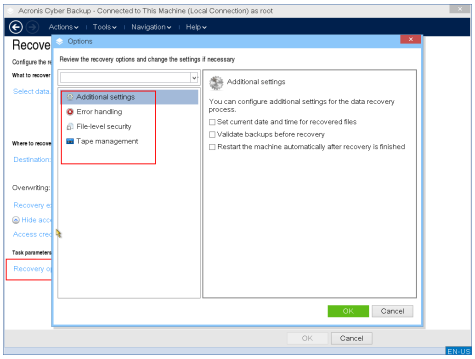
- [When recovering Windows disks] Select an option for recovering the NT signature.
- [When recovering macOS volumes] To recover an APFS-formatted **Data volume** as a bootable macOS system, in the **macOS Installation** section, select the checkbox **Install macOS on the recovered macOS Data volume**. In this case, after the recovery, the system will reboot and installation of macOS will start automatically. Internet connection is required.

  If you clear the **Install macOS on the recovered macOS Data volume** checkbox, the APFS-formatted **Data volume** will be recovered as a non-bootable volume. You can make this volume bootable by manually installing macOS on it.
- [When recovering Linux volumes] If the backed-up machine has logical volumes (LVM) and you want to reproduce the original LVM structure, do the following:
  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**.
  c. Confirm your choice.

14. [When recovering files] Click **Destination**, select recovery location, and then click **OK**.
15. [Optional] [When recovering files] Configure the overwriting rules.



16. [Optional] [When recovering files] Configure the recovery exclusions, and then click **OK**.
17. [Optional] Configure the recovery options, and then click **OK**.

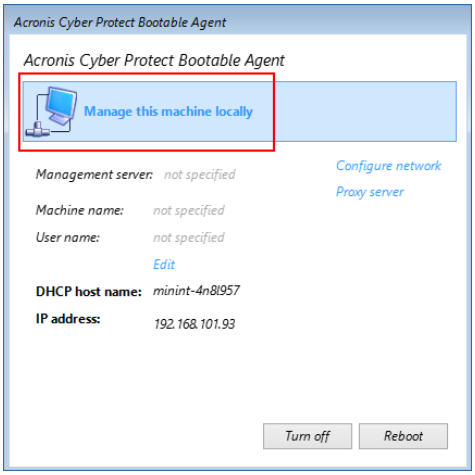


18. To start recovery, click **OK**.

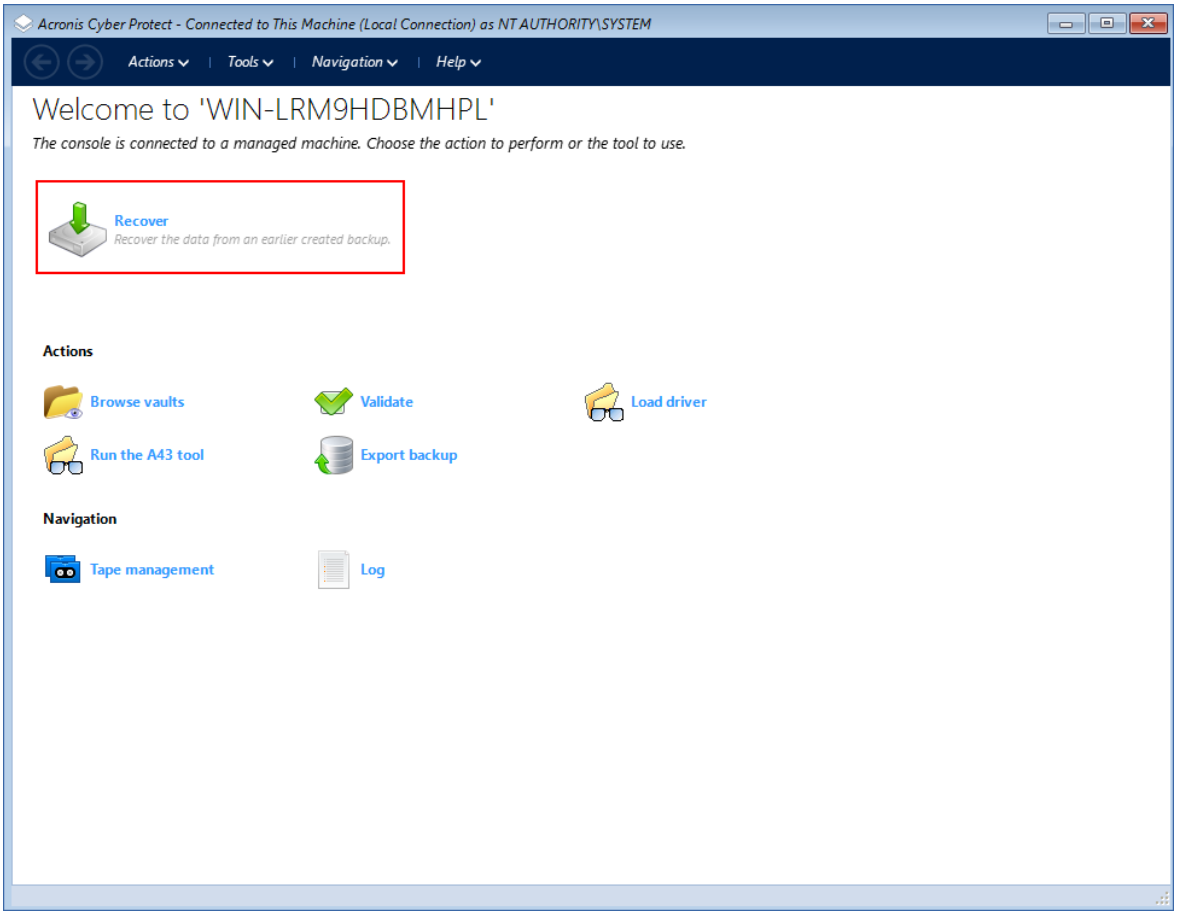
© Acronis International GmbH, 2003-2026

Windows-based bootable media

1. Boot the workload that you want to recover with bootable media.
2. Click **Manage this machine locally**.

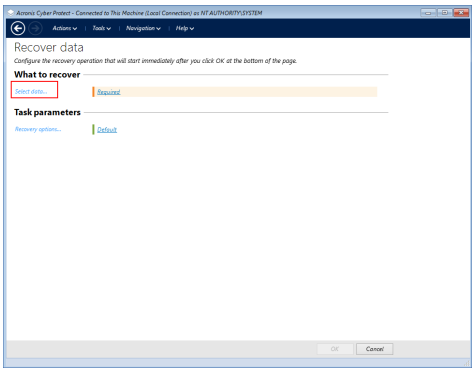


3. Click **Recover**.

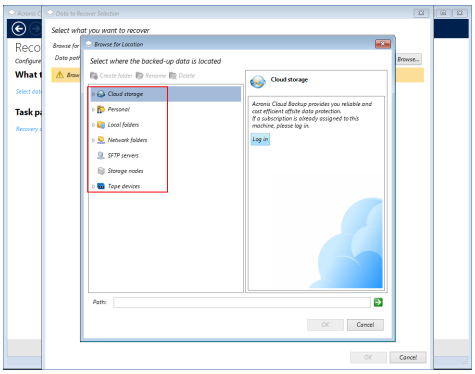


4. In **What to recover**, click **Select data**.

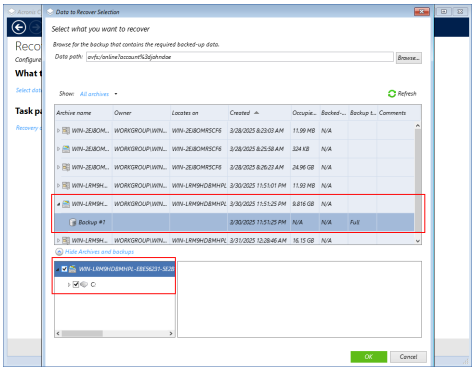
© Acronis International GmbH, 2003-2026



5. Click **Browse**, and then select the backup location.
6. [If the backup is in the cloud storage] Log in to the account to which the backed-up machine is assigned.



7. Click **OK**.
8. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
9. Select a backup archive and a backup (recovery point) from which you want to recover data.



10. [If prompted] Specify the backup encryption password.
11. [If you recover a disk-level backup] Select the recovery scope.

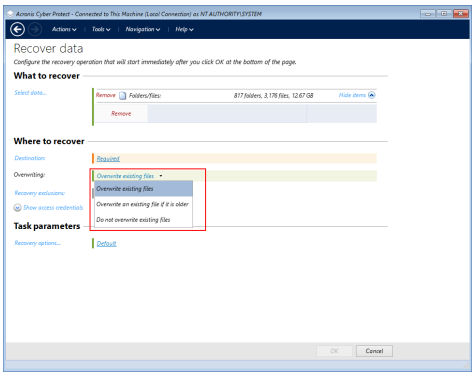
    Disk-level backups contain volumes, disks, and files. File-level backups contain only files.
12. Select the items that you want to recover, and then click **OK**.
13. [Optional] [When recovering disks or volumes] To change that automatic mapping between the backed-up disks or volumes and the target disks or volumes, click the link under **Recover to**, map the disks or volumes manually, and then click **OK**.

© Acronis International GmbH, 2003-2026

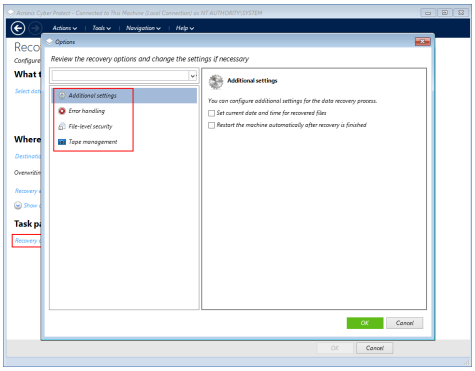
Note

Changing disk layout may affect the operating system bootability. We strongly recommend that you use the disk layout of the original machine.

14. [When recovering disks] Select an option for recovering the NT signature.
15. [When recovering files] Click **Destination**, select recovery location, and then click **OK**.
16. [Optional] [When recovering files] Configure the overwriting rules.



17. [Optional] Configure the recovery exclusions, and then click **OK**.
18. [Optional] Configure the recovery options, and then click **OK**.



19. To start recovery, click **OK**.

Managing disks by using bootable media locally

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.

© Acronis International GmbH, 2003-2026

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 bare metal, on a machine that cannot boot or on a non-Windows machine. You will need a bootable media that you created with Bootable Media Builder, and by using your Acronis Cyber Protect license key. For more information about creating a bootable media, see Linux-based bootable media or Windows-PE based bootable media, respectively.

Note
Disk management via bootable media is not supported on Windows 8 and later. To perform disk management operations on these operating systems, install Acronis Disk Director. For more information, see this knowledge base article.

Running the bootable media requires 1.5 GB of RAM.

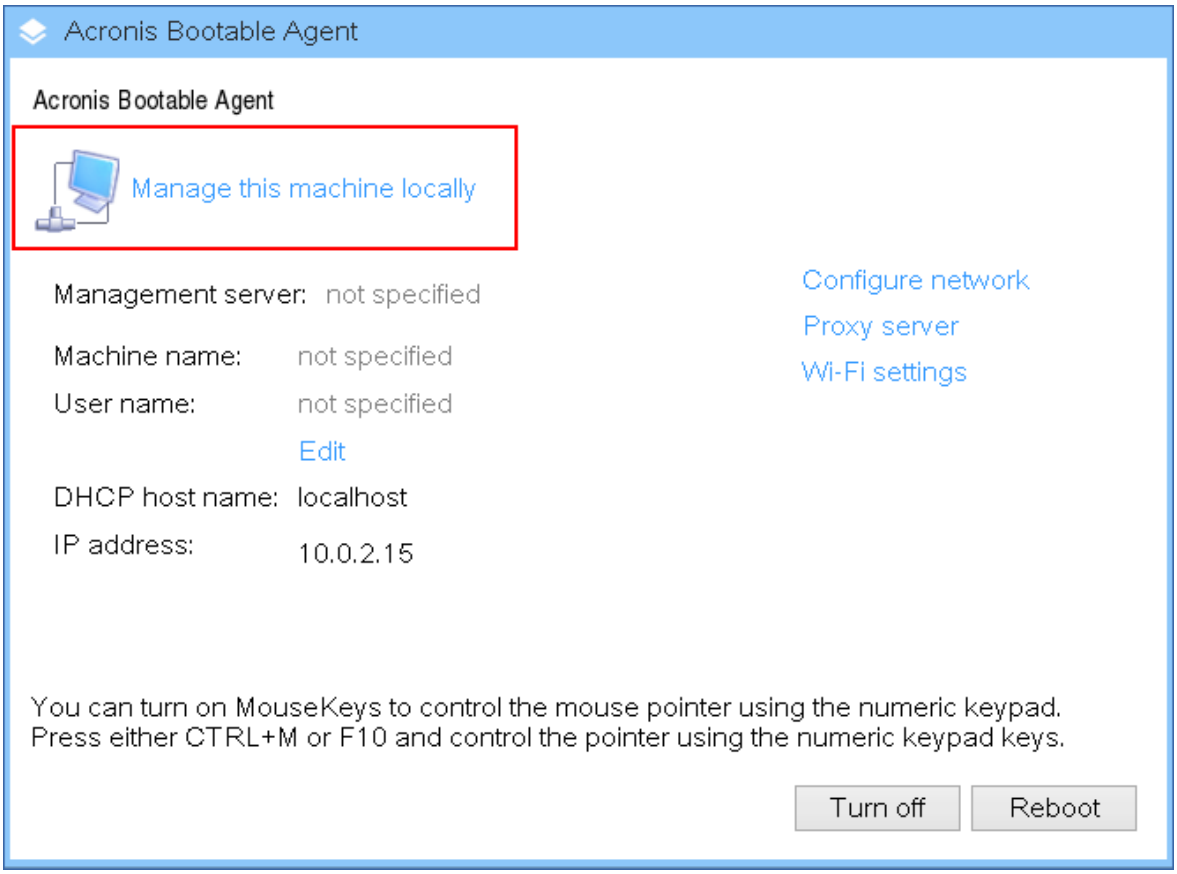
To perform disk management operations

© Acronis International GmbH, 2003-2026

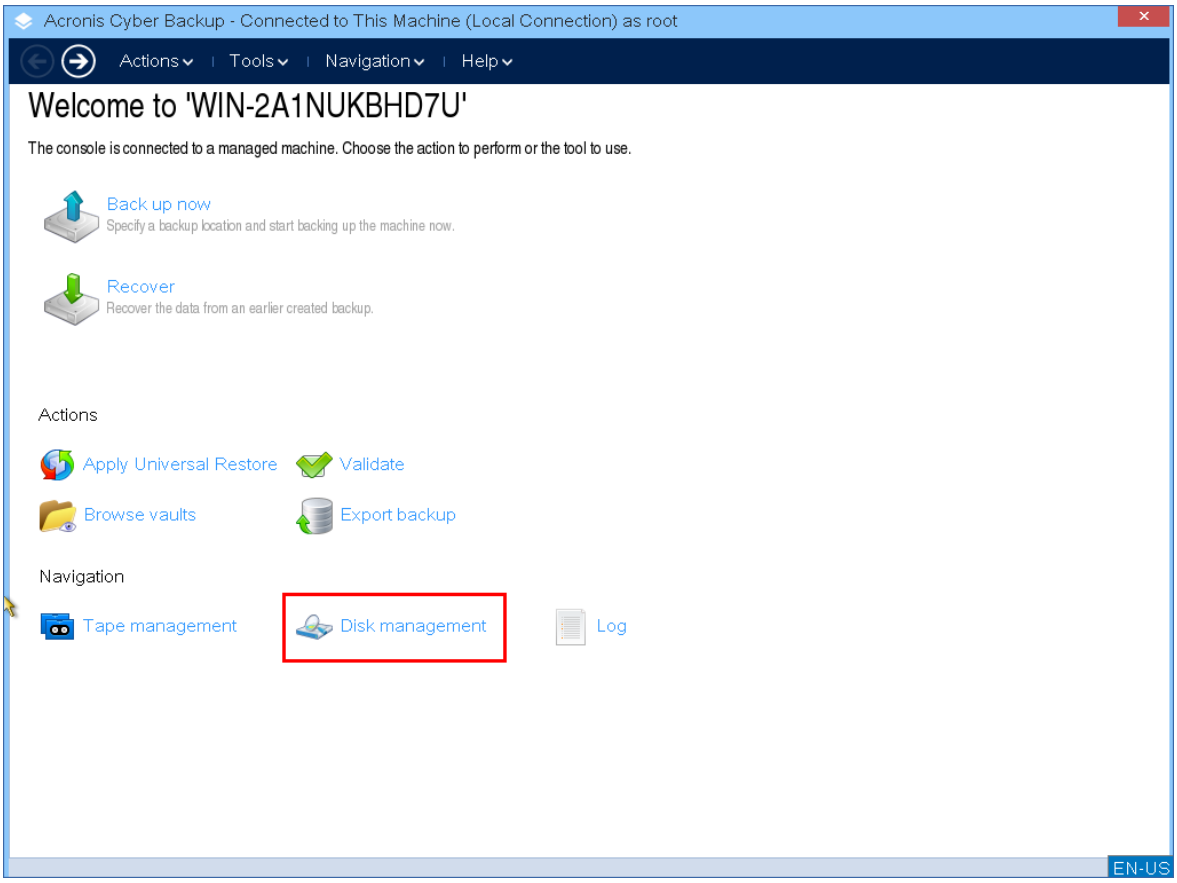
1. Boot from Acronis bootable rescue media.

2. To work on the local machine, click **Manage this machine locally**. For remote connections, see Registering media on the management server.

© Acronis International GmbH, 2003-2026



3. Click **Disk management**.



© Acronis International GmbH, 2003-2026

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:

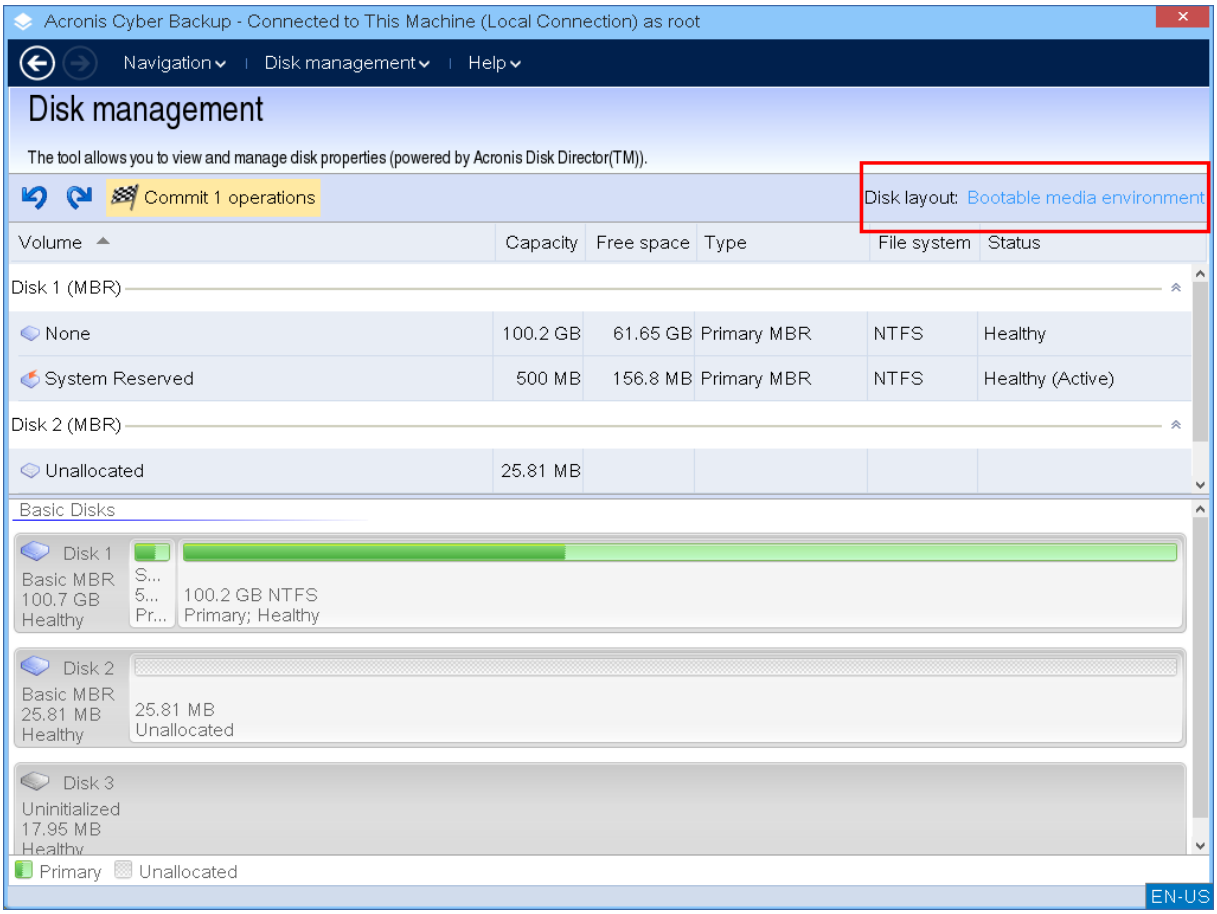
1. Back up the disk on which volumes will be created or managed. Having your most important data backed up to another hard disk, network share or removable media will allow you to work on disk volumes knowing that your data is safe.
2. Test your disk to make sure it is fully functional and does not contain 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.

© Acronis International GmbH, 2003-2026

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

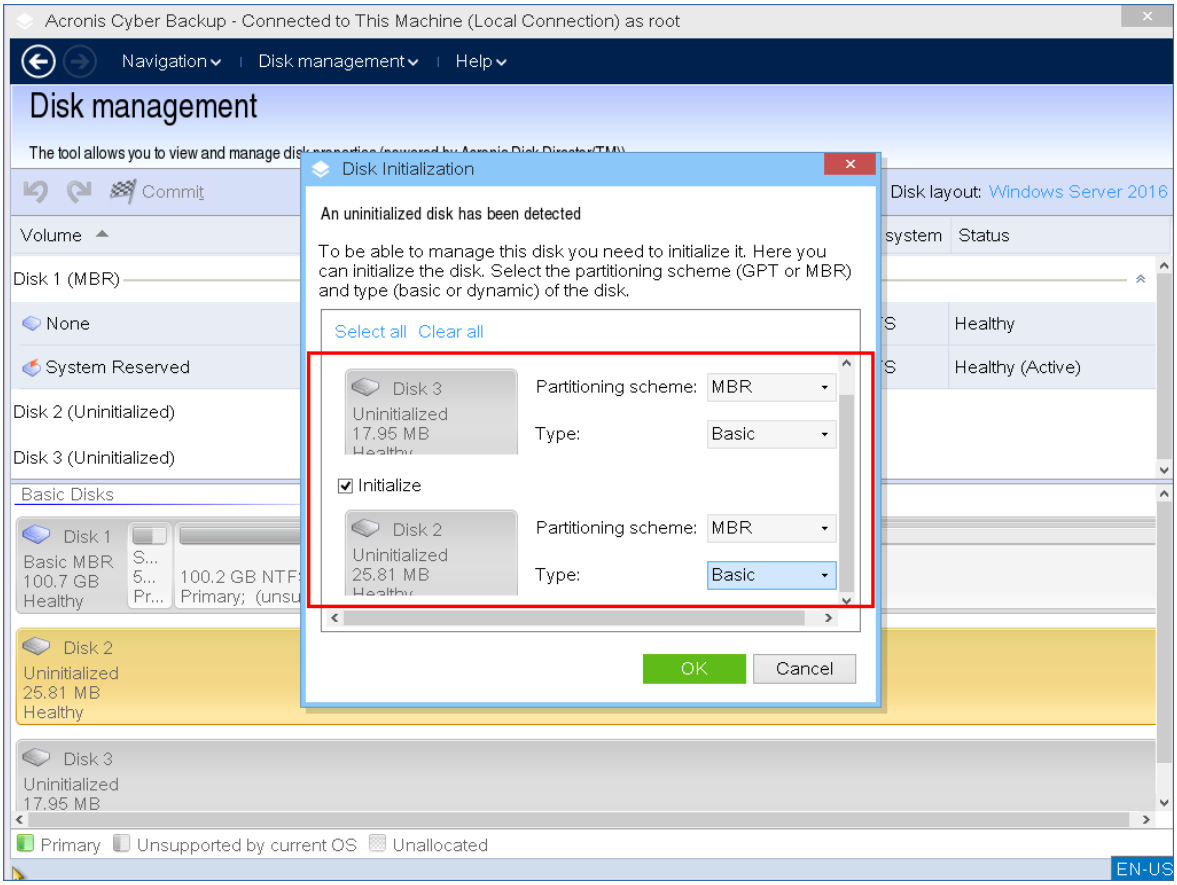
Disk initialization

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

© Acronis International GmbH, 2003-2026

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

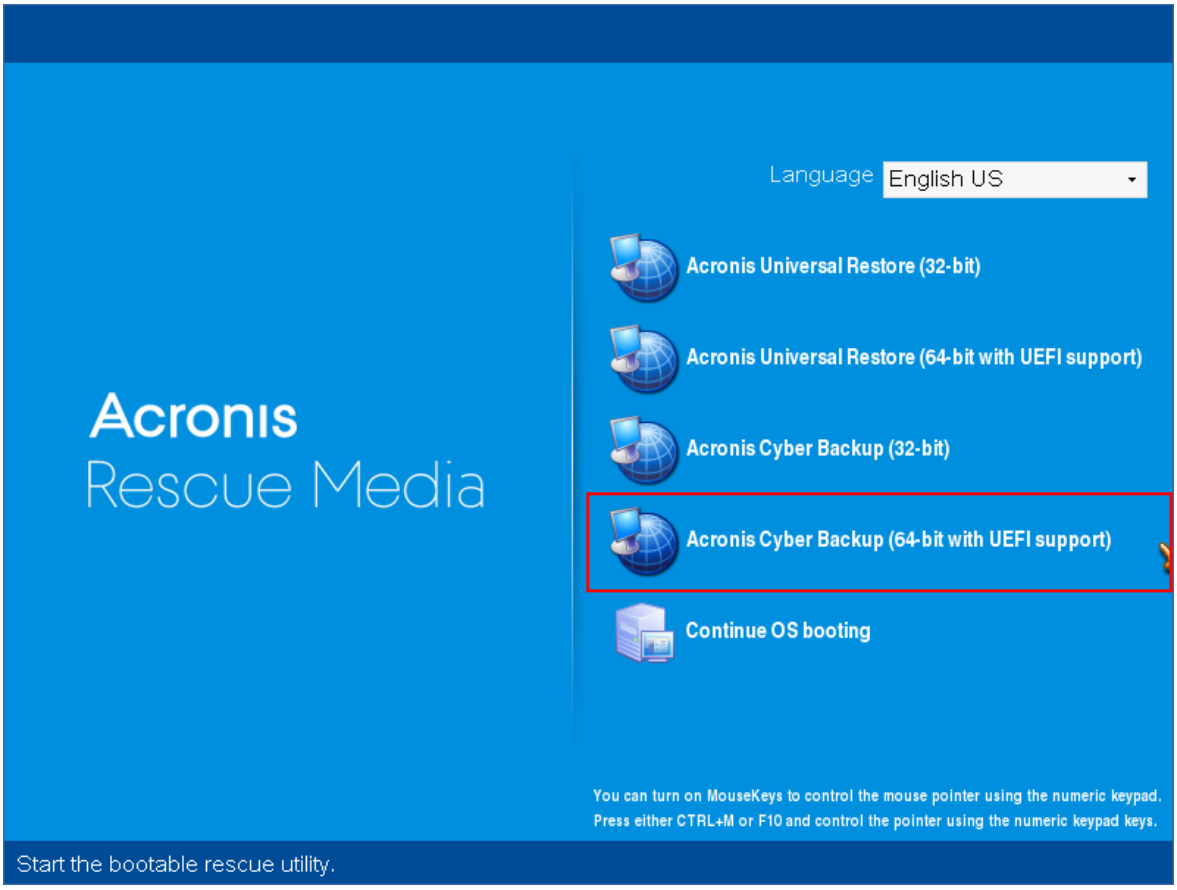
With a full-featured Linux-based bootable media, you can clone basic MBR disks. Disk cloning is not available in the ready-made bootable media that you can download or in a bootable media that is created without a license key.

Note
You can also clone disks by using the Acronis Cyber Protect Command-Line utility.

To clone basic disks under bootable media

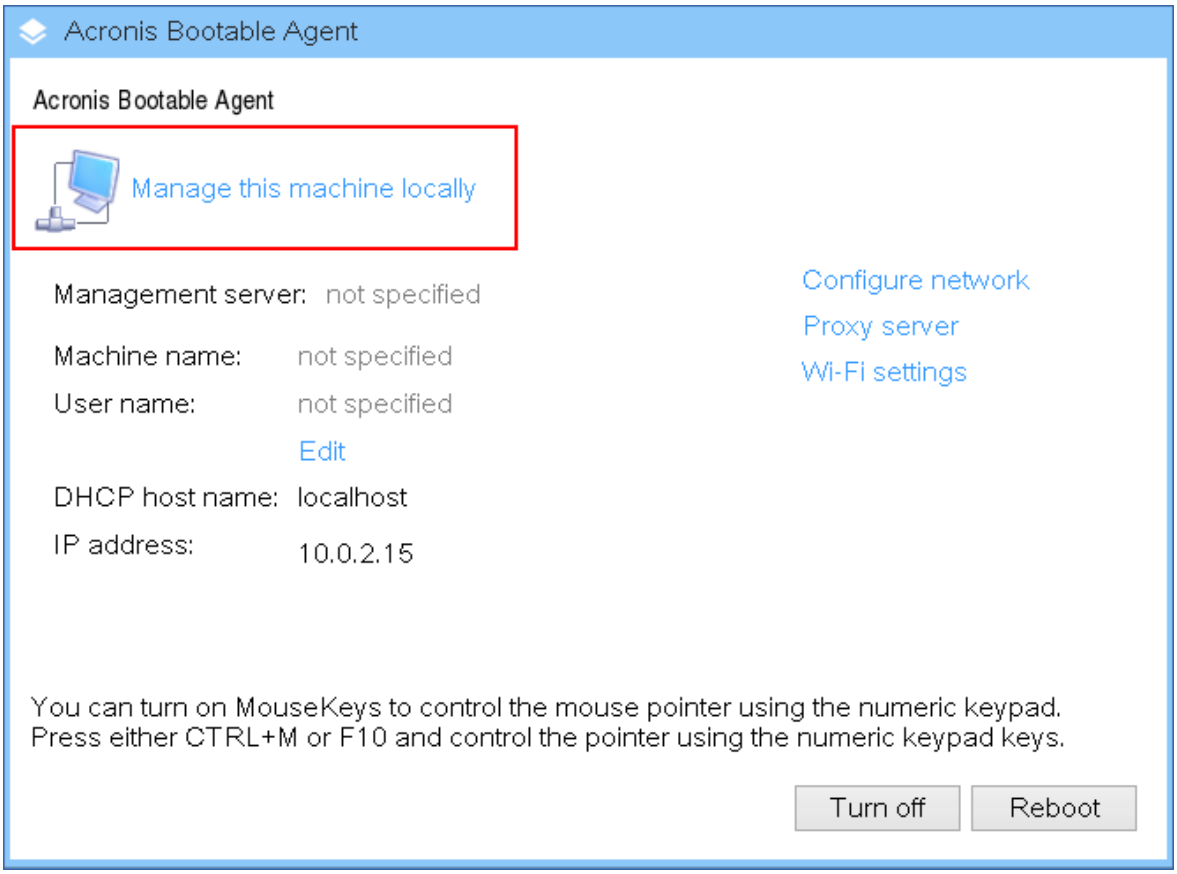
© Acronis International GmbH, 2003-2026

1. Boot from Acronis bootable rescue media.

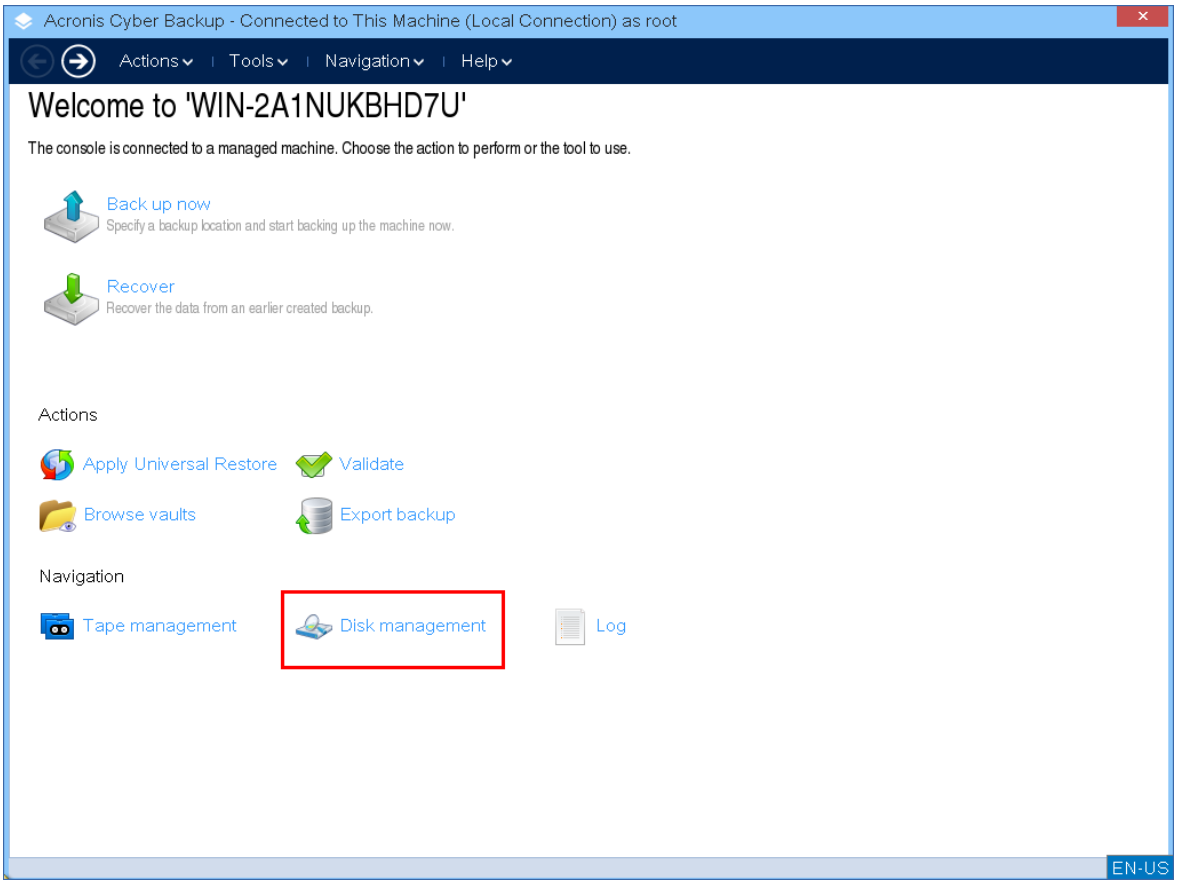


2. To clone a disk of the local machine, click **Manage this machine locally**. For remote connection, see Registering media on the management server.

© Acronis International GmbH, 2003-2026



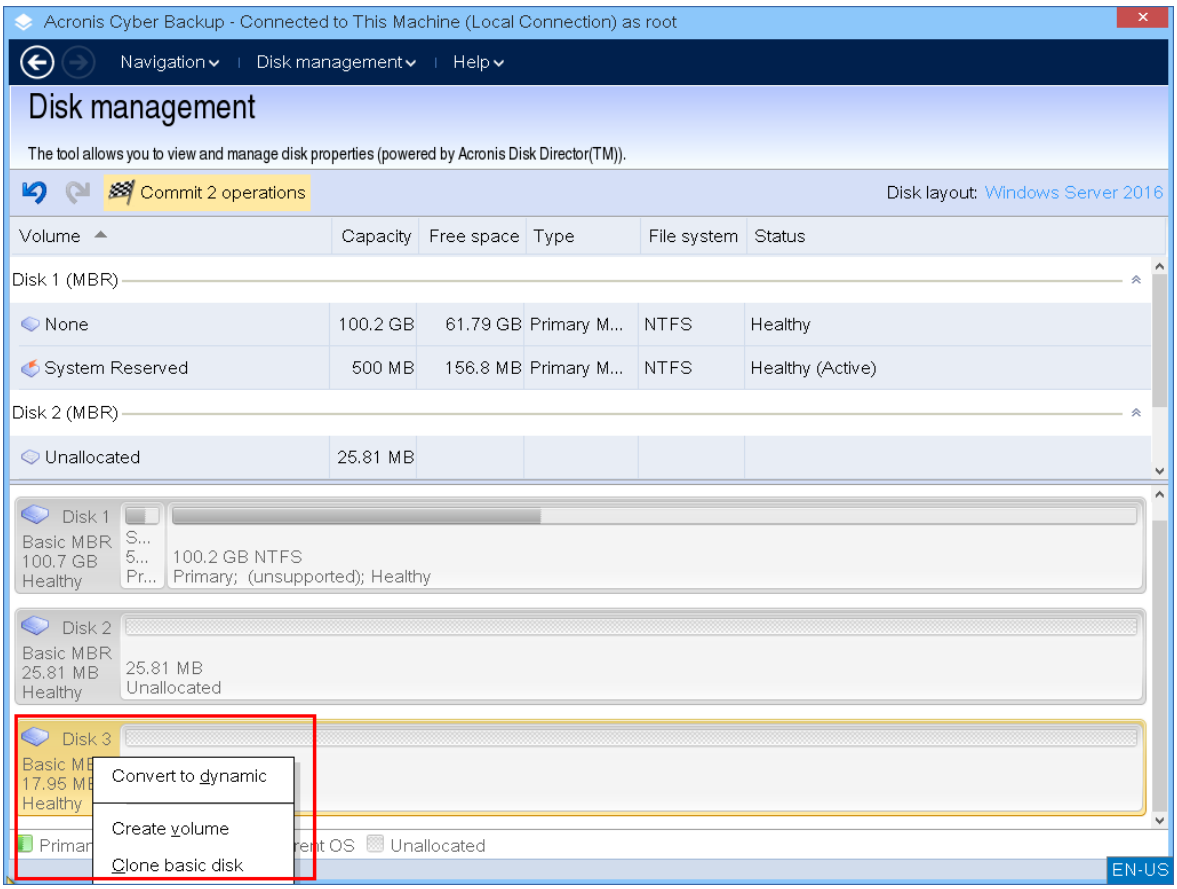
3. Click **Disk management**.



© Acronis International GmbH, 2003-2026

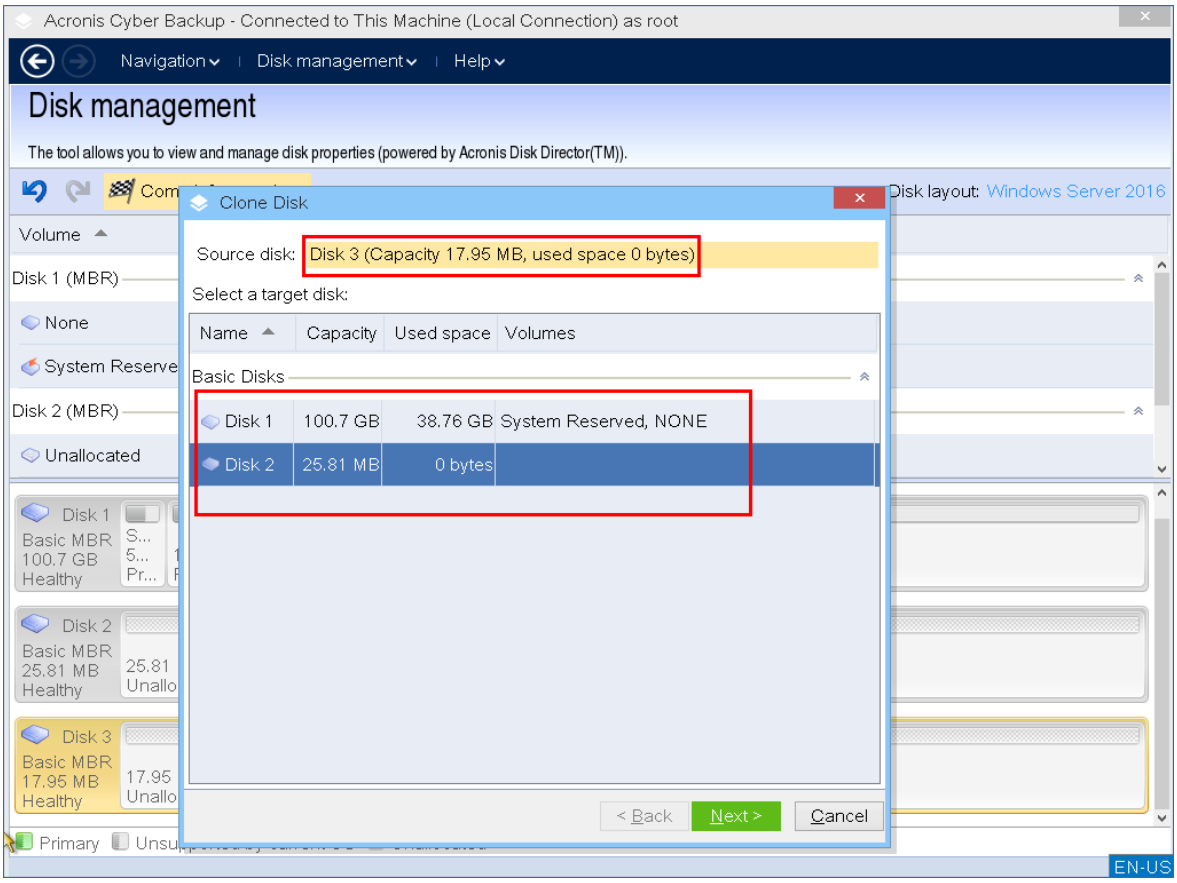
4. The available disks are displayed. Right-click the disk that you want to clone, and then click **Clone basic disk**.

Note
You can clone only entire disks. Partition cloning is not available.



5. 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**.

© Acronis International GmbH, 2003-2026

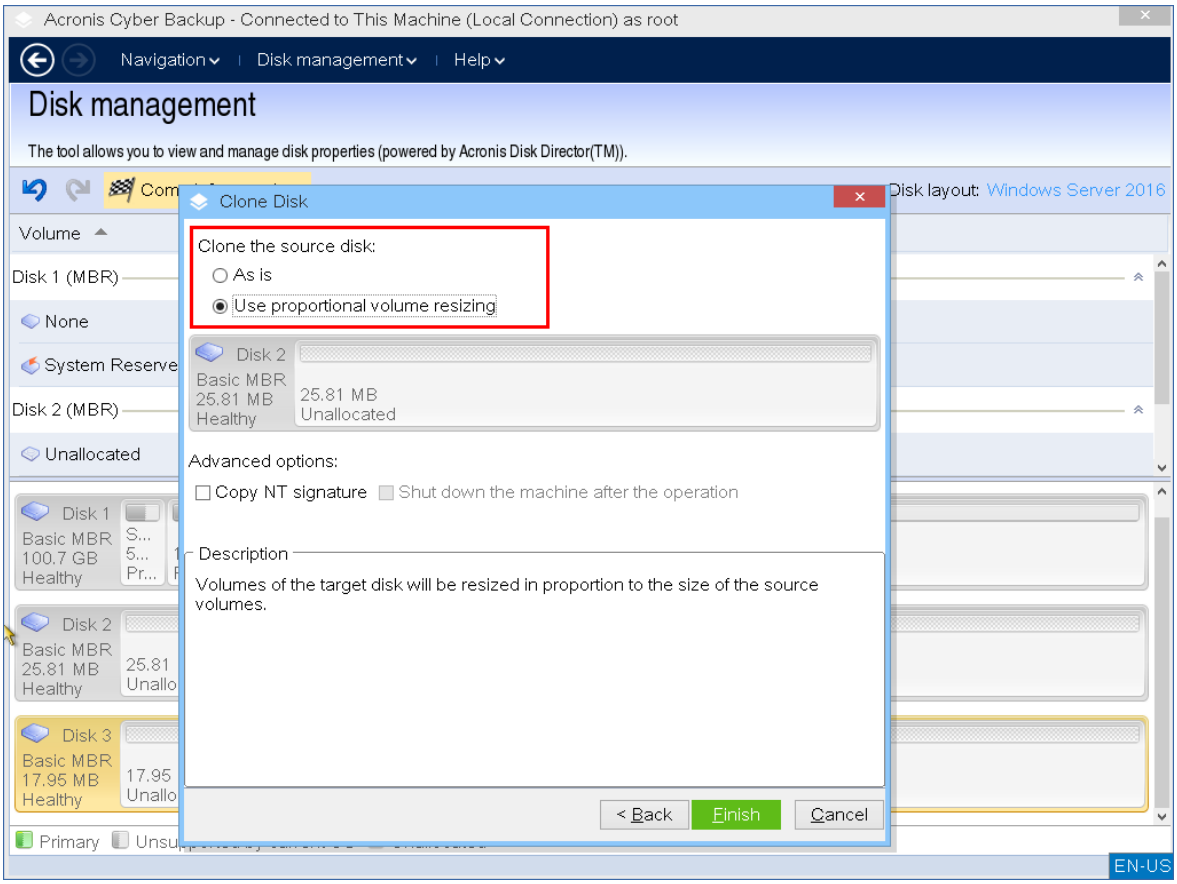


If the target disk is larger, you can clone the disk as is or resize the source disk volumes proportionally (default option), in order to avoid leaving unallocated space on the target disk. If the target disk is smaller, only proportional resizing is available. If safe cloning is impossible even with the proportional resizing, the you will not be able to continue the operation.

Important

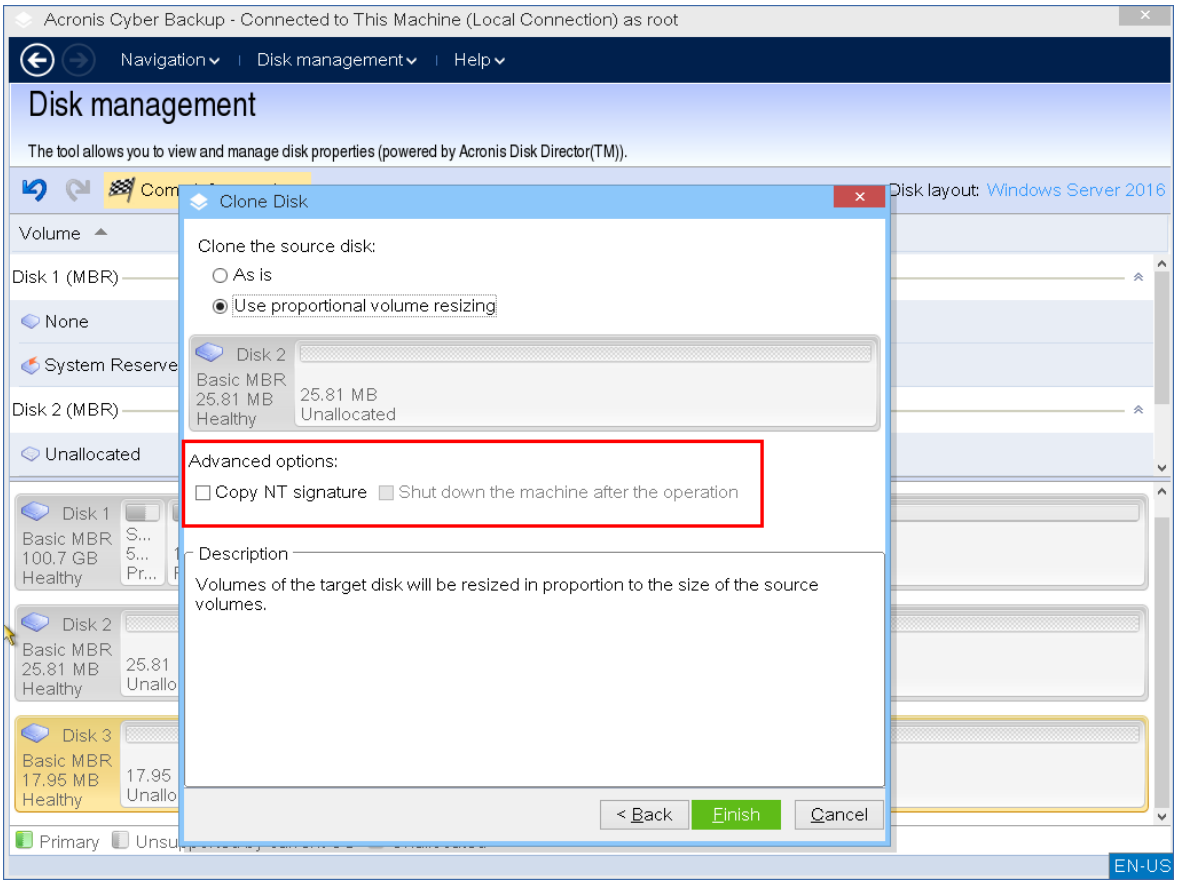
If there is data on the target disk, you will see the warning: "*The selected target disk is not empty. The data on its volumes will be overwritten.*" If you proceed, all the data that is currently on the target disk will be lost irrevocably.

© Acronis International GmbH, 2003-2026



6. Select whether to copy the NT signature or not.

© Acronis International GmbH, 2003-2026



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.

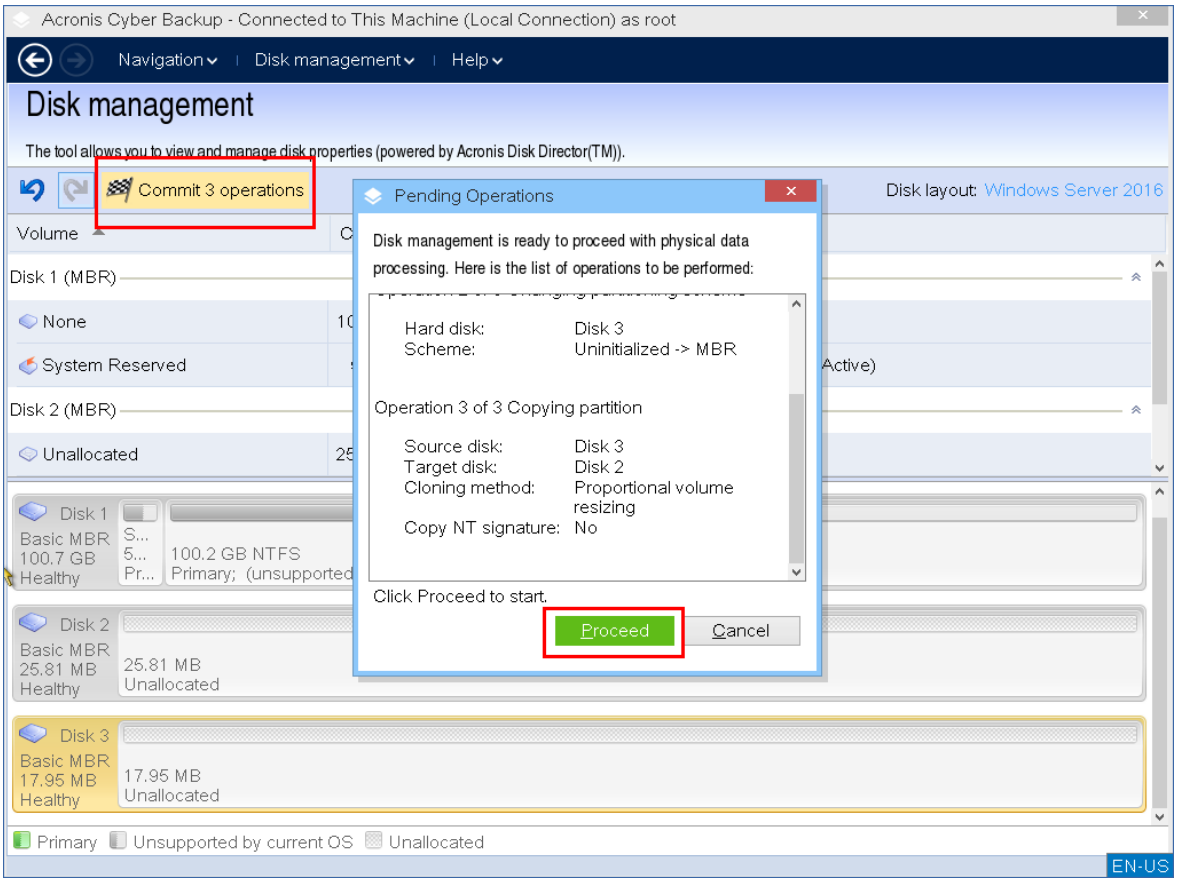
© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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 faill.
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:

© Acronis International GmbH, 2003-2026

- 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:

 © Acronis International GmbH, 2003-2026

- 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.

© Acronis International GmbH, 2003-2026

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

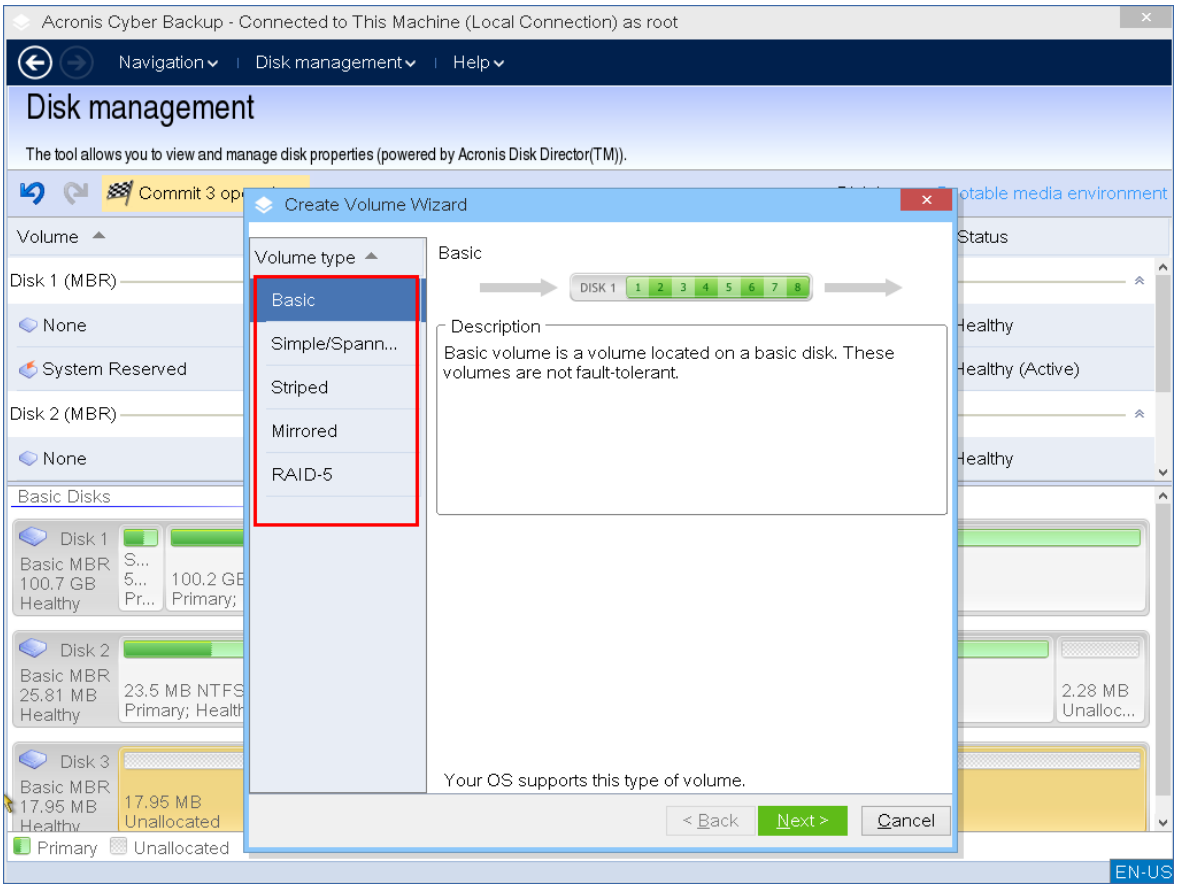
You might need a new volume to:

- 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.

© Acronis International GmbH, 2003-2026



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.

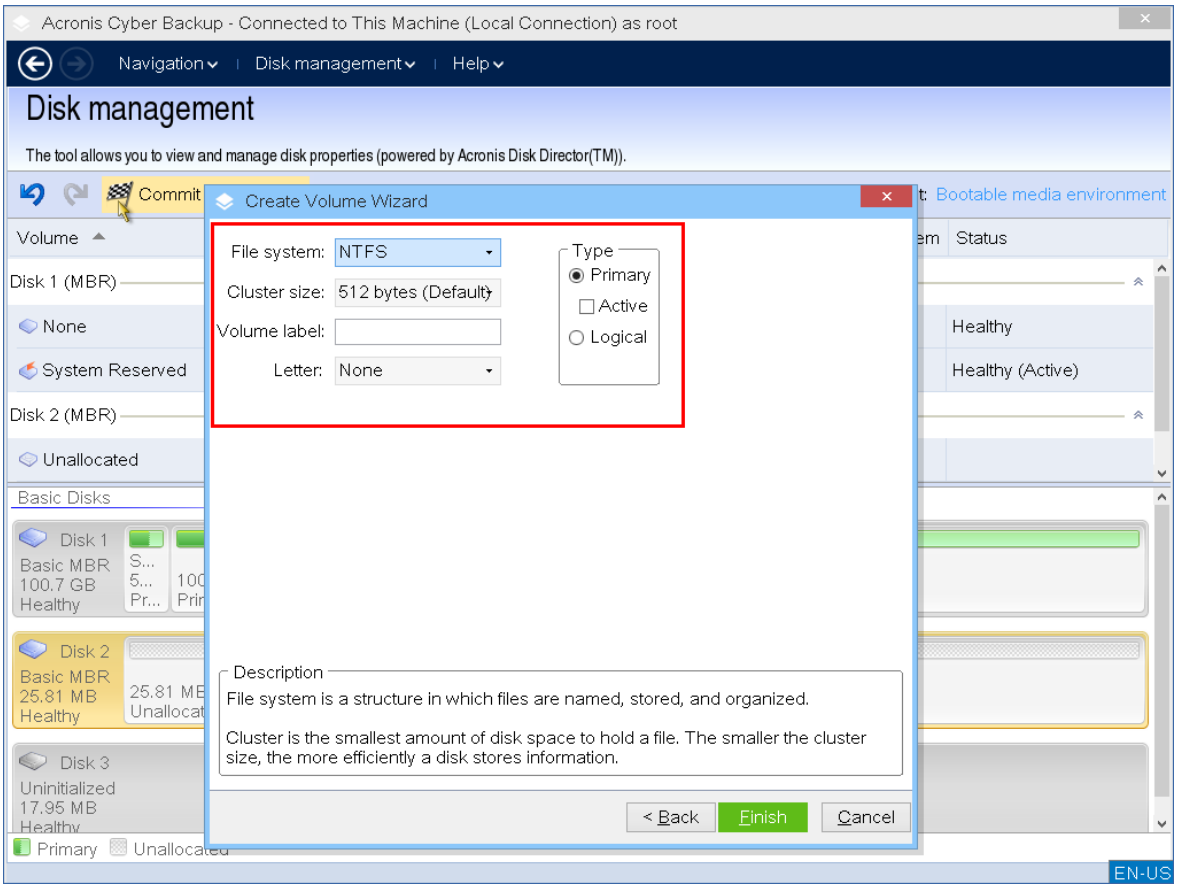
   The maximum value normally reflects the maximum unallocated space possible. In some cases, the proposed maximum value might differ – for example, when the size of one mirror

© Acronis International GmbH, 2003-2026

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.

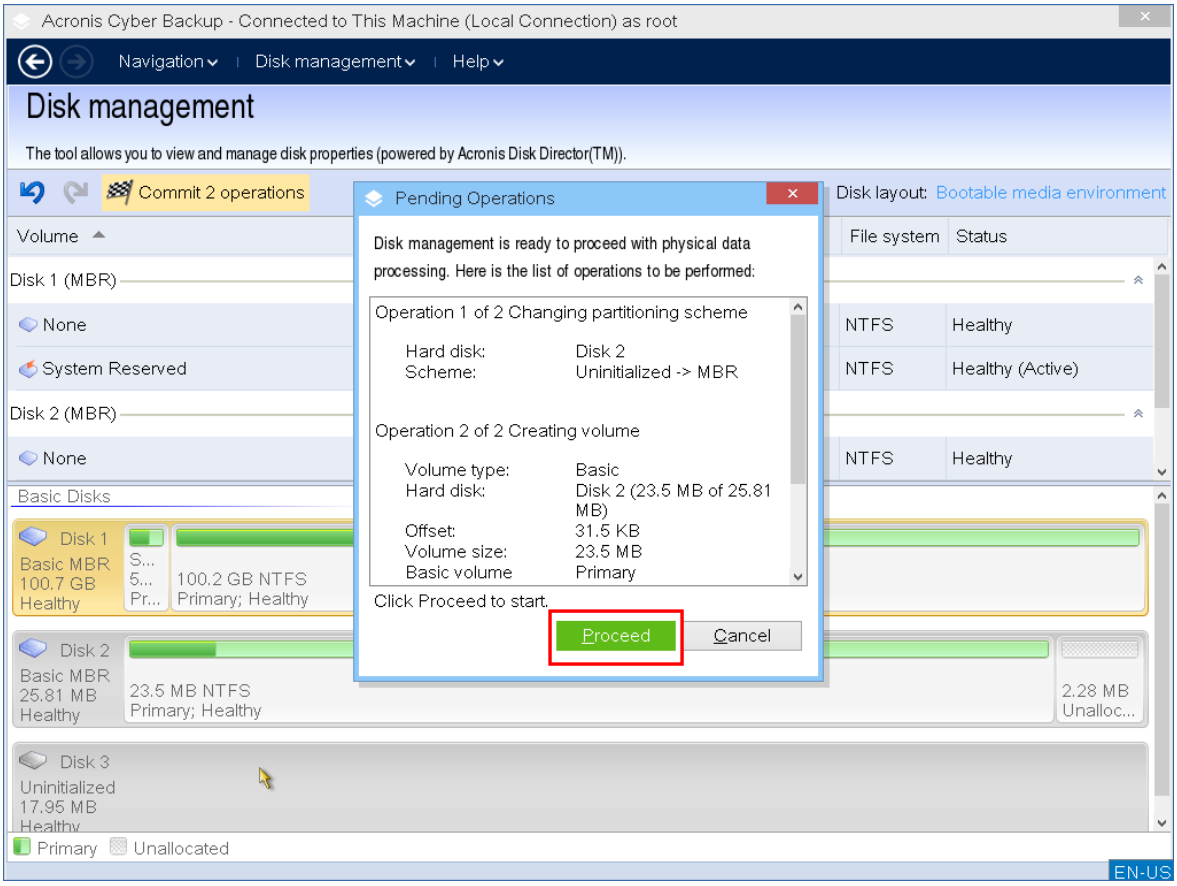
If you are creating a basic volume, which can be made a system volume, you can also select the volume type — **Primary** (**Active Primary**) or **Logical**. Typically, **Primary** is selected when you want to install an operating system to a volume. Select the **Active** (default) value if you want to

© Acronis International GmbH, 2003-2026

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.

6. 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

1. Right-click the volume that you want to delete.
2. Click **Delete volume**.

Note
All the information on this volume will be lost irrevocably.

3. By clicking **OK**, you will add a pending operation of volume deletion.

© Acronis International GmbH, 2003-2026

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 assignement.
4. To complete the added operation, commit it. Exiting the program without committing the operation will effectively cancel it.

 © Acronis International GmbH, 2003-2026

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:

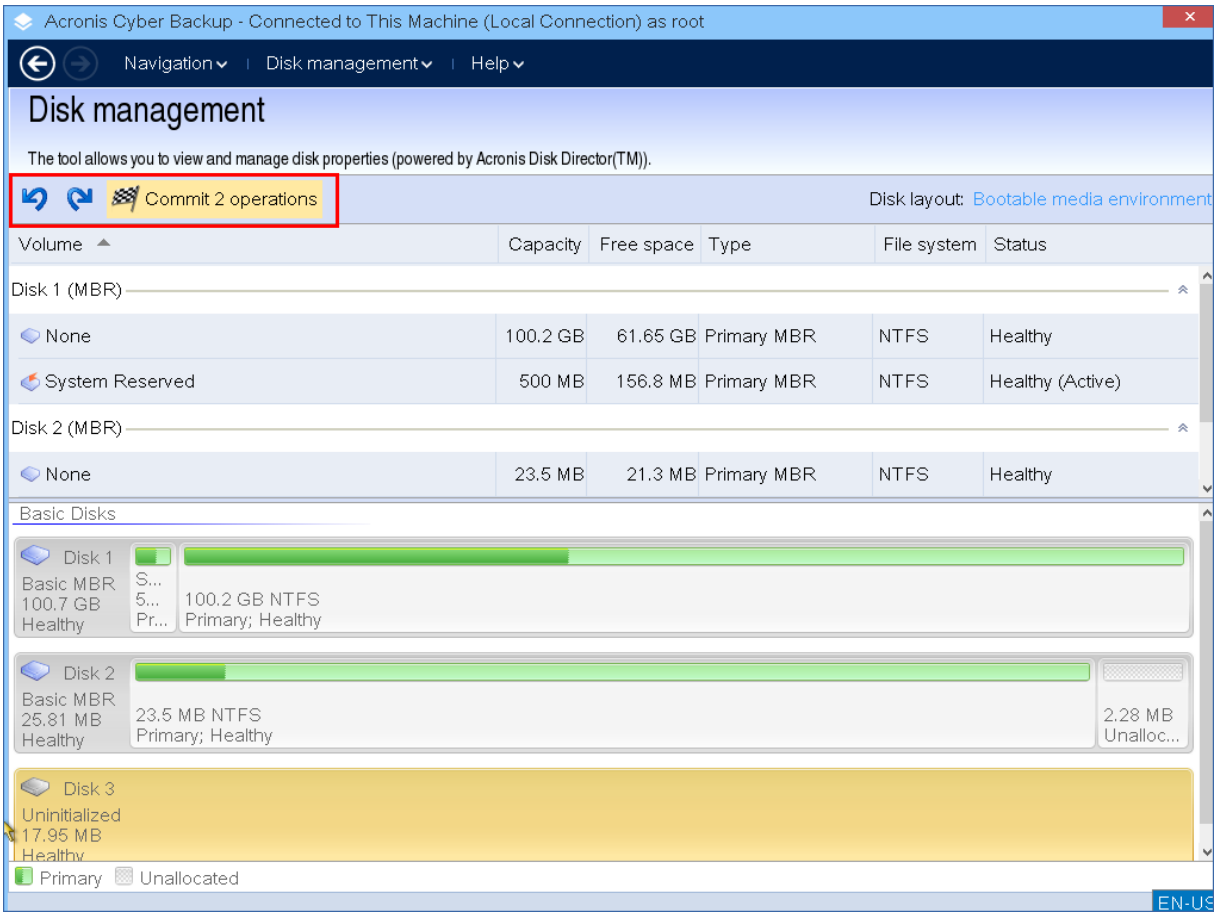
1. Right-click the desired volume, and then click **Format**.
2. Select the cluster size and file system. The possible file systems options are:
   - FAT16 (disabled if the volume size has been set at more than 2 GB)
   - FAT32 (disabled if the volume size has been set at more than 2 TB)
   - NTFS
3. 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 is 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.

© Acronis International GmbH, 2003-2026



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.

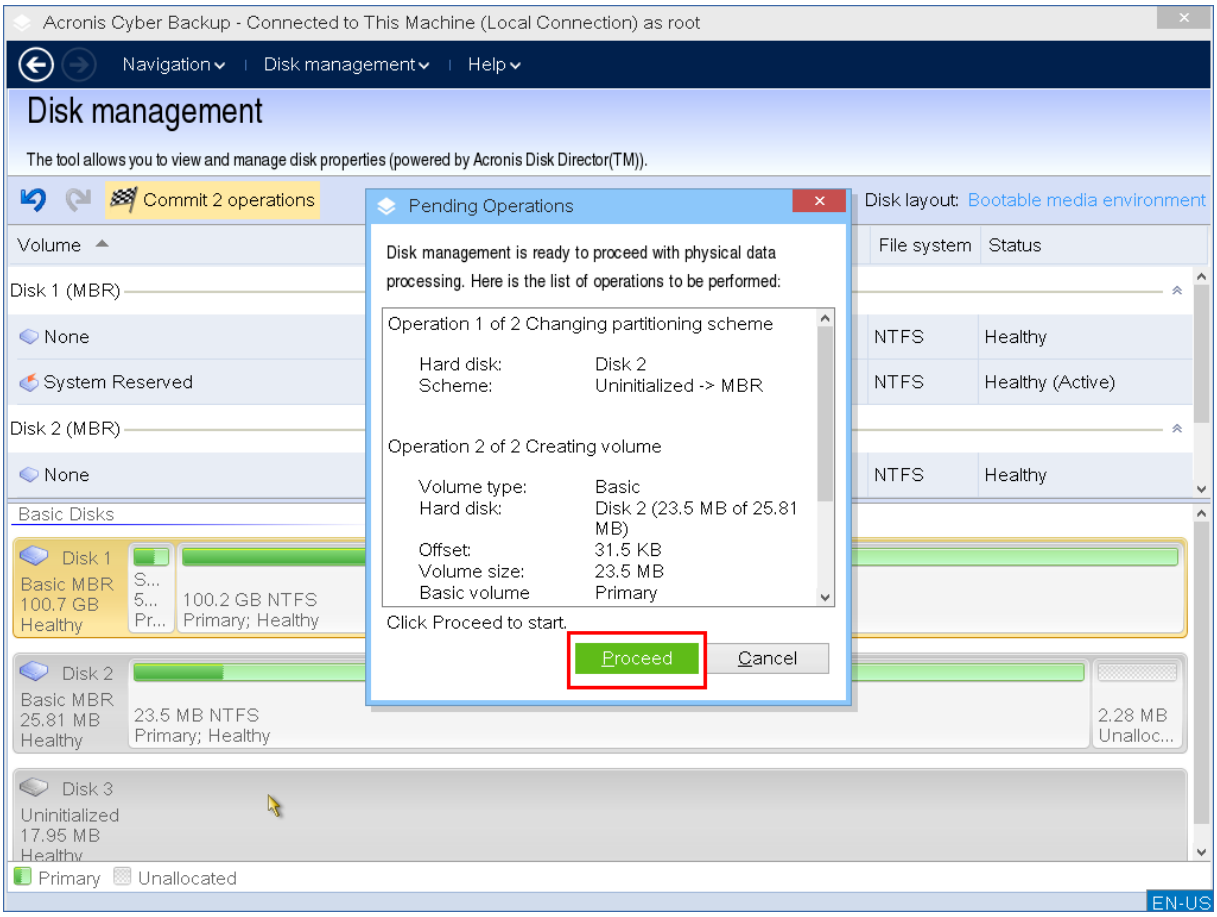
The **Commit** action forwards you to the **Pending Operations** window, where you will be able to view the pending operation list.

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.

© Acronis International GmbH, 2003-2026



Registering bootable media on the management server

Registering bootable media enables you to manage the media via the Cyber Protect 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 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

© Acronis International GmbH, 2003-2026

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 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 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**.

Recovering backups by using bootable media remotely

You can recover backed-up workloads, files, and folders by using a bootable media remotely.

Running the bootable media requires 1.5 GB of RAM.

Prerequisites

- The bootable media is registered as described in "Registering bootable media on the management server" (p. 601).

To recover backups by using bootable media remotely

Workloads

1. Log in to the Cyber Protect console with an account under which a bootable media is registered.
2. Go to **Devices** > **Bootable media**, and then select the bootable media.
3. Click **Recovery**.
4. Select the backup location.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. Select a backup archive and a backup (recovery point) from which you want to recover data.
7. [If prompted] Specify the backup encryption password.
8. Click **Recover** > **Entire machine**.
9. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.

 © Acronis International GmbH, 2003-2026

10. In **Recover to**, select the type of the target machine.
11. In **Target machine**, select the machine that you want to recover, and then click **OK**.

    Important
    By default, the workload on which the bootable media runs is selected as target machine.

12. [Optional] Configure the disk mapping between the backed-up machine and the target machine.

    Note
    Changing disk layout may affect the operating system bootability. We strongly recommend that you use the disk layout of the original machine.

    a. [To configure the mapping on a disk level]
       i. Click **Disk mapping**.
       ii. Configure the disk mapping between the backed-up machine and the target machine.
       iii. Click **Done**.
    b. [To configure the mapping on a volume level]
       i. Click **Disk mapping**, and then, in the upper-right corner, click **Switch to volume mapping**.
       ii. Configure the volume mapping between the backed-up machine and the target machine.
       iii. Click **Done**.
13. Configure the recovery options, and then click **OK**. For more information, see "Recovery options" (p. 548).
14. [Optional] [Only available with Windows-based bootable media when recovering Windows machines on which a protection agent is installed] To join the machine to an Active Directory domain, enable the **Rejoin domain** switch.
    a. Click the **Domain credentials** field.
       i. Specify the domain name.
          If the backup contains data about the domain name, this field is prepopulated.
       ii. Specify the credentials for a user account with domain-joining privileges.
          You can specify the user account as <user name>@<domain> or <domain>\<user name>.
       iii. [Optional] Specify an organizational unit.
          If the backup contains data about the organizational unit, this field is prepopulated.
       iv. Click **Done**.
       As a result, the specified credentials are validated, and if they are correct, the recovered machine will rejoin the domain after the recovery completes.
15. Click **Start recovery**.
16. [Optional] If you prefer to restart the machine manually after the recovery, clear the **Automatically restart the machine, if required** checkbox.
17. To confirm that you want to overwrite the disks of the target machine, click **Start recovery**.

Files and folders

© Acronis International GmbH, 2003-2026

1. Log in to the Cyber Protect console with an account under which a bootable media is registered.
2. Go to **Devices** > **Bootable media**, and then select the bootable media.
3. Click **Recovery**.
4. Select the backup location.
5. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
6. Select a backup archive and a backup (recovery point) from which you want to recover data.
7. [If prompted] Specify the backup encryption password.
8. Click **Recover** > **Files/folders** or **Recover files/folders**.

   Recover > **Files/folders** is shown when you recover from disk-level backups and **Recover files/folders** is shown when you recover from file-level backups.
9. [If prompted] Specify the credentials to access the backup storage, and then click **OK**.
10. Select the items that you want to recover, and then click **Recover**.
    a. In **Recover to**, select the target machine, and then click **OK**.
    b. In **Path**, click **Browse**, select the recovery location, and then click **Done**.
11. Configure the recovery options, and then click **OK**. For more information, see "Recovery options" (p. 548).
12. Click **Start recovery**.
13. Select an overwrite option.
14. If you prefer to restart the machine manually after the recovery, clear the **Automatically restart the machine, if required** checkbox.
15. Click **Proceed**.

Additional remote operations with bootable media

You can use registered bootable media the Cyber Protect console. For example, you can remotely restart or shut down a booted machine, or view details, activities, and alerts that are related to the bootable media.

For more information about recovering backups remotely, see "Recovering backups by using bootable media remotely" (p. 602).

Running the bootable media requires 1.5 GB of RAM.

Prerequisites

- The bootable media is registered as described in "Registering bootable media on the management server" (p. 601).

To restart a booted machine

1. Log in to the Cyber Protect console with an account under which a bootable media is registered.
2. Go to **Devices** > **Bootable media**, and then select the bootable media.
3. Click **Reboot**.
4. To confirm your choice, click **Reboot**.

As a result, the machine that is booted via bootable media restarts.

 © Acronis International GmbH, 2003-2026

To shut down a booted machine

1. Log in to the Cyber Protect console with an account under which a bootable media is registered.
2. Go to **Devices** > **Bootable media**, and then select the bootable media.
3. Click **Shut down**.
4. To confirm your choice, click **Shut down**.

As a result, the machine that is booted via bootable media shuts down.

To view bootable media details

1. Log in to the Cyber Protect console with an account under which a bootable media is registered.
2. Go to **Devices** > **Bootable media**, and then select the bootable media.
3. Click **Details**.

To view bootable media activities

1. Log in to the Cyber Protect console with an account under which a bootable media is registered.
2. Go to **Devices** > **Bootable media**, and then select the bootable media.
3. Click **Activities**.

To view bootable media alerts

1. Log in to the Cyber Protect console with an account under which a bootable media is registered.
2. Go to **Devices** > **Bootable media**, and then select the bootable media.
3. Click **Alerts**.

To delete the bootable media

1. Log in to the Cyber Protect console with an account under which a bootable media is registered.
2. Go to **Devices** > **Bootable media**, and then select the bootable media.
3. Click **Delete**.
4. To confirm your choice, click **Delete**.

As a result, the bootable media disappears from the Cyber Protect console.

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 console can be used only for recovery. This media is based on a Linux kernel. Unlike Windows PE, it does not allow

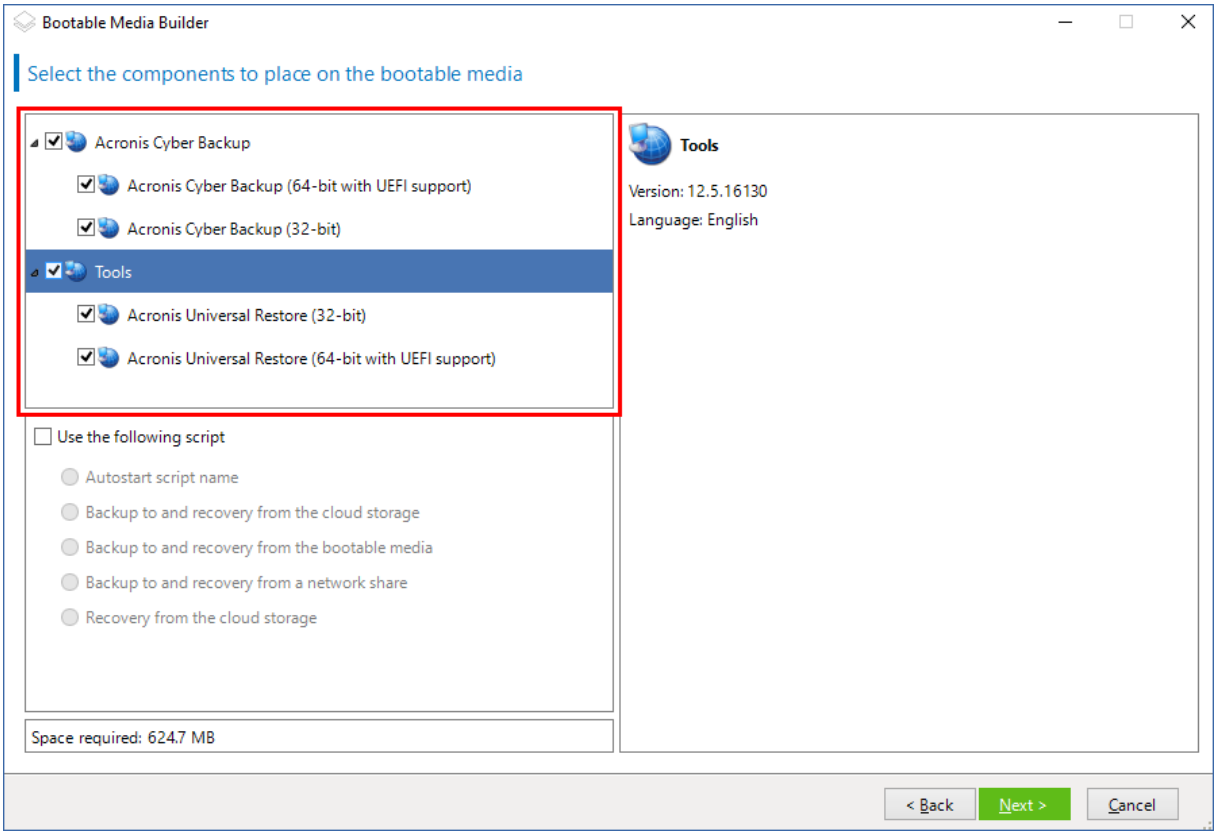
© Acronis International GmbH, 2003-2026

injecting custom drivers on the fly.

- The media builder enables you to create a customized, full-featured Linux-based and Windows-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 this knowledge base article.

32-bit 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).



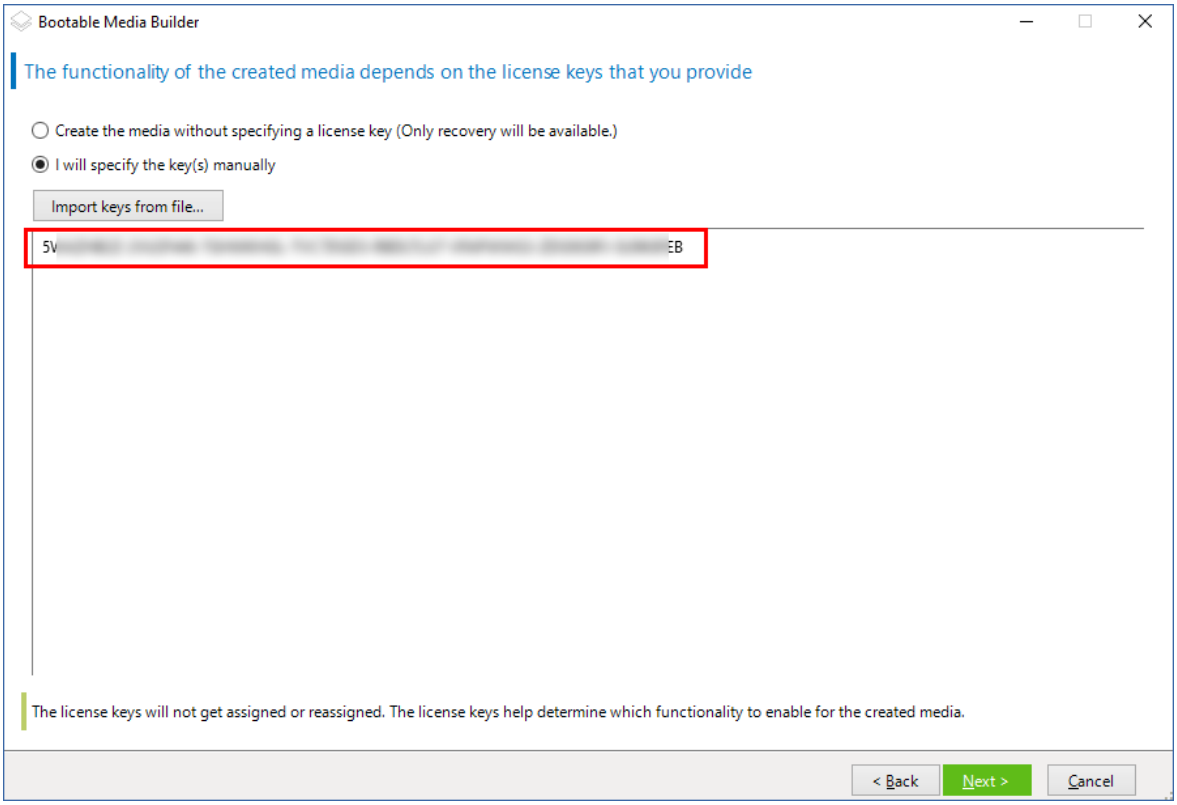
Linux-based bootable media

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

© Acronis International GmbH, 2003-2026

operations.

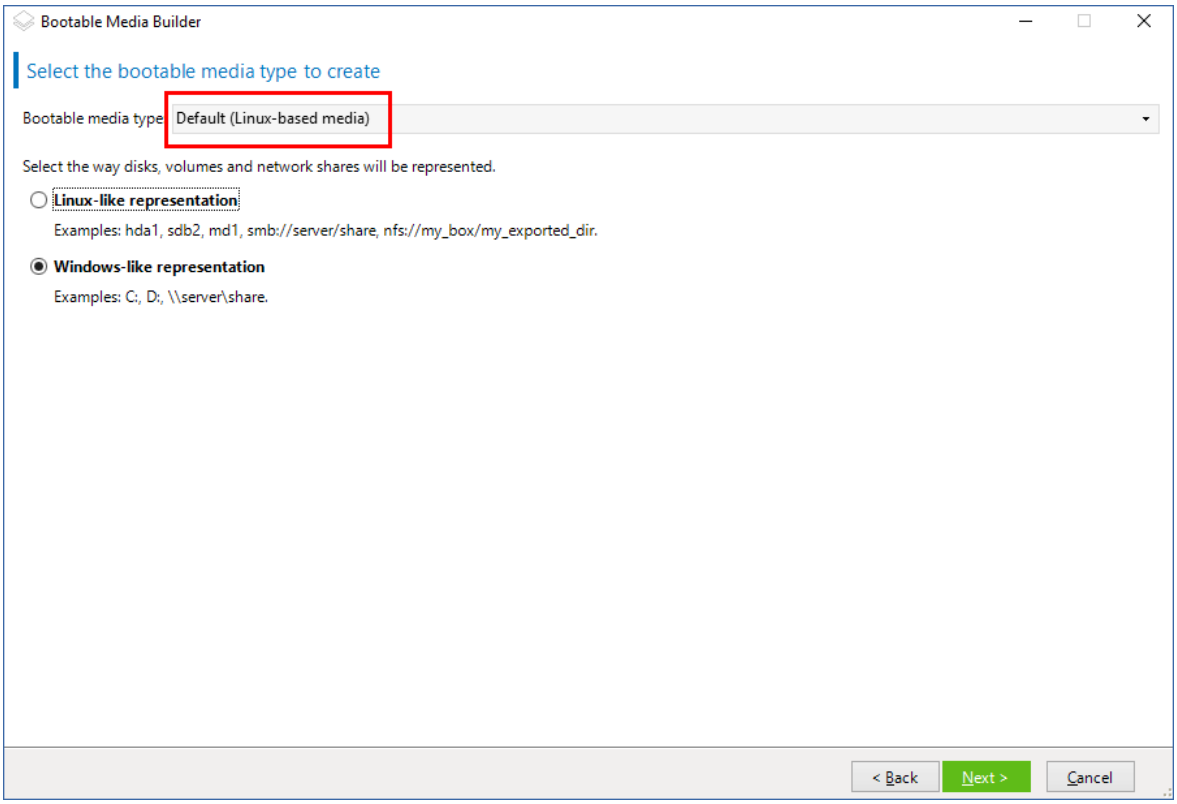


3. Select **Bootable media type: Default (Linux-based media)**.

   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.

© Acronis International GmbH, 2003-2026



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**

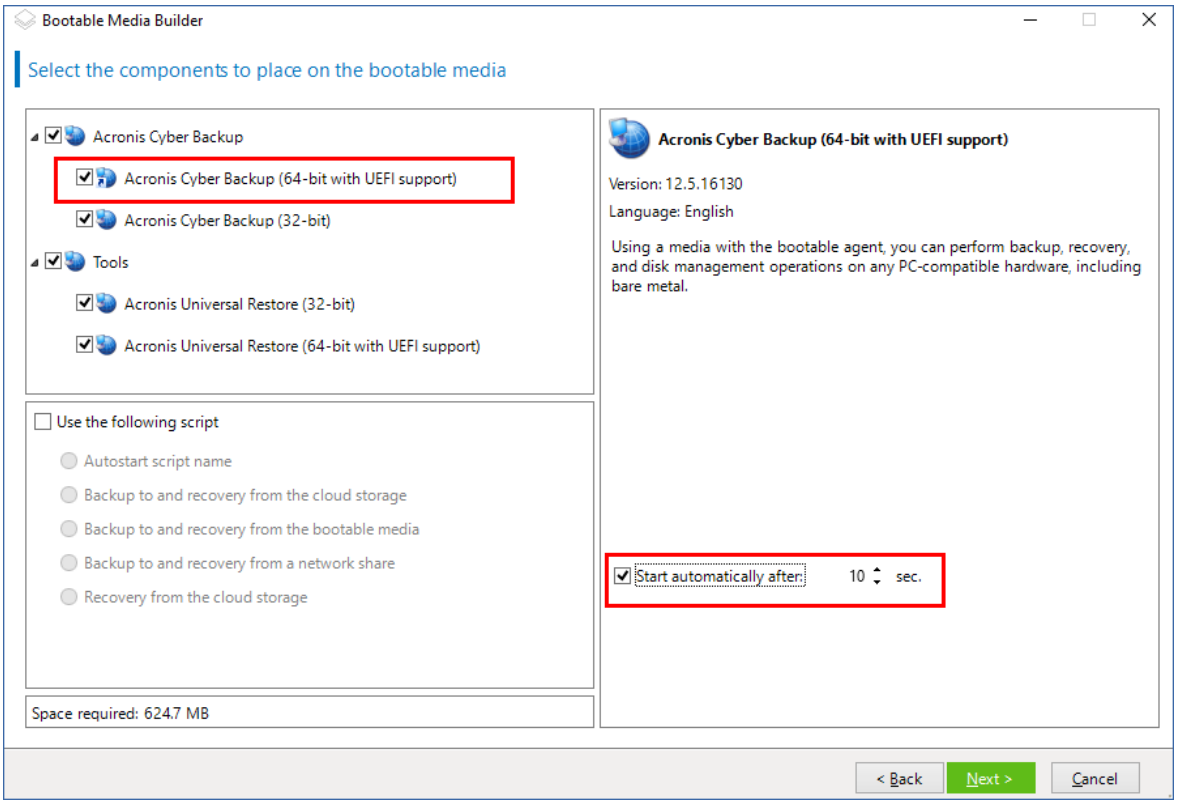
   For more information about the available parameters, see Kernel parameters.
5. [Optional] Select a language that will be used in the bootable media.
6. Select the components to be placed on the media: the Acronis Cyber Protect bootable agent, and/or Universal Restore if you plan to restore the system on dissimilar hardware.

   The bootable agent allows you to perform backup, recovery, and disk management operations on any PC-compatible hardware, including bare metal.

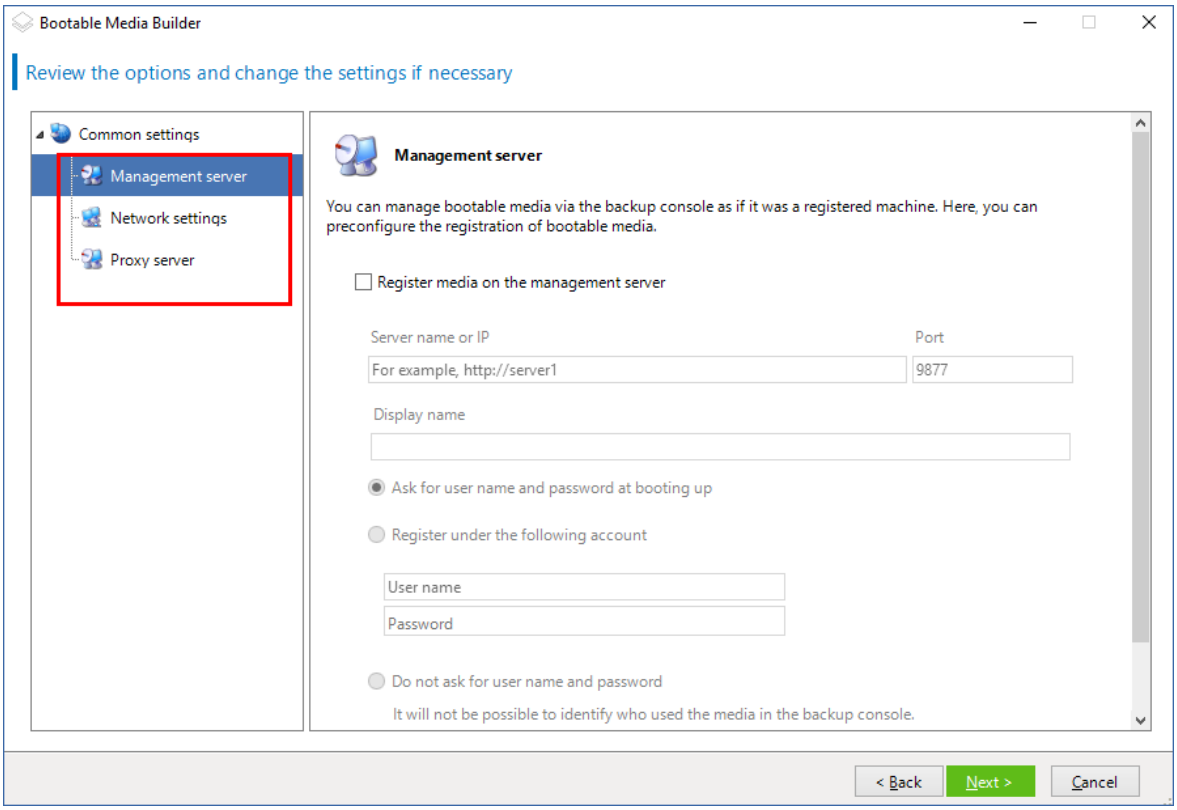
   Universal Restore allows you to boot an operating system recovered to dissimilar hardware or to a virtual machine. The tool finds and installs drivers for devices that are critical for starting the operating system, such as storage controllers, motherboard, or chipset.
7. [Optional] Specify the timeout 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.

© Acronis International GmbH, 2003-2026



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.



© Acronis International GmbH, 2003-2026

10. [Optional] Specify network settings: TCP/IP settings to be assigned to the machine network adapters. For more information, see "Network settings" (p. 621).
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. To specify the network authentication method, click **Wi-Fi settings**, and then select one of the following:
    - Open authentication
    - WEP
    - WEP Shared
    - IEEE 802.1X
    - WPA Personal
    - WPA Enterprise
    - WPA2 Personal
    - WPA2 Enterprise
14. 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.
15. [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.
16. If prompted, specify the host name/IP address and credentials for WDS/RIS, or a path to the media ISO file.
17. 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

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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**

 © Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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 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.

© Acronis International GmbH, 2003-2026

Custom scripts

Important
Creating custom scripts requires the knowledge of the Bash command language and JavaScript Object Notation (JSON). If you are not familiar with Bash, a good place to learn it is http://www.tldp.org/LDP/abs/html. The JSON specification is available at http://www.json.org.

Files of a script

Your script must be located in the following directories on the machine where Bootable Media Builder is installed:

- In Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- In Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

The script must consist of at least three files:

- **<script_file>.sh** - a file with your Bash script. When creating the script, use only a limited set of shell commands, which you can find at https://busybox.net/downloads/BusyBox.html. Also, the following commands can be used:
  - `acrocmd` - the command-line utility for backup and recovery
  - `product` - the command that starts the bootable media user interface

  This file and any additional files that the script includes (for example, by using the dot command) must be located in the **bin** subfolder. In the script, specify the additional file paths as **/ConfigurationFiles/bin/<some_file>**.
- **autostart** - a file for starting **<script_file>.sh**. The file contents must be as follows:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - a JSON file that contains the following:
  - The script name and description to be displayed in Bootable Media Builder.
  - The names of the script variables to be configured via Bootable Media Builder.
  - The parameters of controls that will be displayed in Bootable Media Builder for each variable.

Structure of autostart.json

Top-level object

Pair		Required	Description
Name	**Value type**		
`displayName`	string	Yes	The script name to be displayed in Bootable Media

© Acronis International GmbH, 2003-2026

			Builder.
`description`	string	No	The script description to be displayed in Bootable Media Builder.
`timeout`	number	No	A timeout (in seconds) for the boot menu before starting the script. If the pair is not specified, the timeout will be ten seconds.
`variables`	object	No	Any variables for **<script_file>.sh** that you want to configure via Bootable Media Builder. The value should be a set of the following pairs: the string identifier of a variable and the object of the variable (see the table below).

Variable object

Pair		Required	Description
Name	**Value type**		
`displayName`	string	Yes	The variable name used in **<script_file>.sh**.
`type`	string	Yes	The type of a control that is displayed in Bootable Media Builder. This control is used to configure the variable value. For all supported types, see the table below.
`description`	string	Yes	The control label that is displayed above the control in Bootable Media Builder.
`default`	string if `type` is `string`, `multiString`, `password`, or `enum` number if `type` is `number`, `spinner`, or `checkbox`	No	The default value for the control. If the pair is not specified, the default value will be an empty string or a zero, based on the control type. The default value for a check box can be `0` (the cleared state) or `1` (the selected state).
`order`	number (non-negative)	Yes	The control order in Bootable Media Builder. The higher the value, the lower the control is placed relative to other controls defined in **autostart.json**. The initial value must be `0`.
`min` (for `spinner`	number	No	The minimum value of the spin control in a spin box. If the pair is not specified, the value will be `0`.

© Acronis International GmbH, 2003-2026

only)			
`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",
```

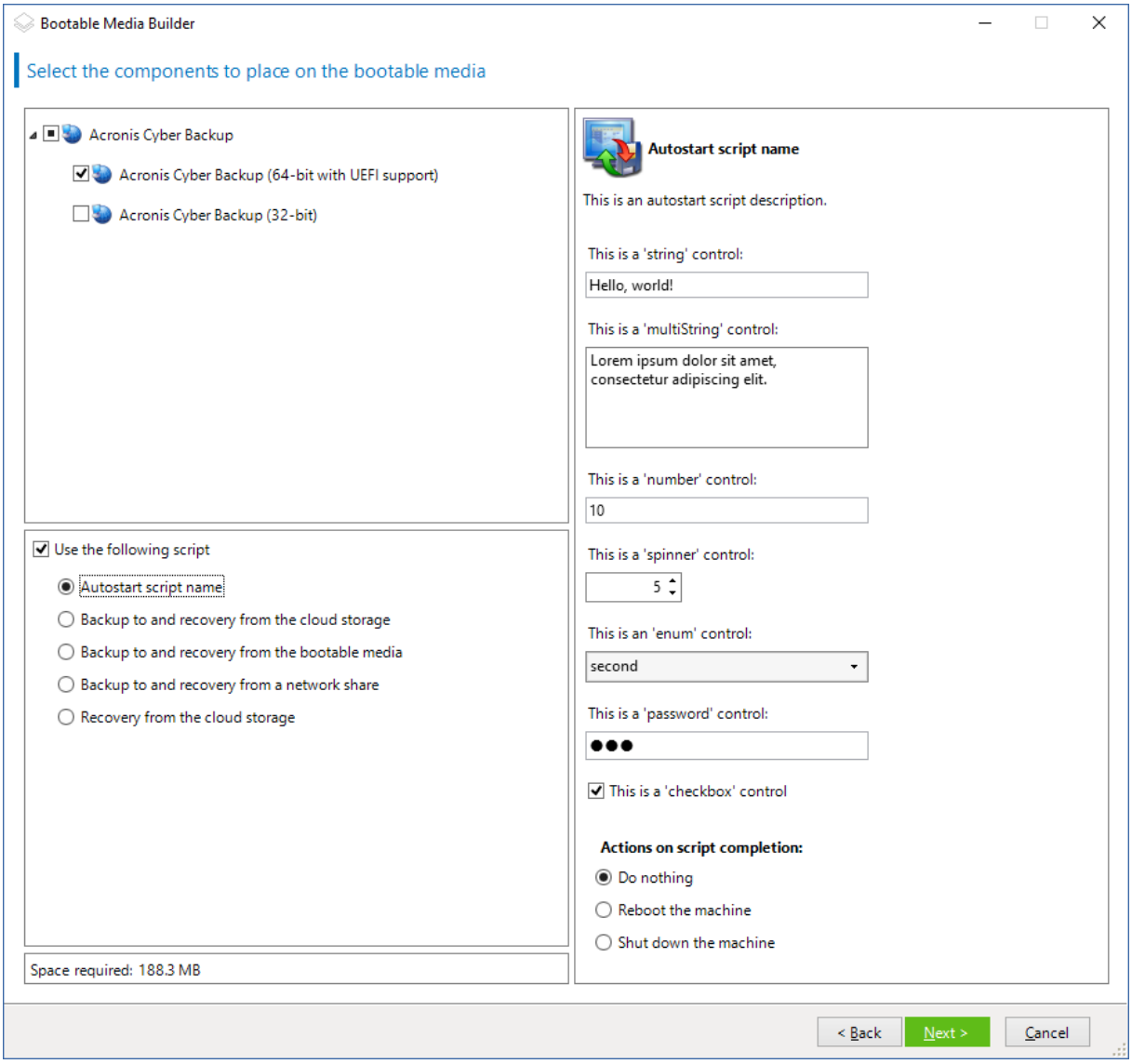

© Acronis International GmbH, 2003-2026

```
                "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"
```


© Acronis International GmbH, 2003-2026

```
            },
            "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.



© Acronis International GmbH, 2003-2026

Management server

While creating bootable media, you have an option to pre-configure the media registration on the management server.

Registering the media enables you to manage the media via the Cyber Protect console as if it was a registered machine. Besides the convenience of remote access, this grants an administrator the capability to trace all operations performed under bootable media. The operations are logged in **Activities**, so it is possible to see who started an operation and when.

If the registration was not pre-configured, it is still possible to register the media after booting the machine from it.

To pre-configure registration on the management server

1. Select the **Register media on the management server** check box.
2. In **Server name or IP**, specify the host name or IP address of the machine where the management server is installed. You can use one of the following formats:
   - `http://<server>`. For example, `http://10.250.10.10` or `http://server1`
   - `<IP address>`. For example, `10.250.10.10`
   - `<host name>`. For example, `server1` or `server1.example.com`
3. In **Port**, specify the port that will be used to access the management server. The default value is 9877.
4. In **Display name**, specify the name that will be displayed for this machine in the Cyber Protect 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 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 console, the media will be available under the

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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 `acrocmd` utility. The choice is available among:

- the default port
- the currently used port
- the new port (enter the port number)

If the port has not been pre-configured, the agent uses port 9876.

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:

© Acronis International GmbH, 2003-2026

1. Select the INF file.
2. Click **Remove**.

Windows-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 example, for building the ISO image manually or adding other tools to the image.

You can create WinRE images without any additional preparation, or create WinPE images after installing Windows Automated Installation Kit (AIK) or Windows Assessment and Deployment Kit (ADK).

WinRE images

Creating WinRE images is supported for the following operation systems:

- Windows 7 (64-bit)
- Windows 8 (32-bit and 64-bit)
- Windows 8.1 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)
- Windows 11 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)
- Windows Server 2022 (64-bit)
- Windows Server 2025 (64-bit)

WinPE 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 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

© Acronis International GmbH, 2003-2026

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).

Note
Disk management via bootable media is not supported on Windows 8 and later. To perform disk management operations on these operating systems, install Acronis Disk Director. For more information, see this knowledge base article.

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 and Windows Automated Installation Kit (AIK) on the same machine.

To prepare a machine

1. Download the AIK image file from the Microsoft website, as follows:
   - For Windows Vista (PE 2.0): https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - For Windows Vista SP1 and Windows Server 2008 (PE 2.1): https://www.microsoft.com/en-us/download/details.aspx?id=9085
   - For Windows 7 (PE 3.0): https://www.microsoft.com/en-gb/download/details.aspx?id=5753
     For Windows 7 SP1 (PE 3.1), you also need the AIK supplement available at https://www.microsoft.com/en-us/download/details.aspx?id=5188
2. Burn the image file to a DVD disk or a USB flash drive.
3. From image file, install the following:
   - Microsoft .NET Framework (NETFXx86 or NETFXx64, depending on your hardware)
   - MSXML (Microsoft XML parser)
   - Windows AIK
4. Install Bootable Media Builder on the same machine.

Preparation: WinPE 4.0 and later

To be able to create or modify PE 4 or later images, install Bootable Media Builder and Windows Assessment and Deployment Kit (ADK) on the same machine.

To prepare a machine

1. Download the ADK setup program from the Microsoft website.
   The following Windows versions are supported:
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)

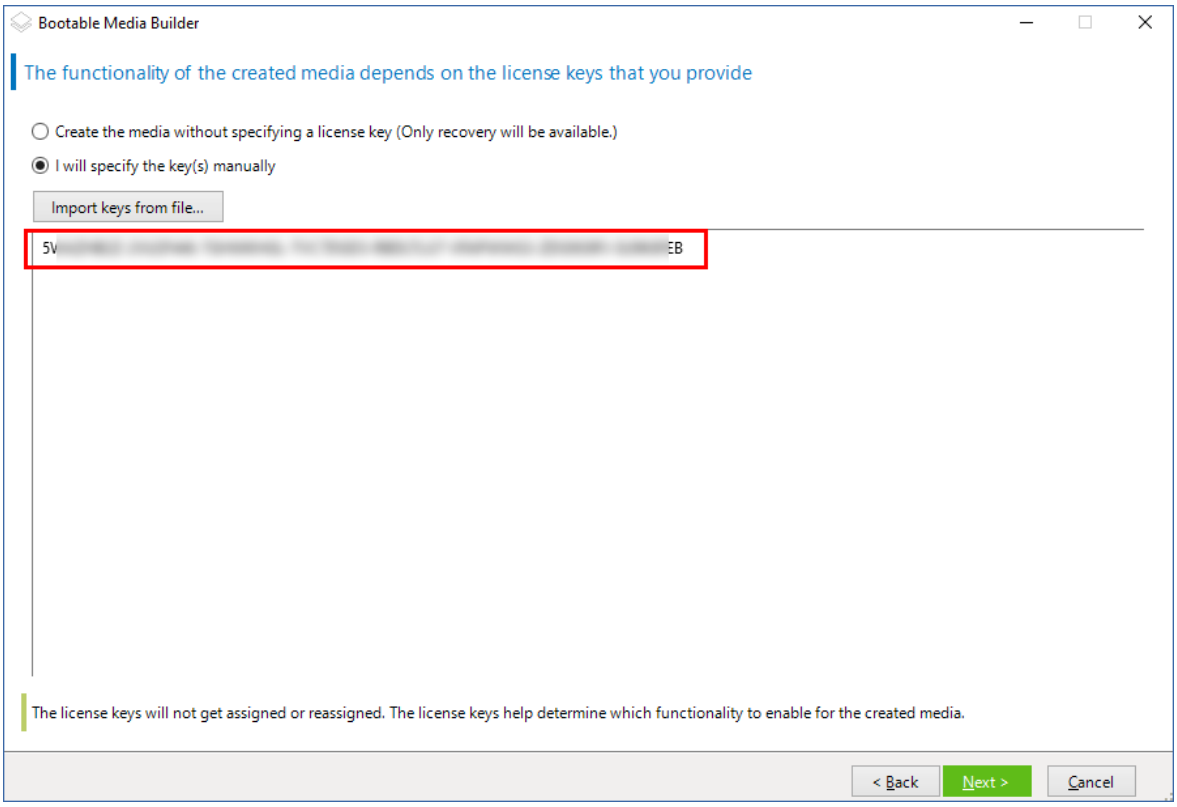
© Acronis International GmbH, 2003-2026

2. Install Assessment and Deployment Kit.
3. Install Bootable Media Builder.

Adding Acronis Plug-in to WinPE

To add Acronis Plug-in to WinPE:

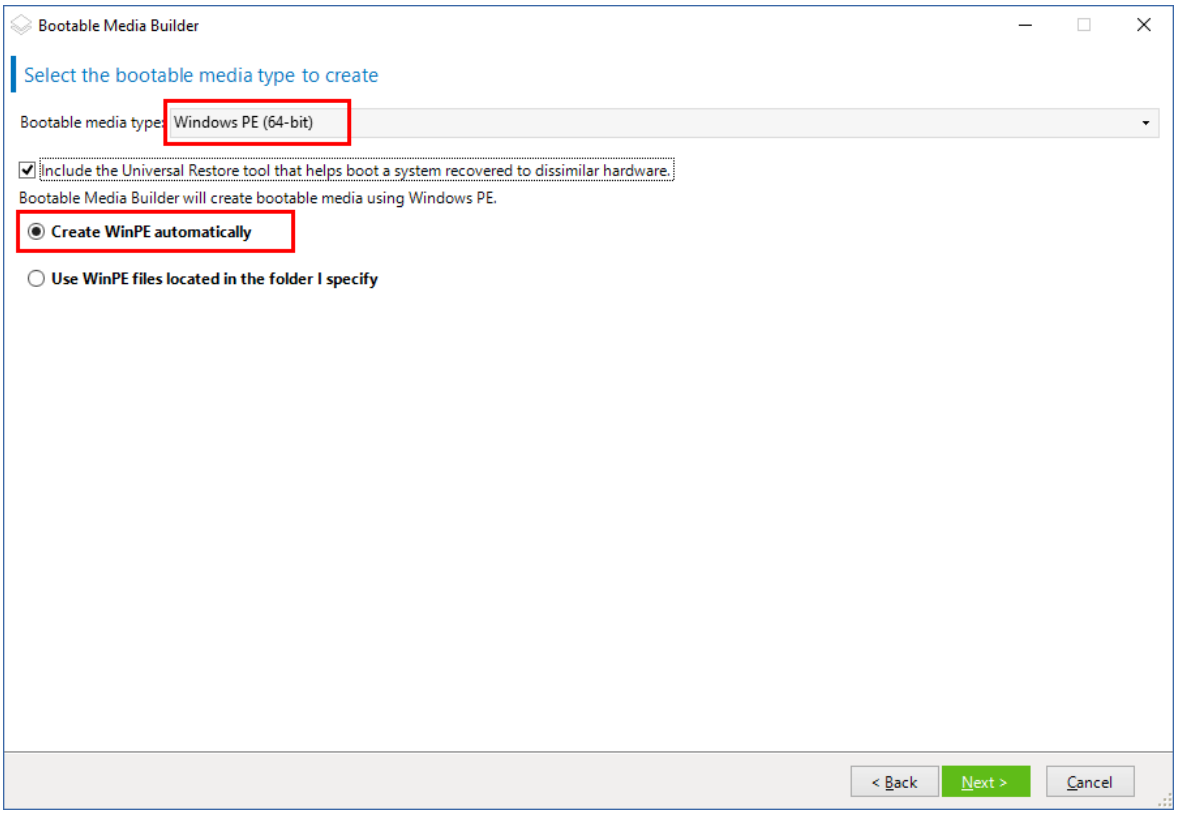
1. Start the Bootable Media Builder.
2. To create a full-featured bootable media, specify an Acronis Cyber Protect license key. This key is used to determine which features will be included in the bootable media. No licenses will be revoked from any machines.
   If you don't specify a license key, the 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.

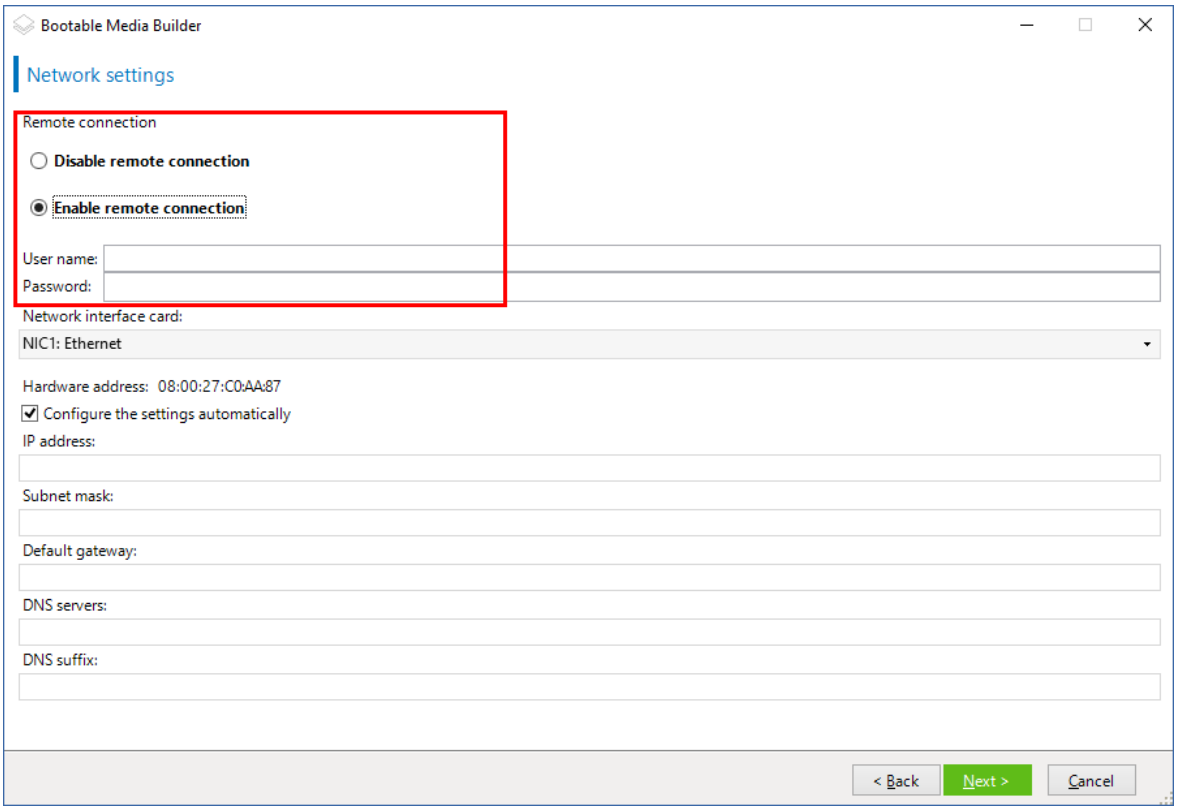
© Acronis International GmbH, 2003-2026



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 console.

© Acronis International GmbH, 2003-2026



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 Advanced and Acronis Cyber Protect Backup Advanced licenses.

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.

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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 bootable media on the management server" (p. 601).

Configuring the display mode for Linux-based bootable media

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, you can configure it manually.

To configure the display mode

1. In the boot menu, press F11.
2. On the command line, enter `vga=ask`, and then proceed with booting.
3. From the list of supported video modes, select the appropriate mode by typing its number (for example, `318`), and then press Enter.

Note
When using Bootable media builder, you can create bootable media in which these settings are preconfigured. For example, to use the same settings as in the procedure above, when configuring the bootable media, specify `vga=0x318` in the **Kernel parameters** window.

NIC teaming support

Teaming (bonding) of network interface cards (NICs) is preserved both during the recovery of a workload with teamed NICs, and after the recovery.

Note
Network configuration, including NIC teaming, is not preserved when you recover to dissimilar hardware.

 © Acronis International GmbH, 2003-2026

You can disable NIC teaming during recovery, if you recover a workload in any of the following ways:

- With downloaded bootable media
- With Linux-based bootable that is created in Bootable media builder
- Via Acronis Startup Recovery Manager
- Via one-click recovery
- Via recovery with restart, by using the Linux recovery environment

To disable NIC teaming during recovery

1. On the backed-up machine, open the following configuration files for editing:
   - Windows (64-bit)

     ```
     C:\Program Files\Common Files\Acronis\BackupAndRecoveryAgent\bootagent_
     abr64.config
     ```

     ```
     C:\Program Files\Common Files\Acronis\BackupAndRecoveryAgent\bootagent_abr64_
     restore.config
     ```

   - Windows (32-bit)

     ```
     C:\Program Files\Common Files\Acronis\BackupAndRecoveryAgent\bootagent_abr.config
     ```

     ```
     C:\Program Files\Common Files\Acronis\BackupAndRecoveryAgent\bootagent_abr_
     restore.config
     ```

   - Linux (64-bit)

     ```
     /usr/lib/Acronis/BackupAndRecoveryAgent/bootagent_abr64.config
     ```

     ```
     /usr/lib/Acronis/BackupAndRecoveryAgent/bootagent_abr64_restore.config
     ```

   - Linux (32-bit)

     ```
     /usr/lib/Acronis/BackupAndRecoveryAgent/bootagent_abr.config
     ```

     ```
     /usr/lib/Acronis/BackupAndRecoveryAgent/bootagent_abr_restore.config
     ```

2. In both configuration files, find the following line:
   - Windows:

     ```
     <kernel64 name="kernel64.dat" value="product=bootagent media_for_windows"
     target="abr64ker.dat"/>
     ```

   - Linux:

© Acronis International GmbH, 2003-2026

```
<kernel64 name="kernel64.dat" value="product=bootagent media_for_linux"
target="abr64ker.dat"/>
```

3. Edit the line as follows:
   - Windows

     ```
     <kernel64 name="kernel64.dat" value="product=bootagent DONT_CREATE_BONDING=1
     media_for_windows" target="abr64ker.dat"/>
     ```

   - Linux

     ```
     <kernel64 name="kernel64.dat" value="product=bootagent DONT_CREATE_BONDING=1
     media_for_linux" target="abr64ker.dat"/>
     ```

4. Save the configuration files.
5. Recover the workload by using any of the supported ways.

As a result, NIC teaming will not be used during recovery.

Note
The recovered workload retains NIC teaming. To disable NIC teaming after recovery, reconfigure the network settings of the workload.

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 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**.

© Acronis International GmbH, 2003-2026

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 Windows-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.

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.

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**.

 © Acronis International GmbH, 2003-2026

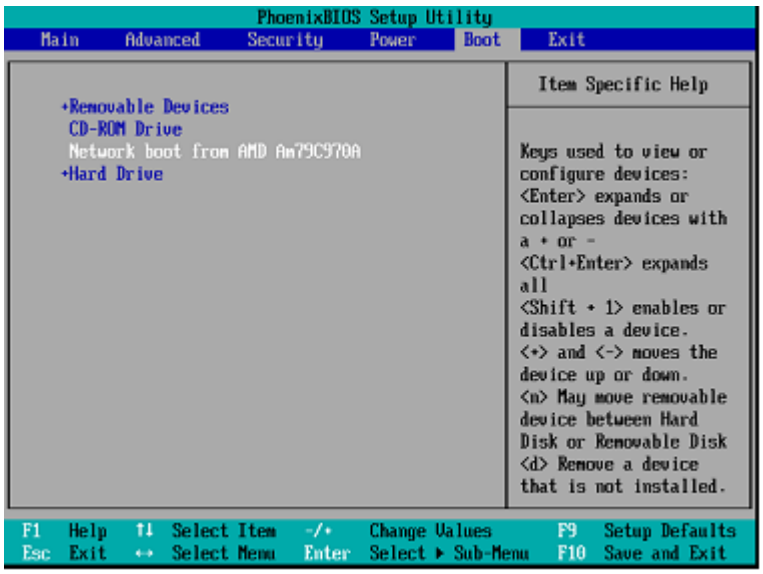
3. Accept the terms of the license agreement and the privacy statement, and then click **Proceed**.
4. Click **Customize installation settings**.
5. Next to **What to install**, click **Change**.
6. Select the **PXE Server** check box. If you do not want to install other components on this machine, clear 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.

© Acronis International GmbH, 2003-2026

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 see: https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/boot-from-pxe-server.

© Acronis International GmbH, 2003-2026

Startup Recovery Manager

Startup Recovery Manager is a bootable component that resides on the hard drive. With Startup Recovery Manager, you can start the bootable rescue utility without using a separate bootable media.

If a failure occurs, restart the machine, wait for the prompt **Press F11 for Acronis Startup Recovery Manager** to appear, and then press F11 or select the Startup Recovery Manager from the boot menu (if you use the GRUB boot loader). Startup Recovery Manager starts and you can perform a recovery.

Startup Recovery Manager is supported for Windows and Linux machines.

Important
Activating Startup Recovery Manager on a machine with encrypted system volume requires at least one non-encrypted volume on the same machine.

Disk space requirements

Startup Recovery Manager requires disk space for temporary files. The requirements vary according to the machine on which Startup Recovery Manager is activated.

The table below summarizes the available options.

Boot mode	Machine without Secure Zone		Machine with Secure Zone
	With non-encrypted system volume	**With encrypted system volume**	**With encrypted or non-encrypted system volume**
BIOS	200 MB on the system volume	400 MB on an unencrypted volume	400 MB on the Secure Zone
UEFI	200 MB on the EFI system partition (ESP)	One of the following: • 400 MB on the EFI system partition (ESP) • 200 MB on the EFI system partition (ESP) and 200 MB on an unencrypted partition that is accessible during the boot process	400 MB on the Secure Zone

© Acronis International GmbH, 2003-2026

Note
Recovery with restart requires additional disk space. To check how much additional space is required, see "Disk space requirements" (p. 541).

Limitations

- [Not applicable to GRUB that is installed to the master boot record] Activating Startup Recovery Manager overwrites the master boot record (MBR) with its own boot code. As a result, you might need to reactivate any third-party boot loaders after the activation.
- [Not applicable to GRUB] Before activating Startup Recovery Manager in Linux, we recommend that you install the boot loader to the root partition's boot record or to the /boot partitions' boot record instead of installing it to the master boot record. Otherwise, manually reconfigure the boot loader after the activation.

Activating Startup Recovery Manager

To enable the boot-time prompt **Press F11 for Acronis Startup Recovery Manager** (or add the **Startup Recovery Manager** item to GRUB menu), you must activate Startup Recovery Manager.

Note
Backup operations that create One-click recovery backups will fail if Startup Recovery Manager is not activated.

To activate Startup Recovery Manager

On a machine with an agent

1. In the Cyber Protect console, select the machine on which you want to activate Startup Recovery Manager.
2. Click **Details**.
3. Enable the **Startup Recovery Manager** switch.

On a machine without an agent

1. Boot the machine by using a bootable media.
2. In the bootable media graphical interface, click **Tools** > **Activate Startup Recovery Manager**.
3. Select **Activate**.
4. Click **OK**.
5. On the **Details** tab, check the **Result** row to verify that the activation succeeded.
6. Click **Close**.

 © Acronis International GmbH, 2003-2026

Deactivating Startup Recovery Manager

Deactivation disables the boot-time prompt **Press F11 for Acronis Startup Recovery Manager** (or removes the **Startup Recovery Manager** item from the GRUB menu).

If Startup Recovery Manager is not activated, you can still recover a machine that fails to boot by using one of the following options:

- Bootable media
- Network boot from a PXE server or Microsoft Remote Installation Services (RIS)

Note
Backup operations that create One-click recovery backups will fail if Startup Recovery Manager is not activated.

To deactivate Startup Recovery Manager

On a machine with an agent

1. In the Cyber Protect console, select the machine on which you want to deactivate Startup Recovery Manager.
2. Click **Details**.
3. Disable the **Startup Recovery Manager** switch.

On a machine without an agent

1. Boot the machine by using a bootable media.
2. In the bootable media graphical interface, click **Tools** > **Deactivate Startup Recovery Manager**.
3. Select **Deactivate**.
4. Click **OK**.
5. On the **Details** tab, check the **Result** row to verify that the deactivation succeeded.
6. Click **Close**.

© Acronis International GmbH, 2003-2026

Protecting mobile devices

The Acronis Cyber Protect 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 Acronis Cyber Protect app on a mobile device that runs one of the following operating systems:

- iOS 17 to iOS 26 (iPhone, iPod, iPad)
- Android 12 to Android 16

Important
To initiate the backup process, you must manually start the app.

What you can back up

- Contacts (name, phone number, and email)
- Photos (the original size and format of your photos are preserved)

  Note
  On iOS, live photos are restored as still images.

- 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, the Acronis Cyber Protect app automatically detects new data on the fly and uploads it to the Cloud.
- The **Use Wi-Fi only** option is enabled by default in the app settings. If this setting is turned on, the Acronis Cyber Protect 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.
- The battery optimization on your device might prevent the Acronis Cyber Protect app from proper operation. To run backups on time, you should stop the battery optimization for the app.

© Acronis International GmbH, 2003-2026

- You have two ways to save energy:
  - The **Back up while charging** functionality is disabled by default. If this setting is turned on, the Acronis Cyber Protect 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** is enabled by default. If this setting is turned on, the Acronis Cyber Protect 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.
- 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 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 Acronis Cyber Protect app, you can recover only the latest data versions. If you need to recover from a specific backup version, use the Cyber Protect console on either a tablet or a computer.
- Retention rules are not applied to backups of mobile devices.
- [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 Acronis Cyber Protect app

Depending on your mobile device, install the app from the App Store or Google Play.

How to start backing up your data

1. Open the app.
2. Sign in with your account.
3. Tap **Set up** to create your backup. Note that this button is displayed only when you have no backup of your mobile device.
4. Select the data categories that you want to back up. By default, all categories are selected.
5. [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**.
6. Tap **Back up**.

© Acronis International GmbH, 2003-2026

7. 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

Warning!
To recover mobile data, you must use the end-user account.

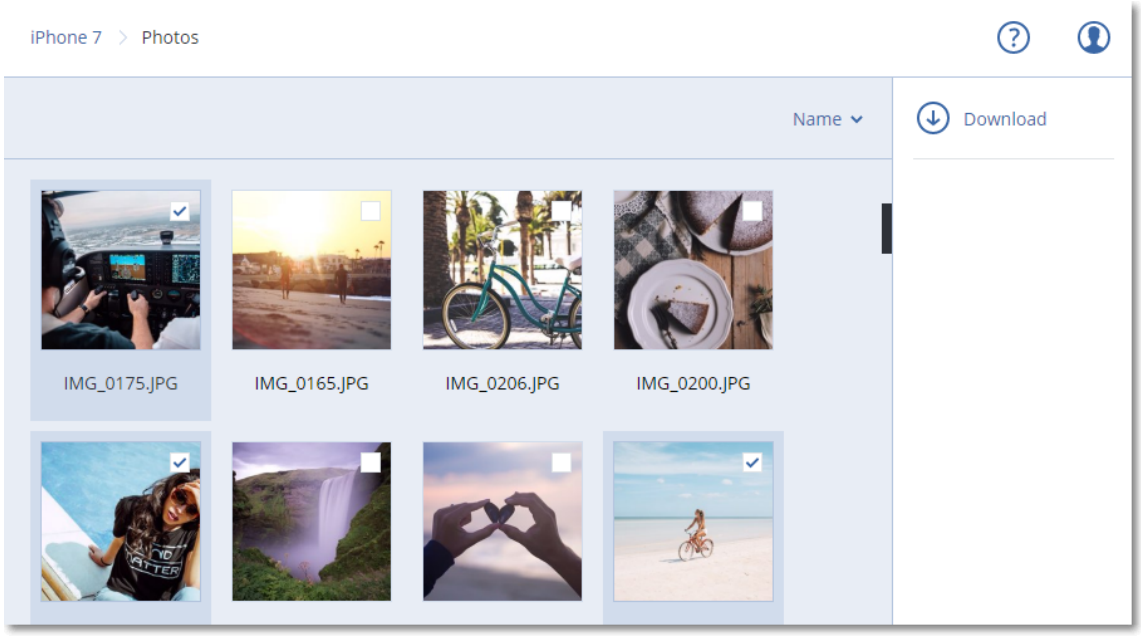
1. Open the Acronis Cyber Protect app.
2. Tap **Browse**.
3. Tap the device name.
4. Do one of the following:
   - To recover all of the backed-up data, tap **Recover all**. No more actions are required.
   - To recover one or more data categories, tap **Select**, and then tap the check boxes for the 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 console

1. On a computer, open a browser and type the Cyber Protect 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**.

© Acronis International GmbH, 2003-2026

- 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.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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 (physical) Entire machine (virtual) Databases to a live SQL Server instance Databases as files	Entire machine (physical) Entire machine (virtual)
Microsoft Exchange Server	Databases to a live Exchange Databases as files Granular recovery to a live Exchange or to Microsoft 365*	Entire machine (physical) Entire machine (virtual) Databases to a live Exchange Databases as files Granular recovery to a live Exchange or to Microsoft 365*	Entire machine (physical) Entire machine (virtual)
Microsoft SharePoint database servers	Databases to a live SQL Server instance Databases as files Granular recovery by using SharePoint Explorer	Entire machine (physical) Entire machine (virtual) Databases to a live SQL Server instance Databases as files Granular recovery by using SharePoint Explorer	Entire machine (physical) Entire machine (virtual)
Microsoft SharePoint front-end web servers	-	-	Entire machine (physical) Entire machine (virtual)
Active Directory Domain Services	-	Entire machine (physical) Entire machine (virtual)	-

* Granular recovery is also available from a mailbox backup.

© Acronis International GmbH, 2003-2026

Requirements for application-aware backups

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 Changing Temp Files and Folder Location (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 and machines with the agent installed inside, 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, recovery of application data from such backups will be impossble. 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.

© Acronis International GmbH, 2003-2026

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://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere-sdks-tools/8-0/virtual-disk-development-kit-programming-guide/backing-up-virtual-disks-in-vsphere/windows-backup-implementations/working-with-microsoft-shadow-copy.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 the built-in domain administrator (DOMAIN\Administrator) when enabling application backup.
  If you do not want to disable UAC, you must provide the credentials of the built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

  Note
  Use the built-in domain administrator account that was configured as part of the creation of the domain. Accounts created later are not supported.

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 the built-in domain administrator (DOMAIN\Administrator) when enabling application backup.
  If you do not want to disable UAC, you must provide the credentials of the built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

  Note
  Use the built-in domain administrator account that was configured as part of the creation of the domain. Accounts created later are not supported.

- 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

© Acronis International GmbH, 2003-2026

- 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 "Requirements for application-aware backups" (p. 644) 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, see "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.

 © Acronis International GmbH, 2003-2026

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 **Exchange Organization Administrators** role group
2010/2013/2016/2019	Databases, Database Availability Groups (DAG)	Membership in the **Server Management** role group.

A full backup contains all of the selected Exchange Server data.

An incremental backup contains the changed blocks of the database files, the checkpoint files, and a small number of the log files that are more recent than the corresponding database checkpoint. Because changes to the database files are included in the backup, there is no need to back up all the transaction log records since the previous backup. Only the log that is more recent than the checkpoint needs to be replayed after a recovery. This makes for faster recovery and ensures successful database backup, even with circular logging enabled.

The transaction log files are truncated after each successful backup.

To select Exchange Server data

1. Click **Devices** > **Microsoft Exchange**.
   The software shows the tree of Exchange Server Database Availability Groups (DAG), machines running Microsoft Exchange Server, and Exchange Server databases. If you configured Agent for Exchange as described in "Mailbox backup", 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, see "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**.

© Acronis International GmbH, 2003-2026

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

Acronis Cyber Protect supports *only* the Always On Availability Group (AAG) for SQL Server 2012 or later. Other cluster configurations, such as Basic Availability Groups, Always On Failover Cluster Instances, database mirroring, and log shipping are *not* supported.

Note
Always On Availability groups are supported only on the Enterprise edition of SQL Server. See https://learn.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2016?view=sql-server-2016&preserve-view=true#RDBMSHA.

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".

© Acronis International GmbH, 2003-2026

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.

 © Acronis International GmbH, 2003-2026

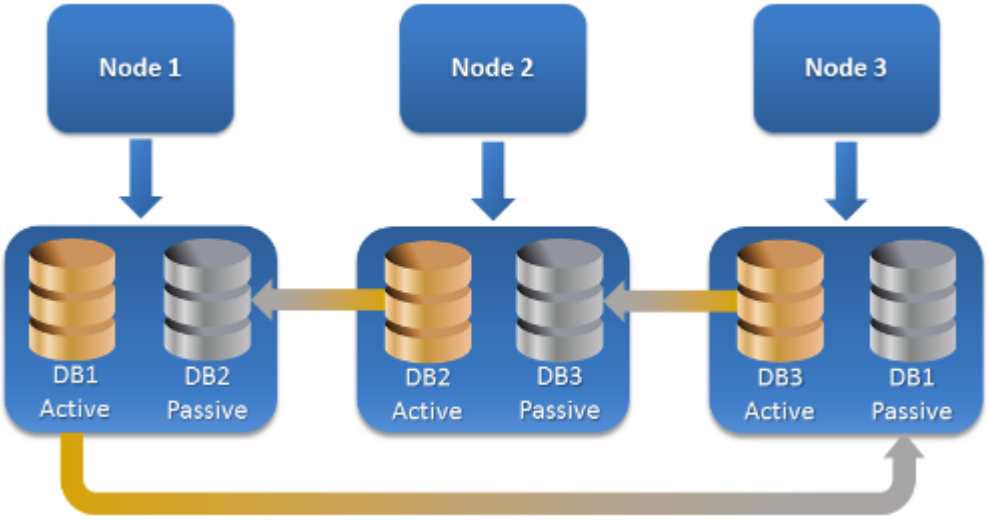
Cluster-aware backup

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 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".

© Acronis International GmbH, 2003-2026

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 individual physical machines, ESXi virtual machines, and Hyper-V virtual machines. It is not available for device groups.

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:

- The applications are backed up in a consistent state and thus will be available immediately after the machine is recovered.
- You can recover the SQL and Exchange databases, mailboxes, and mailbox items without recovering the entire machine.
- 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

© Acronis International GmbH, 2003-2026

machines only. You can enable the VSS full backup option if you want to truncate Exchange transaction logs on a physical machine.

- 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 or Agent for Hyper-V.

Note
Agentless application-aware backup is not supported for Hyper-V and VMware ESXi virtual machines that are running Windows Server 2022 or Windows Server 2025. To protect Microsoft applications on these machines, install the protection agent inside the guest operating system. For more information, see "Configuring application-aware backup of virtual machines running Windows Server 2022 and later" (p. 652).

Agent for VMware (Virtual Appliance) can create application-aware backups, but cannot recover application data from them. To recover application data from backups created by this agent, you need Agent for VMware (Windows), Agent for SQL, or Agent for Exchange on a machine that has access to the location where the backups are stored. When configuring recovery of application data, select the recovery point on the **Backup storage** tab, and then select this machine in **Machine to browse from**.

Additional requirements are listed in "Requirements for application-aware backups" (p. 644) and "Required user rights for application-aware backups" (p. 653).

Note
Application-aware backups of Hyper-V virtual machines may fail with the error "WMI 'ExecQuery' failed executing query." or "Failed to create a new process via WMI" if the backups are performed on a host under high load, due to no or delayed response from Windows Management Instrumentation. Retry these backups in a time slot when the load on the host is lower.

Configuring application-aware backup of virtual machines running Windows Server 2022 and later

To perform application-aware backup on Hyper-V and VMware ESXi virtual machines that are running Windows Server 2022 or Windows Server 2025, you must use agent-based backup. For more information about the backup modes, see "Agent-based and agentless backup" (p. 36).

 © Acronis International GmbH, 2003-2026

	Agent-based backup	Agentless backup
Application-aware backup	Supported	Not supported
Virtual machine icon in the Cyber Protect console		

To configure application-aware backup in the agent-based mode

1. Install the protection agent (such as Agent for Windows, Agent for SQL, or Agent for Exchange) inside the guest operating system of the virtual machine.
2. In the Cyber Protect console, select the machine on which you installed the protection agent.
3. Configure the application-aware backup in a new protection plan.
4. Apply the protection plan to the virtual machine.
5. Run the protection plan.

As a result, a backup archive that contains the application-aware backup will be created.

Required user rights for application-aware backups

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.

© Acronis International GmbH, 2003-2026

If you do not want to disable UAC, you must provide the credentials of the built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

Note
Use the built-in domain administrator account that was configured as part of the creation of the domain. Accounts created later are not supported.

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 UAC, you must provide the credentials of the built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

Note
Use the built-in domain administrator account that was configured as part of the creation of the domain. Accounts created later are not supported.

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.

 © Acronis International GmbH, 2003-2026

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 see 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.

© Acronis International GmbH, 2003-2026

For information about configuring the **ApplicationImpersonation** management role, see 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**.

© Acronis International GmbH, 2003-2026

- 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:

© Acronis International GmbH, 2003-2026

- [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.

© Acronis International GmbH, 2003-2026

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 **Exchange Organization Administrators** role group.
2010/2013/2016/2019	Databases	Membership in the **Server Management** role group.

Alternatively, you can recover the databases (storage groups) as files. The database files, along with transaction log files, will be extracted from the backup to a folder that you specify. This can be useful if you need to extract data for an audit or further processing by third-party tools, or when the recovery fails for some reason and you are looking for a workaround to mount the databases manually.

© Acronis International GmbH, 2003-2026

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 see 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.

© Acronis International GmbH, 2003-2026

- 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

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

© Acronis International GmbH, 2003-2026

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. 647)

- 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.

 © Acronis International GmbH, 2003-2026

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, see "Protecting Microsoft 365 mailboxes" (p. 669).

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.

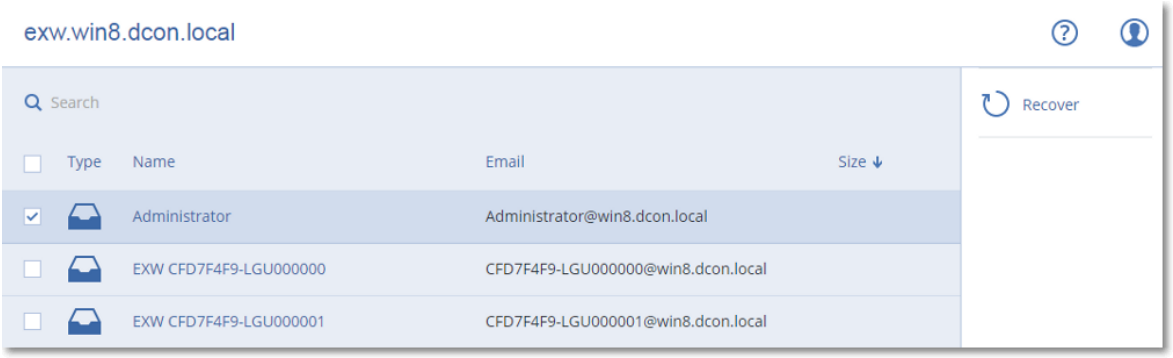
   If the machine is offline, the recovery points are not displayed. Use other ways to recover:
   - [Only when recovering from an application-aware backup] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent 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**.

 © Acronis International GmbH, 2003-2026

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. 655).
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

© Acronis International GmbH, 2003-2026

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.

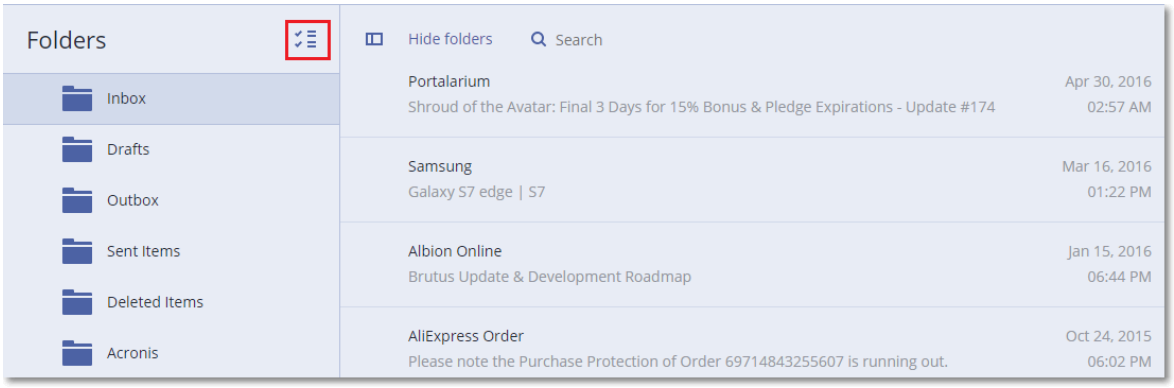
   The following search options are available. Wildcards are not supported.
   - For email messages: search by subject, sender, recipient, and date.
   - For events: search by title and date.
   - For tasks: search by subject and date.
   - For contacts: search by name, email address, and phone number.

   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.

© Acronis International GmbH, 2003-2026



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. 655).
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.

© Acronis International GmbH, 2003-2026

- 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.

© Acronis International GmbH, 2003-2026

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**.

© Acronis International GmbH, 2003-2026

Protecting Microsoft 365 mailboxes

Important
This section is valid for on-premises deployments of Acronis Cyber Protect. If you are using a cloud deployment, see the Acronis Cyber Protect Cloud documentation.

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.

© Acronis International GmbH, 2003-2026

- With Agent for Office 365 in the on-premises deployment (local agent), you can protect up to 5000 workloads. With Agent for Microsoft 365 (cloud agent, available in the cloud deployment), you can protect up to 50000 workloads. For a comparison between the local and the cloud agent, see the Acronis Cyber Protect Cloud documentation.
- 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, see 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 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 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 console.

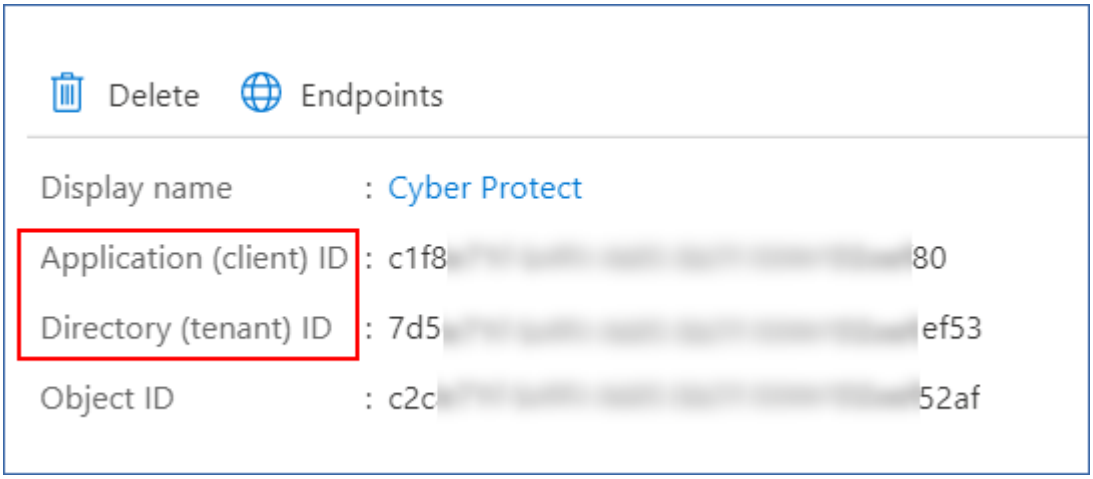
To create an application in Azure Active Directory

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.

© Acronis International GmbH, 2003-2026

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, see the Microsoft documentation.

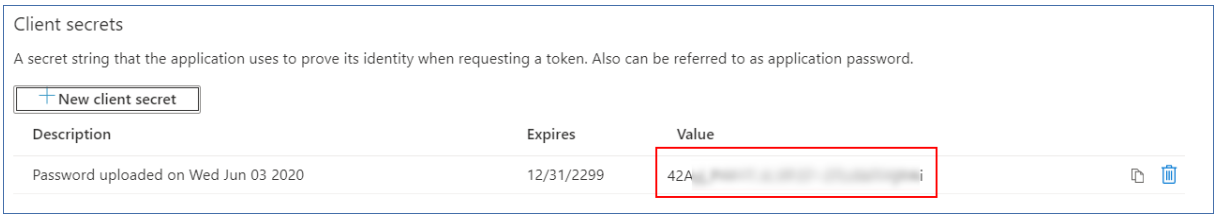
   To grant your application the necessary API permissions

   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.

© Acronis International GmbH, 2003-2026



For more information on the application secret, see 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 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, see 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 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. 662).
2. In the Cyber Protect 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.

© Acronis International GmbH, 2003-2026

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. 663), 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. 662).
2. In the Cyber Protect 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.

© Acronis International GmbH, 2003-2026

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. 655).
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**.

© Acronis International GmbH, 2003-2026

Protecting Google Workspace data

This feature is available only in cloud deployments of Acronis Cyber Protect. For a detailed description of this functionality, see https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html.

© Acronis International GmbH, 2003-2026

Protecting Oracle Database

Protection of Oracle Database is described in a separate document that is available at https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_17_OracleBackup_whitepaper_en-US.pdf.

© Acronis International GmbH, 2003-2026

Protecting SAP HANA

Protection of SAP HANA is described in a separate document available at https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_17_SAP_HANA_whitepaper_en-US.pdf.

© Acronis International GmbH, 2003-2026

Protecting Proxmox virtual machines and containers

You can perform agentless backup of Proxmox virtual machines and containers by installing Agent for Proxmox on the protected host.

Agent for Proxmox is bundled with Agent for Linux (64-bit), and requires that Agent for Linux is also installed on the host. For more information about how to download the installation file, see "Downloading protection agents" (p. 129).

Hosts running Proxmox VE 8.2 or later are supported. In clustered environments, you must install an agent on each node.

The following Proxmox storages are supported for backup and recovery:

- For virtual machines: All storages on which a virtual machine can be created
- For containers: LVM Thin, Ceph/RBD, BtrFS

The following backup location are available for Proxmox virtual machines and containers:

- The cloud storage (including partner-hosted storage)
- Public cloud storages
- Network folders on SMB and NFS shares
- Local folders

Limitations for Proxmox workloads

The following limitations apply to backup and recovery of Proxmox virtual machines and containers.

General

- The following features are not supported:
  - Application-aware backup
  - VM replication
- You cannot recover virtual disks or containers to `CephFS` storage.
- Disks for which the backup option is disabled in Proxmox VE are not backed up.
- During a recovery, selecting the disk provisioning type (thin/thick) will only work if the target storage supports the selected type. For example, LVM storage supports thick disks only. If you select thin disk allocation, this option will be ignored.

Virtual machines

- The following items are not backed up:
  - VM templates
  - Detached disks
  - Snapshots

 © Acronis International GmbH, 2003-2026

- TPM state device content.

  When you recover a virtual machine as a new machine, it will have a new, empty TPM state device. For example, if BitLocker is enabled on such a machine, you must use the BitLocker recovery key.

- At least one `Directory` storage is required for temporary files.
- Changed block tracking (CBT) is not available for powered-off virtual machines and virtual machines that went through a power cycle (power off, then power on). Lacking CBT information might lead to slower backups.
- During a backup, powered off virtual machines are powered on, and then kept in a frozen state that does not use RAM or CPU resources on the host.
- Locked virtual machine cannot be backed up. For example, hibernated virtual machines are locked.

Containers

- Only the following storage types are supported for backup and recovery: LVM Thin, Ceph/RBD, BtrFS.
- Containers for which snapshots are disabled are not supported.
- Changed block tracking (CBT) is not available.
- `OS type` property is not recovered.

Installing Agent for Proxmox

Agent for Proxmox is bundled with Agent for Linux (64-bit), and requires that Agent for Linux is also installed on the protected host.

You must install Agent for Proxmox locally, on the protected host, by using one of the following options:

- Graphical user interface

  For more information, see "Installing protection agents in Linux" (p. 131).
- Command-line interface

  For more information, see "Installing and uninstalling protection agents in Linux" (p. 142).

After you install the agent on the host, you can see all virtual machines and containers that are available on that host in the Cyber Protect console, on the **Devices** > **Proxmox** tab.

Backing up Proxmox workloads

You can back up Proxmox virtual machines and containers.

To back up a workload, create a protection plan. For more information, see "Creating a protection plan" (p. 243).

In the protection plans for Proxmox workloads, only the **Backup** module is available.

 © Acronis International GmbH, 2003-2026

You can also back up the Proxmox host separately, as a Linux server. To avoid double backups, you can configure file filers in the protection plan for the host and exclude the directories that contain the virtual machine data.

Recovering Proxmox workloads

You can recover a backed-up Proxmox virtual machine as:

- A physical machine.
- The original or a new virtual machine on the same hypervisor.
- A new machine on a different hypervisor. See "Cross-platform recovery" (p. 503).

For more information about recovering a virtual machine, see "Recovering a virtual machine as a physical machine" (p. 521) and "Recovering a virtual machine as a virtual machine" (p. 523).

You can recover a backed-up Proxmox container as:

- The original container.
- A new Proxmox container. Cross-platform recovery is not supported.

For more information about recovering a container, see "Recovering containers" (p. 531).

You can recover files from backed-up Proxmox virtual machines and containers to the Proxmox host or network storage attached to it. You cannot perform file-level recovery to a virtual machine or container.

© Acronis International GmbH, 2003-2026

Antimalware and web protection

Note
On Windows workloads, antimalware protection and URL filtering require Agent for Active Protection and Agent for Antimalware protection and URL filtering. For more information, see "Dynamic installation of antimalware components" (p. 159).

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.

Supported operating systems for antivirus and antimalware protection

Note
For endpoints running on Intel or AMD CPUs, this functionality is supported only on processors that include the SSE4.2 instruction set, as follows:

- Intel CPUs released after 2011
- AMD CPUs released after 2012

Important
Protected Process Light (PPL) is a Windows security feature that ensures anti-tampering of antivirus and antimalware and Active Protection processes. Windows legacy operating systems block the usage of the PPL feature. As a result, we cannot guarantee that antimalware and antivirus protection can fully protect workloads running on these operating systems.
For a list of legacy operating systems, see "Agent for Windows (Legacy)" (p. 62).

Active protection, antivirus and antimalware features are supported on the following platforms.

Operating system	Version/Distribution
Windows	• Windows 7 Service Pack 1 and later • Windows Server 2008 R2 Service Pack 1 and later

© Acronis International GmbH, 2003-2026

Operating system	Version/Distribution
	Note For Windows 7, you must install the following updates from Microsoft before installing the protection agent: • Windows 7 Extended Security Updates (ESU) • KB4474419 • KB4490628 For more information on the required updates, see this knowledge base article.
Linux	• Red Hat Linux 7.x, 8.x, 9.x • CloudLinux 6.10, 7.x, 8.x • CentOS 6.5 and later 6.x versions, 7.x, 8.x • Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 • Debian 8.x, 9.x, 10,x, 11.x • Oracle Linux 7.x, 8.x, 9.x • SUSE Enterprise Linux 15.x • openSUSE Leap 15.x **Note** The Behavioral analysis engine supports the following Linux versions: • CentOS 7.x • Debian 10.x, 11.x • CloudLinux 7.x, 8.x • Ubuntu 16.04, 18.04, 20.04, and 22.04
macOS	• macOS 10.13.x – macOS 26

Antivirus and Antimalware protection

Feature	Windows	Linux	macOS
Fully-integrated Active Protection functionality	Yes	No	No
Real-time antimalware protection	Yes	Yes	Yes
Advanced real-time antimalware protection with local signature-based detection	Yes	Yes	Yes
Static analysis for portable executable files	Yes	No	Yes[1]
On-demand antimalware scanning	Yes	Yes[2]	Yes
Potentially unwanted application detection	Yes	Yes	Yes

© Acronis International GmbH, 2003-2026

Feature	Windows	Linux	macOS
Network folder protection	Yes	No[3]	No
Server-side protection	Yes	No	No
Scan of archive files	Yes	No	Yes
Scan of removable drives	Yes	No	Yes
Scan of new and changed files only	Yes	No	Yes
File/folder exclusions	Yes	Yes	Yes[4]
Processes exclusions	Yes	No	Yes
Behavioral analysis engine	Yes	Yes[5]	Yes
Exploit prevention	Yes	No	No
Quarantine	Yes	Yes	Yes
Quarantine auto clean-up	Yes	Yes	Yes
URL filtering (http/https)	Yes	No	Yes[8]
Corporate-wide whitelist	Yes	No	Yes
Microsoft Defender Antivirus management[7]	Yes	No	No
Microsoft Security Essentials management	Yes	No	No
Registering and managing Antivirus and Antimalware protection via Windows Security Center	Yes	No	No

[1] Static analysis for portable executable files is supported only for scheduled scans on macOS.

[2] Start conditions are not supported for on-demand scanning on Linux.

[3] Network folders in Linux are treated as local folders, hence Active Protection will automatically protect network folders in Linux OS, as if they are local folders.

[4] File/folder exclusions are only supported for the case when you specify files and folders that will not be scanned by real-time protection or scheduled scans on macOS.

[5] The Behavioral analysis engine supports the following Linux versions:

- CentOS 7.x
- Debian 10.x, 11.x
- CloudLinux 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.04, and 22.04

© Acronis International GmbH, 2003-2026

Feature	Windows	Linux	macOS
[7] Microsoft Defender Antivirus management is supported on Windows 8.1 and later. [8] URL filtering is supported on macOS 10.15 and later. [9] Removable drives are treated as local drives in Linux.			

Active Protection

Feature	Windows	Linux	macOS
Process Injects detection	Yes	No	No
Automatic recovery of affected files from the local cache	Yes	Yes	Yes
Self-defense for Acronis backup files	Yes	No	No
Self-defense for Acronis software	Yes	No	Yes (Only Active Protection and antimalware components)
Trusted/blocked process management	Yes	No	Yes
Processes/folders exclusions	Yes	Yes	Yes
Ransomware detection based on a process behavior (AI-based)	Yes	Yes	Yes
Cryptomining process detection based on process behavior	Yes	No	No
External drives protection (HDD, flash drives, SD cards)	Yes	No	Yes
Network folder protection	Yes	No*	Yes
Server-side protection	Yes	No	No
Zoom, Cisco Webex, Citrix Workspace, and Microsoft Teams protection	Yes	No	No
*Network folders in Linux are treated as local folders, hence Active Protection will automatically protect network folders in Linux OS, as if they are local folders.			

© Acronis International GmbH, 2003-2026

Antivirus and antimalware protection

Note
Some features might require additional licensing, depending on the applied licensing model.

The **Antivirus & Antimalware** module protects your Windows, Linux, and macOS machines from all recent malware threats. See the full list of supported antimalware features in "Supported operating systems for antivirus and antimalware protection" (p. 681).

Antivirus & Antimalware protection is supported and registered in Windows Security Center.

Antimalware features

- Detection of malware in files in the real-time protection and on-demand modes
- Detection of malicious behavior in processes (for Windows)
- Blocking access to malicious URLs (for Windows)
- Placing dangerous files to the quarantine
- Adding trusted corporate applications to the allowlist

Scanning types

You can configure antivirus and antimalware protection to run constantly in the background or on demand.

Real-time protection

Real-time protection checks all files that are being executed or opened on a machine to prevent malware threats.

To prevent potential compatibility and performance issues, real-time protection cannot work in parallel with other antivirus solutions that also use real-time protection features. The statuses of other installed antivirus solutions are determined through Windows Security Center. If the Windows machine is already protected by another antivirus solution, real-time protection is automatically turned off.

To enable real-time protection, disable or uninstall the other antivirus solution. Real-time protection can replace Microsoft Defender real-time protection automatically.

Note
On machines running Windows Server operating systems, Microsoft Defender will not be turned off automatically when real-time protection is enabled. An administrator must turn off the Microsoft Defender manually to avoid potential compatibility issues.

You can choose one of the following scan modes:

 © Acronis International GmbH, 2003-2026

- **Smart 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 or 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.

Scheduled scan

Antimalware scanning is performed according to a schedule.

You can choose one of the following scan modes.

- **Quick scan**—Checks only workload system files.
- **Full scan**—Checks all files on your workload.
- **Custom scan**—Checks files/folders that were added by the administrator to the Protection plan.

After antimalware scanning completes, you can see details about the workloads that were affected by threats in the **Dashboard** > **Overview** > Recently affected widget.

Antivirus & Antimalware protection settings

To learn how to create a protection plan with the Antivirus & Antimalware protection module, see "Creating a protection plan" (p. 243).

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.

 © Acronis International GmbH, 2003-2026

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**.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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**

© Acronis International GmbH, 2003-2026

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.

 © Acronis International GmbH, 2003-2026

- **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.

© Acronis International GmbH, 2003-2026

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. 373). 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:

 © Acronis International GmbH, 2003-2026

- 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, see "Antivirus & Antimalware protection settings" (p. 686).

 © Acronis International GmbH, 2003-2026

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 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, see 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.

© Acronis International GmbH, 2003-2026

For more details about the Windows Defender Antivirus default actions settings, see 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, see 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 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.

© Acronis International GmbH, 2003-2026

- **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, see 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, see 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, see 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 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 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.

© Acronis International GmbH, 2003-2026

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.

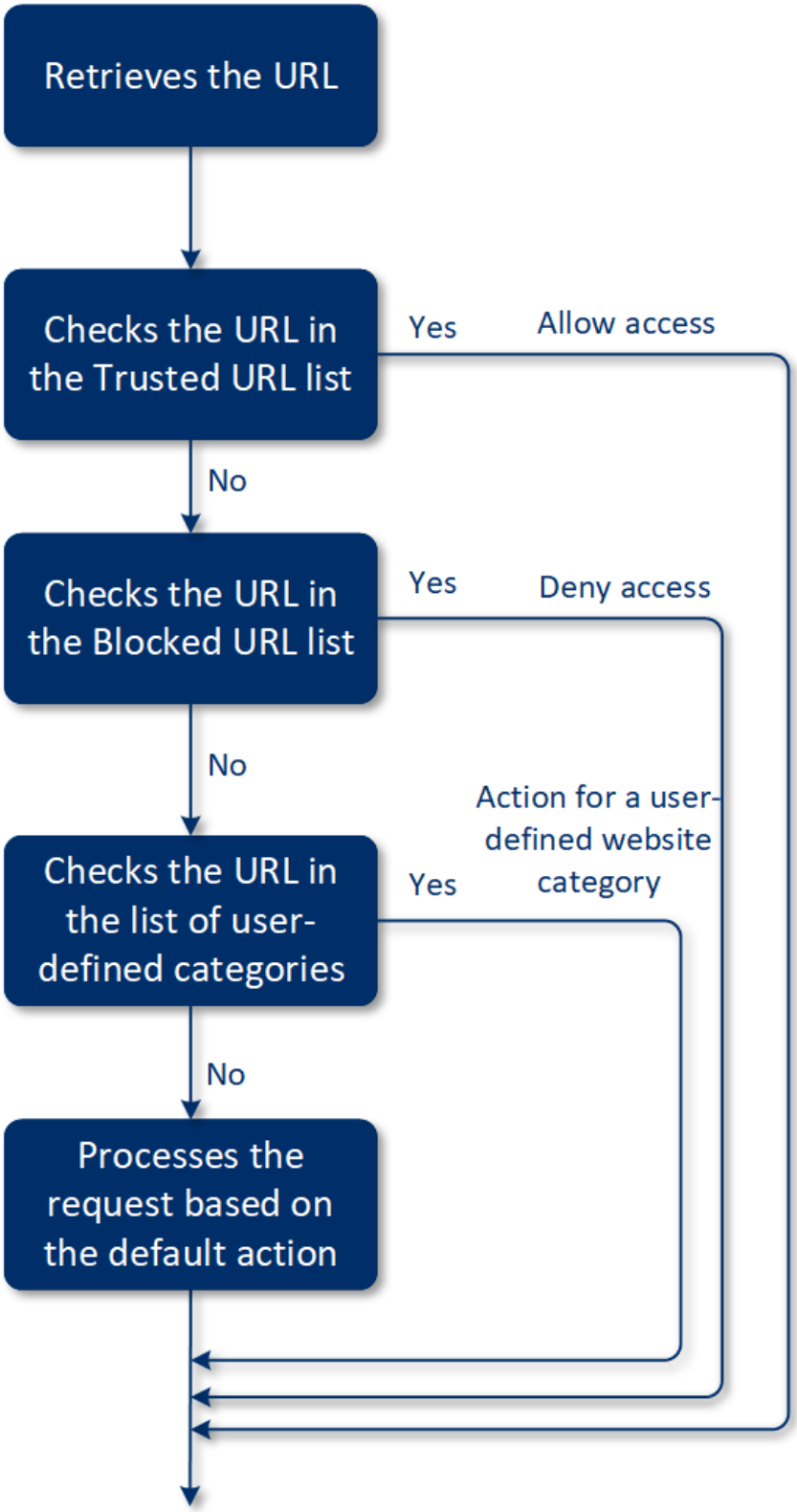
The URL filtering feature requires an Internet connection to function.

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.

© Acronis International GmbH, 2003-2026



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.

© Acronis International GmbH, 2003-2026

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	**Advertising**	This category covers domains whose main purpose is to serve advertisements.
2	**Message boards**	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	**Personal websites**	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	**Corporate/business websites**	This is a broad category that covers corporate websites that typically do not belong to any other category.
5	**Computer software**	This category covers websites offering computer software, typically either open-source, freeware, or shareware. It may also cover some online software stores.
6	**Medical drugs**	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	**Education**	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.

© Acronis International GmbH, 2003-2026

8	**Entertainment**	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	**File sharing**	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	**Finance**	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	**Gambling**	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	**Games**	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. This category does not cover: • Official websites of companies that develop video games (unless they produce online games) • Discussion websites where games are discussed • Websites where non-online games can be downloaded (some of them are covered in the Illegal category) • 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
13	**Government**	This category covers government websites, including government institutions, embassies, and office websites.
14	**Hacking**	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	**Illegal activities**	This category is a broad category related to hate, violence and racism, and it is intended to block the following categories of websites: • Websites belonging to terrorist organizations • Websites with racist or xenophobic content

© Acronis International GmbH, 2003-2026

		• Websites discussing aggressive sports, and/or promoting violence
16	**Health and fitness**	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	**Hobbies**	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	**Web hosting**	This category covers free and commercial website hosting services that allow private users and organizations to create and publish web pages.
19	**Illegal downloads**	This category covers websites related to software piracy, including: • Peer-to-peer (BitTorrent, emule, DC++) tracker websites that are known in helping to distribute copyrighted content without the copyright holder's consent • Warez (pirated commercial software) websites and discussion boards • Websites providing users with cracks, key generators, and serial numbers to facilitate the use of software illegally Some of these websites may also be detected as pornography or alcohol/cigars, since they often use porn or alcohol advertisements to earn money.
20	**Instant messaging**	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	**Jobs/employment**	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	**Mature content**	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	**Narcotics**	This category covers websites sharing information about recreational and illegal drugs. This category also covers websites covering development or growing drugs.
24	**News**	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.

© Acronis International GmbH, 2003-2026

25	**Online dating**	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. 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.
26	**Online payments**	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.
27	**Photo sharing**	This category covers photo-sharing websites whose primary purpose is to let users upload and share photos.
28	**Online stores**	This category covers known online stores. A website is considered an online store if it sells goods or services online.
29	**Pornography**	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.
30	**Portals**	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.
31	**Radio**	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.
32	**Religion**	This category covers websites promoting religion or a sect. It also covers the discussion forums related to one or multiple religions.
33	**Search engines**	This category covers search engine websites, such as Google, Yahoo, and Bing.
34	**Social networks**	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.
35	**Sport**	This category covers websites that offer sports information, news, and tutorials.
36	**Suicide**	This category covers websites promoting, offering, or advocating suicide. It does not cover suicide prevention clinics.

© Acronis International GmbH, 2003-2026

37	**Tabloids**	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	**Waste of time**	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	**Traveling**	This category covers websites that present travel offers and travel equipment, as well as travel destination reviews and ratings.
40	**Videos**	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	**Violent cartoons**	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. This category doesn't cover the websites that offer mainstream cartoons such as “Tom and Jerry”.
42	**Weapons**	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	**Email**	This category covers websites that provide email functionality as a web application.
44	**Web proxy**	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. These are the following reasons this type is detected (and might need to be blocked): • 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. • 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. • For accessing prohibited content. If a simple URL filter is used, it will

© Acronis International GmbH, 2003-2026

		only see the web proxy URLs and not the actual servers that the user visits. • 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. 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.

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

© Acronis International GmbH, 2003-2026

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
File	The file name.
Date quarantined	The date and time when the file was placed in Quarantine.
Device	The device on which the infected file was found.
Threat name	The threat name.
Protection plan	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:

© Acronis International GmbH, 2003-2026

For a Windows machine: `%ProgramData%\%product_name%\Quarantine`

For a Mac/Linux machine: `/usr/local/share/%product_name%/quarantine`

Self-service custom folder on-demand

You can select custom folders on the workload and scan them directly from the context menu.

To access the Scan with Cyber Protect option in the context menu

For workloads with Antivirus and Antimalware enabled in the protection plan, right-click the files/folders on which you want to scan.

Note
This option is available only to administrators of the workload.

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. 463).
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 console, go to **Antimalware protection** > **Whitelist**.
2. Click **Add file**.
3. Specify the path to the file, and then click **Add**.

 © Acronis International GmbH, 2003-2026

Adding quarantined files to the whitelist

You can add files that are quarantined to the whitelist.

1. In the Cyber Protect 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 VirtusTotal 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.

© Acronis International GmbH, 2003-2026

Note
Backup scanning for Microsoft 365 is available only in cloud deployments. You cannot configure a backup scanning plan for Microsoft 365 in an on-premises deployment.

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. 110).

Backup scanning plans are supported for **Entire machine** and **Disks/volumes** 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 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. 350).
- 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.

 © Acronis International GmbH, 2003-2026

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 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

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 detailed information about the features included in each edition, see Acronis Cyber Protect 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 must 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.

© Acronis International GmbH, 2003-2026

Managing your hardware inventory

When you enable the hardware inventory feature, you can view all the hardware components that are available on:

- physical Windows and macOS devices with a license that supports the Hardware inventory feature.
- virtual Windows and macOS machines running on the following virtualization platforms: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo, and Cyber Frame.
  For more information about the supported versions of the virtualization platforms, see "Supported virtualization platforms" (p. 78).

The hardware inventory feature is supported only for devices on which a protection agent is installed.

To obtain the hardware inventory data, you can run automatic or manual scans on the devices.

You can use the hardware inventory data to:

- Discover all hardware assets of the organization.
- Browse through the hardware inventory of all devices in your organization.
- Compare the hardware components on multiple devices.
- View detailed information about a hardware component.

Enabling or disabling the hardware inventory scanning

When hardware inventory scanning is enabled on physical devices and virtual machines, the system automatically collects the hardware data every 12 hours.

Note
If you are working at the unit level, you can view the hardware inventory scanning settings, but you cannot change them.

Enable

To enable the hardware inventory scanning

1. In the Cyber Protect console, go to **Settings**.
2. Click **Management**.
3. Click **Inventory scanning**.
4. Enable the **Hardware inventory scanning** switch.
5. Click **Save**.

Disable

To disable the hardware inventory scanning

© Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Settings**.
2. Click **Management**.
3. Click **Inventory scanning**.
4. Click **Save**.

Starting a hardware inventory scan manually

You can manually start a hardware inventory scan for a single device, and view the current data for the hardware components of the device.

Note
Hardware inventory scanning of virtual machines is supported only when the current date and time of the virtual machine corresponds to the current date and time in UTC. To ensure that the virtual machine uses the correct time settings, disable the **Time synchronization** option of the virtual machine, set the current date, time, and time zone, and then restart **Acronis Agent Core Service** and **Acronis Managed Machine Service**.

Prerequisites

- The device uses a Windows or macOS operating system.
- The devices have a license that supports the Hardware inventory feature.
- A protection agent is installed on the device.
- [If the device is a virtual machine] The machine runs on one of the supported virtualization platforms. For more information, see "Managing your hardware inventory" (p. 710).

To start a hardware inventory scan on a single device

1. In the Cyber Protect console, go to **Devices**.
2. Click the device which you want to scan, and then click **Inventory**.
3. On the **Hardware** tab, click **Scan now**.

Browsing the hardware inventory

You can view and browse the data for all hardware components that are available on all devices in your organization.

Prerequisites

- The devices use Windows or macOS operating system.
- The devices have a license that supports the Hardware inventory feature.
- A protection agent is installed on the device.
- Hardware inventory scan on the devices has finished successfully.
- [If the device is a virtual machine] The machine runs on one of the supported virtualization platforms. For more information, see "Managing your hardware inventory" (p. 710).

To view all hardware components that are available on the Windows and macOS devices

 © Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Devices**.
2. In the **View:** drop-down field, select **Hardware**.

Note
View is a set of columns that determines what data is visible on the screen. The predefined views are **Standard** and **Hardware**. You can create and save custom views that include different sets of columns, and are more convenient for your needs.

The following table describes the data that is visible in the **Hardware** view.

Column	Description
Name	Device name.
Hardware scan status	Status of the hardware scan. • **Completed**. • **Not started**. • **Not supported**. This status is shown for workloads for which the hardware inventory functionality is not supported. For example, virtual machines, mobile devices, and Linux devices. • **Update agent**. This status is shown when an outdated version of agent is installed on the device. Clicking on this action will redirect to **Settings** > **Agents** page, where administrators can update the agent. • **Upgrade license**. Clicking this status opens a dialog where administrators can change the current license to another of the licenses that are available for the organization.
Processor	Models of all processors of the device.
Processor cores	Number of cores of all processors of the device.
Disk storage	Used storage, and total storage of all the disks of the device.
Memory	Total RAM capacity of the device.
Scan date	Date and time of the last hardware inventory scan.
Motherboard	Motherboard of the device.
Motherboard serial number	Serial number of the motherboard.

© Acronis International GmbH, 2003-2026

Column	Description
Serial number	System serial number of the device. This information is collected only for physical devices, and is not available for virtual machines.
BIOS version	Version of the BIOS of the system.
Organization	Organization to which the device belongs.
Owner	Owner of the device.
Domain	Domain of the device.
Operating system	Operating system of the device.
Operating system build	Build of the operating system of the device.

3. [Optional] To add columns in the table, click the gear icon, and select the columns that you want to be visible in the table.
4. [Optional] To narrow the information displayed on the screen, use one or more filters.
   a. Click **Search**.
   b. Click the arrow, and then click **Hardware**.
   c. Select one or a combination of several filters.
      The following table describes the **Hardware** filters.

Filter	Description
Processor model	Multiple selection is possible. Use this filter if you want to view the hardware data of the devices which have the specified processor model.
Processor cores	Use this filter if you want to view the hardware data of the devices which have the specified number of processor cores.
Disk total size	Use this filter if you want to view the hardware data of the devices which have the specified total storage size.
Memory capacity	Use this filter if you want to view the hardware data of the devices which have the specified RAM capacity.

   d. Click **Apply**.
5. [Optional] To sort the data in an ascending order, click a column name.

Viewing the hardware of a single device

You can view detailed information about the motherboard, processors, memory, graphics, storage drives, network, and system of a specific device.

Prerequisites

© Acronis International GmbH, 2003-2026

- The device uses Windows or macOS operating system.
- The device has a license that supports the Hardware inventory feature.
- A protection agent is installed on the device.
- Hardware inventory scan on the device has finished successfully.
- [If the device is a virtual machine] The machine runs on one of the supported virtualization platforms. For more information, see "Managing your hardware inventory" (p. 710).

To view the detailed information about the hardware of a specific device

1. In the Cyber Protect console, go to **Devices** ->**All Devices**.
2. In the **View:** drop-down field, select **Hardware**.
3. Find the device you want to inspect using one of the methods described below.
   - Find the device using the **Filter**:
     a. Click **Filter**.
     b. Select one or a combination of several filter parameters to find the device.
     c. Click **Apply**.
   - Find the device using the **Search**:
     a. Click **Search**.
     b. Type the full device name or part of the device name, and click **Enter**.
4. Click the row listing the device, and click **Inventory**.
5. Click the **Hardware** tab.

   The following hardware data is available.

Hardware component	Information displayed
Motherboard	Name, manufacturer, model, and serial number of the motherboard of the device.
Processors	Manufacturer, model, max clock speed, and number of cores of each processor of the device.
Memory	Capacity, manufacturer, and serial number of the memory of the device.
Graphics	Manufacturer and model of the GPUs of the device.
Storage drives	Model, media type, available space and size of the storage drives of the device.
Network	Mac address, IP address, and type of the network adapters of the device.
System	Product ID, original install date, system boot time, system manufacturer, system model, serial number, BIOS version, boot device,

© Acronis International GmbH, 2003-2026

Hardware component	Information displayed
	system locale, and time zone of the system. **Note** The serial number is collected only for physical devices, and is not available for virtual machines.

© Acronis International GmbH, 2003-2026

Managing software

The software management features that you can enable are:

- Inventory scanning - run automatic or manual inventory scans on the devices and gain complete visibility about the software that is installed on them.

  Note
  This feature is not supported on Windows workloads that run on ARM64 processors.

- Vulnerability assessment - run vulnerability scans to identify vulnerabilities in the operating systems and software that are installed on the devices.
- Patch management - manage patches (updates) for operating systems and software that are installed on your devices, and keep the systems up to date.

Managing your software inventory

The availability of this feature depends on the license that is assigned to your workload.

The feature enables you to view all the software applications that are installed on all Windows and macOS devices.

To obtain the software inventory data, you can run automatic or manual scans on the devices.

You can use the software inventory data to:

- browse and compare the information about all applications that are installed on the company devices
- determine if an application needs to be updated
- determine if an unused application needs to be removed
- ensure that the software version on multiple company devices is the same
- monitor changes in the software status between consecutive scans.

Enabling or disabling the software inventory scanning

When software inventory scanning is enabled on the devices, the system automatically collects the software data every 12 hours.

Note
If you are working at the unit level, you can view the software inventory scanning settings, but you cannot change them.

Enable

To enable software inventory scanning

1. In the Cyber Protect console, go to **Settings**.
2. Click **Management**.

© Acronis International GmbH, 2003-2026

3. Click **Inventory scanning**.
4. Enable the **Software inventory scanning** switch.
5. Click **Save**.

Disable

To disable software inventory scanning

1. In the Cyber Protect console, go to **Settings**.
2. Click **Management**.
3. Click **Inventory scanning**.
4. Disable the **Software inventory scanning** switch.
5. Click **Save**.

Starting a software inventory scan manually

You can start a software inventory scan manually from the **Software inventory** screen, or from the **Software** tab on the **Inventory** screen.

Prerequisites

- The device uses Windows or macOS operating system.
- The device has the required license.

From Software inventory

To start a software inventory scan from the Software inventory screen

1. In the Cyber Protect console, go to **Software management**.
2. Click **Software inventory**.
3. In the **Group by:** dropdown menu, select **Devices**.
4. Find the device which you want to scan, and then click **Scan now**.

From Software

To start a software inventory scan from the Software tab on the Inventory screen

1. In the Cyber Protect console, go to **Devices**.
2. Click the device which you want to scan, and then click **Inventory**.
3. In the **Software** tab, click **Scan now**.

Browsing the software inventory

You can view and browse the data for all software applications that are available on all devices in your organization.

Prerequisites

- The devices use Windows or macOS operating system.
- The devices have the required license.

© Acronis International GmbH, 2003-2026

- At least one software inventory scan on the devices finished successfully.

To view all software applications that are available on all Windows and macOS devices

1. In the Cyber Protect console, go to **Software Management**.
2. Click **Software inventory**.

   By default, the data is grouped by device. The following table describes the data that is visible in the **Software inventory** screen.

Column	Description
Name	Name of the application.
Version	Version of the application.
Status	Status of the application. • **New**. • **Updated**. • **Removed**. • **No Change**.
Vendor	Vendor of the application.
Date installed	Date and time when the application was installed.
Last run	For macOS devices only. Date and time when the application was last active.
Location	Directory where the application is installed.
User	User for whom the application was installed.
System type	For Windows devices only. Bit type of the application. • **X86** for 32-bit applications. • **X64** for 64-bit applications.

3. To group the data by application, in the **Group by:** drop-down field, select **Applications**.
4. To narrow the information displayed on the screen, use one or a combination of the filters.
   a. Click **Filter**.
   b. Select one or a combination of several filters.

      The following table describes the filters in the **Software inventory** screen.

Filter	Description
Device Name	Device name. Multiple selection is possible. Use this filter if you want to compare the software on specific devices.
Application	Application name. Multiple selection is possible. Use this filter if you want to compare the data for a specific

© Acronis International GmbH, 2003-2026

Filter	Description
	application on specific devices or on all devices.
Vendor	Vendor of the application. Multiple selection is possible. Use this filter if you want to view all applications from a specific vendor on specific devices or on all devices.
Status	Application status. Multiple selection is possible. Use this filter if you want to view all applications in the selected status on specific devices or on all devices.
Date installed	Date when the application is installed. Use this filter if you want to view all applications that are installed on a specific date on specific devices or on all devices.
Scan date	Date of the software inventory scan. Use this filter if you want to view the information about the software on specific devices or on all devices that are scanned on that date.

c. Click **Apply**.

5. To browse through the whole software inventory list, use the pagination in the lower left part of the screen.

- Click the number of the page that you want to open.
- In the dropdown list, select the page number of the page that you want to open.

Note
The list might contain information about deleted machines. The current retention policy is to keep data for deleted machines for up to 35 days after the machines were deleted.

Viewing the software inventory of a single device

You can view a list of all the software applications that are installed on a single device, and detailed information about the applications, such as status, version, vendor, installation date, last run, and location.

Prerequisites

- The device uses Windows or macOS operating system.
- The device has the required license.
- At least one software inventory scan on the device finished successfully.

From Software inventory

To view the software inventory of a single device from the Software inventory screen

1. In the Cyber Protect console, go to **Software management**.
2. Click **Software inventory**.

© Acronis International GmbH, 2003-2026

3. In the **Group by:** dropdown menu, select **Devices**.
4. Find the device that you want to inspect, by using one of the following options.
   - Use **Filter**:
     a. Click **Filter**.
     b. In the **Device name** field, select the name of the device that you want to view.
     c. Click **Apply**.
   - Use **Search**:
     a. Click **Search**.
     b. Type the full device name or part of the device name.

From Devices

To view the software inventory of a single device from Devices screen

1. In the Cyber Protect console, go to **Devices**.
2. Click the device that you want to view, and then click **Inventory**.
3. Click the **Software** tab.

Assessing vulnerabilities and managing patches

Vulnerability assessment (VA) is a process of identifying, quantifying, and prioritizing vulnerabilities found in the system. In the vulnerability assessment module, you can scan your machines for vulnerabilities, and check if the operating systems and installed applications are up to date and working properly.

Vulnerability assessment scanning is supported for machines with the following operating systems:

- Windows. For more information, see "Supported Microsoft and third-party products for vulnerability assessment" (p. 721).
- Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure) machines. For more information, see "Supported Linux products for vulnerability assessment" (p. 722).

Use the Patch management (PM) functionality to manage patches (updates) for applications and operating systems that are installed on your devices, and keep the systems up to date. In the patch management module, you can automatically or manually approve update installations on your devices.

Patch management is supported for machines with the Windows operating systems. For more information, see "Supported Microsoft and third-party products for vulnerability assessment" (p. 721).

Vulnerability assessment

The vulnerability assessment process consists of the following steps:

1. You create a protection plan with the enabled vulnerability assessment module, specify the Vulnerability assessment settings, and assign the plan to machines.

 © Acronis International GmbH, 2003-2026

2. The system, by schedule or on demand, sends a command to run the vulnerability assessment scanning to the protection agents installed on machines.
3. The agents get the command, start scanning machines for vulnerabilities, and generate the scanning activity.
4. After the vulnerability assessment scanning is completed, the agents generate the results and send them to the monitoring service.
5. The monitoring service processes the data from the agents and shows the results in the vulnerability assessment widgets and list of found vulnerabilities.
6. When you get a list of found vulnerabilities, you can process it and decide which of the found vulnerabilities must be fixed.

You can monitor the results of the vulnerability assessment scanning in **Monitoring**> **Overview** > **Vulnerabilities / Existing vulnerabilities** widgets.

Supported Microsoft and third-party products for vulnerability assessment

The following Microsoft products and third-party products for Windows operating systems are supported for vulnerability assessment and patch management.

Supported Microsoft products

Desktop operating systems

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 (Enterprise, Professional, Ultimate)

Server operating systems

- Windows Server 2025
- 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

© Acronis International GmbH, 2003-2026

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio and Applications
- Components of operating system

Server applications

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server 2016

Supported third-party products for Windows

Note
The availability of this feature depends on the license that you have.

Cyber Protect supports vulnerability assessment and patch management for a wide range of third-party apps, including collaboration tools and VPN clients that have vital importance in the remote work scenarios, such as the following:

- Microsoft Teams
- Zoom
- Slack
- Webex
- NordVPN
- TeamViewer

For the full list of supported third-party products for Windows, see List of third-party products supported by Patch Management (62853).

Supported Linux products for vulnerability assessment

The following Linux distributions and versions are supported for vulnerability assessment (VA):

© Acronis International GmbH, 2003-2026

- 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, see "Creating a protection plan". 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** - this option is part of the standard protection plan.
  - **Windows third-party products** - the availability of this option depends on the license. For more information about the supported third-party products for Windows OS, refer to List of third-party products supported by Patch Management.
- Linux machines:
  - **Scan Linux packages**

Schedule

Define the schedule according to which to perform the vulnerability assessment scan on the selected machines:

Field	Description
Schedule the task run using the following events	This setting defines when the task will run. The following values are available: • **Schedule by time** – This is the default setting. The task will run according to the specified time. • **When user logs in to the system** – By default, a login of any user will trigger 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 trigger the task. You can modify this setting so that only a specific user

© Acronis International GmbH, 2003-2026

Field	Description
	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.
Schedule type	The field appears if in **Schedule the task run using the following events** you have selected **Schedule by time**. The following values are available: • **Monthly** – Select the months and the weeks or days of the month when the task will run. • **Daily** – This is the default setting. 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.
Start at	The field appears if in **Schedule the task run using the following events** you have selected **Schedule by time** Select the exact time when the task will run.
Run within a date range	The field appears if, in **Schedule the task run using the following events**, you have selected **Schedule by time**. Set a range in which the configured schedule will be effective.
Specify a user account whose login to the operating system will initiate a task	The field appears if, in **Schedule the task run using the following events**, you have selected **When user logs in to the system**. The following values are available: • **Any user** - Use this option if you want the login of any user to trigger the task. • **The following user** - Use this option if you want only the login of a specific user account to trigger the task.
Specify a user account whose logout from the operating system will initiate a task	The field appears if, in **Schedule the task run using the following events**, you have selected **When user logs off the system**. The following values are available: • **Any user** - Use this option if you want the logout of any user to trigger the task. • **The following user** - Use this option if you want only the logout of a

© Acronis International GmbH, 2003-2026

Field	Description
	specific user account to trigger the task.
Start conditions	Defines 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". 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 is 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 Windows machines and third-party products for Windows for vulnerabilities.

To configure the vulnerability assessment for Windows machines

1. In the Cyber Protect console, create a protection plan and enable the **Vulnerability assessment** module.
2. Specify the vulnerability assessment settings:
   - **What to scan** - select one or both options.
     - **Microsoft products** - this option is part of the standard protection features.
     - **Windows third-party products** - this option is part of RMM (service-based licensing mode) or Security and RMM (solution-based licensing mode).
   - **Schedule** – define the schedule for performing the vulnerability assessment.

   For more information about the **Schedule** options, see "Vulnerability assessment settings" (p. 723).
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.

© Acronis International GmbH, 2003-2026

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 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, see "Vulnerability assessment settings" (p. 723).
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 that have patches to be installed, and those that do not have suggested patches. You can use the filter to show only vulnerabilities with patches.

Name	Description
Name	The name of vulnerability.
Affected products	Software products for which the vulnerabilities were found.
Machines	The number of affected machines.
Severity	The severity of found vulnerability. The following levels can be assigned according to the Common Vulnerability Scoring System (CVSS): • **Critical**: 9 - 10 CVSS • **High**: 7 - 9 CVSS • **Medium**: 3 - 7 CVSS • **Low**: 0 - 3 CVSS • **None**

© Acronis International GmbH, 2003-2026

Patches	The number of appropriate patches.
Published	The date and time when the vulnerability was published in Common Vulnerabilities and Exposures (CVE).
Detected	The first date when an existing vulnerability was detected on machines.

You can find the description of found vulnerability by clicking its name in the list.

To start the vulnerability remediation process

1. In the Cyber Protect console, go to **Software management** > **Vulnerabilities**.
2. Select the vulnerability in the list, and then click **Install patches**. The vulnerability remediation wizard will open.
3. Select the patches to be installed on the selected machines, and then click **Next**.
4. Select the machines on which you want to install the patches.
5. Select the restart options.

   The following table provides more information about the restart options.

Option	Description
Restart if required	If you want the workload to be restarted after the software is installed or uninstalled only if the software requires it, select this checkbox.
Always restart	If you want the workload to always be restarted after the software is installed or uninstalled, select this checkbox.
Do not restart	If you do not want the workload to be restarted after the software is installed or uninstalled, select this checkbox.
Schedule automatic restart	This option is available if you selected **Restart if required** or **Always restart**. The option enables automatic restart of the workload.
If a user is logged on to the device, the device will be automatically restarted after:	This option is available if you selected **Schedule automatic restart**. Select the period after which the workload will be restarted automatically. The user who is logged in to the workload will be notified about a pending automatic restart and the time when it will happen. Thus, users can save their work and prepare for the restart.
Additional notifications	This option is available if you selected **Schedule automatic restart**. Select this option if you want the user who is logged in to the workload to be reminded repeatedly about a pending restart before the selected period passes. The timing of notifications depends on the selected period and transitions into a countdown as the restart time nears. This ensures that users stay informed and prepared for the restart. Notifications are triggered by a successful software update or deployment and are

© Acronis International GmbH, 2003-2026

Option	Description
	sent at the following times. **Note** The timing of the first notification coincides with the selected period. • 24 h before the automatic restart. • 8 h before the automatic restart. • 4 h before the automatic restart. • 1 h before the automatic restart. • 30 min before restart. • 15 min before restart. • 5 min before the automatic restart. The last user notification cannot be closed or dismissed.
If no user is logged on to the device, restart it immediately	This option is available if you selected **Schedule automatic restart**. If you select this option and no user is logged in to the workload, the workload will be restarted immediately, without waiting for the selected period before automatic restart to pass.

6. Click **Install patches**.

   As a result, the selected patches are installed on the selected machines.

Patch management

Note

- To enable the **Patch management** module in the protection plan, the **Vulnerability assessment** module must be enabled.

For more information about the supported third-party products for Windows OS, see List of third-party products supported by Patch Management (62853).

Use the patch management functionality to:

- install OS-level and application-level updates
- approve patches manually or automatically
- install patches on-demand or according to a schedule
- precisely define which patches to install by different criteria: severity, category, and approval status
- perform pre-update backup to prevent possible unsuccessful updates
- define the reboot action after patch installation

© Acronis International GmbH, 2003-2026

Note
To work with Windows updates, the patch management feature requires that Windows updates are enabled on the workload. The patch management feature relies on the Windows update service which detects which updates are missing and proposes them based on the existing running OS version.

Important
The patch management feature supports upgrades to Windows 11. However, you must verify that the Windows 10 workloads that you are planning to upgrade are properly prepared for it. See this Microsoft article for details.

The patch management workflow

The patch management workflow includes steps for configuring and applying a protection plan, running a vulnerability assessment scan, configuring patch settings, approving patches and finally, installing patches that are approved. The exact steps of the workflow are as follows.

1. Configure a protection plan that has the **Vulnerability assessment** and **Patch management** modules enabled.

   For more information about creating a protection plan and enabling the **Patch management** module, see "Creating a protection plan" (p. 243).
2. Configure the vulnerability assessment settings.

   For more information about these settings, see "Vulnerability assessment settings" (p. 723).
3. Configure the patch management settings.

   For more information about these settings, see "Configuring patch management settings in the protection plan" (p. 730)
4. Apply the protection plan to one or several machines.
5. Wait for a vulnerability assessment scan to be completed.

   The scan will start automatically, according to the schedule that is configured in the protection plan. Alternatively, you can manually start the scan on demand by clicking the **Run now** icon in the **Vulnerability assessment** module in the protection plan.
6. Approve the patches.

   You can define settings for automatic patch approval, which include an automatic installation of the patches on test machines. For more information, see "Automatic patch approval" (p. 737). Alternatively, you can manually approve patches by setting their approval status to **Approved**. For more information, see "Approving patches manually" (p. 742).
7. Install the patches.

   The approved patches can be installed automatically, according to the schedule that is configured in the protection plan. Alternatively, you can manually install patches on demand. For more information, see "Installing patches on demand" (p. 742).

You can monitor the results of the patch installation in **Monitoring**> **Overview** > **Patch installation history** widget.

© Acronis International GmbH, 2003-2026

Configuring patch management settings in the protection plan

In the **Patch management** module of the protection plan, you can configure the following patch management settings:

- What updates to install for Microsoft and third-party products for Windows OS.
- When to run the automatic patch installation.
- Whether to run a pre-update backup.

For more information about creating a protection plan and enabling the **Patch management** module, see "Creating a protection plan" (p. 243).

Microsoft products

To install the Microsoft updates on the selected machines

1. Enable the **Update Microsoft products** option in the protection plan.
2. Select the installation option.

Option	Description
All updates	Use this option if you want to install all approved updates.
Only Security and Critical updates	Use this option if you want to install all approved security and critical updates.
Updates of specific products (Automatic patch approval and testing)	Use this option if you want to 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. If you want to configure automatic test approval and testing of the patches, select this option. **Important** The patch management feature supports upgrades to Windows 11. However, you must verify that the Windows 10 workloads that you are planning to upgrade are properly prepared for it. See this Microsoft article for details.

For Microsoft products, patch distribution uses the Windows API service. Patches and updates are not downloaded or stored internally or on distribution agents. Instead, they are downloaded from Microsoft CDN. Thus, even with the Updater role assigned, the agent cannot download and distribute patches.

Windows third-party products

To install the third-party updates for Windows OS on the selected machines

© Acronis International GmbH, 2003-2026

1. Enable the **Windows third-party products** option in the protection plan.
2. Select the installation options.

Option	Description
All updates	Use this option if you want to install all approved updates. *
Only major updates	Use this option if you want to install all approved major updates.
Only minor updates	Use this option if you want to install approved minor updates.
Updates of specific products (Automatic patch approval and testing)	Use this option if you want to define custom settings for different products. If you want to update specific products then, for each product, you can define which updates to install by category, severity, or approval status. If you want to configure automatic test approval and testing of the patches, select this option.
Install the latest versions only for applications with detected vulnerabilities	Select this check box if you want to install the latest updates only for applications that have detected vulnerabilities.

For Windows third-party products, patches are distributed directly to managed workloads when internet access is available. If internet access is not available for all workloads, the Updater role should be assigned to an agent that does have internet access. This agent will then download the patches and distribute them to other agents on the network.

Schedule

Define the schedule and conditions according to which the updates will be installed on the selected machines.

Field	Description
Schedule the task run using the following events	This setting defines when the task will be run. The following values are available: • **Schedule by time** – This is the default setting. 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.

© Acronis International GmbH, 2003-2026

Field	Description
	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.
Schedule type	The field appears if, in **Schedule the task run using the following events**, you have selected **Schedule by time**. The following values are available: • **Monthly** – Select the months and the weeks or days of the month when the task will run. • **Daily** – This is the default setting. 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.
Start at	The field appears if, in **Schedule the task run using the following events**, you have selected **Schedule by time** Select the exact time when the task will run.
Configure maintenance window for patches	The field appears if, in **Schedule the task run using the following events**, you have selected **Schedule by time**. Select this setting if you want the patch installation to run only during the time interval that you will specify. If the patch installation process has not completed by the end time defined by the maintenance window for patches, it will be stopped automatically.
Run within a date range	The field appears if, in **Schedule the task run using the following events**, you have selected **Schedule by time**. Set a range in which the configured schedule will be effective.
Specify a user account whose login to the operating system will initiate a task	The field appears if, in **Schedule the task run using the following events**, you have selected **When user logs in to the system**. The following values are available: • **Any user** - Use this option if you want the login of any user to trigger the task. • **The following user** - Use this option if you want only the login of a specific user account to trigger the task.
Specify a user	The field appears if, in **Schedule the task run using the following events**, you have selected **When user logs off the system**.

© Acronis International GmbH, 2003-2026

Field	Description
account whose logout from the operating system will initiate a task	The following values are available: • **Any user** - Use this option if you want the logout of any user to trigger the task. • **The following user** - Use this option if you want only the logout of a specific user account to trigger the task.
Start conditions	Defines 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**. 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 is 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.

Restart options

Configure if you want the workloads to be restarted after the patches installation.

The following table provides more information about the restart options.

Option	Description
Restart if required	If you want the workload to be restarted after the software is installed or uninstalled only if the software requires it, select this checkbox.
Always restart	If you want the workload to always be restarted after the software is installed or uninstalled, select this checkbox.
Do not restart	If you do not want the workload to be restarted after the software is installed or uninstalled, select this checkbox.
Schedule automatic restart	This option is available if you selected **Restart if required** or **Always restart**.

© Acronis International GmbH, 2003-2026

Option	Description
	The option enables automatic restart of the workload.
If a user is logged on to the device, the device will be automatically restarted after:	This option is available if you selected **Schedule automatic restart**. Select the period after which the workload will be restarted automatically. The user who is logged in to the workload will be notified about a pending automatic restart and the time when it will happen. Thus, users can save their work and prepare for the restart.
Additional notifications	This option is available if you selected **Schedule automatic restart**. Select this option if you want the user who is logged in to the workload to be reminded repeatedly about a pending restart before the selected period passes. The timing of notifications depends on the selected period and transitions into a countdown as the restart time nears. This ensures that users stay informed and prepared for the restart. Notifications are triggered by a successful software update or deployment and are sent at the following times. **Note** The timing of the first notification coincides with the selected period. • 24 h before the automatic restart. • 8 h before the automatic restart. • 4 h before the automatic restart. • 1 h before the automatic restart. • 30 min before restart. • 15 min before restart. • 5 min before the automatic restart. The last user notification cannot be closed or dismissed.
If no user is logged on to the device, restart it immediately	This option is available if you selected **Schedule automatic restart**. If you select this option and no user is logged in to the workload, the workload will be restarted immediately, without waiting for the selected period before automatic restart to pass.

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. It allows you to prevent such cases when the installation of updates was unsuccessful and you need to get back to the previous state. 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

© Acronis International GmbH, 2003-2026

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.

Viewing the list of available patches

After a vulnerability assessment scan completes, you can view information about the available patches in **Software management** > **Patches**.

To view details about a specific patch, in the list of patches, click the corresponding patch.

The following table describes the information for the patch that you can view on the screen.

Column	Description
Approval status	The approval status is mainly needed for automatic approval scenarios. You can define one of the following statuses for a patch: • **Approved** – the patch was installed on at least one machine and validated as ok • **Declined** – the patch is not safe and may corrupt a machine system • **Pending approval** – the patch status is unclear and should be validated
License agreement	• Agreed • Disagreed. If you disagree with the license agreement, then the patch status becomes **Declined** and it will not be installed
Severity	The severity of the patch: • **Critical** • **High** • **Medium** • **Low** • **None**
Vendor	The vendor of the patch
Affected product	Product for which the patch is applicable
Installed versions	Product versions that are already installed
Version	Version of the patch
Stability	Stability score of the patch that indicates if it is safe to install the patch. You can use this information to estimate the potential impact of a patch before its installation, and whether a patch is stable or can expose the organization to vulnerabilities. A patch can have one of the following stability scores: • **Stable** - Indicates that the patch has no reported issues or concerns based on sentiment analysis and other data sources, and that the patch is known (there is enough data about this particular patch). You can confidently install this patch

© Acronis International GmbH, 2003-2026

	without significant risk. • **Minor issues** - Suggests that the patch has some reported issues, such as issues in product functionality or UI, but they are minor, non-critical, or have clear workarounds. Usually, you can proceed with the patch installation in most environments, but you should review the issues first. • **Caution** - Highlights that the patch has significant or widespread issues reported, such as causing system instability, breaking functionality, or introducing security vulnerabilities. In this case, you should delay the patch installation, test it thoroughly in a controlled environment, or wait for vendor updates. • **Critical issues** - Indicates that the patch has severe, high-impact issues that could cause major disruptions, such as system crashes, data loss, or critical application failures. You must avoid installing this patch until the vendor releases a fix or guidance. When you click the values in this column, you can see the following additional information about the patch: patch overview, potential risks, statistics and metrics, specific configurations, insights and recommendations, and user experience. The **Stability** information is gathered from diverse external sources by using AI search engines.
Category	The category to which the patch belongs: • **Critical update** – broadly released fixes for specific problems addressing critical, non-security related bugs. • **Security update** – broadly released fixes for specific products addressing security issues. • **Definition update** – updates to virus or other definition files. • **Update rollup** – 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). • **Service pack** – 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. • **Tool** – utilities or features that aid in accomplishing a task or set of tasks. • **Feature pack** – new feature releases, usually rolled into products at the next release. • **Update** – broadly released fixes for specific problems addressing non-critical, non-security related bugs. • **Application** – patches for an application.
Release date	The date when the patch was released
Last reported	The date of the last time when the patch was reported
First installed	The date of the first successful installation of the patch on a machine
Microsoft KB	If the patch is for a Microsoft product, the field shows the KB article ID

© Acronis International GmbH, 2003-2026

Machines	Number of affected machines
Vulnerabilities	The number of vulnerabilities. If you click on it, you will be redirected to the list of vulnerabilities.
Size	The average size of the patch
Language	The language which is supported by the patch
Vendor site	The official site of the vendor

Configuring the patch lifetime in the list

You can keep the list of patches up to date by configuring the patch lifetime in the list on the **Patches** screen. This setting defines how long the detected available patch will be visible in the list of patches. The patch will be removed from the list after it is successfully installed on all the machines on which it was indicated as missing, or after the lifetime in the list passes.

To configure the patch lifetime in the list

1. In the Cyber Protect console, go to **Software management** > **Patches**.
2. Click **Settings**.
3. In **Lifetime in list**, select the appropriate option.

Option	Description
Forever	The patch will always stay in the list.
7 days	The patch will be removed from the list seven days after its first installation. For example, let us assume that you have two machines on which patches must be installed. One of them is online, and the other one is 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 from the list 30 days after its first installation.

Automatic patch approval

Automatic patch approval makes the process of installing updates on machines easier. With automatic patch approval, the installation of patches is not delayed by the manual patch approval process. Important updates and fixes are installed faster, which increases the reliability of your system.

You can use automatic patch approval in test scenarios for automatic installation of patches. If the patches are installed successfully on the test machines, the patches will be automatically installed on the production machines, too. For more information about this scenario, see "Use case for automatic patch approval and testing" (p. 738).

 © Acronis International GmbH, 2003-2026

You can also use automatic patch approval in scenarios for automatic installation of patches in your production environment, skipping the testing phase. For more information about this scenario, see "Use case for automatic patch approval without testing" (p. 741).

Important
The patch management feature supports upgrades to Windows 11. However, you must verify that the Windows 10 workloads that you are planning to upgrade are properly prepared for it. See this Microsoft article for details.

Configuring automatic patch approval

You can configure automatic patch approval and ensure that the installation of patches is not delayed by the manual patch approval process.

To configure automatic patch approval

1. In the Cyber Protect console, go to **Software management** > **Patches**.
2. Click **Settings**.
3. Enable **Automatic patch approval**.
4. Configure the settings for automatic patch approval.
   a. Select the automatic patch approval option.

Option	Description
Automatic patch approval and testing	The approval status of the patch will change to **Approved** when the selected number of days passes after a successful installation of the patch. We recommend that you use this setting if you want to test the patches by installing them on a test machine first, ensure that everything is working as expected, and then install the patches in your production environment.
Automatic patch approval without testing	The approval status of the patch will change to **Approved** when the selected number of days passes after the patch was found.

   b. Select the number of days that must pass after the condition from the automatic patch approval option is met. After this period, the approval status of the patches will automatically change from **Pending approval** to **Approved**.
5. Select **Automatically accept the license agreements**.
6. Click **Apply**.

Use case for automatic patch approval and testing

If you want to test the new patches on a test machine before installing them on your production machines, you can configure two protection plans - a plan for installation of patches for test purposes, and a plan for installation of tested patches on production machines. Thus, you will

 © Acronis International GmbH, 2003-2026

ensure that the patches that you install in your production environment are safe and your production machines work correctly after the patch installation.

The use case consists of the following stages:

1. Configure the settings for Automatic patch approval. Select the **Automatic patch approval and testing** option. For more information, see "Configuring automatic patch approval" (p. 738).
2. Configure a protection plan for test purposes (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 **Pending approval**. This step is needed to validate the patches and check if the machines work properly after patch installation. For more information, see "Configuring the Test patching protection plan" (p. 739).
3. Configure a protection plan for the production environment (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**. For more information, see "Configuring the Production patching protection plan" (p. 740).
4. Run the Test patching plan and check the results. Leave the approval status of the machines that have no issues as **Pending approval**, but change the approval status of the machines working incorrectly to **Declined**. According to the number of days set in the **Automatic patch approval** setting, the status of the patches will automatically change from **Pending approval** to **Approved**. When you run the Production patching plan, only the **Approved** patches will be installed on the production machines. For more information, see "Running the Test patching protection plan and decline unsafe patches" (p. 741).
5. Run the Production patching plan.

Configuring the Test patching protection plan

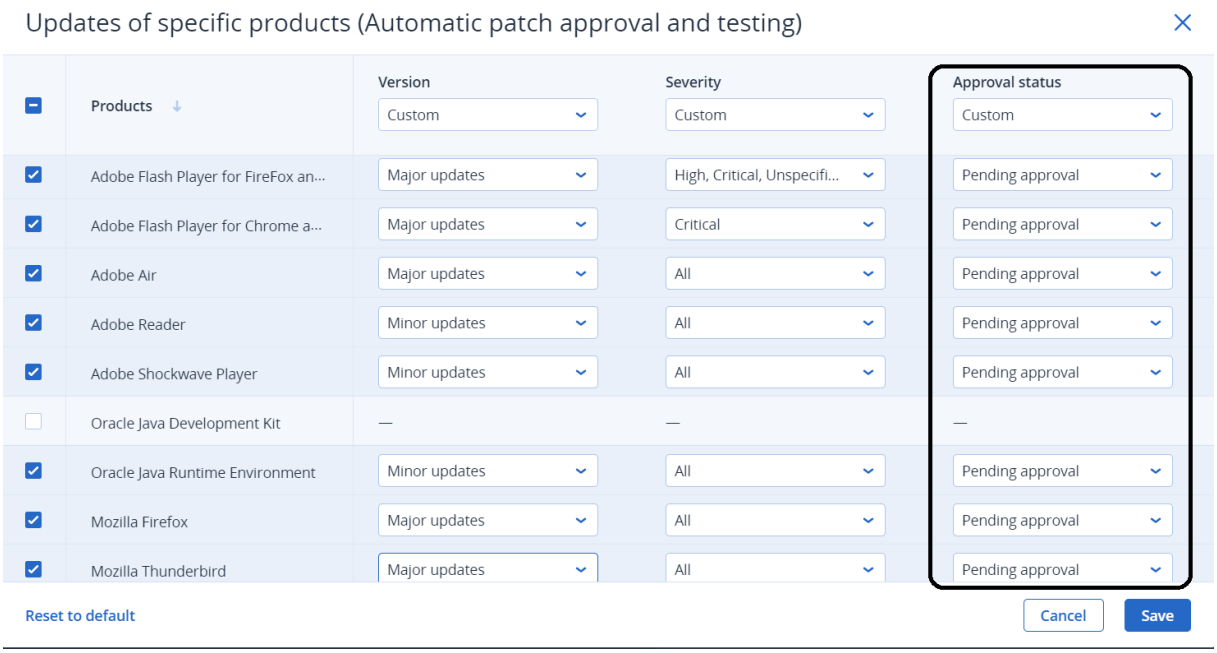
You can configure a protection plan with patch installation settings for your machines in the test environment.

To configure the Test patching protection plan

1. In the Cyber Protect console, go to **Management** > **Protection plans**.
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, see "Configuring patch management settings in the protection plan" (p. 730).

Important
For all the products to be updated, select the **Pending approval** approval status. Thus, the agent will install only **Pending approval** patches on the selected machines in the test environment.

© Acronis International GmbH, 2003-2026



Configuring the Production patching protection plan

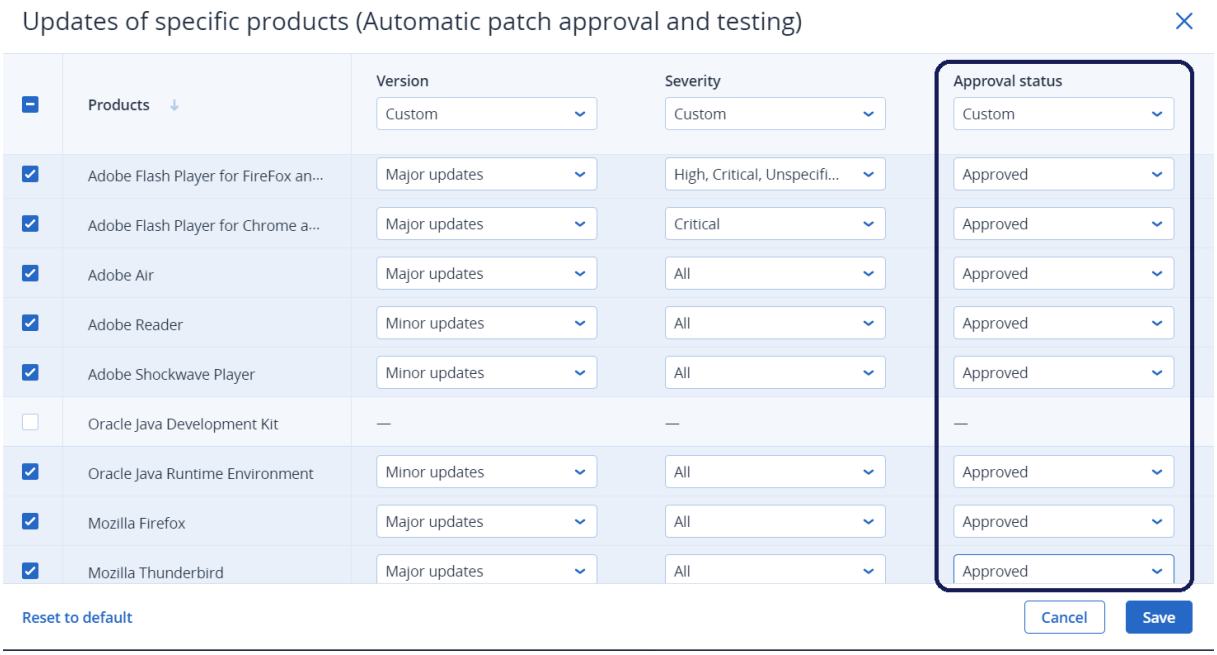
You can configure a protection plan with patch installation settings for your machines in the production environment.

To configure the Production patching protection plan

1. In the Cyber Protect console, go to **Management** > **Protection plans**.
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, see "Configuring patch management settings in the protection plan" (p. 730).

Important
For all the products to be updated, set the **Approval status** to **Approved**. Thus, the agent will install only **Approved** patches on the selected machines in the production environment.

© Acronis International GmbH, 2003-2026



Running the Test patching protection plan and decline unsafe patches

After patches are installed on the machines in your test environment, you can check if everything is working as expected. You can leave the approval status of the machines that have no issues as **Pending approval**, but change the approval status of the machines working incorrectly to **Declined**.

To run the Test patching protection plan and decline the patches that are not safe

1. Run the Test patching protection plan (by schedule or manually).
2. Depending on the result, see which of the installed patches are safe.
3. Go to **Software management** > **Patches** and set the **Approval status** to **Declined** for the patches that are not safe.

Use case for automatic patch approval without testing

If you want to automatically install new patches on your production machines as soon as possible, without installing them on test machines first, you can configure only one protection plan.

The use case consists of the following stages:

1. Configure the settings for Automatic patch approval. Select the **Automatic patch approval without testing** option. For more information, see "Configuring automatic patch approval" (p. 738).
2. Configure a protection plan for the production environment (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**. For more information, see "Configuring the Production patching protection plan" (p.

© Acronis International GmbH, 2003-2026

740).

3. Run the Production patching plan.

Approving patches manually

You can manually approve a patch and speed up its installation by skipping the testing phase.

Prerequisites

- A protection plan that has the **Patch management** module enabled is applied to at least one Windows machine.
- There are patches that are still not installed on the machine or machines on which the protection plan is applied.

To manually approve patches

1. In the Cyber Protect console, go to **Software management** > **Patches**.
2. Select the patches that you want to install, and then accept their license agreements.
3. Set the **Approval status** of the patches to **Approved**.

   The approval status of the patches is set to **Approved**. The patches will be automatically installed on the machines based on the schedule defined in the protection plan. If you want to install the patches immediately, follow the procedure that is described in "Installing patches on demand" (p. 742).

Installing patches on demand

You can manually install patches on demand when you do not want to wait for the scheduled installation time.

You can start the manual patch installation from three screens: **Patches**, **Vulnerabilities**, and **All devices**.

Important
The patch management feature supports upgrades to Windows 11. However, you must verify that the Windows 10 workloads that you are planning to upgrade are properly prepared for it. See this Microsoft article for details.

To manually install a patch

From Patches

1. In the Cyber Protect console, go to **Software management** > **Patches**.
2. Accept the license agreements for the patches that you want to install.
3. In the **Install patches** wizard, select the patches that you want to install, and then click **Install**.
4. Select the machines on which you want to install the patches.
5. Select the restart options.

   The following table provides more information about the restart options.

 © Acronis International GmbH, 2003-2026

Option	Description
Restart if required	If you want the workload to be restarted after the software is installed or uninstalled only if the software requires it, select this checkbox.
Always restart	If you want the workload to always be restarted after the software is installed or uninstalled, select this checkbox.
Do not restart	If you do not want the workload to be restarted after the software is installed or uninstalled, select this checkbox.
Schedule automatic restart	This option is available if you selected **Restart if required** or **Always restart**. The option enables automatic restart of the workload.
If a user is logged on to the device, the device will be automatically restarted after:	This option is available if you selected **Schedule automatic restart**. Select the period after which the workload will be restarted automatically. The user who is logged in to the workload will be notified about a pending automatic restart and the time when it will happen. Thus, users can save their work and prepare for the restart.
Additional notifications	This option is available if you selected **Schedule automatic restart**. Select this option if you want the user who is logged in to the workload to be reminded repeatedly about a pending restart before the selected period passes. The timing of notifications depends on the selected period and transitions into a countdown as the restart time nears. This ensures that users stay informed and prepared for the restart. Notifications are triggered by a successful software update or deployment and are sent at the following times. **Note** The timing of the first notification coincides with the selected period. • 24 h before the automatic restart. • 8 h before the automatic restart. • 4 h before the automatic restart. • 1 h before the automatic restart. • 30 min before restart. • 15 min before restart. • 5 min before the automatic restart. The last user notification cannot be closed or dismissed.
If no user is logged on to the device, restart it immediately	This option is available if you selected **Schedule automatic restart**. If you select this option and no user is logged in to the workload, the workload will be restarted immediately, without waiting for the selected period before automatic restart to pass.

© Acronis International GmbH, 2003-2026

6. Click **Install patches**.

From Vulnerabilities

1. In the Cyber Protect console, go to **Software management** > **Vulnerabilities**.
2. Perform the remediation process, as described in "Managing found vulnerabilities" (p. 726).

From All devices

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Select the machine on which you want to install the patches.
3. Click **Patch**.
4. Select the patches that you want to install, and then click **Next**.
5. Select the restart options.

   The following table provides more information about the restart options.

Option	Description
Restart if required	If you want the workload to be restarted after the software is installed or uninstalled only if the software requires it, select this checkbox.
Always restart	If you want the workload to always be restarted after the software is installed or uninstalled, select this checkbox.
Do not restart	If you do not want the workload to be restarted after the software is installed or uninstalled, select this checkbox.
Schedule automatic restart	This option is available if you selected **Restart if required** or **Always restart**. The option enables automatic restart of the workload.
If a user is logged on to the device, the device will be automatically restarted after:	This option is available if you selected **Schedule automatic restart**. Select the period after which the workload will be restarted automatically. The user who is logged in to the workload will be notified about a pending automatic restart and the time when it will happen. Thus, users can save their work and prepare for the restart.
Additional notifications	This option is available if you selected **Schedule automatic restart**. Select this option if you want the user who is logged in to the workload to be reminded repeatedly about a pending restart before the selected period passes. The timing of notifications depends on the selected period and transitions into a countdown as the restart time nears. This ensures that users stay informed and prepared for the restart. Notifications are triggered by a successful software update or deployment and are sent at the following times.

© Acronis International GmbH, 2003-2026

Option	Description
	Note The timing of the first notification coincides with the selected period. • 24 h before the automatic restart. • 8 h before the automatic restart. • 4 h before the automatic restart. • 1 h before the automatic restart. • 30 min before restart. • 15 min before restart. • 5 min before the automatic restart. The last user notification cannot be closed or dismissed.
If no user is logged on to the device, restart it immediately	This option is available if you selected **Schedule automatic restart**. If you select this option and no user is logged in to the workload, the workload will be restarted immediately, without waiting for the selected period before automatic restart to pass.

6. Click **Install patches**.

© Acronis International GmbH, 2003-2026

Connecting to workloads for remote desktop or remote assistance

The remote desktop and assistance functionality is a convenient way to connect to the workloads in your organization for remote control or remote assistance.

You can use the remote desktop functionality to perform the following tasks.

- Connect to remote Windows, macOS, and Linux workloads by using NEAR in view-only mode.
- Connect to remote Windows workloads by using RDP.
- Connect to remote macOS workloads by using Apple Screen Sharing in view-only or curtain mode.
- Connect to managed workloads and remotely control them by using cloud remote connections.
- Connect to unmanaged workloads and remotely control them by using direct remote connections.
- Observe multiple monitors at the same time in multi-view.
- Record remote sessions (when connected via NEAR).

You can use the remote assistance functionality to perform the following tasks.

- Connect to remote Windows, macOS, and Linux workloads by using NEAR in control mode.
- Connect to remote macOS workloads by using Apple Screen Sharing in control mode.
- Provide remote assistance to workloads by using cloud remote connections.
- Transfer files between the local and remote workloads.
- Perform basic management actions on the remote workload: restart, shut down, sleep, empty recycle bin, and log out the remote user.
- Monitor the remote workload by periodically taking screenshots of its desktop.

Important

To activate the complete remote desktop and assistance functionality for a managed workload, you must configure and apply a remote management plan to the workload. Although you can apply only one remote management plan on a workload, depending on your needs, you can configure different remote management plans and apply them to different workloads.

In that way, you can control the availability of the features in the remote management plans to correspond to the licenses that are assigned to your workloads.

For more information about remote management plans and working with them, see "Remote management plans" (p. 752).

© Acronis International GmbH, 2003-2026

Note

The remote desktop and assistance functionality requires:

- a one-time installation of Connect Client on the managing (host) workload. When you try to perform a remote action (remote control or remote assistance) on a target workload for the first time, the system prompts you to download the client. Alternatively, you can download Connect Client from the **Downloads** window in the Protection console. For more information about the settings that you can configure, see "Configuring the Connect Client settings" (p. 782).
- installation of Connect Agent on the managed workloads. The Connect Agent is a module that is part of the Protection agent.
- for macOS remote workloads, the required system permissions should be granted to the Connect Agent.

For more information about the platforms supported by each remote desktop and assistance component, see "Supported operating systems for remote desktop and assistance" (p. 747).

Supported operating systems for remote desktop and assistance

The following table lists the supported operating systems by each of component of the remote desktop and assistance functionality.

Remote desktop component	Supported platforms
Connect Client	• Windows 7 or later • macOS 10.13 or later • Linux: openSUSE 8 Debian 9, 10 Ubuntu 18.4-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Connect Agent	• Windows 7 or later • Windows Server 2008 R2 or later • macOS 10.13 or later • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30

© Acronis International GmbH, 2003-2026

Remote desktop component	Supported platforms
	Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Remote connection protocols

The remote desktop functionality uses the following protocols for remote connections.

NEAR

NEAR is a highly secure protocol developed by Acronis that has the following characteristics.

- ### H.264

  NEAR implements three quality modes: **Smooth**, **Balanced** and **Sharp**. In **Smooth** mode, NEAR uses hardware H.264 encoding on macOS and Windows to encode the desktop picture, and falling back to software encoder if hardware encoder is not available. The picture size is currently limited to Full HD resolution (1920x1080).

- ### Adaptive codec

  In **Balanced** and **Sharp** quality modes, NEAR uses Adaptive codec, which provides full picture quality in 32 bit, compared to the 'video' mode used by H.264.

  In **Balanced** mode, the picture quality is automatically adjusted according to your current network conditions and retains the current framerate.

  In **Sharp** mode, the picture is full quality, but it might be with a reduced framerate, if your network, processor, or video card are overloaded.

  Adaptive codec is using OpenCL on Windows and macOS when it is available in their graphics drivers.

- ### Sound transfer

  NEAR is capable of capturing the remote computer sound and transfer that to host. For more information about enabling remote sound redirection on Windows, macOS, and Linux, see "Remote sound redirection" (p. 749).

- ### Different login options

  You can use the following methods to log in to the remote workload.

  Workload credentials: log in to the remote workload using administrator credentials that are registered in the workload.

© Acronis International GmbH, 2003-2026

Ask for permission to observe or control: the user who is logged in to the remote workload will be asked to allow or deny the connection.

- Security

  Your data is always two-way encrypted with AES encryption in NEAR.

RDP

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that enables connecting to the remote Windows computer over a network connection.

Apple Screen Sharing

Apple Screen Sharing is a VNC client by Apple included as part of macOS version 10.5 and later.

Remote sound redirection

Connect Client supports audio streaming via the NEAR connection protocol. For more information about NEAR, see "Remote connection protocols" (p. 748).

Redirecting sound from a remote Windows workload

For Windows workloads, the remote sound should be transmitted automatically. Ensure that there are sound output devices (speakers or headphones) connected to the remote workload.

Redirecting sound from a remote macOS workload

To enable sound redirection from a macOS workload, ensure that:

- The workload has the Protection agent installed.
- The workload has a sound capture driver installed.
- The workload uses the NEAR protocol for remote connections.

Note
For macOS 10.15 Catalina, the Microphone permission must be granted to the Connect Agent. For more information about granting the Microphone permission to the Connect Agent, see "Granting the required system permissions to the Connect Agent" (p. 750).

The agent works with the following sound capture drivers: Soundflower or Blackhole.

The installation process on the newest versions is described on the Blackhole wiki page: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Note
Connect Client currently supports only the 2-channel version of Blackhole.

© Acronis International GmbH, 2003-2026

Alternatively, if Homebrew is installed on the workload, you can install Blackhole by running the following command:

```
brew install --cask blackhole-2ch
```

Note
While the sound of a remote macOS workload is redirected, the user who is logged in to the remote workload will not hear the sound.

Redirecting sound from a remote Linux workload

The remote sound redirection should work automatically with most Linux distributions. If the remote sound redirection is not working by default, install PulseAudio driver by running the following command:

```
sudo apt-get install pulseaudio
```

Granting the required system permissions to the Connect Agent

To enable all features from the remote desktop functionality on macOS workloads, in addition to the full disk access permission, you must grant the following permissions to the Connect Agent:

- **Screen Recording** - enables screen recording of the macOS workload via NEAR. Until this permission is granted, all remote control connections are denied.
- **Accessibility** - enables remote connections in control mode via NEAR.
- **Microphone** - enables sound redirection from the remote macOS workload to the local workload via NEAR. To enable the sound redirection feature, a sound capture driver must be installed on the workload. For more information, see "Remote sound redirection" (p. 749).
- **Automation** - enables the empty recycle bin action.

After you start the agent on the macOS workload, it will check if the agent has these rights and will ask you to grant the permissions, if needed.

To grant the Screen Recording permission

1. In the **Grant required system permissions to Cyber Protect Agent** dialog, click **Set up system permissions**.
2. In the **System permissions** dialog, on the **Screen Recording**row, click **Acquire**.
3. Click **Open System Settings**.
4. For **Connect Agent**, enable the toggle.

If the agent does not have the permission when you try to access the workload remotely, it will show the Screen Recording permission request dialog. Only the local user may answer the dialog.

To grant the Accessibility permission

 © Acronis International GmbH, 2003-2026

1. In the **Grant required system permissions to Cyber Protect Agent** dialog, click **Set up system permissions**.
2. In the **System permissions** dialog, on the **Accessibility** row, click **Acquire**.
3. Click **Open System Settings**.
4. Click the lock icon in the bottom-left corner of the window so that it changes to an unlocked icon. The system will ask you for an administrator password to make changes.
5. Select **Connect Agent**.

To grant the Microphone permission

1. In the **Grant required system permissions to Cyber Protect Agent** dialog, click **Set up system permissions**.
2. In the **System permissions** dialog, on the **Microphone** row, click **Acquire**.
3. In the confirmation window, click **Allow**.

Note
To let the agent utilize the given permission and redirect the sound of the workload, you must also install a sound capture driver on the macOS workload . For more information, see "Remote sound redirection" (p. 749).

To grant the Automation permission

1. In the **Grant required system permissions to the Connect Agent** dialog, click **Set up system permissions**.
2. In the **System permissions** dialog, on the **Automation** row, click **Acquire**.
3. In the confirmation window, click **Allow**.

Connections to remote workloads for remote desktop or remote assistance

The remote desktop and assistance functionality provides several ways to establish remote direct or cloud connections to your workloads.

Direct connections are established via TCP/IP in the local area network (LAN) between Connect Client and the remote workload that does not have an agent installed. They do not require Internet access.

Cloud connections are established between Connect Client and the agent.

The following table provides more info about the cloud connection options.

Cloud connection	Cloud connection option	View mode	Supported remote action	Available for
via NEAR	from Connect Client to Connect Agent	Control View-only	Remote desktop Remote assistance	managed workloads

 © Acronis International GmbH, 2003-2026

Cloud connection	Cloud connection option	View mode	Supported remote action	Available for
via RDP	from Connect Client to Connect Agent from web client to Connect Agent	Control	Remote desktop	managed workloads
via Apple Screen Sharing	from Connect Client to Connect Agent	Control View-only Curtain	Remote desktop Remote assistance	managed workloads

The following table provides more info about the direct connection options.

Direct connection	Direct connection option	Supported remote action	Available for
via RDP	from Connect Client to RDP server	Remote desktop	unmanaged workloads
via Apple Screen Sharing	from Connect Client to Apple Screen Sharing server	Remote desktop Remote assistance	unmanaged workloads

Remote management plans

Remote management plans are plans that you apply on the Protection agent to enable and configure the remote desktop and assistance functionality on your managed workloads.

If no remote management plan is applied on a workload, the remote desktop and assistance functionality will be limited to remote actions (restart, shut down, sleep, empty recycle bin, and log out remote user).

Note
The availability of the feature and the settings that you can configure in the remote management plan depends on the license that is assigned to the workload.

Creating a remote management plan

You can create a remote management plan, and then assign it to a workload to configure the remote desktop and assistance functionality on the managed workload.

Note
The availability of the remote management plan's settings depends on the license that is assigned to the workload.

To create a remote management plan

© Acronis International GmbH, 2003-2026

From Remote management plans

1. In the Cyber Protect console, go to **Management** > **Remote management plans**.
2. Create a remote management plan by using one of the two options.
   - If there are no remote management plans in the list, click **Create**.
   - If there are remote management plans in the list, click **Create plan**.
3. [Optional] To change the default name of the plan, click the pencil icon, enter the name of the plan, and then click **Proceed**.
4. Click **Connection protocols**, and enable the protocols that you want to be available in this remote management plan for remote connections - NEAR, RDP, or Apple Screen Sharing.
5. [Optional] For the NEAR protocol, in the **Security settings** section, select or clear the checkboxes to enable or disable the corresponding settings, and then click **Done**.

Setting	Description	Available for
Lock the workload when the user disconnects from the console session	If you select this setting, the remote workload will be locked when you disconnect from the console session.	Windows, macOS
Allow only one user at a time to connect using NEAR or to transfer files	If you select this setting, connections using NEAR and file transfers will not be possible while there is an active remote connection to the workload.	Windows, macOS, Linux
Allow the workload's administrator to connect to any non-admin user session	If you select this setting, the administrator will be allowed to connect to any standard user session on the workload. If both **Allow the workload's administrator to connect to any non-admin user session** and **Allow system session creation** are clear, you will only be able to connect to active administrator sessions on the remote macOS workloads.	Windows, macOS
Allow system session creation	If you select this setting, when establishing remote connections, the administrator will connect in	macOS

© Acronis International GmbH, 2003-2026

Setting	Description	Available for
	a new session, instead of one of the existing active sessions.	
Allow clipboard synchronization	If you select this setting, you will be able to transfer data between your clipboard and the clipboard of the remote workload. For example, you will be able to copy some text from a file on the remote workload and paste it in a file on your workload, and the opposite.	Windows, macOS, Linux

6. Click **Security settings**, select or clear the checkboxes to enable or disable the corresponding setting, and then click **Done**.

Setting	Description
Show if the workload is controlled remotely	If you select this setting, a notification will be displayed on the desktop of the remote workload when there is an active remote desktop connection to the workload.
Ask for the user's permission to take screenshots of the workload	If you select this setting, the user of the remote workload will be notified when the administrator requests screenshot transmission from the workload.

7. Click **Workload management**, select the features that you want to be available on the remote workloads, and then click **Done**.

Setting	Description	Available on
File transfer	Enables the file transfers between local and remote workloads.	Windows, macOS, Linux
Screenshot transmission	Enables the transmission of screenshots of the desktop of the remote workload to the Cyber Protect console.	Windows, macOS, Linux

8. Click **Display settings**, select or clear the checkboxes to enable or disable the corresponding setting, and then click **Done**.

© Acronis International GmbH, 2003-2026

Note
The **Display settings** are only available for connections via NEAR.

Setting	Description	Available on
Use Desktop Deduplication for desktop capturing	Desktop duplication is one of the screen capture methods on Windows. In some environments, it might be unstable. If you do not use Desktop deduplication, you will use the basic method (BitBlt) instead- it is much slower, but more stable.	Windows
Use OpenCL acceleration	OpenCL acceleration can speed up the Adaptive codec, which is responsible for the **Balanced** quality mode, by running some computations on the graphics processing unit (GPU). This requires an installation of an OpenCL driver on the remote Linux. Adaptive Codec is using OpenCL on macOS and Windows, if it is available in your graphics drivers.	Linux
Use hardware H.264 encoding	NEAR supports three quality modes: **Smooth**, **Balanced**, and **Sharp**. **Smooth** mode uses hardware H.264 encoding to encode the desktop picture. **Balanced** mode uses Adaptive codec, which provides full picture quality in 32 bit, compared to the 'video' mode used by H.264. The picture quality is automatically adjusted according to your current network conditions and retains the current framerate.	Windows, macOS

© Acronis International GmbH, 2003-2026

Setting	Description	Available on
	Sharp mode uses Adaptive codec, which provides full picture quality in 32 bit, compared to the 'video' mode used by H.264. The picture quality is always full, but it might be with reduced frames per seconds, if your network or processor/video card are overloaded.	

9. Click **Toolbox**, select or clear the checkboxes to enable or disable the corresponding setting, and then click **Done**.

Setting	Description	Available on
Show last logged-in users	If you select this setting, the information about the users who last logged in to the workloads will be visible in the workload's details. For more information about the last logged-in users, see "Viewing the last logged-in user" (p. 338).	Windows, macOS, Linux

10. [Optional] To add workloads to the plan:
    a. Click **Add workloads**.
    b. Select the workloads, and then click **Add**.
    c. If there are compatibility issues that you want to resolve, follow the procedure as described in "Resolving compatibility issues" (p. 253).
11. Click **Create**.

From All devices

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Click the workload to which you want to apply a remote management plan.
3. Click **Protect**, and then click **Add plan**.
4. Click **Create plan**, and select **Remote management**.
5. [Optional] To change the default name of the plan, click the pencil icon, enter the name of the plan, and then click **Proceed**.
6. Click **Connection protocols**, and enable the protocols that you want to be available in this remote management plan for remote connections - NEAR, RDP, or Apple Screen Sharing.
7. [Optional] For the NEAR protocol, in the **Security settings** section, select or clear the checkboxes to enable or disable the corresponding settings, and then click **Done**.

© Acronis International GmbH, 2003-2026

Setting	Description	Available for
Lock the workload when the user disconnects from the console session	If you select this setting, the remote workload will be locked when you disconnect from the console session.	Windows, macOS
Allow only one user at a time to connect using NEAR or to transfer files	If you select this setting, connections using NEAR and file transfers will not be possible while there is an active remote connection to the workload.	Windows, macOS, Linux
Allow the workload's administrator to connect to any non-admin user session	If you select this setting, the administrator will be allowed to connect to any standard user session on the workload. If both **Allow the workload's administrator to connect to any non-admin user session** and **Allow system session creation** are clear, you will only be able to connect to active administrator sessions on the remote macOS workloads.	Windows, macOS
Allow system session creation	If you select this setting, when establishing remote connections, the administrator will connect in a new session, instead of one of the existing active sessions.	macOS
Allow clipboard synchronization	If you select this setting, you will be able to transfer data between your clipboard and the clipboard of the remote workload. For example, you will be able to copy some text from a file on the remote workload and paste it in a file on your workload, and the opposite.	Windows, macOS, Linux

© Acronis International GmbH, 2003-2026

8. Click **Security settings**, select or clear the checkboxes to enable or disable the corresponding setting, and then click **Done**.

Setting	Description
Show if the workload is controlled remotely	If you select this setting, a notification will be displayed on the desktop of the remote workload when there is an active remote desktop connection to the workload.
Ask for the user's permission to take screenshots of the workload	If you select this setting, the user of the remote workload will be notified when the administrator requests screenshot transmission from the workload.

9. Click **Workload management**, select the features that you want to be available on the remote workloads, and then click **Done**.

Setting	Description	Available on
File transfer	Enables the file transfers between local and remote workloads.	Windows, macOS, Linux
Screenshot transmission	Enables the transmission of screenshots of the desktop of the remote workload to the Cyber Protect console.	Windows, macOS, Linux

10. Click **Display settings**, select or clear the checkboxes to enable or disable the corresponding setting, and then click **Done**.

Note
The **Display settings** are only available for connections via NEAR.

Setting	Description	Available on
Use Desktop Deduplication for desktop capturing	Desktop duplication is one of the screen capture methods on Windows. In some environments, it might be unstable. If you do not use Desktop deduplication, you will use the basic method (BitBlt) instead- it is much slower, but more stable.	Windows
Use OpenCL acceleration	OpenCL acceleration can speed up the Adaptive codec,	Linux

© Acronis International GmbH, 2003-2026

Setting	Description	Available on
	which is responsible for the **Balanced** quality mode, by running some computations on the graphics processing unit (GPU). This requires an installation of an OpenCL driver on the remote Linux. The Adaptive Codec is using OpenCL on macOS and Windows, if it is available in your graphics drivers.	
Use hardware H.264 encoding	NEAR supports three quality modes: **Smooth**, **Balanced**, and **Sharp**. **Smooth** mode uses hardware H.264 encoding to encode the desktop picture. **Balanced** mode uses Adaptive codec, which provides full picture quality in 32 bit, compared to the 'video' mode used by H.264. The picture quality is automatically adjusted according to your current network conditions and retains the current framerate. **Sharp** mode uses Adaptive codec, which provides full picture quality in 32 bit, compared to the 'video' mode used by H.264. The picture quality is always full, but it might be with reduced frames per seconds, if your network or processor/video card are overloaded.	Windows, macOS

11. Click **Toolbox**, select or clear the checkboxes to enable or disable the corresponding setting, and then click **Done**.

© Acronis International GmbH, 2003-2026

Setting	Description	Available on
Show last logged-in users	If you select this setting, the information about the users who last logged in to the workloads will be visible in the workload's details. For more information about the last logged-in users, see "Viewing the last logged-in user" (p. 338).	Windows, macOS, Linux

12. Click **Create**.

Adding a workload to a remote management plan

You can add workloads to a remote management plan after the plan was created.

To add a workload to a remote management plan

From Remote management plans

1. In the Cyber Protect console, go to **Management** > **Remote management plans**.
2. Click the remote management plan.
3. Depending on whether or not the plan was already applied to any workload, do the following:
   - Click **Add workloads**, if the plan was not applied to any workloads yet.
   - Click **Manage workloads**, if the plan was applied to any workloads.
4. Select a workload from the list, and then click **Add**.
5. Click **Save**.
6. Click **Confirm** to apply the required service quota to the workload.

From All devices

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Click the workload to which you want to apply a remote management plan.
3. Click **Protect**, and then click **Add plan**.
4. In **Select a plan from the list below**, select **Remote management** to view only the remote management plans.
5. Click **Apply**.
6. Click **Confirm** to apply the required service quota to the workload.

Removing workloads from a remote management plan

Depending on your needs, you can remove workloads from a remote management plan.

To remove workloads from a remote management plan

© Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Management** > **Remote management plans**.
2. Click the remote management plan.
3. Click **Manage workloads**.
4. Select one or several workloads that you want to remove from the remote management plan, and then click **Remove**.
5. Click **Done**.
6. Click **Save**.

Additional actions with remote management plans

From the **Remote management plans** screen, you can perform the following additional actions with remote management plans: view details, edit, view the activities, view the alerts, rename, enable, disable, clone, export, import, set as favorite, set as default, and delete.

View details

To view the details of a remote management plan

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **View details**.

Edit

To edit a plan

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Edit**.
3. Edit the settings, and then click **Save**.

Activities

To view the activities related to a remote management plan

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Activities**.
3. Click an activity to view more details about it.

Alerts

To view the alerts

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Alerts**.

Rename

To rename a remote management plan

© Acronis International GmbH, 2003-2026

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Rename**.
3. Enter the new name of the plan, and then click **Proceed**.

Enable

To enable a remote management plan

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Enable**.

Disable

To disable a remote management plan

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Disable**.

Clone

To clone a remote management plan

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Clone**.
3. Click **Create**.

Export

To export a remote management plan

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Export**.
   The plan configuration is exported in a JSON format to the local machine.

Import

Prerequisites

- A JSON file with the plan configuration is available on the machine from which you are logged in to the console.

To import a remote management plan

1. On the **Remote management plans** screen, **Import plan**.
2. In the window that opens, browse to the JSON file.
3. Click the file, and then click **Open**.
   The remote management plan appears on the screen. You can now apply it to workloads.

© Acronis International GmbH, 2003-2026

Set as default

To set a remote management plan as default

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Set as default**.
3. In the confirmation window, click **Set**.
   On the **Remote management plans** screen, the **Default** tag appears next to the plan name.

Set as favorite

To set a remote management plan as favorite

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Add to favorites**.
   On the **Remote management plans** screen, the a star icon appears next to the plan name.

Delete

To delete a remote management plan

1. On the **Remote management plans** screen, click the **More actions** icon of the remote management plan.
2. Click **Delete**.
3. Select **I confirm**, and then click **Delete**.

Workload credentials

You can add administrator or non-administrator credentials of the remote workloads (username and password, or VNC password), save them in the cloud credentials store, and then use them for automatic authentication when connecting to the workloads that you manage. In that way, instead of entering these credentials manually every time during the authentication step of the connection, you can save them in the credentials store once, assign them to multiple workloads, and then the Connect Client will use these credentials every time you want to connect to the workloads remotely.

Adding credentials

You can add credentials and then use them for remote connections to multiple workloads.

To add credentials to a workload and save them in the Credentials store

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Click the workload for which you want to add credentials.
3. Access the **Settings** menu in one of the following ways:
   - Click **Remote desktop**, and then click **Settings**.
   - Click **Manage**, and then click **Settings**.

© Acronis International GmbH, 2003-2026

4. Click **Add credentials**.
5. In the **Credentials store**, click **Add credentials**.
6. Enter the credentials.

Field	Description
Credentials name	Identifier of the credentials that will be visible in the credentials store.
Username	Username that will be used for remote connections to the target workload.
Password	Password that will be used for remote connections to the target workload.
VNC password	This field is available for Apple Screen Sharing only.

7. Click **Save**.

Assigning credentials to a workload

After you add credentials, you can use them to authenticate automatically when you connect to a workload that you manage.

Note
Using Microsoft Entra ID (formerly Azure AD) accounts with the NEAR protocol requires additional configuration. See this KB article.

To assign saved credentials for automatic authentication to a workload

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Access the **Settings** menu in one of the following ways:
   - Click **Remote desktop**, and then click **Settings**.
   - Click **Manage**, and then click **Settings**.
3. On the tab of the supported protocol (NEAR, RDP, or Apple Screen Sharing), click **Add credentials**.
4. In the **Credentials store**, select the credentials from the list, and then click **Select credentials**.

Deleting credentials

You can delete credentials that are not needed anymore.

To delete credentials from the Credentials store

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Access the **Settings** menu in one of the following ways:
   - Click **Remote desktop**, and then click **Settings**.
   - Click **Manage**, and then click **Settings**.

© Acronis International GmbH, 2003-2026

3. On the tab of the supported protocol (NEAR, RDP, or Apple Screen Sharing), click **Delete**.
4. In the confirmation window, click **Delete**.

Unassigning credentials from a workload

You can unassign credentials from a workload, but still keep them in the Credentials store.

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Access the **Settings** menu in one of the following ways:
   - Click **Remote desktop**, and then click **Settings**.
   - Click **Manage**, and then click **Settings**.
3. On the tab of the supported protocol (NEAR, RDP, or Apple Screen Sharing), click **Unassign**.
4. In the confirmation window, click **Unassign**.

Working with managed workloads

Managed workloads are workloads on which the Protection agent is installed.

You can perform the following actions on the remote managed workloads:

- connect for remote assistance or remote desktop by using NEAR in **Control** or **View-only** mode
- connect for remote desktop by using RDP in **Control** mode
- connect for remote assistance or remote desktop by using Apple Screen Sharing in **Control**, **View-only**, or **Curtain** mode
- connect for remote desktop via a web client
- restart, shut down, sleep, empty recycle bin, log out remote user from the remote workloads
- transfer files between your workload and the remote workloads
- monitor them by taking screenshots

Note
The remote desktop connections to managed workloads require installing a Protection agent and applying a remote management plan on the workload.

Configuring RDP settings

You can configure the settings that will be applied automatically for remote control RDP connections to the managed workload.

To configure the RDP settings of a workload

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Access the **Settings** menu in one of the following ways:
   - Click **Remote desktop**, and then click **Settings**.
   - Click **Manage**, and then click **Settings**.

© Acronis International GmbH, 2003-2026

3. On the **RDP** tab, configure the settings.

Setting	Description
Audio playback	This setting enables or disables the redirection of the remote workload sound on your local workload.
Audio recording	This setting determines whether audio recording (speaking to the microphone) will be transferred to the remote workload.
Redirect printers	If you select this setting, the printers from your workload will be available on the remote workload. **Note** Printer redirection is not supported for remote desktop connections via a web client.
Redirect files	This setting defines whether files from your local workload will be shared to remote workload.
Color depth	This setting determines the number of colors in the picture that RDP will transfer. Higher value requires higher bandwidth. **High color**: 16 bit **True color**: • 24 bit for RDP connections via the web client • 32 bit for RDP connections via Connect Client

4. Click the close button.

Connecting to managed workloads for remote desktop or remote assistance

Note
The availability of the connection protocols that you can use for remote connections depends on the remote management plan configuration and on the remote workload's operating system.

Prerequisites

- [For Apple Screen Sharing connections] Apple Screen Sharing is enabled on the macOS workload.

To remotely connect to a managed workload for remote desktop or remote assistance

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Click the workload to which you want to connect.
3. Click **Remote desktop**.
   By default, NEAR is selected as a connection protocol.
4. [Optional] In the **Connection protocol** drop-down list, select the connection protocol that you want to use.

© Acronis International GmbH, 2003-2026

5. Click the view mode that you want to use.

Protocol	Remote connections to	View mode	Supported remote action
NEAR	Windows Linux macOS	**Control** - In this mode, you will be able to observe and perform operations on the remote workload. **View-only**- In this mode, you will be only able to observe the remote workload.	Remote desktop Remote assistance
RDP	Windows	**Control** - In this mode, you will be able to view and perform operations on the remote workload. **Note** If RDP is disabled in the OS settings of the workload, a pop-up window will appear. Use this window to enable RDP for the workload for the current session or in general: • If you want to enable RDP for this workload only for the current session, select **Disable it after the session is over**, and then click **Allow**. • If you want to enable RDP for this workload, click **Allow**.	Remote desktop
Apple Screen Sharing	macOS	**Control** - In this mode, you will be able to observe and perform operations on the remote workload. **View-only** - In this mode, you will be only able to observe the remote workload. **Curtain** - available only for macOS workloads. If you connect to the remote workload in curtain mode, the display of the remote workload will be dimmed, and the remote user will not be able to see your actions on the workload.	Remote desktop Remote assistance

6. [If a remote management plan is not applied to the workload] In the **Apply remote management plan** window, do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.

© Acronis International GmbH, 2003-2026

Note
The system automatically suggests the most appropriate plan, depending on the protocol that you selected in the previous step.

- If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

  For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).

7. [If the corresponding feature is not enabled in the remote management plan that is applied to the workload] In the **Update remote management plan** window, click **Update**, enable the feature, save the changes, and then start this procedure from step 1.
8. [If Connect Client is not installed on your workload] In the **Connect to workload** dialog, click **Download Connect Client**, download and install the client on your workload, and then click **Connect**.
9. [If a confirmation pop-up appears] Click **Open Connect Client**.
10. In the **Authentication** window, select an authentication option, and then provide the required credentials.

Note
If you have assigned credentials to the workload, authentication will be done automatically and this step will be skipped. For more information, see "Assigning credentials to a workload" (p. 764).

Authentication option	Description
With remote workload credentials	You will be allowed to establish the remote connection after you provide username and password of an administrator user of the remote workload. This option is available for NEAR, RDP, and Apple Screen Sharing. You can use this option to authenticate for remote desktop and remote assistance.
Ask for permission to observe	You will be allowed to establish the remote connection in observe mode after the user who is logged in on the remote workload allows it. This option is available for NEAR and Apple Screen Sharing. You can use this option to authenticate for remote assistance.
Ask for permission to control	You will be allowed to establish the remote connection in control mode after the user who is logged in on the remote workload allows it. This option is available for NEAR and Apple Screen Sharing. You can use this option to authenticate for remote assistance.

11. Click **Connect**, and then click the session to display (if more than one user session is available on the workload).

 © Acronis International GmbH, 2003-2026

Connect Client will open a new viewer window on which you will be able to see the remote workload's desktop. The viewer has a toolbar with additional actions that you can perform on the remote workload after the remote connection is established. For more information, see "Using the toolbar in the Viewer window" (p. 778).

Connecting to a managed workload via a web client

You can establish a remote desktop connection to a managed workload via a web client.

Note
Printer redirection is not supported for remote desktop connections via a web client.

Prerequisites

- The management server is installed on a Linux machine.
- RDP is enabled on the managed workload.
- Your browser supports HTML5.

To remotely connect to a workload via a web client

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Click the workload which you want to connect remotely, and then click **Remote desktop**>**Connect via web client**.
3. [If a remote management plan is not applied to the workload] In the **Apply remote management plan** window, do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.
   - If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

     For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).
4. [If the corresponding feature is not enabled in the remote management plan that is applied to the workload] In the **Update remote management plan** window, click **Update**, enable the feature, save the changes, and then start this procedure from step 1.
5. Enter the login and password to access the workload, and then click **Connect**.

   Note
   If you have assigned credentials to the workload, authentication will be done automatically and this step will be skipped. For more information, see "Assigning credentials to a workload" (p. 764).

Transferring files

You can easily transfer files between the local workload and a managed workload.

To remotely transfer files between your workload and a managed workload

 © Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Click the workload with which you want to transfer files.
3. Click **Manage**, and then **Transfer files**.
4. [If a remote management plan is not applied to the workload] In the **Apply remote management plan** window, do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.

     Note
     The system automatically suggests the most appropriate plan.

   - If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

     For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).
5. [If **Allow connections via NEAR** or **File transfer** is disabled in the remote management plan that is applied to the workload] In the **Update remote management plan** window, click **Update**, enable the settings, save the changes, and then start this procedure from step 1.
6. [If Connect Client is not installed on your workload] In the **Connect to workload** dialog, click **Download Connect Client**, download and install the client on your workload, and then click **Connect**.
7. [If a confirmation pop-up appears] Click **Open Connect Client**.
8. In the **Authentication** window, select an authentication option, and then provide the required credentials.

Authentication option	Description
With remote workload credentials	You will be allowed to establish the remote connection after you provide username and password of an administrator user of the remote workload.
Ask for permission to transfer files	You will be allowed to transfer files after the user who is logged in on the remote workload allows it.

9. [To view hidden files] In the **File transfer** window, click **View**, and then click **Show hidden files**.
10. Browse to the files that you want to transfer, and then drag and drop them to the desired destination.

    Note
    The files of the local workload are listed in the left pane, and the files of the remote workload are listed in the right pane.
    When a file transfer begins, it is listed in the **Tasks** pane.

© Acronis International GmbH, 2003-2026

11. [Optional] If you want to remove the completed tasks from the **Tasks** pane, click **Clear finished**.
12. When all transfers complete, close the window.

Sharing clipboard content between workloads

You can send the clipboard content of your workload to a remote workload, or get the clipboard content from a remote workload via NEAR. For example, you may want to copy some text from a file on the remote workload and paste it into a document on your workload, and the opposite.

Send clipboard

To send the clipboard content from your workload to a remote workload

1. Start a remote control session to a managed workload via NEAR.
   For more information, see "Connecting to managed workloads for remote desktop or remote assistance" (p. 766).
2. [Optional] If you want the contents of your clipboard and the remote workloads's clipboard to be synchronized automatically, in the **Viewer** toolbar, click the **Other** icon, and then select **Clipboard auto sync**.
3. To share the content from your clipboard to the remote workload's clipboard, do the following.
   - If **Clipboard auto sync** is disabled, perform the corresponding steps:
     a. On your local workload, copy the text or image that you want to send.
     b. In the **Viewer** toolbar of the remote workload, click the **Others** icon.
     c. Click **Send clipboard**.
     d. Open the file in which you want to paste the content, and then paste it.
   - If **Clipboard auto sync** is enabled, depending on the content that you want to share, perform the corresponding steps.

Option	Actions
If you want to share one or several files in your local clipboard	a. On your local workload, copy the file or files that you want to send. b. Open the remote workload's **Viewer** window. c. In the alert pop-up that appears, click **Send to remote computer**. d. Paste the content to the remote workload.
If you want to share a text from a file in your local clipboard	a. On your local workload, copy the text that you want to send. b. Open the remote workload's **Viewer** window. c. Open the file in which you want to paste the content. d. Paste the content to the file.

© Acronis International GmbH, 2003-2026

Get clipboard

Prerequisites

2FA is enabled for your user account.

To get the clipboard content from a remote workload to your workload

1. Start a remote control session to a managed workload via NEAR.
   For more information, see "Connecting to managed workloads for remote desktop or remote assistance" (p. 766).
2. If you want the contents of your clipboard and the remote workloads's clipboard to be synchronized automatically, in the **Viewer** toolbar, click the **Other** icon, and then select **Clipboard auto sync**.
3. To get the content from the remote workload's clipboard to your clipboard, do the following.
   - If **Clipboard auto sync** is disabled, perform the corresponding steps.
     a. On the remote workload, copy the text or image that you want to share.
     b. In the **Viewer** toolbar of the remote workload, click the **Others** icon.
     c. Click **Get clipboard**.
     d. On the local workload, open the file in which you want to paste the content.
     e. Paste the content to the file.
   - If **Clipboard auto sync** is enabled, depending on the content that you want to get, perform the corresponding steps.

Option	Actions
If you want to get one or several files from the remote workload's clipboard to your local clipboard	a. On the remote workload, copy the file or files that you want to get. b. In the alert pop-up that appears, click **Receive clipboard**. c. On your local workload, paste the content.
If you want to get a text from the remote workload's clipboard to your local clipboard	a. On the remote workload, copy the text that you want to get. b. On your local workload, paste the content to a file.

Performing control actions on managed workloads

You can manage a remote workload by performing the following basic control actions on it: empty recycle bin, sleep, restart, shut down, and log out remote user.

Empty recycle bin

To empty the recycle bin on the remote workload

 © Acronis International GmbH, 2003-2026

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Click the workload on which you want to perform this action.
3. Click **Manage**, and then click **Empty recycle bin**.
4. [If a remote management plan is not applied to the workload] In the **Apply remote management plan** window, do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.
   - If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

     For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).
5. Select the user session for which you want to perform this action, and then click **Empty recycle bin**.

Sleep

To put a remote workload to sleep

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Click the workload on which you want to perform this action.
3. Click **Manage**, and then click **Sleep**.
4. [If a remote management plan is not applied to the workload] In the **Apply remote management plan** window, do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.
   - If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

     For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).

Restart

To restart a remote workload

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Click the workload on which you want to perform this action.
3. Click **Manage**, and then click **Restart**.
4. [If a remote management plan is not applied to the workload] In the **Apply remote management plan** window, do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.
   - If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

     For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).

 © Acronis International GmbH, 2003-2026

5. Depending on the operating system that is installed on the remote workload, do one of the following:
   - For Windows workloads, select if you want to allow the user who is currently logged in locally to the workload to save the changes before the workload is restarted, select the user, and then click **Restart** again.
   - For macOS workloads, select if you want to allow the user who is currently logged in locally to the workload to save the changes before the workload is restarted, and then click **Restart** again.
   - For Linux workloads, click **Restart**.

Shut down

To shut down a remote workload

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Click the workload on which you want to perform this action.
3. Click **Manage**, and then click **Shut down**.
4. [If a remote management plan is not applied to the workload] In the **Apply remote management plan** window, do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.
   - If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

     For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).
5. Depending on the operating system that is installed on the remote workload, do one of the following:
   - For Windows workloads, select if you want to allow the user who is currently logged in locally to the workload to save the changes before the workload is shut down, select the user, and then click **Shut down** again.
   - For macOS workloads, select if you want to allow the user who is currently logged in locally to the workload to save the changes before the workload is shut down, and then click **Shut down** again.
   - For Linux workloads, click **Shut down** again.

Log out remote user

To log out the user of a remote workload

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Click the workload on which you want to perform this action.
3. Click **Manage**, and then click **Log out remote user**.
4. [If a remote management plan is not applied to the workload] In the **Apply remote management plan** window, do one of the following:

 © Acronis International GmbH, 2003-2026

- If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.
- If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

  For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).

5. Select the user that you want to log out, and then click **Log out**.

Monitoring workloads via screenshot transmission

You can monitor the status of a workload by using the Screenshot transmission feature.

Prerequisites

- The workload is online.
- A user is logged in to the workload.

  This user will approve screenshot transmissions if the **Ask for permission to take screenshots** option is enabled in the remote management plan.

Monitoring a workload

To monitor a workload via screenshot transmission

1. In the Cyber Protect console, go to **Devices** > **Screenshot transmission**.
2. Click the workload that you want to monitor.
3. [If a remote management plan is not applied to the workload] Click **Apply a remote management plan**, and then do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.
   - If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

     For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).
4. [If **Screenshot transmission** is disabled in the remote management plan that is applied to the workload] Click **Go to remote management plan** window, click **Edit**, enable **Screenshot transmission**, save the changes, and then start this procedure from step 1.
5. [If **Ask for permission to take screenshots** is enabled in the remote management plan that is applied to the workload] Click **Request screenshot transmission**.

   You will see the screenshot after the user that is logged in the remote workload approves the request.
6. [Optional] Select the user session.
7. [Optional] Select the display.
8. [Optional] Select refresh rate at which to take a new screenshot of the desktop.
9. [Optional] Select the image quality.
10. [Optional] To download the screenshot, click the download icon.

 © Acronis International GmbH, 2003-2026

Taking a screenshot

To take a screenshot of a managed workload

1. In the Cyber Protect console, go to **Devices** > **Machines with agents**.
2. Click the workload from which you want to take a screenshot.
3. Click **Manage**, and then click **Take desktop screenshot**.
4. [If a remote management plan is not applied to the workload] Click **Apply a remote management plan**, and then do one of the following:
   - If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.
   - If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

     For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).
5. [If **Screenshot transmission** is disabled in the remote management plan that is applied to the workload] Click **Go to remote management plan** window, click **Edit**, enable **Screenshot transmission**, save the changes, and then start this procedure from step 1.
6. [If **Ask for permission to take screenshots** is enabled in the remote management plan that is applied to the workload] Click **Request screenshot transmission**.

   You will see the screenshot after the user of the remote workload approves the request.
7. [Optional] Select the user session.
8. [Optional] Select the display.
9. [Optional] Select refresh rate at which to take a new screenshot of the desktop.
10. [Optional] Select the image quality.
11. [Optional] To download the screenshot, click the download icon.

Observing multiple managed workloads simultaneously

You can observe the desktops of multiple remote workloads simultaneously in a single window. This functionality requires that NEAR or Apple Screen Sharing is enabled in the remote management plans that are applied to the workloads.

Note
The number of desktops that you can see simultaneously in the window depends on the size of your monitor.

To observe multiple workloads simultaneously

1. In the Cyber Protect console, go to **Devices** > **All devices**.
2. Select the workloads which you want to observe.
3. Click **Multi view**.
4. [If a remote management plan is not applied to any of the workloads] In the **Apply remote management plan** window, do one of the following:

 © Acronis International GmbH, 2003-2026

- If you want to apply an existing remote management plan, click the **Available plans** field, select the plan, and then click **Apply**.

  Note
  The system automatically suggests the most appropriate plan.

- If you want to create a new remote management plan, click **Add new**, configure the settings, click **Create**, and then, in the confirmation window, click **Confirm**.

  For more information about creating and configuring a remote management plan, see "Creating a remote management plan" (p. 752).

5. [If the corresponding feature is not enabled in the remote management plan that is applied to the workloads] In the **Update remote management plan** window, click **Update**, enable the feature, and then start this procedure from step 1.
6. [If Connect Client is not installed on your workload] In the **Connect to workload** dialog, click **Download Connect Client**, download and install the client on your workload, and then click **Connect**.
7. [If a confirmation pop-up appears] Click **Open Connect Client**.
8. In the **Authentication** window, select an authentication option, and then provide the required credentials.

Authentication option	Description
With remote workload credentials	You will be allowed to establish the remote connection after you provide username and password of an administrator user on the remote workload.
Ask for permission to observe	You will be allowed to establish the remote connection in observe mode after the user who is logged in on the remote workload allows it.

9. If you want to use the same authentication method and credentials when connecting to all the remote workloads that you selected in step 2, select **Use on other computers**.
10. Click **Connect**.

    In toolbar of the multi-view window, you can select a view mode in which to connect to a workload. This action will open a separate Viewer window for that workload.

    Note
    If any of the selected workloads is offline, or has an outdated version of the agent installed, it will not be shown in the multi-view window.
    All multi-view connections to remote workloads are in **View-only** mode.

© Acronis International GmbH, 2003-2026

Using the toolbar in the Viewer window

After you connect to a remote workload, you can use the toolbar of the viewer window to quickly perform the different actions.

Icon	Description
	AI chat Shows or hides the AI chat panel.
	Actual size Scales the remote workload's desktop so that one pixel of the remote desktop corresponds to one pixel on the viewer window.
	Zoom to fit Scales the remote workload desktop to fit the viewer window.
	Lock and **Unlock screen** Shows a placeholder on the remote workload's display so that the remote user will not see your actions.
	Take screenshot Save the remote server's desktop image to a local file.
	Select display Select the remote workload display that you want to view and the desired resolution. Available for Apple Screen Sharing connections to macOS, and NEAR connections to any operating system. If the remote computer has multiple displays, you can choose from the following display modes for multiple monitors: • **Combined** - all remote displays are shown within a single window. • **Splitted** - each remote display is shown in a separate window. This mode is very convenient if you have multiple displays that are connected to your local workload. In this case, for example, you can arrange to see one remote display on each local display. If you close any of the remote workload displays, the remote connection will be ended. To view the displays of the remote workload, you must reconnect to it again. Available for NEAR connections only
	Image quality Adjusts the remote screen image quality from black and white to the

© Acronis International GmbH, 2003-2026

Icon	Description
	highest possible on Apple Screen Sharing connections.
	NEAR image quality Adjusts the quality/performance ratio on NEAR connections. The left side of the slider (Smooth) prioritizes performance over image quality, the right one (Sharp) means the best quality of remote desktop screen, but probably worse performance.
	Send Ctrl+Alt+Del Sends a Ctrl + Alt + Delete sequence to the remote workload. Available for Windows and Linux workloads.
	File Transfer Opens the File Manager window to exchange files between remote and local workload. Available for NEAR connections.
	Pin toolbar Turns off automatic hiding of viewer toolbar. Available for Windows workloads.
	Full screen Switches to the full screen mode and scales the remote workload to completely fill your local screen. Available for Windows workloads.
	Close Closes the Viewer window and ends the remote control session. Available for Windows workloads.

Depending on the connection type, additional options might be available when you click the **Other** icon.

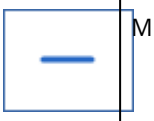
Option	Description
Start recording / Stop recording	Record the current remote desktop session. Session recordings are saved as .crec files on the local workload. You can open .crec files with Acronis Connect Client. Available for NEAR connections
Clipboard auto sync	When you enable this option, the client will be automatically synchronizing your local clipboard and the clipboard of the remote workload.

© Acronis International GmbH, 2003-2026

Option	Description
	Available for NEAR connections
Send clipboard	Use **Send Clipboard** to replace the remote workload's clipboard contents with the contents of the local clipboard. The option is disabled if **Clipboard auto sync** is enabled. For more information, see "Sharing clipboard content between workloads" (p. 771). Available for NEAR connections
Get clipboard	Use **Get Clipboard** to transfer the contents of the remote workload's clipboard to the local workload's clipboard. The option is disabled if **Clipboard auto sync** is enabled. For more information, see "Sharing clipboard content between workloads" (p. 771). Available for NEAR connections
Smart keyboard / Raw keys / Raw keys with all shortcuts	Changes the keyboard input mode for the current connection. **Smart keyboard** - the client transmits Unicode codes of the locally typed symbols to the remote computer **Raw keys** - the client uses the raw codes of the keyboard buttons you press. **Raw keys with all shortcuts** - the client disables local system shortcuts so that they are also transmitted to the remote operating system.
Keyboard focus on mouse hover	When enabled, the client only captures the keyboard input while your local mouse cursor is placed over the Viewer window. When disabled, the client captures your keyboard whenever its window is active.
Show connection info / Hide connection info	When **Show connection info** is selected, a small information panel will appear over the remote desktop screen, showing the most essential information about current connection.
Remote sound	Enables the client to redirect the sound from the remote computer to the local one. Available for NEAR connections
Preferences	Configure the settings of Connect Client. For more information, see "Configuring the Connect Client settings" (p. 782).

In the AI chat window, the following icons are available.

© Acronis International GmbH, 2003-2026

Icon	Description
	Minimizes (hides) the AI chat window.
	Ends the current chat session and opens the chat feedback form.
	Enables viewing past chat sessions and starting a new chat.

Recording and playing remote sessions

You can record a remote session via NEAR in Acronis Connect Client.

To record a remote session

1. On the Viewer toolbar in Connect Client, click **Other**, and select **Start Recording**.
2. Select a name and location for the record.

   By default, the file will be named with the current date and time and located in the **Documents** folder in the current user home directory. While the recording is active, in the **Viewer** toolbar you will see a flashing red circle over the top right corner of the remote screen and the recording timer.
3. To stop the recording, click **Other**, and then click **Stop Recording**. On a Mac, you can also click **Stop** on the toolbar.

   All .crec files made by Acronis Connect Client will be opened with Acronis Connect Client by default.

To play a recording

1. Locate a recording file.
2. Open it.

   The recording player of Acronis Connect Client opens. Note that it is not possible to navigate through the recording. To find a certain moment in the recording, wait until the player reaches it.
3. [Optional] To adjust playback speed, use the **<<** and **>>** icons in the playback controls section.

   The recording is stored as a sequence of events that have been transmitted to and from the remote server during a connection. This ensures the best quality of the recording at the minimum file size. However, this also means that it is not possible to navigate through the recording. At the moment it is also not possible to convert the recordings to a video format.

© Acronis International GmbH, 2003-2026

Configuring the Connect Client settings

After you install Connect Client on your workload, you can configure its settings according to your preferences.

To configure the settings of Connect Client

1. In the start menu, find **Connect Client** and start it.
2. Configure the settings on the **General** tab.

Option	Description
Write verbose logs	Select this option to allow Connect Client to write verbose logs. If disabled, the client will only write general information to the log file.
Proxy settings	Select whether to use the default System proxy, or configure a Custom SOCKSS proxy.

3. Configure the settings on the **Viewer** tab.

Option	Description
Ask for confirmation when closing a viewer	Select this option if you want Connect Client to display a confirmation message when you attempt closing the Viewer window in order to prevent accidental closing.
When minimized	Select whether to suspend the Viewer activity when minimized, in order to reduce the CPU load.
When maximized	Select whether to enable the full screen mode when maximized.
Clipboard transfer	Enable showing the Clipboard transfer indicator in the Viewer window whenever you copy or paste text and images.
Keyboard Mode	Enable showing the Input mode indicator in the Viewer window title whenever mouse and keyboard events are being sent to the remote machine.
Clipboard	Select **Automatically synchronize clipboard** to enable automatic clipboard synchronization, when available.
Send keyboard events	Choose whether to grab your local keyboard input whenever the Connect Client window is active or only when your local mouse pointer is over it.
Viewer background color	Change the Viewer window background color.
Reconnect	Select **Enable to reconnect automatically**, if you want Connect

© Acronis International GmbH, 2003-2026

Option	Description
automatically	Client to automatically re-establish the connection if it has been interrupted.
H.264	You can disable hardware decoders.
Close when idle	Select the time interval of being idle after which to close the Viewer window.

4. Configure the settings on the **Keyboard** tab.

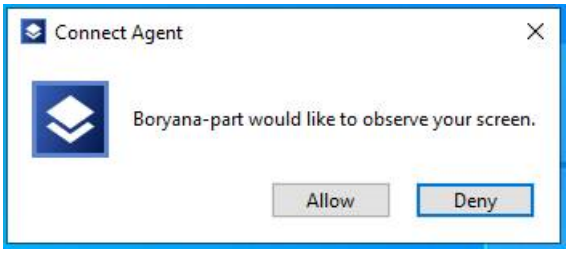
Option	Description
Modifier mappings	Change the behavior of modifier keys with a pop-up menu. These settings are stored separately for NEAR, Apple Screen Sharing, and RDP connections.
Input mode	For each type of connection (selected in the header of pane), select the default keyboard input mode.

5. Click **OK**.

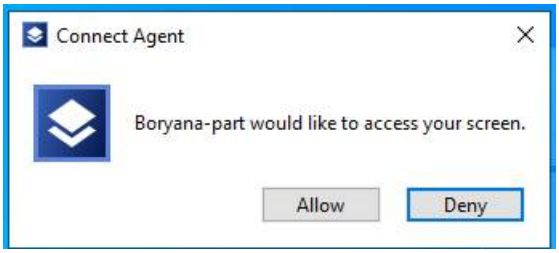
The remote desktop notifiers

The Connect Agent displays action dialogs (notifiers) on the remote workload's desktop in the following cases:

- when you try to connect to the workload remotely by asking for permission to observe. The user who is logged in to the remote workload locally can allow or deny the request.



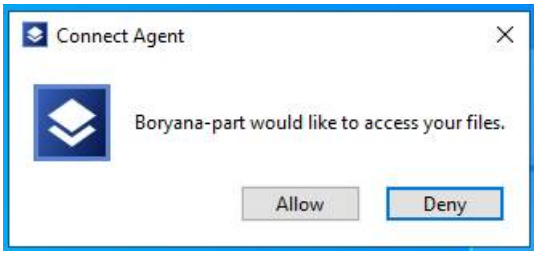
- when you try to connect to the workload remotely by asking for permission to control. The user who is logged in to the remote workload locally can allow or deny the request.



- when you try to exchange files between your workload and the remote workload by asking for permission to transfer files. The user who is logged in to the remote workload locally can allow or

© Acronis International GmbH, 2003-2026

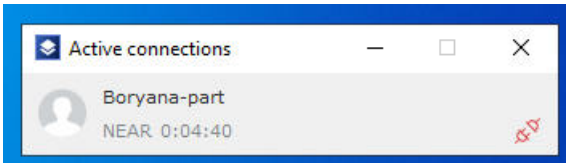
deny the request.



When you establish a remote desktop connection to a workload, the user who is logged in to the workload will view a different connection notifier that contains the following information:

- name of the user who is connected remotely
- connection protocol that is used to establish the remote connection
- duration of the remote connection

The user who is logged in to the remote workload locally can end the connection at any time by clicking the **Disconnect** icon or the **Close** icon.



© Acronis International GmbH, 2003-2026

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.

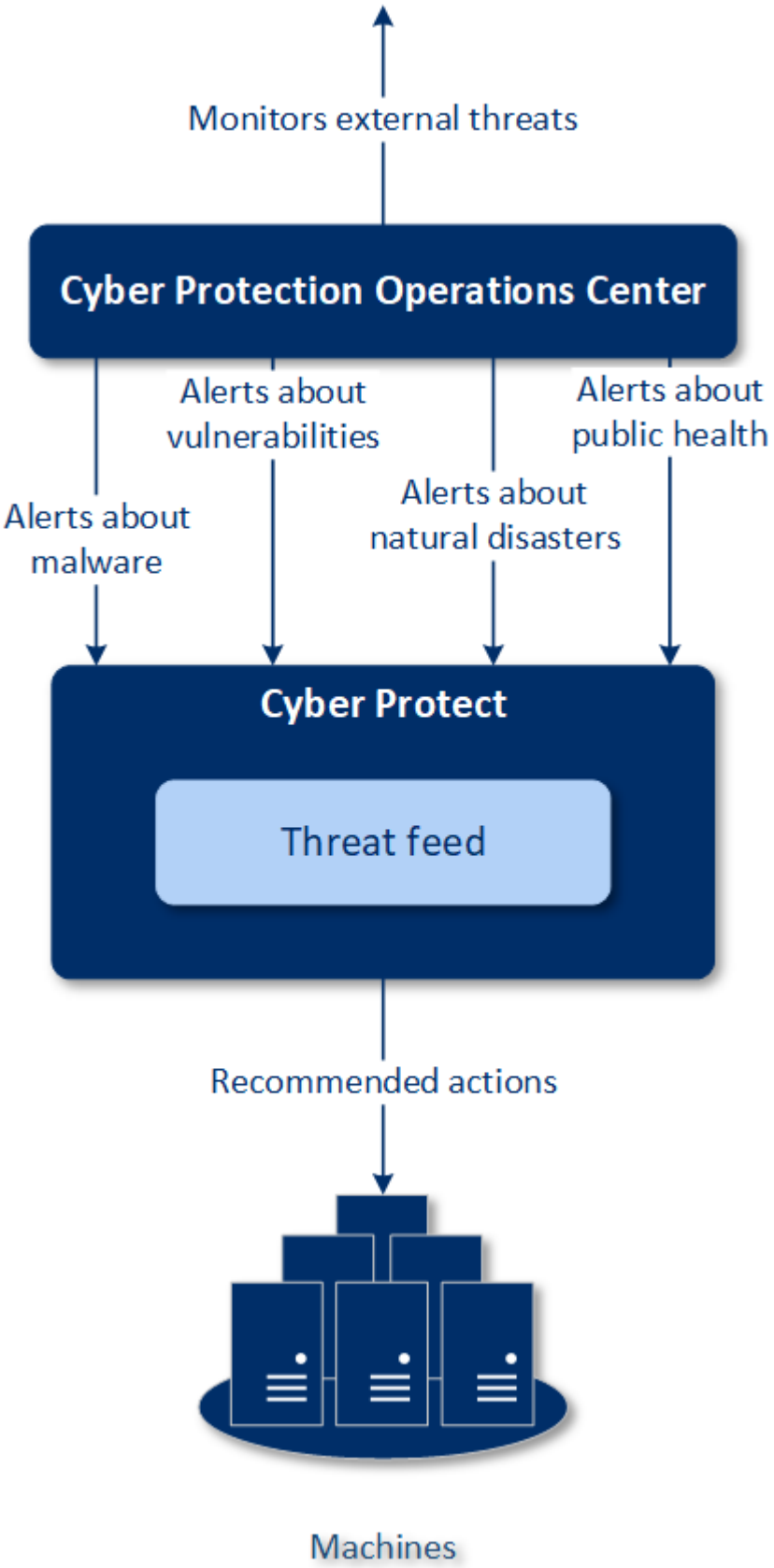
A security alert can be resolved with the number of specific actions that are provided by the security experts. There are some alerts that are used just for notifying you about the upcoming threats but no recommended actions are available.

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 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.

© Acronis International GmbH, 2003-2026



© Acronis International GmbH, 2003-2026

To run the recommended actions on received alerts from Acronis Cyber Protection Operations Center, do the following:

1. In the Cyber Protect 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

With Data protection map you can:

- Receive detailed information about stored data (classification, locations, protection status, and additional information) on your workloads.
- Check whether data is protected. Data is considered protected if a protection plan with backup module enabled is applied to the workload.
- Perform actions for data protection.

Note
The **Data protection map** option is disabled by default in newly created protection plans.

© Acronis International GmbH, 2003-2026

How it works

1. First, you create a protection plan with the Data protection map module enabled.
2. Then, after the plan was performed and your data were discovered and analyzed, you will get the visual representation of data protection on the Data protection map widget.

You can also go to **Devices** > **Data protection map** and find there information about unprotected files per device.

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 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 **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 a more detailed information about the unprotected files on a particular device, click on the name of the device.

   You will see the number of unprotected files per extension and per location. Define the extensions in the search field, for which you want to get the information about unprotected files.
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, see "Creating a protection plan" (p. 243).

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:

 © Acronis International GmbH, 2003-2026

- **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. 373). 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:

 © Acronis International GmbH, 2003-2026

`.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.

© Acronis International GmbH, 2003-2026

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 available for machines running Windows 10 and later. 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 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**.

© Acronis International GmbH, 2003-2026

Working with the Centralized Dashboard

Centralized Dashboard user roles

To access the Centralized Dashboard, the user must:

- be a member of the Active Directory or a system user on the machine on which Centralized Dashboard is installed.
- have a user account in the Management console with an administrative account role at the Organization (root) level for the management server on which the Centralized Dashboard is installed. For more information about adding administrative accounts, see "Adding administrative accounts" (p. 334).

The data that the user with access to the Centralized Dashboard will be allowed to view depends on the Centralized Dashboard user roles that are assigned to the user.

The following table provides more information about the user roles in the Centralized Dashboard.

User role	Description
DASHBOARDAMS	This role is assigned automatically to all users accounts in the Management console by default. It ensures that users can access the Centralized Dashboard. However, the role does not guarantee that users will see data on the Centralized Dashboard. For example: • users with the **Read-only** role in the Management console (for the management server on which the Centralized Dashboard is installed) will be able to access the Centralized Dashboard, but will not see any data until an AMS-specific role is assigned to them • users with the **Administrator** role at the Organization (root) level in the Management console (for the management server on which the Centralized Dashboard) is installed will see the data for all management servers that are connected to the Centralized Dashboard.
ALLAMS	This role is assigned automatically to users that have the **Administrator** role at the Organization (root) level in the Management console (for the management server on which the Centralized Dashboard is installed). These users can view the data for all management servers that are connected to the Centralized Dashboard.

© Acronis International GmbH, 2003-2026

User role	Description
NOAMS	This role is assigned automatically to users in the Management console (for the management server on which the Centralized Dashboard is installed) who are not **Administrator** role at the Organization (root) level. These users do not access to the data from any management server. They will be able to log in to the Centralized Dashboard, but will see an empty screen.
AMS-specific role	For each management server that is connected to the Centralized Dashboard, a specific user role is created in the Centralized Dashboard. When you want to allow a user to view the data of a particular management server, and to hide the data for the rest of the management servers, use this AMS-specific role.

Assigning Centralized Dashboard user roles

By default, user accounts in the Management console with the **Administrator** administrative account role at the Organization (root) level for the management server on which the Centralized Dashboard is installed will be assigned the ALLAMS role to the Centralized Dashboard and will have access to the data for all management servers that are registered to the Centralized Dashboard. All other user accounts initially will not have access to any data in the Centralized Dashboard.

Administrator users can change the default Centralized Dashboard user roles that are assigned to the users so that they serve the organization's needs.

Prerequisites

- Your user must be a member of the Active Directory or a system user on the machine on which Centralized Dashboard is installed.
- Your user must have a user account in the Management console with an **Administrator** administrative account role at the Organization (root) level for the management server on which the Centralized Dashboard is installed.

To assign a Centralized Dashboard user role

1. Log in to the Centralized Dashboard.
2. Click **Settings**, and then click **List Users**.
3. For the user to whom you want to assign a Centralized Dashboard user role, click **Edit record**.
4. In the **Roles** field, select or remove roles as necessary.
5. Click **Save**.

© Acronis International GmbH, 2003-2026

Logging in to the Centralized Dashboard

After you install the Centralized Dashboard component, you can log in to the web interface and start monitoring the data for the management servers that are registered to the Centralized Dashboard.

Prerequisites

- Your user is assigned the DASHBOARDAMS role in the Centralized Dashboard.
- Your user is assigned the ALLAMS role, or the relevant roles for monitoring data from specific management servers.

To log in to the web interface of the Centralized Dashboard

1. Navigate to the Centralized Dashboard URL.
2. Log in by using your Acronis Cyber Protect credentials.

Viewing data from multiple management servers

On the Centralized Dashboard, you can see data for multiple management servers on a single screen.

Prerequisites

- At least one management server is registered to the Centralized Dashboard.
- Your user is assigned the DASHBOARDAMS role in the Centralized Dashboard.
- Your user is assigned the ALLAMS role, or the relevant roles for monitoring data from specific management servers.

To view the data from multiple management servers

1. Navigate to the Centralized Dashboard URL.
2. Log in by using your Acronis Cyber Protect credentials.

   The information on the Centralized Dashboard is presented in widgets. The following table provides more information about the widgets.

Widget	Description
Alerts	The widget displays a summary of all active alerts for the selected time range.
Activities	The widget displays the total number of activities grouped by activity status: **Succeeded with warnings**, **Succeeded**, **Failed**, and **Cancelled**. Each bar in the chart represents a day or an hour, depending on the selected time range.
Devices	The widget displays a summary of the devices that are registered in the management servers that are registered to the Centralized Dashboard, and their protection status. You can add or remove columns from the widget, based on a predefined list, by clicking the ellipsis button of the widget, and then selecting the **Edit chart** menu.

© Acronis International GmbH, 2003-2026

3. [Optional] To change the localization of the dashboard, click the flag icon in the upper right corner of the screen, and then select the language that you prefer.
4. [Optional] To filter the data by management server, in the **Filters** section:
   a. Click the **AMS** field, and then select one ore more management servers from the list.
   b. Click **Apply filters**.
5. [Optional] To change the period for which data is displayed, in the **Filters** section:
   a. Click **Period**, and then select the period.
   b. Click **Apply filters**.
6. [Optional] To change the time grain, in the **Filters** section:
   a. Click **Time grain**, and then select the time grain.
   b. Click **Apply filters**.
7. [Optional] To change the default auto-refresh interval:
   a. Click the ellipsis button (**...**), and then click **Set auto-refresh interval**.
   b. Select the interval at which you want the data on the screen to be refreshed, and then click **Save for this session**.

Viewing licensing information from multiple management servers

On the Centralized Dashboard, you can see licensing data for multiple management servers on a single screen. You can also download the data from the widgets, as described in "Downloading the Centralized Dashboard data" (p. 796)

Prerequisites

- At least one management server is registered to the Centralized Dashboard.
- Your user is assigned the DASHBOARDAMS role in the Centralized Dashboard.
- Your user is assigned the ALLAMS role, or the relevant roles for monitoring data from specific management servers.

To view the licensing data from multiple management servers

1. Navigate to the Centralized Dashboard URL.
2. Log in by using your Acronis Cyber Protect credentials.
3. Click the **Licenses** tab.

   The information on the page is presented in widgets. The following table provides more information about the widgets.

Widget	Description
License assignment	The widget displays licensing data for each management server that is registered to the Centralized Dashboard.
License keys	The widget displays the licenses of the workloads that are registered in the

 © Acronis International GmbH, 2003-2026

Widget	Description
	management servers. The widget also includes the **My Acronis Account** link to Acronis Customer Portal (https://account.acronis.com), where you can manage the licenses.

4. [Optional] To change the localization of the dashboard, click the flag icon in the upper right corner of the screen, and then select the language that you prefer.
5. [Optional] To filter the data by management server, in the **Filters** section:
   a. Click the **AMS** field, and then select one ore more management servers from the list.
   b. Click **Apply filters**.
6. [Optional] To change the default auto-refresh interval:
   a. Click the ellipsis button **...**, and then click **Set auto-refresh interval**.
   b. Select the interval at which you want the data on the screen to be refreshed, and then click **Save for this session**.

Navigating to the web console of a connected management server

From the Centralized Dashboard, you can access the web console of any of the registered management servers without additional authentication.

To navigate to the web console of a local management server

1. Log in to the Centralized Dashboard.
2. In the **Devices** widget, perform one of the following actions:
   - Click the device name from the chart.
     You are redirected to the **Devices** screen in the console of the management server. The device is preselected automatically.
   - Click the name of the management server.
     You are redirected to the console of the management server.

Downloading the Centralized Dashboard data

From the Centralized Dashboard screen, you can download data in the following ways:

- Download the data that is visible on the screen as an image.
- Download the data of a widget as an image.
- Download the data of a widget as a CSV file.
- Download the data from a widget as an Excel file.

Download dashboard data

To download the dashboard data as an image file

© Acronis International GmbH, 2003-2026

1. Click the ellipsis button (**...**).
2. Click **Download as image**.

Note
The file will be downloaded to the default download folder of the browser.

Download widget data

To download the data from a widget

1. Click the ellipsis button (**...**).
2. Click **Download**, and then select the option that you prefer.

Option	Description
Export to .CSV	Use this option if you want to save the data from the widget as a CSV file. The file will include only the data that is visible on the dashboard.
Export to Excel	Use this option if you want to save the data from the widget as an Excel file. The file will include only the data that is visible on the dashboard.
Export to full .CSV	Use this option if you want to save the full data from the widget as a CSV file. The file will include all the data from the widget. The file will include all data from the widget, including the records that are not visible on the dashboard.
Export to full Excel	Use this option if you want to save the full data from the widget as an Excel file. The file will include all data from the widget, including the records that are not visible on the dashboard.
Download as image	Use this option if you want to download an image of the widget.

Note
- The data will be downloaded to the default download folder of the browser.
- The maximum number of records per CSV file is 100000.

Centralized Dashboard configuration

The management server on which the Centralized Dashboard component is installed must have a minimum of 8 CPUs and 8 GB RAM. Such a configuration supports up to:

- 20 management servers
- 20,000 devices in total (registered in all the management servers)
- 100,000 backups
- 10,000,000 activities
- 100,000 alerts

The expected performance for such configurations is the following:

© Acronis International GmbH, 2003-2026

- The average delay for displaying data in the Centralized Dashboard is two minutes.
- The average time for the loading of widgets (UI responsiveness) is one second.

Configurations that have greater numbers of devices or management servers registered to the same Centralized Dashboard might have an increased delay and decreased UI responsiveness.

© Acronis International GmbH, 2003-2026

Centralized Dashboard database queries

You can run queries in the Centralized Dashboard database to extract specific information from the database and use it in custom tools in your organization. For example, your system might need information about a specific type of alerts generated for specific devices, and might use this information to automatically open a ticket.

Note
To connect to the Centralized Dashboard, use the same domain name or address of the Microsoft SQL server that was provided during the installation of the database for the management server. For more information, see "Database for the management server" (p. 106).

Basic queries in the Centralized Dashboard database

The following examples list the most basic queries that you can use to extract data from the Centralized Dashboard database.

The following query returns information about the alerts in specific status, for example BackupFailed:

```
SELECT *
FROM active_resources_alerts_view
WHERE type = 'BackupFailed';
```

The following query returns information about the last successful backup that was performed after a specific date:

```
SELECT *
FROM backups
WHERE created_time > '2023-01-01 12:00:00';
```

The following query returns information about the total used storage for all archives:

```
SELECT SUM(size)
FROM archives;
```

The following query returns information about the total used storage for all vaults:

```
SELECT vault_pk, SUM(size) as consumed
FROM archives
GROUP BY vault_pk;
```

The following query returns information about the agent versions:

```
SELECT device_name, agent_version
FROM device_grid_view;
```


© Acronis International GmbH, 2003-2026

Centralized Dashboard database views and tables

You can use the information about the Centralized Dashboard database views and tables to create your own queries.

The Views schema provides the main information that you will need to create the most common queries. However, if you ever need more details, you can investigate the Raw Data schema too.

Materialized Aggregates schema

The Materialized Aggregates schema consists of the following tables: `tasks_daily_stats` and `backup_resources_daily_stats`.

The `tasks_daily_stats` table contains statistics about tasks completion statuses per hour.

Column name	Column type	Description
acep_source	VARCHAR(256) NOT NULL	ID of the management server that is registered to the Centralized Dashboard. This field is the FK on `collector_addresses`.
result_code	VARCHAR(256) NOT NULL	Status of completed tasks: ok, error, warning, cancelled, abandoned, timedout, or outofsync.
hour_begin	DATETIME NOT NULL	Timestamp of the hour for bucket start.
count	INT	Number of tasks in per hour in the corresponding bucket.

The `backup_resources_daily_stats` table contains statistics about backups of each device.

Column name	Column type	Description
acep_source	VARCHAR(256) NOT NULL	ID of the management server that is registered to the Centralized Dashboard. This field is the FK on `collector_addresses`.
resource_id	VARCHAR(256)	Resource ID. This field is part of the primary key.

© Acronis International GmbH, 2003-2026

Column name	Column type	Description
	NOT NULL	
tenant_id	VARCHAR(256) NOT NULL	Tenant ID. This field is part of the primary key.
archives_ count	BIGINT	Number of backups of the device
backups_ count	BIGINT	Number of recovery points of the device
oldest_ backup	DATETIME	Oldest recovery point of the device
latest_ backup	DATETIME	Latest recovery point of the device
used_total	BIGINT	Used total storage of the backups of the device
used_cloud	BIGINT	Used cloud storage of the backups of the device
used_local	BIGINT	Used local storage of the backups of the device

Views schema

The Views schema consists of the following tables: `collector_addresses_view`, `active_resources_alerts_view`, `tasks_daily_stats_view`, and `device_grid_view`.

The `collector_addresses_view` table contains information about the management servers that are registered to the Centralized Dashboard.

Column name	Column type	Description
origin	VARCHAR(256)	Name of the management server that is registered to the Centralized Dashboard.
address	VARCHAR(256)	IP address of the management server that is registered to the Centralized Dashboard.

© Acronis International GmbH, 2003-2026

The `active_resources_alerts_view` table contains information about the alerts that are generated for the tenants in all management servers that are registered to the Centralized Dashboard.

Column name	Column type	Description
origin	VARCHAR(256)	Name of the management server that is registered to the Centralized Dashboard.
address	VARCHAR(256)	IP address of the management server that is registered to the Centralized Dashboard.
id	VARCHAR(256)	Alert ID
resource_id	VARCHAR(256)	Resource ID
severity	VARCHAR(256)	Alert severity
tenant_id	VARCHAR(256)	Tenant ID
created_at	DATETIME	Time when the alert was created on the tenant
deleted_at	DATETIME	Time when alert was dismissed on the tenant
received_at	DATETIME	Time when alert was received
type	VARCHAR(256)	Alert type
source	VARCHAR(256)	Alert source
category	VARCHAR(256)	Alert category

The `tasks_daily_stats_view` table contains information about the tasks that were completed per hour for all tenants in the management servers that are registered to the Centralized Dashboard.

Column name	Column type	Description
origin	VARCHAR(256)	Name of the management server that is registered to the Centralized Dashboard.
result_status	VARCHAR(23) NOT NULL	Status of completed tasks:

© Acronis International GmbH, 2003-2026

Column name	Column type	Description
		Succeeded, Failed, Succeeded with warnings, Cancelled, or Failed.
hour_begin	DATETIME NOT NULL	Timestamp of the hour for bucket start.
count	INT	Number of tasks in the bucket.

The `device_grid_view` table contains information about all the devices that are available in the tenants in the management servers that are registered to the Centralized Dashboard.

Column name	Column type	Description
origin	VARCHAR(256)	Name of the management server that is registered to the Centralized Dashboard.
address	VARCHAR(256)	IP address of the management server that is registered to the Centralized Dashboard.
device_name	NVARCHAR(256)	Device name
device_id	VARCHAR(256) NOT NULL	Device ID
device_ protection_status	VARCHAR(256) NOT NULL	Protection status of the device
device_state	VARCHAR(256)	Device state
device_type	VARCHAR(256)	Device type
device_groups	NVARCHAR(MAX)	Device group(s)
applied_policy_ names	NVARCHAR(MAX)	Protection plans
last_successful_ backup	DATETIME	Date and time of the last successful backup of the device
next_backup	DATETIME	Date and time of the next backup
agent_name	NVARCHAR(256)	Agent
agent_is_active	TINYINT	Agent state
agent_version	VARCHAR(256)	Agent version
os	VARCHAR(256)	Operating system of the device

© Acronis International GmbH, 2003-2026

Column name	Column type	Description
archives_count	BIGINT	Number of backups of the device
backups_count	BIGINT	Number of recovery points of the device
oldest_backup	DATETIME	Date and time of the oldest recovery point of the device
latest_backup	DATETIME	Date and time of the latest recovery point of the device
used_total	BIGINT	Total used storage
used_cloud	BIGINT	Used cloud storage
used_local	BIGINT	Used local storage
registered_at	DATETIME	Date and time of the device registration to Cyber Protect.
unit_name	VARCHAR(256)	Unit to which the device belongs
alert_count	INT	Total alerts
comment	NVARCHAR(MAX)	Comment
ip_address	VARCHAR(256)	IP address(es)

Raw data schema

The raw data schema shows the relationships between the tables in the Centralized Dashboard database. Primary keys are marked as PK and foreign keys are marked as FK. If the PK or FK is composite, the digit in brackets shows the order in which the key is constructed.

Note
The raw data schema tables and relationships might be updated in future releases.

The following table provides more information about the columns in the `collector_addresses` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	
source_uid	VARCHAR(256)	
address	VARCHAR(256)	
hostname	VARCHAR(256)	

The following table provides more information about the columns in the `tenants` table.

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
tenant_id	BIGINT	
uuid	VARCHAR(256)	PK(1)
external_id	VARCHAR(256)	
customer_type	VARCHAR(256)	
created_at	DATETIME	
updated_at	DATETIME	
deleted_at	DATETIME	
version	BIGINT	
nesting_level	SMALLINT	
kind	VARCHAR(256)	
parent_id	BIGINT	FK(1) to `tenants`.uuid
brand_id	INT	
brand_enabled	TINYINT	
company_name	VARCHAR(256)	
tenant_name	VARCHAR(256)	
barrier	SMALLINT	
parent_has_access	TINYINT	
owner_id	BIGINT	

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
mfa_status	VARCHAR(256)	
status	VARCHAR(256)	
pricing_mode	VARCHAR(256)	
path	VARCHAR(256)	
id	BIGINT	
internal_tag	VARCHAR(256)	
customer_id	VARCHAR(256)	
public_uuid	VARCHAR(256)	
currency	VARCHAR(256)	
production_start_date	DATETIME	

The following table provides more information about the columns in the `alerts` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
id	VARCHAR(256)	PK(1)
resource_id	VARCHAR(256)	FK(1) to `grpm_resources`.resource_id
severity	VARCHAR(256)	
tenant_id	VARCHAR(256)	FK(2) to `grpm_resources`

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
		.tenant_id FK(1) to `tenants`.uuid
created_at	DATETIME	
deleted_at	DATETIME	
received_at	DATETIME	
type	VARCHAR(256)	
source	VARCHAR(256)	
category	VARCHAR(256)	

The following table provides more information about the columns in the `tasks` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
shard_key	VARCHAR(256)	
id	BIGINT	
uuid	VARCHAR(256)	PK(1)
type	VARCHAR(256)	
queue	VARCHAR(256)	
issuer_id	VARCHAR(256)	
assigned_agent_id	VARCHAR(256)	
tenant_id	VARCHAR(256)	FK(2) to `grpm_`

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
		resources .tenant_id FK(1) to tenants.uuid
euc_id	VARCHAR(256)	
policy_id	VARCHAR(256)	
policy_type	VARCHAR(256)	
resource_id	VARCHAR(256)	FK(1) to grpm_resources .resource_id
resource_type	VARCHAR(256)	
result_code	VARCHAR(256)	
created_at	DATETIME	
started_at	DATETIME	
completed_at	DATETIME	
started_by	VARCHAR(256)	
result_error_code	VARCHAR(MAX)	
result_error_domain	VARCHAR(MAX)	
error_codes	VARCHAR(MAX)	
error_text	VARCHAR(MAX)	

The following table provides more information about the columns in the `grpm_resources` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to collector_addresses .source_uid FK(0) to <any other table>.acep_

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
		source
acep_time_key	INT	
resource_id	VARCHAR(256) NOT NULL	PK(1)
resource_key	BIGINT	
resource_type	VARCHAR(256)	
is_webhosting_server	TINYINT	
installed_application	VARCHAR(256)	
tenant_id	VARCHAR(256) NOT NULL	PK(2) FK(1) to `tenants`.uuid
euc_id	VARCHAR(256)	FK(1) to `tenants`.uuid
partner_id	VARCHAR(256)	FK(1) to `tenants`.uuid
cloud_connection_id	VARCHAR(256)	
inside_virtual	TINYINT	
device_memory	BIGINT	
guest_os	VARCHAR(256)	
list_of_disks_with_types	VARCHAR(MAX)	
has_hdd	TINYINT	
created_at	DATETIME	
updated_at	DATETIME	
deleted_at	DATETIME	
hwi_os_name	VARCHAR(MAX)	
hwi_os_version	VARCHAR(MAX)	
hwi_os_build_type	VARCHAR(MAX)	
hwi_os_family	VARCHAR(MAX)	
hwi_os_manufacturer	VARCHAR(MAX)	
virt_host_version		
hostname	VARCHAR(256)	

© Acronis International GmbH, 2003-2026

The following table provides more information about the columns in the `grpm_resources_status` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
resource_id	VARCHAR(256)	PK(1) FK(1) to `grpm_resources`.resource_id
resource_key	BIGINT	
tenant_id	VARCHAR(256)	PK(2) FK(1) to `tenants`.uuid FK(2) to `grpm_resources`.tenant_id
created_at	DATETIME	
updated_at	DATETIME	
deleted_at	DATETIME	
state	VARCHAR(256)	
severity	VARCHAR(256)	
applied_policy_names	NVARCHAR(MAX)	
last_success_backup	DATETIME	

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
next_backup	DATETIME	
group_names	NVARCHAR(MAX)	
ip_addresses	VARCHAR(256)	
comment	NVARCHAR(MAX)	

The following table provides more information about the columns in the `grpm_resources_bindings` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
resource_id	VARCHAR(256)	PK(1) FK(1) to `grpm_resources`.resource_id
resource_key	BIGINT	
agent_id	VARCHAR(256)	PK(2) FK(1) to `grpm_agents`.agent_id
agents	VARCHAR(MAX)	
tenant_id	VARCHAR(256)	FK(1) to `tenants`.uuid FK(2) to

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
		grpm_resources.tenant_id FK(2) to grpm_agents.tenant_id
euc_id	VARCHAR(256)	FK(1) to tenants.uuid
partner_id	VARCHAR(256)	FK(1) to tenants.uuid
created_at	DATETIME	
updated_at	DATETIME	
deleted_at	DATETIME	

The following table provides more information about the columns in the `grpm_agents` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to collector_addresses.source_uid FK(0) to <any other table>.acep_source
acep_time_key	INT	
agent_id	VARCHAR(256) NOT NULL	PK(1)
agent_type	VARCHAR(256)	
tenant_id	VARCHAR(256)	PK(2) FK(1) to tenants.uuid
euc_id	VARCHAR(256)	FK(1) to tenants.uuid

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
partner_id	VARCHAR(256)	always empty
is_active	TINYINT	
is_domain_controller	TINYINT	
host_os_family	VARCHAR(256)	
host_os_version	VARCHAR(256)	two ints separated by '.'
created_at	DATETIME	
updated_at	DATETIME	
deleted_at	DATETIME	
registered_at	DATETIME	
os_product_type	INT	
version	VARCHAR(256)	
is_online	TINYINT	
name	VARCHAR(256)	

The following table provides more information about the columns in the `backup_resources` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
backup_pk	BIGINT	PK(1) FK(1) to `backups`.pk

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
resource_id	VARCHAR(256)	PK(2) FK(1) to `grpm_resources`.resource_id

The following table provides more information about the columns in the `backups` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
pk	BIGINT	PK(1)
row_ver	BIGINT	
archive_pk	BIGINT	FK(1) to `archives`.pk
id	VARCHAR(256)	
tenant_id	VARCHAR(256)	FK(1) to `tenants`.uuid
created_at	DATETIME	

The following table provides more information about the columns in the `archives` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
		.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
pk	BIGINT	PK(1)
row_ver	BIGINT	
vault_pk	BIGINT	FK(1) to `vaults`.pk
id	VARCHAR(256)	
tenant_id	VARCHAR(256)	FK(1) to `tenants`.uuid
size	BIGINT	
created	DATETIME	

The following table provides more information about the columns in the `vaults` table.

Column name	Column type	Links
acep_date	DATETIME NOT NULL	
acep_source	VARCHAR(256)	PK(0) FK to `collector_addresses`.source_uid FK(0) to `<any other table>`.acep_source
acep_time_key	INT	
pk	BIGINT	PK(1)
euc	VARCHAR(256)	FK(1) to `tenants`.uuid
id	VARCHAR(256)	

© Acronis International GmbH, 2003-2026

Column name	Column type	Links
tenant_id	VARCHAR(256)	FK(1) to `tenants`.uuid
storage_type	VARCHAR(64)	

Configuring the retention period of the backup data from a local management server

For each local management server that is registered to the Centralized Dashboard, you can configure the duration for which backup data remains visible on the Centralized Dashboard.

To configure the retention period of the backup data of a local management server

1. On the local management server, navigate to `C:\Program Files\Acronis\TaskManager`, and then open the `task_manager.yaml` file.
2. In the `acep` section, add or change the `snapshot-max-period` setting as follows:

```
acep:
  db-chunk-size: 1000
  page-size-limit: 5000000
  response-time-limit: 50s
  snapshot-max-period: 60d  # Adjust to the desired number of days
  db-request-time-jitter: 5s
  logged-errors-limit: 50
```

3. To apply the new configuration, save the changes and then restart the AMS service.
4. Wait for the data to be synched with the Centralized Dashboard.
   It might take up to 24 hours for the updated snapshot data to be reflected on the Centralized Dashboard.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.

The tape libraries that you use must be dedicated to Cyber Protect. Shared tape libraries are not supported.

To learn if your specific device is supported, use the Hardware Compatibility Tool as described at https://care.acronis.com/content/57237. You can send a report about the test results to Acronis. Hardware with confirmed support is listed in the Hardware Compatibility List.

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 `ArsmDmlDbProtocol`. The string may contain up to 32765 characters.
5. Start the Removable Storage Management service.

To relocate the database in Linux:

© Acronis International GmbH, 2003-2026

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="ArsmDmlDbProtocol" 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">
```

 © Acronis International GmbH, 2003-2026

```
            "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>
```

 © Acronis International GmbH, 2003-2026

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 for tape devices

- Tape devices are not supported when a machine is booted from 32-bit Linux-based bootable media.
- You cannot back up Microsoft 365 mailboxes and Microsoft Exchange mailboxes to a tape device.
- You cannot recover individual mailboxes from backups of Exchange databases.
- You cannot create application-aware backups of physical and virtual machines.
- In macOS, only file-level backup to a managed tape-based location is supported.
- 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.
- You cannot use deduplication for backups that are stored on tapes.
- 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.

© Acronis International GmbH, 2003-2026

- With a backup that is stored on a tape, you cannot perform recovery under an operating system if a restart of the operating system is required. For such a recovery, use a bootable media.
- You can validate backups that are stored on tapes, but you cannot select for validation an entire tape-based location or tape device.
- A managed tape-based location cannot be protected with encryption. Encrypt your backups instead.
- Devices that use the Network Data Management Protocol (NDMP) are not supported.
- Barcode printers are not supported.
- Linear Tape File System (LTFS) formatted tapes are not supported.
- LTO-9 media must be calibrated before the first use. The calibration process might take up to two hours to complete. Tape libraries that do not support automatic calibration send the non-calibrated LTO-9 media to the **Unrecognized** pool and do not use them for backup.

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

© Acronis International GmbH, 2003-2026

Tape written on a locally attached tape device (tape drive or tape library) by...	Bootable Media	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5/15	+	+	+	-
	Agent for Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5/15	+	+	+	-
	Agent for Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5/15	+	+	+	-
Tape written on a tape device through...	Backup Server	9.1	-	-	-	-
		Echo	-	-	-	-
	Storage Node	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5/15	+	+	+	+

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.

© Acronis International GmbH, 2003-2026

Before backing up

1. Load tapes to the tape device.
2. Log in to the Cyber Protect 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.
- Both stand-alone tapes and tape libraries are supported.

© Acronis International GmbH, 2003-2026

Note
When backing up a stand-alone tape, the tape cannot be automatically changed. Ensure that the tape has sufficient capacity or be ready to change it manually if needed. Otherwise, the backup will fail.

Before backing up

1. Load tapes to the tape device.
2. Log in to the Cyber Protect 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.

© Acronis International GmbH, 2003-2026

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 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.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

- 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.

© Acronis International GmbH, 2003-2026

Tape was used by...	Tape is read by...	Tape is sent to pool...
Agent	The same agent	Where the tape was before
	Another agent	**Imported tapes**
	Storage node	**Imported tapes**
Storage node	The same storage node	Where the tape was before
	Another storage node	**Imported tapes**
	Agent	**Imported tapes**
Third-party backup application	Agent or storage node	**Unrecognized tapes**

Tapes of certain types are sent to specific pools:

Tape type	Tape is sent to pool...
Empty tape	**Free tapes**
Empty write-protected tape	**Unrecognized tapes**
Cleaning tape	**Unrecognized tapes**

The fast inventorying can be applied to entire tape devices. The full inventorying can be applied to entire tape devices, individual drives, or slots. For stand-alone tape drives, the full inventorying is always performed, even if the fast inventorying is selected.

Combination of fast and full inventorying

Full inventorying of an entire tape device may take a long time. If you need to inventory only a few tapes, proceed as follows:

1. Perform the fast inventorying of the tape device.
2. Click the **Unrecognized tapes** pool. Find the tapes you want to inventory and note which slots they occupy.
3. Perform the full inventorying of these slots.

What to do after inventorying

If you want to back up to tapes that were placed in the **Unrecognized tapes** or **Imported tapes** pool, move 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.

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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.

 © Acronis International GmbH, 2003-2026

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**.

© Acronis International GmbH, 2003-2026

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).

Important
Acronis Storage Node version 17 requires agents version 17. It does not work with older agents, such as v16, v15, and v12.5. Do not install the storage node component if you still have older agents running on protected workloads.

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. 846).

Important
Acronis Storage Node version 17 requires agents version 17. It does not work with older agents, such as v16, v15, and v12.5. Do not install the storage node component if you still have older agents running on protected workloads.

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**.

 © Acronis International GmbH, 2003-2026

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, see "Generating a registration token" (p. 156).
   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, see "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**.

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 (including NAS as an SMB/CIFS share)
  - On a SAN storage that appears to the operating system as a network folder
- 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

© Acronis International GmbH, 2003-2026

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, see "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, see "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, see "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

© Acronis International GmbH, 2003-2026

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:

© Acronis International GmbH, 2003-2026

- 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 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.

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

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, see "Installing a storage node and a catalog service".

 © Acronis International GmbH, 2003-2026

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.
- Data catalog cannot be enabled for managed locations created on tape devices.
- The following data cannot be displayed in the catalog:
  - Data from 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.

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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**.

Immutable storage

Immutable storage provides a critical layer of protection for backup data by preventing deletion or modification of restore points until their retention period expires. This safeguard ensures that backups remain intact even if credentials are compromised, ransomware disables security tools, or administrative errors occur. While enabling immutability may slightly increase storage costs because older restore points cannot be deleted before their retention period expires, this predictable expense is minimal compared to the financial and operational impact of losing critical data. Real-world incidents have demonstrated that immutability can be the difference between a full recovery and catastrophic data loss.

Immutable storage is available for all cloud backups stored in a supported cloud storage instance. See "Supported storages and agents" (p. 848).

With immutable storage, you can access deleted backups during the specified retention period. You can recover content from these backups, but you cannot change, move, or delete them. When the retention period ends, the deleted backups are permanently deleted.

The immutable storage contains the following backups:

- Backups that are deleted manually.
- Backups that are deleted automatically, according to the settings in the **How long to keep** section in a protection plan or the **Retention rules** section in a cleanup plan.

In the cloud deployment, the cloud storage space used by the backups in immutable storage is charged accordingly.

Immutable storage modes

- **Governance mode**
  In this mode, all deleted backups remain in immutable storage for the specified retention period. This prevents ransomware or malicious actors from tampering with or erasing backup data and ensures the integrity of backups, which is essential for reliable disaster recovery.
  In this mode, you can change the retention period or switch to Compliance mode. Immutable storage can be disabled only by contacting the Support team.
- **Compliance mode**
  In addition to the benefits of the Governance mode, the Compliance mode helps organizations meet the regulatory requirements for data retention and security by preventing changes in the retention policy, including changing the retention period or disabling it.

 © Acronis International GmbH, 2003-2026

Important
Selecting Compliance mode is irreversible. After selecting this mode, you cannot change the retention period or switch back to Governance mode. Immutable storage cannot be disabled in this mode.

Supported storages and agents

- [On-premises deployment] Immutable storage is supported only on Acronis Cyber Infrastructure storage (version 6.0.1 or later) that is registered in the Cyber Protect console. For more information about how to add Acronis Cyber Infrastructure storage, see "About Acronis Cyber Infrastructure" (p. 363).

  Immutable storage requires a protection agent version 16.0.37277 or later.
- [Cloud deployment] Immutable storage is supported only on the cloud storage.
  - Immutable storage is available for Acronis-hosted and partner-hosted cloud storages that use Acronis Cyber Infrastructure version 6.0.1 or later.
  - All storages that can be used with Acronis Cyber Infrastructure Backup Gateway are supported. For example, Acronis Cyber Infrastructure storage, Amazon S3 and EC2 storages, and Microsoft Azure storage.
  - Immutable storage requires that TCP port 40440 is open for the Backup Gateway service inAcronis Cyber Infrastructure. TCP port 40440 is automatically opened with the **Backup (ABGW) public** traffic type. For more information about the traffic types, see Acronis Cyber Infrastructure documentation.

  Immutable storage requires a protection agent version 24.01 (build 24.1.37195) or later.
- Only TIBX (Version 12) backups are supported.

Enabling immutable storage

You can enable the immutable storage in the Cyber Protect console.

To enable immutable storage

1. Log in to the Cyber Protect console as an administrator.
2. Go to **Settings** > **Storage node**.
3. Select the Acronis Cyber Infrastructure storage node for which you want to enable immutable storage, and then click **Immutable storage settings**.
4. Turn on the **Immutable storage** switch.
5. Click **Enable**.
6. Specify a retention period between 14 and 3650 days.

   The default retention period is 14 days. A longer retention period will result in increased storage usage.
7. Select the immutable storage mode and, if prompted, confirm your choice.

 © Acronis International GmbH, 2003-2026

- **Governance mode**
  In this mode, all deleted backups remain in immutable storage for the specified retention period. This prevents ransomware or malicious actors from tampering with or erasing backup data and ensures the integrity of backups, which is essential for reliable disaster recovery.
  In this mode, you can change the retention period or switch to Compliance mode. Immutable storage can be disabled only by contacting the Support team.
- **Compliance mode**
  In addition to the benefits of the Governance mode, the Compliance mode helps organizations meet the regulatory requirements for data retention and security by preventing changes in the retention policy, including changing the retention period or disabling it.

  Important
  Selecting Compliance mode is irreversible. After selecting this mode, you cannot change the retention period or switch back to Governance mode. Immutable storage cannot be disabled in this mode.

8. Click **Close**.
9. To add an existing archive to the immutable storage, create a new backup in that archive by running the corresponding protection plan manually or on a schedule.

   Note
   If you delete a backup before adding the archive to the immutable storage, the backup is deleted permanently.

Disabling immutable storage

Warning!
We strongly advise against disabling immutable storage:

- Immutable storage is the last line of defense against accidental or malicious deletion of backups.
- Ransomware protection alone is not enough—immutability ensures recoverability even if credentials are compromised.
- Cost impact is predictable and limited, while the risk of data loss without immutability is high and unpredictable.
- Industry best practice and insurance requirements increasingly mandate immutable backups.
- Disabling immutability exposes your organization to SLA breaches, compliance risks, and reputational damage.

Important
Immutable storage can be disabled only in Governance mode.

Prerequisites

- You have the storage ID. To learn how to find it, see "Finding the storage ID" (p. 850).

 © Acronis International GmbH, 2003-2026

To disable immutable storage

1. On the machine with the management server, open the command-line interface. For example, Command Prompt or Terminal.
2. In the command-line interface, navigate to the following folder:
   - Windows: `%ProgramFiles%\Acronis\AccountServer`
   - Linux: `/usr/lib/Acronis/AccountServer`
3. In the `AccountServer` folder, run the `immutable_storage` tool with the following parameter:
   - Windows

     ```
     immutable_storage.exe -s <storage ID>
     ```

     For example:

     ```
     immutable_storage.exe -s 40d0921a-93e3-4612-b7da-132ad02cf3df
     ```

   - Linux

     ```
     sudo chmod +x immutable_storage
     ```

     ```
     sudo ./immutable_storage -s <storage ID>
     ```

     For example:

     ```
     sudo chmod +x immutable_storage
     ```

     ```
     sudo ./immutable_storage -s 40d0921a-93e3-4612-b7da-132ad02cf3df
     ```

If immutable storage is disabled, everything that has been located on this storage is marked for deletion and will be deleted within 24 hours.

Important
24 hours is the maximum time frame, and the files may be erased much earlier, for example, in 1 hour.

Finding the storage ID

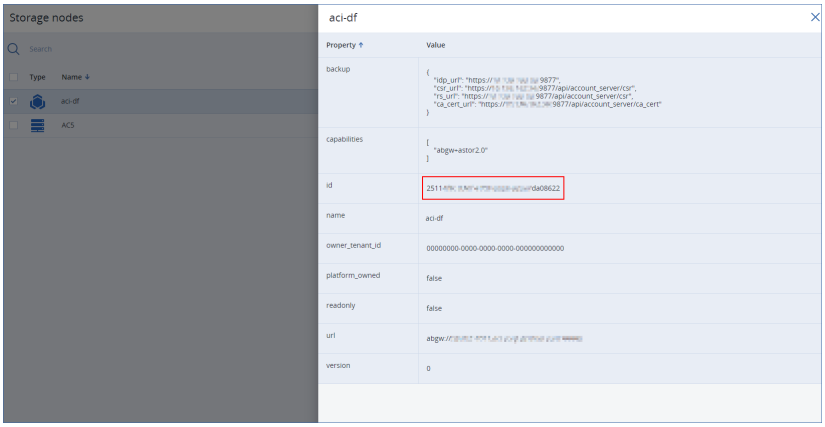
To disable the immutable storage in the on-premises deployment, you must know the storage ID.

To find the storage ID

1. Log in to the Cyber Protect console as an administrator.
2. Go to **Settings** > **Storage node**.
3. Select the storage node, and then click **Details**.
4. On the pane that opens, click **All properties**.

© Acronis International GmbH, 2003-2026

5. Check the value for the **id** property.



Accessing deleted backups in immutable storage

During the retention period, you can access deleted backups in immutable storage and recover data from them.

A deleted backup can be part of a deleted archive or non-deleted archive.

Note
To allow access to deleted backups, port 40440 on the backup storage should be enabled for incoming connections.

To access a deleted backup

In a deleted archive

1. On the **Backup storage** tab, select the cloud storage that contains the deleted backup.
2. To see the deleted archives, click **Show deleted**.
3. Select the archive that contains the backup that you want to recover.
4. Click **Show backups**.
5. Select the backup that you want to recover.
6. Proceed with the recovery operation, as described in "Recovery" (p. 502).

In a non-deleted archive

1. On the **Backup storage** tab, select the cloud storage that contains the deleted backup.
2. Select the archive that contains the backup that you want to recover.
3. Click **Show backups**, and then click **Show deleted**.
4. Select the backup that you want to recover.
5. Proceed with the recovery operation, as described in "Recovery" (p. 502).

© Acronis International GmbH, 2003-2026

Compatibility with Advanced Format (4K-sector) hard disks

Backup and recovery are supported on traditional hard disks with 512-byte sector size, and on Advanced Format disks with 4096-byte sector size.

When you recover data from one disk to another, both disks must have the same logical sector size (this is the size that is presented to the operating system). The volumes on the disk are automatically aligned, if necessary. Thus, the start of a cluster in the file system always matches the start of a physical sector on the disk.

International Disk Drive Equipment and Materials Association (IDEMA) specifies two types of Advanced Format disks:

- 512-byte emulation (512e) disks
  These disks have a 512-byte logical sector size.
- 4K native (4Kn) disks
  These disks have a 4096-byte logical sector size.
  4Kn disks are commonly used as external drives with USB connection. System boot might not be supported with these disks.

For more information about Advanced Format, see https://idema.org/initiatives/advanced-format.

To check the logical sector size of a disk

Windows

1. Ensure that the disk contains an NTFS volume.
2. Run the following command as an administrator, specifying the drive letter of the NTFS volume (for example, `D`):

   ```
   fsutil fsinfo ntfsinfo D:
   ```

3. Check the value in the **Bytes Per Sector** line.
   For example:

   ```
   Bytes Per Sector: 512
   ```

Linux

1. Check the device name of the disk.
   For example `/dev/sdb`.
2. Run the following command as the root user, specifying the device name of the disk:

   ```
   parted /dev/sdb print
   ```

3. Check the first value in the **Sector size (logical/physical)** line.

© Acronis International GmbH, 2003-2026

For example:

```
Sector size (logical/physical): 512B/4096B
```


© Acronis International GmbH, 2003-2026

Command-line reference

Command-line reference is a separate document available at https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_16_Command_Line_Reference/index.html.

© Acronis International GmbH, 2003-2026

Troubleshooting

You can save an agent log to a .zip file. If a backup fails for an unknown reason, this file will help the technical support personnel to identify the problem.

By default, the information in the log is optimized for the last three days, but you can change this period.

To collect agent logs

1. Do one of the following:
   - Under **Devices**, select the machine from which you want to collect the logs, and then click **Activities**.
   - Under **Settings** > **Agents**, select the machine from which you want to collect the logs, and then click **Details**.
2. [Optional] To change the default period for which system information is included, click the arrow next to the **Collect system information** button, and then select the period.
3. Click **Collect system information**.
4. If prompted by your web browser, specify where to save the file.

© Acronis International GmbH, 2003-2026

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

© Acronis International GmbH, 2003-2026

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.

© Acronis International GmbH, 2003-2026

Index

3

32-bit or 64-bit? 606

4

40 to 160 MB of RAM per 1 TB of unique data 843

A

About Acronis Cyber Infrastructure 363

About Secure Zone 360

About the Physical Data Shipping service 436

Absence of applications competing for resources 843

Accessing a virtual appliance via an SSH client 191

Accessing deleted backups in immutable storage 851

Accessing the Cyber Protect console 229

Acronis account 19

Acronis Customer portal 23

Acronis Customer portal, cloud console, and local console 23

Acronis Cyber Protect 17 editions and licensing 38

Acronis patented technologies 18

Acronis PXE Server 632

Actions with protection plans 244

Activating a management server 42

Activating Startup Recovery Manager 636

Active device discovery by using Device Sense™ 210

Active Protection 684, 686, 693

Active Protection settings 687

Adaptive codec 748

Adding a backup location 363

Adding a custom message to the web console 236

Adding a machine running Linux 125

Adding a machine running macOS 125

Adding a machine running Windows 120

Adding a managed location 839

Adding a Microsoft 365 organization 670

Adding a Scale Computing HC3 cluster 129

Adding a vCenter or an ESXi host 125

Adding a workload to a remote management plan 760

Adding Acronis Plug-in to WinPE 625

Adding administrative accounts 334

Adding credentials 763

Adding devices to static groups 256

Adding licenses to your Acronis account 40

Adding machines from the Cyber Protect console 120

Adding multiple devices 203

Adding quarantined files to the whitelist 707

Adding the AR_RETENTION_LOCK_SUPPORT variable 95

Adding the console to the list of local intranet sites 231

Adding the console to the list of trusted sites 232

Adding VLANs 628

© Acronis International GmbH, 2003-2026

Additional actions with remote management plans 761

Additional options 368

Additional remote operations with bootable media 604

Additional requirement for virtual machines 653

Additional requirements for application-aware backups 644

Additional requirements for machines running Windows 654

Additional scheduling options 379

Administering user accounts and organization units 330

Administrative account in multiple units 333

Administrative account roles 332

Administrative accounts 331

Advanced 695

Advanced storage options 358, 817

Agent-based and agentless backup 36

Agent components 207

Agent for Exchange (for mailbox backup) 64

Agent for Hyper-V 67

Agent for Linux 65

Agent for Mac 66

Agent for Nutanix 68

Agent for Nutanix (Virtual Appliance) 175

Agent for Office 365 64

Agent for Oracle 65

Agent for oVirt 68

Agent for oVirt (Virtual Appliance) 170

Agent for oVirt (Virtual Appliance) – required roles and ports 175

Agent for Scale Computing HC3 – required roles 169

Agent for Scale Computing HC3 (Virtual Appliance) 67

Agent for SQL, Agent for Exchange (for database backup and application-aware backup), Agent for Active Directory 63

Agent for Synology 68, 181

Agent for Virtuozzo 68

Agent for VMware (Virtual Appliance) 67

Agent for VMware (Windows) 67

Agent for Windows 62

Agent for Windows (Legacy) 62

Agent for Windows XP SP2 70

Agent installation parameters 141, 146

Agents 28

Agents with the Updater role 321

Alerts 403

Alerts configuration file 285

Allocating licenses to a management server 45

Allowing only HTTPS connections to the web console 235

Allowing processes to modify backups 688

Alternative options 389

Always incremental (single-file) 344

Antimalware and web protection 681

Antimalware features 685

Antimalware scan of backups 707

Antivirus & Antimalware protection settings 686

Antivirus and antimalware protection 685

Antivirus and Antimalware protection 682

© Acronis International GmbH, 2003-2026

Apple Screen Sharing 749

Application-aware backup 651

Applying a protection plan to a group 266

Applying a protection plan to a workload 245

Approving patches manually 742

Are the required packages already installed? 90

Assessing vulnerabilities and managing patches 720

Assigning Centralized Dashboard user roles 793

Assigning credentials to a workload 764

Assigning licenses to workloads 54

Attaching SQL Server databases 658

Automatic adding to the whitelist 706

Automatic domain rejoin 547

Automatic driver search 544

Automatic patch approval 737

Availability of the backup options 400

Availability of the recovery options 548

B

Back up a typical machine before backing up several machines with similar contents 843

Back up different machines at different times 843

Backing up 824-825

Backing up a machine to a locally attached tape device 823

Backing up clustered Hyper-V machines 498

Backing up databases included in an AAG 648

Backing up Nutanix virtual machines 181

Backing up Proxmox workloads 679

Backing up the Exchange cluster data 650

Backing up to a tape device attached to a storage node 824

Backup 75, 339

Backup administrator role 335

Backup and recovery in vSphere Client 472

Backup consolidation 403

Backup file name 404

Backup file name vs. simplified file naming 407

Backup format 408

Backup format and backup files 409

Backup module cheat sheet 341

Backup operator role 336

Backup options 400

Backup replication 464

Backup scanning details 275

Backup scanning plans 463

Backup schedule 364

Backup schemes 364

Backup schemes, operations, and limitations 364

Backup to and recovery from a network share 614

Backup to and recovery from the bootable media 614

Backup to and recovery from the cloud storage 613

Backup types 366

Backup validation 410, 550

Backup window 433

Basic disk cloning 583

© Acronis International GmbH, 2003-2026

Basic operations with reports 283

Basic parameters 144

Basic precautions 581

Basic queries in the Centralized Dashboard database 799

Basic rsyslog configuration 296

Before backing up 824-825

Before you start 160, 163, 170, 176, 181

Behavior detection 689

Behavior detection settings 689

Boot mode 550

Bootable media 559

Bootable Media Builder 605

Broadcom (VMware) ESXi virtual machine 504

Browsing the hardware inventory 711

Browsing the software inventory 717

Built-in groups 254

By total size of backups 344

C

Cache storage options 324

calculate hash 424

Cataloging 844

Cataloging best practices 846

Categories to filter 699

CEF activity examples 303

CEF alert examples 301

Centralized Dashboard 27

Centralized Dashboard configuration 797

Centralized Dashboard database queries 799

Centralized Dashboard database views and tables 800

Centralized Dashboard user roles 792

Certificate installation 297

Change volume label 599

Change volume letter 598

Changed block tracking (CBT) 410

Changed Block Tracking (CBT) 479

Changing the backup format to version 12 (TIBX) 409

Changing the download location 323

Changing the graphics adapter for Agent for oVirt (Virtual Appliance) 174

Changing the language 230

Changing the Microsoft 365 access credentials 672

Changing the recovery environment 542

Changing the SQL Server or Exchange Server access credentials 668

Changing the user account for Agent for VMware 495

Check access to the drivers in bootable environment 544

Check device IP address 378

Checking for software updates 221

Choosing the operating system for disk management 581

Citrix Hypervisor/XenServer 85

Cleanup 467

Cloud console 25

Cloud deployment 190, 230, 501

Cloud storage 413

Cluster-aware backup 650

Cluster backup mode 411

Coexistence with third-party software 817

© Acronis International GmbH, 2003-2026

Collecting diagnostic information 317

Command-line reference 854

Common backup rule 93

Common installation rule 93

Common parameters 136

Common requirements 644

Common restrictions 841

Compatibility issues with plans 252

Compatibility with Advanced Format (4K-sector) hard disks 852

Compatibility with Dell EMC Data Domain storages 94

Compatibility with encryption software 93

Compatibility with RSM and third-party software 817

Components 27

Components for remote installation 124

Components to install 103

Compression level 412

Configuration troubleshooting 311

Configuring a PostgreSQL instance 109

Configuring a web browser for Integrated Windows Authentication 230

Configuring Agent for Nutanix (Virtual Appliance) 178

Configuring Agent for oVirt (Virtual Appliance) 172

Configuring an already registered Agent for VMware 128

Configuring application-aware backup of virtual machines running Windows Server 2022 and later 652

Configuring automatic patch approval 738

Configuring encryption as a machine property 386

Configuring encryption in the protection plan 386

Configuring iSCSI devices 631

Configuring network settings 628

Configuring passive device discovery 209

Configuring patch management settings in the protection plan 730

Configuring proxy server settings in Cyber Protect Monitor 281

Configuring RDP settings 765

Configuring retention rules 384

Configuring the action on detection for Real-time protection 690

Configuring the Connect Client settings 782

Configuring the display mode for Linux-based bootable media 629

Configuring the patch lifetime in the list 737

Configuring the Production patching protection plan 740

Configuring the retention period of the backup data from a local management server 816

Configuring the scan mode for Real-time protection 690

Configuring the severity of alerts 285

Configuring the source of protection definitions on an air-gapped management server 330

Configuring the Test patching protection plan 739

Configuring the virtual appliance 161, 165

Conflict between a new and existing plan 250

© Acronis International GmbH, 2003-2026

Conflict between an individual and group plan 250

Connecting to a machine booted from media 628

Connecting to a managed workload via a web client 769

Connecting to discovered devices remotely 219

Connecting to managed workloads for remote desktop or remote assistance 766

Connecting to workloads for remote desktop or remote assistance 746

Connections to remote workloads for remote desktop or remote assistance 751

Considerations for users with the Advanced license 399

Continuous data protection (CDP) 350

Control type 617

Conversion plans 388

Conversion to a virtual machine 388

Conversion to a virtual machine with a separate conversion plan 394

Conversion to a virtual machine with the protection plan 391

Copying Microsoft Exchange Server libraries 667

Copyright statement 18

Corporate whitelist 706

CPU priority 434

Create a bootable media or download a ready-made one? 559

Create a volume 594

Creating a backup 473

Creating a dynamic group 256

Creating a pool 830

Creating a protection plan 243

Creating a remote management plan 752

Creating a replication plan 477

Creating a SIEM log forwarding plan 287

Creating a static group 255

Creating backups by using bootable media locally 562

Creating bootable media 533

Creating the .mst transform and extracting the installation packages 134

Creating the transform file and extracting the installation packages 151

Creating units 338

Criteria 415

Cross-platform recovery 503

Cross-platform recovery via bootable media 509

Cryptomining process detection 688

Cryptomining process detection settings 689

Custom groups 255

Custom pools 830

Custom scripts 615

Customizing installation settings 103

Cyber Frame / Virtuozzo Infrastructure 89

Cyber Frame virtual machine 506

Cyber Protect console 36

Cyber Protect Monitor 279

Cyber Protection 268

D

Data catalog 844

© Acronis International GmbH, 2003-2026

Data Deduplication 75

Data protection map 787

Data protection map settings 788

Data protection map widget 273

Database backup 646

Database for Scan Service 110

Database for the management server 106

Date and time for files 551

Deactivating Startup Recovery Manager 637

Debian syslog configuration example 294

Decreasing the license quota of an offline management server 51

Deduplication 841

Deduplication best practices 841

Deduplication restrictions 841

Default actions 694

Default administrators 333

Default backup file name 406

Default backup options 320

DefaultBlockSize 820

Delete a volume 597

Deleting a pool 830

Deleting a protection plan 247

Deleting a virtual machine running from a backup 471

Deleting all alerts 787

Deleting backups 456

Deleting backups outside the Cyber Protect console 458

Deleting credentials 764

Deleting the SIEM log forwarding plan 289

Deleting your Acronis account 22

Deploying Agent for Nutanix from a QCOW2 template 177

Deploying Agent for Nutanix from the Cyber Protect console 177

Deploying Agent for oVirt (Virtual Appliance) 171

Deploying Agent for Scale Computing HC3 (Virtual Appliance) 163

Deploying Agent for VMware (Virtual Appliance) from an OVF template 160

Deploying Agent for VMware (Virtual Appliance) via the web interface 126

Deploying protection agents through Group Policy 150

Deploying the OVF template 161

Deploying the vCenter plugin 472

Deploying the virtual appliance 164

Deploying virtual appliances 160

Deployment 363

Deployment agent 123

Detecting tape devices 828

Device discovery 201

Device discovery by using Device Sense ™ 208

Device discovery requirements 203

Device groups 254

Different login options 748

Direct selection 345, 348

Disable automatic DRS for the agent 161

Disabling automatic assignment for an agent 486

Disabling browsing of the folder tree 248

Disabling immutable storage 849

Disabling One-click recovery 430

© Acronis International GmbH, 2003-2026

Disaster recovery 558

Discovered machines 269

Discovering multiple devices 202

Disk-level backup 841

Disk conversion

basic to dynamic 591

dynamic to basic 592

GPT to MBR 591

MBR to GPT 590

Disk health monitoring 269

Disk health status alerts 273

Disk health widgets 270

Disk initialization 582

Disk operations 582

Disk provisioning 479

Disk space requirements 541, 635

Distribution algorithm 484

Do not show messages and dialogs while processing (silent mode) 414, 552

Do not start when connected to the following Wi-Fi networks 377

Do not start when on metered connection 376

Documentation 364

Downloading files from the cloud storage 535

Downloading large files 536

Downloading protection agents 129

Downloading the Centralized Dashboard data 796

Downloading the protection definitions to an online management server 325

Downloading the setup program 183

Drivers for Universal Restore 622

Dumping the report data 284

Dynamic disk conversion

MBR to GPT 591

Dynamic installation of antimalware components 159

E

Editing a pool 830

Editing a protection plan 245

Editing the company profile 19

Editing the SIEM log forwarding plan 289

Eject tapes after each successful backup of each machine 444

Ejecting 836

Email notifications 317, 412

Email server 318

Enable file recovery from disk backups stored on tapes 443

Enable VSS full backup 449

Enabling immutable storage 848

Enabling One-click recovery 428

Enabling or disabling a protection plan 247

Enabling or disabling the hardware inventory scanning 710

Enabling or disabling the software inventory scanning 716

Enabling the Last backup and Backup status columns in vSphere Client 475

Encryption 385

Erasing 836

Error handling 413, 480

Event export (files) troubleshooting 312

Event export (syslog) troubleshooting 313

© Acronis International GmbH, 2003-2026

Event filtering (optional) 297

Event parameters 372

Example 374-378, 383

Emergency backup in case of bad blocks on the hard disk 372

Installing the packages manually in Fedora 14 92

Examples 147-149

Exchange Server clusters overview 649

Exclude hidden files and folders 416

Exclude system files and folders 417

Excluding devices from discovery 219

Exclusions 692, 696, 704

Existing vulnerabilities 274

Exporting and importing the report structure 284

Exporting backups 455

Extensions and exception rules 789

Extracting files from local backups 538

F

Failback options 480

Failing back 479

Failing over to a replica 478

Fast incremental/differential backup 414

File-level backup 841

File-level backup snapshot 417

File-level security 552

File exclusions 552

File filters 415

Files forwarding method 290

Files of a script 615

Finalization 469

Finalization of machines running from cloud backups 469

Finalization vs backup recovery 469

Finalizing a virtual machine running from a backup 472

Finding the storage ID 850

Firewall configuration 98

Fits the time interval 375

Flashback 553

Forensic backup process 418

Forensic data 417

Format volume 599

Full path recovery 553

G

Generating a registration token 156

get content 423

Getting started with a tape device 823

Getting started with Acronis Cyber Protect 17 19

Getting the certificate for backups with forensic data 420

Granting access permission to the user account 494

Granting the required system permissions to the Connect Agent 750

H

H.264 748

Hardware inventory widgets 277

High-speed LAN 843

High Availability of a recovered machine 498

© Acronis International GmbH, 2003-2026

How creating Secure Zone transforms the disk 360

How do files get into the quarantine folder? 705

How it works 270, 351, 419, 465, 546, 687, 697, 785, 788

How many agents are required for cluster-aware backup and recovery? 650

How many agents are required for cluster data backup and recovery? 648

How many agents do I need? 160, 164, 170

How many virtual appliances do I need? 176

How the deployment agent works 123

How to create Secure Zone 361

How to delete Secure Zone 362

How to distinguish backups that are protected on continuous basis 356

How to enable or disable cataloging 846

How to get forensic data from a backup? 419

How to populate units with machines 333

How to recover data to a mobile device 640

How to recover your entire machine to the latest state 357

How to reduce bottlenecks 460

How to review data via the Cyber Protect console 640

How to start backing up your data 639

I

Ignore bad sectors 414

Ignore failed VSS writers 448

Immutable storage 847

Immutable storage modes 847

Important tips 381

In-archive deduplication 409

In cloud deployments 161

In Linux 224, 230, 333

In macOS 224

In on-premises deployments 161

In Windows 224, 229, 333

Include or exclude files matching specific criteria 415

Information parameters 147

Inheritance of roles 332

Installation 71, 97, 113, 127, 846

Installation in a Docker container 114

Installation parameters 136, 144

Installing a storage node and a catalog service 838

Installing a TLS certificate for syslog forwarding 297

Installing Acronis PXE Server 632

Installing Agent for Proxmox 679

Installing Agent for Synology 183

Installing Agent for VMware (Windows) 127

Installing agents locally 129

Installing agents remotely 216

Installing and uninstalling protection agents in Linux 142

Installing or uninstalling the product by specifying parameters manually 135

Installing patches on demand 742

Installing protection agents in Linux 131

Installing protection agents in macOS 133

Installing protection agents in Windows 129

© Acronis International GmbH, 2003-2026

Installing the Centralized Dashboard component 111

Installing the management server 102, 114

Installing the management server in Linux 113

Installing the management server in Windows 102

Installing the packages from the repository 90

Installing the packages manually 91

Installing the product by using the .mst transform 135

Interaction with Windows Removable Storage Manager (RSM) 817

Intermediate snapshots 391

Inventorying 832

Inventorying methods 832

J

JSON activity examples 305

JSON alert examples 305

K

Kernel parameters 610

Known issues 54

L

LAN-free backup 481

License co-termination 47

License issue 250

License types 38

Limitation 113

Limitations 54, 71, 79, 83-84, 86-89, 120, 170, 176, 182, 269, 343, 350, 360, 389, 482, 503, 510, 521, 542, 551, 636, 669, 708, 845

Limitations for backup file names 405

Limitations for Proxmox workloads 678

Limitations for tape devices 821

Limiting the total number of simultaneously backed-up virtual machines 498

Linux 69, 347

Linux-based 561

Linux-based bootable media 606

Linux-based or Windows-based bootable media? 561

Linux packages required for installation of agents and management server in Linux 89

list backups 422

list content 422

Local connection 629

Local console of an on-premises management server 25

Location encryption 844

Location of the OVF tempate 161

Log out inactive users after 319

Log truncation 425

Logging and health check troubleshooting 316

Logging in to the Centralized Dashboard 794

LVM snapshotting 426

M

Mac 347

Mailbox backup 654

Malicious website access 699

Managed location 344

Management server 620

© Acronis International GmbH, 2003-2026

Management Server 27

Management server installation parameters 140, 145

Managing company contacts 20

Managing disks by using bootable media locally 577

Managing found vulnerabilities 726

Managing licenses 39

Managing quarantined files 705

Managing registration tokens 157

Managing software 716

Managing the detected unprotected files 788

Managing workloads in the Cyber Protect console 229

Managing your hardware inventory 710

Managing your software inventory 716

Manual adding to the whitelist 706

Manual binding 485

Mass storage drivers to install anyway 544

Materialized Aggregates schema 800

McAfee Endpoint Encryption and PGP Whole Disk Encryption 94

Microsoft 81

Microsoft BitLocker Drive Encryption and CheckPoint Harmony Endpoint 93

Microsoft Exchange Server 411

Microsoft Hyper-V virtual machine 504

Microsoft Security Essentials 696

Microsoft SQL Server 411

Migrating the management server 192

Mirrored-Striped Volume 594

Mirrored Volume 594

Missing updates by categories 274

Monitoring and reporting 267

Monitoring workloads via screenshot transmission 775

Mount points 426, 553

Mounting Exchange Server databases 661

Mounting volumes from a backup 453

Move a tape back to the slot after each successful backup of each machine 443

Moving to another pool 831

Moving to another slot 831

Multi-core processor with at least 2.5 GHz clock rate 843

Multi-volume snapshot 427

Multiplexing 445

Multistreaming 444

N

Names without variables 406

Navigating to the web console of a connected management server 796

NEAR 748

Network folder protection 687

Network port 622

Network requirements 501

Network settings 621

NFS 343

NIC teaming support 629

No recent backups 275

No successful backups for a specified number of consecutive days 403

Notarization of backups with forensic data 419

© Acronis International GmbH, 2003-2026

Nutanix 88

Nutanix virtual machine 507

O

Observing multiple managed workloads simultaneously 776

Obtaining application ID and application secret 670

Off-host data protection plans 462

Offline on-premises management server 34

On-premises deployment 229, 501

On-premises deployment and cloud deployment 26

On-premises deployments 190

On what workloads, agents, and backup locations are bottlenecks shown? 462

On Windows Event Log event 371

One-click recovery 428

Online on-premises management server 34

Only one deduplicating location on each storage node 843

Operations on the source machine 192

Operations on the target machine 194

Operations with backups 452

Operations with bootable media 561

Operations with pools 830

Operations with tapes 831

Operators 265

Options description 424

Oracle 87

Other components 32

Output speed during backup 435

Overview of tape support 817

Overview of the physical data shipping process 436

Overwrite a tape in the stand-alone tape drive when creating a full backup 444

oVirt/Red Hat Virtualization 4.2 and 4.3/Oracle Virtualization Manager 4.3 175

oVirt/Red Hat Virtualization 4.4, 4.5 175

P

Parallel operations 821

Parallels 86

Parameters 610

Parameters for writing to tapes 819

Passive device discovery by using Device Sense ™ 209

Patch installation history 274

Patch installation status 274

Patch installation summary 274

Patch installation widgets 274

Patch management 728

Pending operations 599

Performance 480, 554

Performance and backup window 432

Performing a permanent failover 479

Performing control actions on managed workloads 772

Physical Data Shipping 436

Physical machine 503

Place the deduplication database and deduplicating location on separate physical devices 842

Plan and deployment troubleshooting 315

© Acronis International GmbH, 2003-2026

Ports 111

Ports used by Device Sense ™ 211

Ports, services, and processes used by Acronis Cyber Protect 225

Post-backup command 439

Post-data capture command 440

Post-recovery command 555

Power off target virtual machines when starting recovery 556

Power on after recovery 557

Power on the target virtual machine when recovery is complete 557

Pre-backup command 438

Pre-configuring multiple network connections 621

Pre-data capture command 439

Pre-recovery command 554

Pre/Post commands 437, 480, 554

Pre/Post data capture commands 439

Predefined pools 829

Predefined scripts 613

Preparation 113, 127, 543

WinPE 2.x and 3.x 624

WinPE 4.0 and later 624

Prepare drivers 543

Preparing machines for remote installation by using a GPO 213

Preparing machines for remote installation manually 213

Prerequisites 111, 114, 150, 191-192, 197, 200, 222, 236, 296, 350, 430, 468, 486, 823-824

Prerequisites for remote installation 122

Protecting a domain controller 642

Protecting Always On Availability Groups (AAG) 648

Protecting Database Availability Groups (DAG) 649

Protecting Google Workspace data 675

Protecting Microsoft 365 mailboxes 669

Protecting Microsoft applications 642

Protecting Microsoft SharePoint 642

Protecting Microsoft SQL Server and Microsoft Exchange Server 642

Protecting mobile devices 638

Protecting Oracle Database 676

Protecting Proxmox virtual machines and containers 678

Protecting SAP HANA 677

Protection of collaboration and communication applications 708

Protection of virtualization environments 488

Protection plans and modules 242

Protection settings 320

Protection status 269

Proxmox container 508

Proxmox VE 84

Proxmox virtual machine 508

Proxy server 111

Public clouds 81

Q

Quarantine 689, 705

Quarantine location on machines 705

© Acronis International GmbH, 2003-2026

R

RAID-5 594

Raw data schema 804

RDP 749

Re-attempt, if an error occurs 413

Re-attempt, if an error occurs during VM snapshot creation 414

Readability of tapes written by older Acronis products 822

Real-time protection 685, 690, 695

Recently affected 275

Recommendations 551

Recording and playing remote sessions 781

Recovering a machine with One-click recovery 430

Recovering a physical machine as a physical machine 510

Recovering a physical machine as a virtual machine 511

Recovering a virtual machine 474

Recovering a virtual machine as a physical machine 521

Recovering a virtual machine as a virtual machine 523

Recovering applications 643

Recovering backups by using bootable media locally 571

Recovering backups by using bootable media remotely 602

Recovering containers 531

Recovering ESXi configuration 539

Recovering Exchange databases 659

Recovering Exchange mailboxes and mailbox items 661

Recovering files 534

Recovering files by using bootable media 538

Recovering files by using the Cyber Protect console 534

Recovering mailbox items 664, 673

Recovering mailboxes 663, 672

Recovering mailboxes and mailbox items 672

Recovering Proxmox workloads 680

Recovering SQL databases 656

Recovering system databases 658

Recovering the Exchange cluster data 651

Recovering the master database 658

Recovering under an operating system from a tape device 826

Recovering under bootable media from a locally attached tape device 827

Recovering under bootable media from a tape device attached to a storage node 828

Recovering workloads by using bootable media 533

Recovery 76, 502, 669

Recovery cheat sheet 502

Recovery environments 541

Recovery from the cloud storage 614

Recovery of databases included in an AAG 649

Recovery of physical machines 510

Recovery of virtual machines 521

Recovery options 548

Recovery to an Exchange Server 662

Recovery to Microsoft 365 663

© Acronis International GmbH, 2003-2026

Recovery with restart 540

Red Hat and Linux 85

Red Hat syslog configuration example 291

Red Hat Virtualization/oVirt virtual machine 507

Redirecting sound from a remote Linux workload 750

Redirecting sound from a remote macOS workload 749

Redirecting sound from a remote Windows workload 749

Redistribution 485

Registering a management server to the Centralized Dashboard 197

Registering an already installed Agent for VMware 127

Registering and unregistering machines manually 152

Registering bootable media on the management server 601

Registering license co-termination 48

Registering the media from the media UI 601

Registration 363

Remote connection 324, 629

Remote connection protocols 748

Remote installation of agents 212

Remote management plans 752

Remote sound redirection 749

Remote wipe 791

Removing 836

Removing Agent for VMware (Virtual Appliance) 225

Removing machines from the Cyber Protect console 225

Removing the vCenter plugin 473

Removing workloads from a remote management plan 760

Renaming 835

Renaming the SIEM log forwarding plan 289

Replicating backups between managed locations 400

Replication 398

Replication of virtual machines 475

Replication options 479

Replication vs. backing up 476

Reports 282

Requesting license co-termination 48

Required ports 175

Required ports for backup and replication of VMware virtual machines 496

Required privileges for Agent for VMware 488

Required roles 175

Required user rights 655

Required user rights for application-aware backups 653

Required user rights for the service logon account 105

Requirements 453, 539

Requirements for application-aware backups 644

Requirements for ESXi virtual machines 645

Requirements for Hyper-V virtual machines 645

Requirements on User Account Control (UAC) 122, 206

Requirements on user accounts 662

Rescanning 834

© Acronis International GmbH, 2003-2026

Resolving compatibility issues 253

Resolving plan conflicts 250

Restart and verify 297

Restrictions 399, 476

Results 824, 826

Retention lock 94

Retention rules 380

Retention rules according to the backup scheme 382

Reverting to the original initial RAM disk 545

Revoking a protection plan 246

rsyslog configuration example 296

Rules for Linux 346

Rules for macOS 346

Rules for Windows 345

Rules for Windows, Linux, and macOS 345

Running a backup manually 379

Running a backup on a schedule 367

Running a virtual machine from a backup 470

Running a virtual machine from a backup (Instant Restore) 468

Running an active device discovery scan by using Device Sense ™ 210

Running pre-freeze and post-thaw scripts automatically 486

Running the Test patching protection plan and decline unsafe patches 741

S

Safe recovery 546

Save battery power 376

Save system information if a recovery with reboot fails 552

Scale Computing 84

Scale Computing HyperCore virtual machine 506

Scan Service 110

Scanning types 685

Schedule 723, 788

Schedule by events 369

Schedule by time 367

Schedule scan 690, 694

Scheduled scan 686

Scheduling 441

Scheduling the updates 322

Scripts in bootable media 613

Search query 256

Sector-by-sector backup 442

Secure Zone 343

Security 319, 749

Security Administrator role 336

Seeding an initial replica 480

Select the snapshot provider 449

Selecting a destination 357

Selecting data to back up 344

Selecting disks/volumes 344

Selecting entire machine 344

Selecting ESXi configuration 350

Selecting Exchange Server data 647

Selecting Exchange Server mailboxes 655

Selecting files/folders 347

Selecting mailboxes 672

Selecting SQL databases 646

Selecting the backed-up data for recovery 845

© Acronis International GmbH, 2003-2026

Selection rules for Linux 349

Selection rules for macOS 349

Selection rules for Windows 348

Self-protection 688

Self-service custom folder on-demand 706

Sequence of actions 834

Server-side protection 688

Service logon account 104

Set active volume 598

Setting the root password on a virtual appliance 191

Setting trusted and blocked connections 688

Setting up a machine to boot from PXE 633

Setting up the Group Policy object 152

SFTP server and tape device 343

Sharing clipboard content between workloads 771

Show notification about the last login of the current user 319

SID changing 556

SIEM data format and examples 300

SIEM forwarding methods 290

SIEM log forwarding 286

SIEM troubleshooting 307

SIEM validation errors 308

Signing a file with ASign 537

Simple Volume 593

Skip the task execution 448

Smart protection 785

Software-specific recovery procedures 93

Software inventory widgets 276

Software requirements 62

Sound transfer 748

Source of the latest protection definitions 324

Spanned Volume 593

Special operations with virtual machines 468

Specifying a tape set 837

Splitting 442

SQL Server high-availability solutions overview 648

SSH connections to a virtual appliance 190

SSL certificate settings 239

Start conditions 373

Starting a hardware inventory scan manually 711

Starting a software inventory scan manually 717

Starting the Secure Shell daemon 191

Startup Recovery Manager 635

Stopping failover 478

Storage node installation parameters 141

Storage nodes 838

Striped Volume 593

Structure of autostart.json 615

Sufficient free space in the location 843

Support for virtual machine migration 487

Supported cluster configurations 648, 650

Supported Cyber Protect features by operating system 226

Supported data sources and destinations for continuous data protection 352

Supported file systems 72, 581

Supported hardware 818

Supported Linux products for vulnerability

© Acronis International GmbH, 2003-2026

assessment 722

Supported locations 357, 398, 464-465, 467

Supported Microsoft and third-party products for vulnerability assessment 721

Supported Microsoft Exchange Server versions 77

Supported Microsoft products 721

Supported Microsoft SharePoint versions 77

Supported Microsoft SQL Server versions 77

Supported mobile devices 638

Supported operating systems and environments 62

Supported operating systems for antivirus and antimalware protection 681

Supported operating systems for Cyber Protect Monitor 70

Supported operating systems for Management Server 68

Supported operating systems for protection agents 62

Supported operating systems for remote desktop and assistance 747

Supported operating systems for Storage Node 70

Supported operations with logical volumes 75

Supported Oracle Database versions 78

Supported SAP HANA versions 78

Supported storages and agents 848

Supported third-party products for Windows 722

Supported virtualization platforms 78

Supported web browsers 76

Syncing license renewals or co-termination to an offline management server 49

Syslog server forwarding method 290

System requirements 97, 846

System requirements for the agent 160, 164, 170

System requirements for the virtual appliance 176

System settings 317

T

Tape-related backup options 821

Tape devices 817

Tape management 443, 556, 828

Tape management database 818

Tape pools 829

Task failure handling 447

Task start conditions 447

Testing a replica 477

The Activities tab 277

The backup location's host is available 374

The Backup storage tab 452

The Overview dashboard 267

The patch management workflow 729

The Plans tab 251

The remote desktop notifiers 783

The TapeLocation folder 819

The tool "tibxread" for getting the backed-up data 421

The way of using Secure Zone 93

Threat feed 785

Tip 399

Tips for further usage of the tape library 826

TLS certificate configuration 296

© Acronis International GmbH, 2003-2026

Top-level object 615

Transferring files 769

Transferring license quota to another management server 50

Transferring protection definitions to an HTTP server 329

Troubleshooting 542, 855

Troubleshooting device discovery 220

Types of conversion to virtual machine 390

Types of dynamic volumes 593

Types of management servers 33

U

Unassigning credentials from a workload 765

Unattended installation or uninstallation 134

Unattended installation or uninstallation in macOS 148

Unattended installation or uninstallation in Windows 134

Unattended installation or uninstallation parameters 136, 144

Understanding the detection of bottlenecks 458

Uninstallation parameters 142, 147

Uninstalling the product 223

Units 330

Units and administrative accounts 330

Universal Restore in Linux 545

Universal Restore in Windows 543

Universal Restore process 545

Universal Restore settings 544

Unregistering a management server 55

Unregistering a management server from the Centralized Dashboard 200

Unregistering an inaccessible offline management server 60

Unregistering an offline management server 56

Unregistering an online management server 55

Update 71

Updates 320

Updating Agent for Synology 187

Updating agents 222

Updating protection agents on BitLocker-encrypted workloads 223

Updating the protection definitions 320

Updating the protection definitions in an air-gapped environment 325

Updating virtual appliances 190

Upgrading the management server 117

Upgrading to Acronis Cyber Protect 17 38

URL filtering 696

URL Filtering 693

URL filtering settings 699

Usage examples 398, 407, 476, 486

Usage scenarios 453

Use a disk cache to accelerate the recovery 556

Use case for automatic patch approval and testing 738

Use case for automatic patch approval without testing 741

Use tape sets within the tape pool selected for backup 446

Use the following tape devices and drives 444

© Acronis International GmbH, 2003-2026

User is idle 374

Users logged off 375

Using a certificate issued by a trusted certificate authority 240

Using a self-signed certificate 239

Using Acronis Cyber Protect with other security solutions in your environment 709

Using locally attached storage 497

Using passwords with special characters or blank spaces 158

Using policy rules 345, 348

Using the toolbar in the Viewer window 778

Using Universal Restore 543

Using variables 407

V

Validating backups 455

Validation 465

Variable object 616

Viewing bottleneck details 460

Viewing data from multiple management servers 794

Viewing details about items in the whitelist 707

Viewing licensing information from multiple management servers 795

Viewing the backup status in vSphere Client 475

Viewing the distribution result 485

Viewing the hardware of a single device 713

Viewing the last logged-in user 338

Viewing the list of available patches 735

Viewing the software inventory of a single device 719

Views schema 801

Virtual machine binding 484

Virtuozzo Server 88

Virtuozzo Server container 505

Virtuozzo Server virtual machine 505

VM power management 480, 556

VMware (Broadcom) 78

Volume operations 593

Volume Shadow Copy Service (VSS) 448

Volume Shadow Copy Service (VSS) for virtual machines 450

Volume Shadow Copy Service VSS for virtual machines 480

Vulnerability assessment 720

Vulnerability assessment for Linux machines 726

Vulnerability assessment for Windows machines 725

Vulnerability assessment settings 723

Vulnerability assessment widgets 274

Vulnerable machines 274

W

Wait until the conditions from the schedule are met 448

Warn about local or domain password expiration 319

Weekly backup 451

What do I need to use application-aware backup? 652

What does a disk or volume backup store? 346

What if I do not see backups stored on tapes? 826

© Acronis International GmbH, 2003-2026

What is a backup file? 405

What is a bottleneck? 458

What is a tape device? 817

What to do after inventorying 833

What to scan 723

What you can back up 638

What you can do with a replica 476

What you need to know 638

Where can I see backup file names? 405

Where to get the Acronis Cyber Protect app 639

Which accounts can be administrative? 331

Which backup type do I need? 37

Which machine performs the operation? 400

Whitelist settings 707

Why are there monthly backups with an hourly scheme? 383

Why back up Microsoft 365 mailboxes? 669

Why use application-aware backup? 651

Why use Secure Zone? 360

Why use the media builder? 605

Windows 68, 346

Windows-based 561

Windows-based bootable media 623

Windows Azure and Amazon EC2 virtual machines 500

Windows Defender Antivirus 694

Windows event log 452, 557

WinPE images 623

WinRE images 623

Work across subnets 634

Working in VMware vSphere 472

Working with managed workloads 765

Working with the Centralized Dashboard 792

Workload credentials 763

Workloads 35

WriteCacheSize 820

© Acronis International GmbH, 2003-2026